appgate

CMMC 2.0: MAPPING APPGATE SDP ACCESS CONTROLS FOR DEFENSE CONTRACTORS

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is a Department of Defense (DoD) framework designed to safeguard Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB) supply chain.

Table of Contents

BACKGROUND

The Cybersecurity Maturity Model Certification (CMMC) serves as a unified framework for implementing robust cybersecurity measures across the Defense Industrial Base (DIB). Building upon the National Institute of Standards and Technology (NIST) Special Publication 800-171, CMMC establishes a structured process for validating cybersecurity requirements in alignment with Defense Federal Acquisition Regulation Supplement (DFARS) regulations.

CMMC originally outlined five levels of cybersecurity maturity for supplier organizations, ranging from Level 1, focused on basic safeguarding of Federal Contract Information (FCI), to Level 5, aimed at advanced protection of Controlled Unclassified Information (CUI). This tiered approach allowed organizations to progressively enhance their cybersecurity posture based on the sensitivity of the data they handle and their risk profile. While this initial framework provided a valuable foundation, CMMC 2.0 introduces a streamlined model with three distinct levels of cybersecurity maturity, designed to simplify compliance and reduce the cost burden on smaller contractors. These levels are:

- **Level 1 (Foundational):** Establishing a baseline of cybersecurity hygiene practices to safeguard Federal Contract Information (FCI).
- **Level 2 (Advanced):** Implementing practices aligned with NIST SP 800-171 to protect Controlled Unclassified Information (CUI).
- **Level 3 (Expert):** Adopting advanced cybersecurity practices to safeguard CUI and mitigate the risks posed by Advanced Persistent Threats (APT).

WITH CMMC 2.0, THE DOD HAS REVISED THE STANDARDS AND STREAMLINED THE MODEL FROM FIVE LEVELS TO THREE.

CMMC MODEL 1.0	MODEL		ASSESSMENT
LEVEL 5 ADVANCED CUI, critical programs	**171** practices	**5** processes	Third-party
LEVEL 4 PROACTIVE Transition Level	**156** practices	**4** processes	None
LEVEL 3 GOOD CUI	**130** practices	**3** processes	Third-party
LEVEL 2 INTERMEDIATE Transition Level	**72** practices	**2** maturity processes	None
LEVEL 1 BASIC FCI only	**17** practices		Third-party

CMMC MODEL 2.0	MODEL	ASSESSMENT
LEVEL 3	**110+** requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	**110** requirements based on NIST SP 800-171	Triennial third-party assessment & annual affirmation; triennial self-assessemt & annual affirmation for select programs
LEVEL 1	**15** requirements	Annual self-assessment & annual affirmation

All entities operating within the DIB, regardless of their size or contract type, are obligated to comply with the relevant CMMC level for their specific business activities.

The overarching aim of CMMC is to furnish DIB members with a mature and validated set of cybersecurity measures aligned with established guidelines. This ensures a secure and verifiable supply chain for the U.S. Armed Forces, safeguarding against attempts to disrupt or exploit critical supply chains. Every facet of a DIB member's operations, encompassing their infrastructure and data systems, must adhere to the rigorous CMMC requirements governing the supply chain.

NIST has developed industry-specific guidance to assist in defining organizational focus areas, fortifying the risk profiles of DIB members throughout the acquisition process. This guidance ensures a comprehensive approach to end-to-end risk management, contributing to the overall security and resilience of the defense supply chain.

APPGATE'S ZERO TRUST NETWORK ACCESS CONTROL FOR CMMC MODEL 2

Appgate's Zero Trust Network Access (ZTNA) solution

Appgate SDP is architected on the fundamental principle of "never trust, always verify." This approach mandates that users, applications, and devices undergo rigorous authentication and authorization before interacting. Leveraging mutual Transport Layer Security (mTLS), Appgate SDP establishes a secure, encrypted tunnel for every connection, ensuring the confidentiality and integrity of data in transit.

By implementing network segmentation, Appgate SDP effectively prevents lateral movement, mitigating the risk of unauthorized access propagation within the network. The solution's default-deny stance ensures that access is granted only when explicitly authorized, adhering to the principle of least privilege. Furthermore, Appgate SDP simplifies and automates granular user access control, enabling organizations to define and enforce fine-grained permissions for individual users and groups in modern and legacy environments.

This comprehensive approach to network security directly aligns with the stringent requirements of CMMC 2.0, providing defense contractors with robust security measures to safeguard sensitive information, maintain compliance, and fortify their cybersecurity posture.

APPGATE SDP ALIGNMENT WITH CMMC REQUIREMENTS AND NIST 800-171 STANDARDS

CMMC LEVEL 1 DOMAIN: ACCESS CONTROLS (AC)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.1.001	**Authorized Access Control** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 2 3.1.1	**52.204-21 b.1.i** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	**3.1.1** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). **DISCUSSION** Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.	Appgate enforces access control by leveraging identity properties (roles, groups, and attributes), device posture (health, compliance, and running processes), and contextual information (location, risk score, other security events). Access policies are defined using ABAC/RBAC to limit access based on user roles. Device claims and device claim scripts ensure devices meet security posture requirements before access is granted. Single Packet Authorization (SPA) cloaks network. Appgate can leverage user claim APIs to enhance identification by calling out to other identity information stores. For example, it can query an HR application to verify a user's citizenship status, check a training application to confirm completion of required training such as Information Assurance (IA), HIPAA, or PCI compliance, and interact with an ERP solution to gather additional context about the user's role and responsibilities. This integration allows for more precise and informed access control decisions, ensuring that only properly identified and authenticated users, processes, and devices can access sensitive systems and data. This comprehensive approach ensures compliance with identification requirements while enhancing overall security. Appgate for containers, such as Kubernetes (K8s), can enforce access controls at the container level, ensuring that only authorized processes and microservices communicate with each other. Additionally, Appgate's always-on functionality, running as a service, ensures continuous enforcement of access policies, even as users and devices move between different network environments. The Appgate connector can securely manage and broker connections between devices and systems, ensuring that only authenticated and authorized connections are established, thus providing a robust framework for access control. Identity and Access Management (IAM), Privileged Access Management (PAM), and Data-at-Rest (DAR) Encryption. IAM systems manage user identities. PAM solutions monitor and control access, ensuring that privileged accounts are used appropriately. DAR encryption protects data at rest, ensuring only authorized users can decrypt and access sensitive information. In addition to these technologies, key processes must be implemented to comply with the control requirements. Establishing access control policies defines who has access to resources based on roles and responsibilities. Regular access reviews ensure user access rights remain appropriate. User provisioning and deprovisioning processes quickly grant and revoke access as employees join, leave, or change roles. Security training and awareness programs educate users on the importance of access control and best security practices.	For more information on how Appgate SDP enforces access control, refer to the following sections in the Appgate Admin Guide: - **Identity Attributes and Access Policies (ABAC/RBAC):** See "Access Management" for details on configuring identity attributes and defining access policies. - **Device Posture and Device Claim Scripts:** Refer to "Device Claim Scripts" for details on configuring device claims and ensuring security posture requirements. - **Single Packet Authorization (SPA):** Review the "Single Packet Authorization" section for details on SPA configuration. - **User Claim APIs for Enhanced Identification:** Look at "User Claim Scripts" for using APIs to query external identity information stores. - **Appgate for Containers (Kubernetes):** See "SDP Kubernetes Injector" for details on enforcing access controls at the container level. - **Appgate Always-On Functionality:** Refer to "Windows Always-On Client" for always-on client configuration. - **Appgate Connector:** See "Connector (Advanced)" and "Connector (Express)" for details on managing secure connections between devices and systems.

DOMAIN: *ACCESS CONTROLS (AC) (CONT)*

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.1.002	**Transaction and Function Control** Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 2 3.1.2	**52.204-21 b.1.ii** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	**3.1.2** Limit information system access to the types of transactions and functions that authorized users are permitted to execute. **DISCUSSION** Access control policies can be defined based on organizational roles and responsibilities to ensure that only authorized transactions and functions are executed by users. This involves setting up specific permissions and privileges that restrict user actions to those that are necessary for their role.	Appgate enforces transaction and function control by defining granular access policies that specify what actions users can perform based on their roles and attributes. This is achieved through the use of Attribute and Role-Based Access Control (ABAC/RBAC models) and policy scripting to enforce specific permissions. Device posture and compliance checks further ensure that only secure and compliant devices can execute authorized transactions. Key technologies include IAM that links user to role in order to enforce Role-Based Access Control (RBAC) permissions based on user roles, application-level access controls to restrict actions within applications, audit logging to monitor user activities, and Multi-Factor Authentication (MFA) for added security. Key processes include establishing access control policies that define permissible transactions and functions for each role, conducting regular access reviews and audits to ensure permissions are appropriate, implementing efficient user provisioning and deprovisioning processes, and providing comprehensive security training and awareness programs. These combined technologies and processes ensure compliance with transaction and function control requirements.	For more information on how Appgate SDP enforces transaction and function control, refer to the following sections in the Appgate Admin Guide: - **Access Policies (ABAC/RBAC):** Look at "Access Management" for details on configuring identity attributes and defining access policies using ABAC/RBAC. - **Device Posture and Compliance Checks:** Refer to "Device Claim Scripts" for configuring device claims and checking device posture and compliance. - **Audit Logging:** Review the "Audit Logs" section for information on monitoring user activities. - **User Provisioning and Deprovisioning Processes:** Review the sections on "User Claims" and "Policy Assignment" for information on managing user access rights and provisioning. - **Multi-Factor Authentication (MFA):** See "Multi-Factor Authentication" for details on configuring MFA.
AC.1.003	**External Connections** Verify and control/limit connections to and use of external information systems. • FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 Rev 2 3.1.20	**52.204-21 b.1.iii** Verify and control/limit connections to and use of external information systems.	**3.1.20** Verify and control/limit connections to and use of external information systems. **DISCUSSION** External connections can introduce risks to the information system. Policies and procedures should be established to verify and control the connections to and the use of external systems. This includes monitoring and managing connections to ensure they are secure and comply with organizational policies.	Appgate verifies and controls external connections by monitoring and managing all connections through secure gateways. Policies can be set to restrict external access based on the user's role, device posture, and other contextual factors. Single Packet Authorization (SPA) and mutual Transport Layer Security (mTLS) are used to secure these connections, ensuring that only authenticated and authorized users and devices can establish external connections. Organizations should establish clear policies and procedures for verifying and controlling external connections, including regular audits and monitoring to ensure compliance with security standards. Managing and reviewing entitlements helps to restrict connections to trusted entities. Regular security assessments and penetration testing can identify vulnerabilities in external connections, while incident response plans ensure prompt action in case of a security breach. Comprehensive training and awareness programs educate employees on the risks and best practices associated with external connections. Together, these technologies and processes ensure secure and controlled use of external information systems.	For more information on how Appgate SDP verifies and controls external connections, refer to the following sections in the Appgate Admin Guide: - **Secure Gateways and Policies:** Review the "Gateway" and "Access Management" sections for details on configuring secure gateways and setting policies to restrict external access based on user roles and device posture. - **Single Packet Authorization (SPA) and Mutual TLS (mTLS):** Refer to the "Single Packet Authorization" and "Mutual TLS" sections for details on securing external connections. - **Entitlements and Audit Logging:** Refer to the "Entitlements" and "Audit Logs" sections for information about managing and reviewing entitlements and monitoring user activities. - **Security Assessments and Incident Response:** For information on conducting regular security assessments and incident response plans, refer to the "System Security -Best Practice" section.

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.1.004	**Control Public Information** Control information posted or processed on publicly accessible information systems. • FAR Clause 52.204-21 b.1.iv • NIST SP 800-171 Rev 2 3.1.22	**52.204-21 b.1.iv** Control information posted or processed on publicly accessible information systems.	**3.1.22** Control information posted or processed on publicly accessible information systems. **DISCUSSION** Organizations need to ensure that information posted on public systems does not expose sensitive information. This involves implementing controls to manage what information can be posted and by whom, ensuring compliance with privacy and security policies.	While Appgate is primarily a Zero Trust Network Access (ZTNA) solution not directly designed for protecting public information on websites, it can still play a role in controlling access to systems that manage public information. Appgate can enforce strict access policies to ensure that only authorized users within an organization can access and manage content on publicly accessible information systems. By using ABAC/RBAC combined with other context, Appgate ensures that only users with appropriate permissions can post or process information on these systems. This indirect control helps to prevent unauthorized access to the backend systems managing public content, thereby contributing to the overall security and integrity of public information. Web content management systems (CMS) with granular access controls are essential for managing who can post and edit content on publicly accessible information systems. Data loss prevention (DLP) tools can monitor and restrict the sharing of sensitive information, ensuring compliance with privacy and security policies. Additionally, security information and event management (SIEM) systems can provide real-time monitoring and alerts for unauthorized attempts to post or process sensitive information on public systems. Additionally, implementing web application firewalls (WAFs) can provide an added layer of security by monitoring and controlling the flow of information to and from public systems, ensuring that only authorized and sanitized content is accessible. In addition to these technologies, several key processes must be implemented to comply with the control requirements. Organizations should establish clear policies and procedures that define what information can be posted on public systems and by whom. Regular reviews and audits of publicly accessible content are necessary to ensure ongoing compliance with security and privacy policies. Training and awareness programs should educate employees on the risks associated with posting information on public platforms and the importance of adhering to established policies.	For more information on how Appgate SDP ensures identification and access control, refer to the following sections in the Appgate Admin Guide: - **Access Policies (ABAC/RBAC):** See "Access Management" for details on configuring identity attributes and defining access policies using ABAC/RBAC. - **Device Claims and Scripts:** Refer to "Device Claim Scripts" for details on configuring device claims and checking device posture and compliance. - **User Claim APIs:** Review the section on "User Claim Scripts" to learn how to use APIs to query external identity information stores like HR applications, training applications, and ERP solutions. - **Identity and Access Management (IAM):** Review "Identity Providers" for details on managing user identities and integrating with various IdPs. - **Multi-Factor Authentication (MFA):** See "Multi-Factor Authentication" for details on configuring MFA. - **Continuous Authentication:** Refer to "Real-time (Re) Evaluations" for details on continuous authentication and regularly re-evaluating user and device attributes to ensure ongoing compliance with security policies.

DOMAIN: IDENTIFICATION AND AUTHETICATION (IA)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
IA.1.076	**Identification** Identify information system users, processes acting on behalf of users, or devices. • FAR Clause 52.204-21 b.1.v • NIST SP 800-171 Rev 2 3.5.1	**52.204-21 b.1.v** Identify information system users, processes acting on behalf of users, or devices.	**3.5.1** Identify information system users, processes acting on behalf of users, or devices. **DISCUSSION** Identification of users, processes, and devices is a prerequisite for access control decisions. Organizations need to identify and authenticate entities before granting access to systems and resources. This includes verifying the identity of users and the legitimacy of devices.	Appgate ensures identification by requiring all users and devices to be registered within the system. Access policies are configured to verify user identities with ABAC/RBAC and contextual information. Device claims and scripts check the device's posture and compliance. Appgate's dynamic policies can adjust access based on the health and status of the device, ensuring that only identified users and legitimate devices can access the network. Appgate can leverage user claim APIs to enhance identification by calling out to other identity information stores. For example, it can query an HR application to verify a user's citizenship status, check a training application to confirm completion of required training such as Information Assurance (IA), HIPAA, or PCI compliance, and interact with an ERP solution to gather additional context about the user's role and responsibilities. This integration allows for more precise and informed access control decisions, ensuring that only properly identified and authenticated users, processes, and devices can access sensitive systems and data. This comprehensive approach ensures compliance with identification requirements while enhancing overall security. Essential technologies include Identity and Access Management (IAM) systems to manage user identities and Multi-Factor Authentication (MFA) for enhanced security. Secure digital certificates and cryptographic keys also validate the identities of devices and processes. Key processes include establishing identity verification procedures to ensure proper identification before access is granted, conducting regular audits and reviews of user and device identities, and implementing effective user provisioning and deprovisioning processes. Training and awareness programs are essential to educate users on the importance of identity verification and maintaining security. These combined technologies and processes ensure effective identification of information system users, processes, and devices.	For more information on how Appgate SDP ensures identification and access control, refer to the following sections in the Appgate Admin Guide: - **User and Device Registration:** Review "Identity Providers" for details on registering users and devices within the system. - **Access Policies (ABAC/RBAC):** Refer to "Access Management" for details on configuring access policies using ABAC/RBAC and contextual information. - **Device Claims and Scripts:** Review the "Device Claim Scripts" section to understand how to verify device posture and compliance. - **User Claim APIs:** See the "User Claim Scripts" section for detials on enhancing identification by querying external identity information stores. - **Identity and Access Management (IAM):** Review "Identity Providers" for information about managing user identities. - **Multi-Factor Authentication (MFA):** Refer to "Multi-Factor Authentication" for details on configuring MFA. - **Identity Verification Procedures:** Refer to the sections on "User Claims" and "Policy Assignment" for infromation on establishing identity verification procedures and managing user access rights.
IA.1.077	**Authentication** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. • FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 Rev 2 3.5.2	**52.204-21 b.1.vi** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	**3.5.2** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. **DISCUSSION** Authentication establishes the validity of a claimed identity. Multifactor authentication, where two or more factors are required, is an effective method for verifying identities. This includes using something the user knows (password), something the user has (security token), and something the user is (biometric verification).	Appgate applies to the "Authentication" control by leveraging its authentication mechanisms to verify the identities of users, processes, and devices before granting access to organizational information systems. Appgate supports multi-factor authentication (MFA), which enhances security by requiring two or more verification factors. This includes something the user knows (password), something the user has (security token), and something the user is (biometric verification). Appgate's integration with various identity providers (IdPs) enables seamless authentication against trusted sources such as LDAP, RADIUS, SAML, and OIDC. By using identity claims and token-based authentication, Appgate ensures that only authenticated and authorized entities can access protected resources. Additionally, Appgate supports continuous authentication, which involves regularly re-evaluating user and device attributes to ensure ongoing compliance with security policies. This includes monitoring changes in device posture, user location, and risk scores. If any changes occur that might affect the security posture, Appgate can prompt for re-authentication or adjust access rights accordingly. This dynamic and adaptive approach to authentication ensures that access decisions remain accurate and secure over time.	For more information on how Appgate SDP applies to the "Authentication" control, refer to the following sections in the Appgate Admin Guide: - **Multi-Factor Authentication (MFA):** Details on configuring MFA can be found in the sections on "Multi-Factor Authentication" and "MFA Providers." - **Identity Providers (IdPs):** Information on integrating with various IdPs such as LDAP, RADIUS, SAML, and OIDC can be found in "Identity Providers." - **Continuous Authentication:** Guidance on continuous authentication and real-time re-evaluations of user and device attributes is available in the "Real-time (Re)Evaluations" section.

DOMAIN: MEDIA PROTECTION (MP)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MP.1.118	**Media Disposal** Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. • FAR Clause 52.204-21 b.1.vii • NIST SP 800-171 Rev 2 3.8.3	**FAR Clause 52.204-21 b.1.vii** (i) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	**NIST SP 800-171 Rev 2 3.8.3** Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Appgate's Zero Trust Network Access (ZTNA) does not directly handle media disposal. Its primary function is to provide secure access to network resources and does not extend to the physical destruction or sanitization of media. Other tools or processes must be implemented to comply with this control.	Appgate's Zero Trust Network Access (ZTNA) does not provide direct controls for media disposal. Refer to other organizational policies and procedures for secure media disposal practices.

DOMAIN: PHYSICAL PROTECTION (PE)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
PE.1.131	**Limit Physical Access** Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. • FAR Clause 52.204-21 b.1.ix • NIST SP 800-171 Rev 2 3.10.1	**52.204-21 b.1.ix** Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	**3.10.1** Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. **DISCUSSION** Organizations can limit physical access to systems and equipment by employing physical safeguards. This includes physical barriers, security guards, and surveillance systems.	Appgate primarily focuses on controlling digital access to organizational information systems rather than physical access. Therefore, it does not directly apply to the control requirements for limiting physical access to organizational information systems, equipment, and operating environments. Appgate can apply user location to decide if access is granted or denied.	Not Applicable
PE.1.132	**Escort Visitors** Escort visitors and monitor visitor activity. • FAR Clause 52.204-21 b.1.x • NIST SP 800-171 Rev 2 3.10.3	**52.204-21 b.1.x** Escort visitors and monitor visitor activity.	**3.10.3** Escort visitors and monitor visitor activity. **DISCUSSION** Visitor access to sensitive areas should be controlled and monitored. This ensures that visitors do not gain unauthorized access to sensitive information or systems.	Appgate primarily focuses on controlling digital access to organizational information systems rather than physical access. Therefore, it does not directly apply to the control requirements for escorting visitors to organizational information systems, equipment, and operating environments.	Not Applicable
PE.1.133	**Monitor Physical Access** Maintain audit logs of physical access. • FAR Clause 52.204-21 b.1.xi • NIST SP 800-171 Rev 2 3.10.4	**52.204-21 b.1.xi** Maintain audit logs of physical access.	**3.10.4** Maintain audit logs of physical access. **DISCUSSION** Audit logs should be maintained to record physical access to facilities containing information systems. These logs help in tracking who accessed the facilities and identifying any unauthorized access attempts.	Appgate primarily focuses on controlling digital access to organizational information systems rather than physical access. Therefore, it does not directly apply to the control requirements for monitoring physical access to organizational information systems, equipment, and operating environments.	Not Applicable

DOMAIN: PHYSICAL PROTECTION (PE) (CONT)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
PE.1.134	**Control Physical Access** Control and manage physical access devices. • FAR Clause 52.204-21 b.1.xii • NIST SP 800-171 Rev 2 3.10.5	**52.204-21 b.1.xii** Control and manage physical access devices.	**3.10.5** Control and manage physical access devices. **DISCUSSION** Physical access devices, such as keys, locks, and access cards, should be managed to ensure they are only available to authorized personnel. Regular audits and controls should be in place to manage and monitor the use of these devices.	Appgate primarily focuses on controlling digital access to organizational information systems rather than physical access. Therefore, it does not directly apply to the control requirements for managing and controlling physical access to organizational information systems, equipment, and operating environments.	Not Applicable

DOMAIN: SYSTEM AND COMMUNICATION PROTECTION (SC)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SC.1.175	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. • FAR Clause 52.204-21 b.1.xii • NIST SP 800-171 Rev 2 3.13.1	**52.204-21 b.1.xii** Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	**3.13.1** Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. **DISCUSSION** Boundary protection strategies can include proxies, gateways, routers, firewalls, and encrypted tunnels to monitor and control communications at the system boundaries. The organization must safeguard information that is transmitted across these boundaries.	Appgate applies to the control of monitoring, controlling, and protecting organizational communications at the external and internal boundaries of information systems through its secure access mechanisms. Appgate can enforce boundary protection strategies by utilizing proxies, gateways, and encrypted tunnels to safeguard information transmitted across these boundaries. By leveraging Zero Trust Network Access (ZTNA) principles, Appgate ensures that all communications are authenticated, authorized, and encrypted, providing robust security for data in transit. Appgate's use of Single Packet Authorization (SPA) and mutual Transport Layer Security (mTLS) further enhances boundary protection by ensuring that only legitimate and authenticated users and devices can initiate communication. These technologies help prevent unauthorized access and ensure that all transmitted data is protected against interception and tampering. Additionally, Appgate's integration with various identity providers (IdPs) and continuous monitoring of device posture and user context provides a dynamic and adaptive security model that adjusts to evolving threats and ensures compliance with security standards.	For detailed information, refer to the following sections in the Appgate SDP Admin Guide: - **Gateways and Proxies:** Refer to the "Gateway" section for detials on configuring secure gateways and proxies. - **Encryption and Tunnels:** Review the "Mutual TLS" and "Single Packet Authorization" sections to learn how to secure communications with encrypted tunnels. - **Access Management:** Refer to "Access Management" for policies on controlling and monitoring user and device communications.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. • FAR Clause 52.204-21 b.1.xiii • NIST SP 800-171 Rev 2 3.13.5	**52.204-21 b.1.xiii** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	**3.13.5** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. **DISCUSSION** Organizations should segment their networks to isolate publicly accessible systems from internal systems. This can be done through subnetting, VLANs, and DMZs to provide an additional layer of security and control over network traffic.	Appgate enables the implementation of subnetworks by creating logically separated zones within the network. These zones can be configured using VLANs and DMZs to isolate publicly accessible systems from internal systems. Access policies are enforced to ensure that only authorized traffic can move between these zones, providing an additional layer of security and control over network communications.	Refer to the Appgate SDP Admin Guide sections on "Network Segmentation' for information on configuring VLANs and DMZs, "Access Policies" for enforcing traffic control, and "Boundary Protection" for strategies to isolate and protect subnetworks.

DOMAIN: SYSTEM AND INFORMATION INTEGRITY (SI)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SI.1.210	**System and Information Integrity** Identify, report, and correct information and information system flaws in a timely manner. • FAR Clause 52.204-21 b.1.xiv • NIST SP 800-171 Rev 2 3.14.1	**52.204-21 b.1.xiv** Identify, report, and correct information and information system flaws in a timely manner.	**3.14.1** Identify, report, and correct information and information system flaws in a timely manner. **DISCUSSION** Organizations identify and correct flaws to ensure the continued security and functionality of information systems. Regular monitoring, vulnerability assessments, and timely updates are crucial to maintain system integrity.	To address the control of "System and Information Integrity" for identifying, reporting, and correcting information and information system flaws in a timely manner, several tools, technologies, and processes are essential. Vulnerability management systems are crucial as they scan systems for vulnerabilities and provide detailed reports to help prioritize remediation efforts. Security Information and Event Management (SIEM) systems collect, analyze, and report on security events across the organization, aiding in the identification and timely response to system flaws. Additionally, patch management tools automate the deployment of patches and updates to ensure systems are up-to-date and secure, while configuration management tools help maintain secure configurations across all devices and applications. Key processes must also be implemented to comply with these control requirements. Regular monitoring involves continuously observing systems for security events and vulnerabilities to detect and address issues promptly. Conducting vulnerability assessments regularly helps identify and evaluate security weaknesses within the system. Ensuring timely updates and patch management is critical to mitigate known vulnerabilities by keeping all software and systems current. Furthermore, establishing a clear process for incident reporting and response ensures that security incidents are reported and handled efficiently. Appgate can also address this control by providing robust network access controls that help limit the exposure of systems to potential flaws. Appgate's Zero Trust Network Access (ZTNA) solution ensures that only authenticated and authorized users and devices can access the network, reducing the risk of exploitation of system flaws. While Appgate does not directly identify or correct system flaws, it integrates effectively with vulnerability management and SIEM systems to enhance overall security and facilitate timely responses to identified issues.	For detailed information, refer to the following sections in the Appgate SDP Admin Guide: - **Dynamic least privilege access model:** Refer to this section for details on dynamically adjusting access controls based on security assessments. - **Real-time Monitoring:** Refer to this section to learn how to detect incidents or deviations from established security baselines and trigger appropriate responses. - **Security Policies:** Refer to this section for details on configuring access policies, enforcing additional authentication requirements, and isolating affected systems to prevent further compromise. - **Integration with Security Tools:** Refer to this section to learn how Appgate integrates with other security tools, such as SIEM and vulnerability management platforms, to receive up-to-date threat intelligence and vulnerability information for dynamic policy adjustments.

DOMAIN: SYSTEM AND INFORMATION INTEGRITY (SI) (CONT)

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SI.1.211	**System and Information Integrity** Provide protection from malicious code at appropriate locations within organizational information systems. • FAR Clause 52.204-21 b.1.xv • NIST SP 800-171 Rev 2 3.14.2	**52.204-21 b.1.xv** Provide protection from malicious code at appropriate locations within organizational information systems.	**3.14.2** Provide protection from malicious code at appropriate locations within organizational information systems. **DISCUSSION** Protection from malicious code includes deploying anti-virus software, intrusion detection systems, and other protective measures at critical points within the system to prevent, detect, and mitigate threats.	To fully meet the requirements of "System and Information Integrity" as outlined by FAR Clause 52.204-21 b.1.xv and NIST SP 800-171 Rev 2 3.14.2, it is essential to implement a combination of technologies and processes that provide comprehensive protection against malicious code. This includes deploying Intrusion Prevention Systems (IPS), Endpoint Detection and Response (EDR) solutions, Data Loss Prevention (DLP) tools, code scanning, Intrusion Detection Systems (IDS), analytics tools, deviation detection, and AI/ML-based security tools. These technologies work together to prevent, detect, and mitigate threats at various points within the information system. Appgate addresses this control by providing robust network access controls that limit the risk of malicious code infiltrating organizational information systems. While Appgate does not directly provide anti-virus or IDS capabilities, it integrates effectively with these solutions to enhance overall security. Appgate's Zero Trust Network Access (ZTNA) solution ensures that only authenticated and authorized users and devices can access the network, reducing potential entry points for malicious code. By segmenting the network and enforcing strict access controls, Appgate helps to contain and limit the spread of any malicious code that might breach initial defenses. Key processes must also be implemented to comply with these control requirements. Establishing comprehensive malware protection policies ensures consistent application of security measures across the organization. Regularly updating and patching software reduces vulnerabilities that malicious code could exploit. Conducting regular security assessments and penetration tests help identify and address potential weaknesses. Implementing security training and awareness programs educates users on recognizing and avoiding potential threats. These processes, combined with robust anti-malware technologies and Appgate's ZTNA solution, form a comprehensive approach to maintaining system and information integrity.	For more information on how Appgate SDP enforces system and information integrity, refer to the following sections in the Appgate SDP Admin Guide: - **Integration with Security Information and Event Management (SIEM) Systems:** See "LogForwarder" for details on exporting audit logs to SIEMs. - **Integration with Endpoint Detection and Response (EDR) Solutions**: Refer to "Authentication and Authorization Processes" for details on leveraging user and device attributes to enhance security. - **Integration with Threat Intelligence Platforms:** Refer to the "Risk Engine Integration and ZTP Settings" section for details on dynamically adjusting to threat levels. - **Regular Monitoring and Review of Security Alerts and Advisories:** See the "System Monitoring and Logs" section. - **Establishing a Robust Incident Response Plan:** Refer to the "Troubleshooting Chapter" for procedures on configuring and troubleshooting appliances. - **Regular Security Assessments and Audits:** See "Administration and Security Best Practices" for guidelines on conducting security assessments and audits. - **Training and Awareness Programs:** Check the "Security Best Practices" section to educate employees on recognizing and responding to security alerts.

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SI.1.212	**System and Information Integrity** Monitor information system security alerts and advisories and take appropriate actions in response. • FAR Clause 52.204-21 b.1.xvi • NIST SP 800-171 Rev 2 3.14.3	**52.204-21 b.1.xvi** Monitor information system security alerts and advisories and take appropriate actions in response.	**3.14.3** Monitor information system security alerts and advisories and take appropriate actions in response. **DISCUSSION** Organizations need to stay informed about potential threats by monitoring security alerts and advisories from credible sources and responding appropriately to mitigate risks.	To address the control of "System and Information Integrity" for monitoring information system security alerts and advisories and taking appropriate actions in response, several tools, technologies, and processes are essential. Security Information and Event Management (SIEM) systems are vital as they collect, analyze, and correlate security event data from various sources to detect potential threats in real-time. Threat intelligence platforms aggregate and analyze data from multiple sources, providing up-to-date information on emerging threats and vulnerabilities. Additionally, endpoint detection and response (EDR) tools monitor endpoint activities and detect suspicious behavior, allowing for rapid response to security incidents. Key processes must also be implemented to comply with these control requirements. Organizations need to establish a continuous monitoring process to stay informed about potential threats by observing security alerts and advisories from credible sources. This involves setting up alerting mechanisms to notify security teams of potential issues promptly. Conducting regular threat assessments helps evaluate the impact of identified threats and determine appropriate mitigation strategies. Furthermore, implementing an incident response plan ensures that the organization can respond quickly and effectively to security incidents, minimizing potential damage and recovery time. Appgate can also address this control by providing robust network access controls that enhance overall security posture. Appgate's Zero Trust Network Access (ZTNA) solution ensures that only authenticated and authorized users and devices can access the network, reducing the risk of unauthorized access and potential exploitation of vulnerabilities. While Appgate does not directly monitor security alerts and advisories, it integrates effectively with SIEM and threat intelligence platforms to enhance the organization's ability to detect and respond to threats. By leveraging Appgate's network access controls in conjunction with other security tools and processes, organizations can better manage security alerts and advisories, taking appropriate actions to mitigate risks.	For more information on how Appgate SDP integrates with tools and processes to address the control of "System and Information Integrity" for monitoring security alerts and advisories, refer to the following sections in the Appgate SDP Admin Guide: **Integration with Security Information and Event Management (SIEM) Systems:** -"LogForwarding" for details on exporting audit logs to SIEMs and integrating with SIEM platforms to collect, analyze, and correlate security event data. **Integration with Threat Intelligence Platforms:** -"Risk Engine Integration and ZTP Settings" section for details on dynamically adjusting to threat levels based on information from threat intelligence platforms. **Integration with Endpoint Detection and Response (EDR) Solutions:** -"Authentication and Authorization Processes" for leveraging user and device attributes to enhance security and integrate with EDR tools for monitoring endpoint activities and detecting suspicious behavior. **Continuous Monitoring and Alerting Mechanisms:** -"System Monitoring and Logs" section for details on setting up alerting mechanisms and continuous monitoring processes to stay informed about potential threats and security advisories. **Incident Response Plan:** -"Troubleshooting Chapter" for procedures on configuring and troubleshooting appliances, which includes guidelines on implementing an incident response plan to respond quickly and effectively to security incidents. **Regular Threat Assessments and Mitigation Strategies:** -"Administration and Security Best Practices" section for guidelines on conducting regular threat assessments and implementing mitigation strategies in response to identified threats. **Training and Awareness Programs:** -"Security Best Practices" section for educating employees on recognizing and responding to security alerts and advisories to enhance overall security posture.

CMMC Control Number	CMMC Control Description	Far Clause	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SI.1.213	**System and Information Integrity** Update malicious code protection mechanisms when new releases are available. • FAR Clause 52.204-21 b.1.xvii • NIST SP 800-171 Rev 2 3.14.4	**52.204-21 b.1.xvii** Update malicious code protection mechanisms when new releases are available.	**3.14.4** Update malicious code protection mechanisms when new releases are available. **DISCUSSION** Regular updates to malicious code protection mechanisms are essential to defend against evolving threats. This includes timely installation of patches and updates to anti-virus software and other security tools.	To address the control of "System and Information Integrity" for updating malicious code protection mechanisms when new releases are available, several tools, technologies, and processes are essential. Anti-virus software and endpoint protection platforms are critical as they detect and mitigate malicious code. These tools must be regularly updated to incorporate the latest threat signatures and protection mechanisms. Patch management systems are also vital as they automate the deployment of security patches for operating systems and applications, ensuring vulnerabilities are addressed promptly. Key processes must also be implemented to comply with these control requirements. Organizations should establish a routine schedule for checking and applying updates to all security tools and systems. This involves coordinating with vendors to stay informed about the latest releases and ensuring that updates are tested and applied without delay. Regularly conducting vulnerability assessments helps identify any gaps that might be mitigated by the latest updates. Additionally, implementing a change management process ensures that updates are applied systematically and that any issues arising from updates are promptly addressed. Appgate can also address this control by providing robust network access controls that enhance overall security posture. Appgate's Zero Trust Network Access (ZTNA) solution ensures that only authenticated and authorized users and devices can access the network, reducing the risk of unauthorized access and potential exploitation of vulnerabilities. While Appgate does not directly update malicious code protection mechanisms, it integrates effectively with endpoint protection platforms and patch management systems to enhance the organization's ability to defend against evolving threats. By leveraging Appgate's network access controls in conjunction with other security tools and processes, organizations can ensure their malicious code protection mechanisms are up-to-date and effective.	For more information on how Appgate SDP integrates with tools and processes to address the control of "System and Information Integrity" for updating malicious code protection mechanisms, refer to the following sections in the Appgate SDP Admin Guide: **Integration with Endpoint Protection Platforms:** -"Authentication and Authorization Processes" for details on leveraging user and device attributes to enhance security and integrate with endpoint protection platforms for detecting and mitigating malicious code. **Integration with Patch Management Systems:** - "Policy Management" section for details on configuring and managing policies, including device and client controls, crucial for ensuring timely deployment of security patches through integrated patch management systems. **Routine Updates and Vulnerability Assessments:** -"System Monitoring and Logs" section for details on setting up alerting mechanisms and continuous monitoring processes to stay informed about potential threats and security advisories, essential for coordinating routine updates to all security tools and systems. **Change Management Process:** -"Troubleshooting Chapter" for procedures on configuring and troubleshooting appliances, which includes guidelines on implementing a change management process to apply updates systematically and promptly address any issues promptly. **Regular Security Assessments and Mitigation Strategies:** -"Administration and Security Best Practices" section for guidelines on conducting regular vulnerability assessments and implementing mitigation strategies in response to identified threats, ensuring malicious code protection mechanisms are up-to-date and effective.

CMMC LEVEL 2 DOMAIN: ACCESS CONTROLS (AC)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.2.016	**Control CUI Flow** Control the flow of CUI in accordance with approved authorizations. • NIST SP 800-171 Rev 2 3.1.3	Control the flow of CUI in accordance with approved authorizations. **DISCUSSION** This control focuses on limiting the flow o f Controlled Unclassified Information (CUI) within an organization and ensuring that only authorized personnel have access to it. The goal is to protect CUI from unauthorized access or leakage, especially during transmission over networks or between systems. Effective control mechanisms must be established to manage and monitor how CUI is handled and transmitted, which includes encryption, access control, and logging of CUI-related activities.	Appgate plays a critical role in controlling network access to CUI by leveraging identity attributes, device posture, and contextual information to enforce precise access policies. Through Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC), Appgate ensures that only authorized users and devices can access CUI over the network. These access controls are dynamic, adjusting in real-time based on factors such as user identity, device compliance status, and environmental conditions, such as geographic location. While Appgate does not directly control the handling of CUI, it provides a robust framework to prevent unauthorized access to CUI through the network. Appgate's logging capabilities are also essential for maintaining oversight of CUI access. Detailed logs are generated for every access attempt, capturing who accessed CUI, when, and under what conditions. These logs can be forwarded to a Security Information and Event Management (SIEM) system, where they can be correlated with logs from other security tools like EDR, DRM, DLP, and NGFWs. This integration allows for a comprehensive security posture, where alerts and events generated by these tools can trigger Appgate's API to dynamically adjust access policies in response to emerging threats, thus enhancing the overall security of CUI.	For more information on how Appgate controls network access to CUI, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring policies that control network access to CUI. - **Device Posture and Device Claim Scripts:** Refer to 'Device Claim Scripts' for guidelines on setting up device posture requirements that influence access to CUI. - **Single Packet Authorization (SPA):** Review the 'Single Packet Authorization' section for details on securing network access to CUI using SPA. - **Logging and Auditing:** See 'Logging and Auditing' for monitoring CUI access, and learn how these logs can be integrated with SIEM systems for enhanced security management.
AC.3.017	**Separation of Duties** Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 2 3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion. **DISCUSSION** Separation of duties is a critical component of risk management in an organization. It involves dividing responsibilities and tasks among different individuals to reduce the potential for unauthorized or malicious activities. By ensuring that no single individual has control over all aspects of a critical process, organizations can minimize the risk of errors, fraud, and other harmful activities. This control helps to ensure that sensitive tasks are not performed by a single individual, thereby reducing the risk of collusion and ensuring that critical activities are checked and balanced.	Appgate supports the separation of duties by enabling fine-grained access control policies that ensure different roles within the organization have distinct and separate access rights. Using Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), Appgate allows organizations to define and enforce access policies that prevent any single user from having complete control over critical processes or systems. This approach helps mitigate the risk of insider threats and collusion by ensuring that sensitive tasks require the involvement of multiple individuals. Moreover, Appgate's policy-driven framework enables the automation of separation of duties across the environment. This automation ensures that access controls are consistently applied, reducing the risk of human error and maintaining uniform enforcement of security policies. Appgate also integrates seamlessly with Security Information and Event Management (SIEM) systems, allowing logs and alerts related to role assignments and access controls to be monitored and correlated with other security events. This integration further enhances the organization's ability to detect and respond to any potential violations of separation of duties, thereby strengthening overall security.	For more information on how Appgate enforces separation of duties, refer to the following sections in the Appgate 9/Admin Guide: - **Access Management:** See 'Access Management' for details on configuring role-based and attribute-based access control policies. - **Role-Based Access Control (RBAC):** Refer to 'RBAC Configuration' for enforcing role-based access. - **Attribute-Based Access Control (ABAC):** Refer to 'ABAC Configuration' for enforcing attribute-based access control. - **Logging and Auditing:** Look at 'Logging and Auditing' for monitoring and enforcing separation of duties and integrating with SIEM systems for comprehensive oversight.

DOMAIN: *ACCESS CONTROLS (AC) (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.2.007	**Least Privilege** Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 2 3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts. **DISCUSSION** The principle of least privilege is a security concept that limits users' access rights to the minimum necessary to perform their job functions. This control applies to all users, including administrators and those with privileged accounts. By enforcing least privilege, organizations reduce the potential attack surface and minimize the risk of unauthorized access to critical systems and data. This control ensures that users have only the access they need, which helps prevent accidental or intentional misuse of privileges.	Appgate implements the principle of least privilege by dynamically enforcing access policies that limit users' access rights based on their role, identity, device posture, and other contextual factors. Appgate uses both Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) to ensure that users are granted only the necessary access to perform their job functions, with all other access being restricted. This approach helps minimize the risk of unauthorized access to sensitive systems and data, particularly for privileged accounts. In addition, Appgate's continuous monitoring and auditing capabilities allow organizations to track access to critical resources in real-time. Any deviations from the principle of least privilege are detected and can be addressed promptly. Logs generated by Appgate can be forwarded to a Security Information and Event Management (SIEM) system, where they can be correlated with data from other security tools to provide a comprehensive view of the organization's security posture.	For more information on how Appgate enforces least privilege, refer to the following sections in the Appgate Admin Guide: - **Access Management**: See 'Access Management' for details on configuring least privilege policies. - **Role-Based Access Control (RBAC):** Refer to 'RBAC Configuration' for enforcing role-based access. - **Attribute-Based Access Control (ABAC):** Refer to 'ABAC Configuration' for enforcing attribute-based access control. - **Logging and Auditing:** Look at 'Logging and Auditing' for tracking and auditing least privilege enforcement.
AC.2.008	**Non-Privileged Account Use** Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 Rev 2 3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions. **DISCUSSION** This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a new logon.	Appgate enforces the use of non-privileged accounts by providing granular control over user access to systems and data. Through role-based access control (RBAC) and attribute-based access control (ABAC), Appgate ensures that users can only access the resources they are authorized to use, based on their role and context. This minimizes the risk of unauthorized access to sensitive systems and data by limiting the actions that users can perform within the environment. Appgate's policy-driven approach allows organizations to enforce strict access control policies that segregate privileged and non-privileged roles, reducing the potential for unauthorized actions. Additionally, by integrating with IAM systems and forwarding audit logs to SIEM platforms, Appgate ensures that any actions taken by non-privileged accounts are properly monitored and recorded for compliance and security purposes.	For more information on how Appgate enforces the use of non-privileged accounts, refer to the following sections in the Appgate Admin Guide: - **Role-Based Access Control (RBAC):** See 'User Roles and Access Policies' for details on configuring non-privileged accounts. - **Integration with Identity and Access Management (IAM) Systems:** Refer to 'Identity Management Integration' for guidance on assigning and managing non-privileged roles. - **Logging and Monitoring:** Review 'Audit and Compliance Logging' for details on tracking the use of non-privileged accounts.
AC.3.018	**Privileged Functions** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 Rev 2 3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. **DISCUSSION** Privileged functions include, for example, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Unauthorized execution of privileged functions can have significant adverse impacts on organizational operations, assets, and individuals. Capturing the execution of privileged functions in audit logs is essential to ensuring accountability and detecting potential misuse.	Appgate prevents non-privileged users from executing privileged functions by enforcing strict access control policies and capturing all actions in detailed audit logs. The system ensures that only users with the appropriate privileges can execute sensitive functions, and any attempt to perform these actions is recorded for review and compliance purposes. By integrating with security information and event management (SIEM) systems, Appgate allows organizations to monitor and respond to any unauthorized attempts to perform privileged actions. This comprehensive logging and monitoring capability enables organizations to maintain accountability and detect potential misuse of privileged functions. Logs related to privileged actions can be automatically forwarded to SIEM systems, where they can be analyzed alongside other security data to ensure a swift response to any anomalies.	For more information on how Appgate prevents unauthorized execution of privileged functions, refer to the following sections in the Appgate Admin Guide: - **Role-Based Access Control (RBAC):** See 'RBAC Configuration' for enforcing role-based access. - **Logging and Auditing:** Look at 'Logging and Auditing' for details on capturing privileged function execution. - **Security Information and Event Management (SIEM) Integration:** Review the 'SIEM Integration' section for details on monitoring and responding to security events.

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.2.009	**Unsuccessful Logon Attempts** Limit unsuccessful logon attempts. • NIST SP 800-171 Rev 2 3.1.8	Limit unsuccessful logon attempts. **DISCUSSION** This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the criticality of those components.	Appgate enforces security policies that limit unsuccessful logon attempts by integrating with the configurations set in the organization's Identity Provider (IdP) systems, such as SAML, OIDC, or Active Directory. Appgate ensures that accounts are locked, or other protective actions are initiated after a predefined number of failed logon attempts, as specified by the IDP. This approach helps protect against brute force attacks and unauthorized access attempts by adhering to the policies already established within the IdP. In addition, Appgate provides detailed logging and auditing capabilities to track unsuccessful logon attempts and other security-related events. These logs can be forwarded to a Security Information and Event Management (SIEM) system, where they can be correlated with other security data to detect patterns of unsuccessful logon attempts and mitigate the risk of security breaches.	For more information on how Appgate limits unsuccessful logon attempts, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring logon attempt policies. - **Logging and Auditing:** Refer to 'Audit and Compliance Logging' for details on tracking unsuccessful logon attempts. - **Multi-Factor Authentication (MFA):** Review the 'MFA Configuration' section for enhancing logon security.
AC.2.005	**Privacy & Security Notices** Provide privacy and security notices consistent with applicable CUI rules. • NIST SP 800-171 Rev 2 3.1.9	Provide privacy and security notices consistent with applicable CUI rules. **DISCUSSION** Privacy and security notices inform users about the organization's policies and procedures regarding the handling of Controlled Unclassified Information (CUI) and other sensitive data. These notices serve as a reminder of the user's responsibilities and the legal and regulatory requirements associated with accessing, using, and disseminating CUI. By providing clear and consistent notices, organizations can ensure that users are aware of their obligations and the potential consequences of non-compliance.	Appgate supports the provision of privacy and security notices through its integration with Identity and Access Management (IAM) systems, which can deliver customized messages to users upon login or when accessing specific resources. These notices can include reminders about the organization's policies on handling Controlled Unclassified Information (CUI), legal obligations, and security best practices. Appgate's Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) mechanisms ensure that users are only presented with notices that are relevant to their roles and the resources they are accessing. This approach helps to reinforce security awareness and compliance with CUI handling requirements. Additionally, Appgate allows organizations to configure a Message of the Day (MOTD) banner or set conditions that prompt or notify users as they attempt to access resources containing CUI. This ensures that users are explicitly reminded of their obligations and the organization's policies each time they access sensitive information. The MOTD or prompt can be tailored to the specific security requirements and can serve as an acknowledgment mechanism that users must agree to before proceeding, further enhancing compliance with CUI handling protocols. Appgate also supports logging and auditing of user interactions with these privacy and security notices, providing organizations with the ability to track whether users have acknowledged the notices and taken appropriate action. These logs can be integrated into a Security Information and Event Management (SIEM) system to ensure ongoing compliance and provide a comprehensive view of security monitoring.	For more information on how Appgate supports privacy and security notices, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for details on configuring login notices, Message of the Day banners, and user prompts. - **Role-Based Access Control (RBAC):** Refer to 'RBAC Configuration' for delivering targeted notices based on user roles. - **Logging and Auditing:** Look at 'Logging and Auditing' for tracking user acknowledgment of notices and integrating with SIEM systems for comprehensive monitoring.

DOMAIN: ACCESS CONTROLS (AC) (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.2.010	**Session Lock** Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 Rev 2 3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. **DISCUSSION** Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are an essential security control for preventing unauthorized access to systems when users are temporarily away.	While Appgate does not directly implement session lock features at the operating system level, it enforces inactivity timeouts that require users to reauthenticate after a defined period of inactivity. This mechanism is crucial for preventing unauthorized access to sensitive resources when a user steps away from their workstation. Inactivity timeout policies can be configured to prompt users for Multi-Factor Authentication (MFA), require a justification for continued access, or, with IT Service Management (ITSM) integration, mandate that a support ticket be approved before access to resources is granted. These capabilities ensure that even when a session is left unattended, the user must validate their identity and provide a reason to regain access, thereby enhancing security and reducing the risk of unauthorized access to sensitive information. Appgate's dynamic policies provide flexibility and can be tailored to the organization's specific security requirements, ensuring that controls are consistently applied across various devices and environments.	For more information on how Appgate enforces inactivity timeout policies and related access conditions, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring inactivity timeouts and reauthentication policies. - **Multi-Factor Authentication (MFA):** Refer to 'MFA Configuration' for enforcing MFA upon session reactivation. - **IT Service Management (ITSM) Integration:** Review 'ITSM Integration' for details on requiring ticket approval as a condition for reaccessing resources. - **Logging and Auditing**: Review 'Logging and Auditing' for monitoring inactivity and reauthentication events.
AC.3.019	**Session Termination** Terminate (automatically) a user session after a defined condition. • NIST SP 800-171 Rev 2 3.1.11	Terminate (automatically) a user session after a defined condition. **DISCUSSION** Session termination is a security control that automatically ends a user session after a specific condition is met, such as a period of inactivity or the completion of a transaction. This control helps prevent unauthorized access to systems and data by ensuring that sessions are not left open indefinitely. Automatic session termination reduces the risk of someone gaining unauthorized access to an active session, especially in environments where users may forget to log out or close their sessions.	Appgate implements session termination policies that automatically end user sessions after a defined condition is met, such as a period of inactivity or the completion of a task. This control is essential for maintaining the security of systems and data, particularly in environments where users may leave sessions open unintentionally. By ensuring that sessions are automatically terminated, Appgate reduces the risk of unauthorized access to active sessions, protecting both the organization and its users from potential security breaches. Appgate's session termination policies can be customized to fit the needs of the organization, allowing administrators to define specific conditions under which a session should be terminated. This flexibility ensures that session termination controls are aligned with the organization's security objectives and compliance requirements. Additionally, Appgate's logging and auditing features track session termination events, providing comprehensive oversight for compliance and security monitoring.	For more information on how Appgate enforces session termination policies, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring session termination policies. - **Device Posture and Device Claim Scripts:** Refer to 'Device Claim Scripts' for ensuring compliance with session termination requirements. - **Logging and Auditing:** Look at 'Logging and Auditing' for tracking and monitoring session terminations.
AC.2.013	**Control Remote Access** Monitor and control remote access sessions. • NIST SP 800-171 Rev 2 3.1.12	Monitor and control remote access sessions. **DISCUSSION** Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when properly configured, can provide a secure communication channel over untrusted networks.	Appgate provides comprehensive monitoring and control of remote access sessions through its ability to enforce access policies based on identity, device posture, and context. By integrating with various authentication sources and using policy-driven access control, Appgate ensures that only authorized users can initiate remote access sessions. It also provides detailed logging and auditing capabilities to monitor the activities of remote users, ensuring compliance with organizational policies. Appgate's robust approach to remote access management allows organizations to maintain tight control over who can access resources remotely, under what conditions, and from which devices, thereby reducing the risk of unauthorized access and ensuring that all remote activities align with the organization's security policies.	For more information on how Appgate controls remote access, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for details on configuring remote access policies. - **Device Posture and Device Claim Scripts:** Refer to 'Device Claim Scripts' for details on configuring device posture requirements for remote access. - **Logging and Auditing:** Review 'Logging and Auditing' for monitoring and logging remote access sessions.

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.3.014	**Remote Access** Confidentiality Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. • NIST SP 800-171 Rev 2 3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. **DISCUSSION** This requirement ensures that information is protected when accessed remotely, often over untrusted networks like the internet. Cryptographic mechanisms, such as encryption protocols, are used to safeguard data as it traverses these networks, preventing unauthorized disclosure of sensitive information during remote access sessions. The strength of the cryptographic mechanisms employed should be appropriate to the sensitivity of the information being accessed.	Appgate employs advanced cryptographic mechanisms, such as mutual TLS (mTLS) and Single Packet Authorization (SPA), to protect the confidentiality of remote access sessions. These mechanisms ensure that data transmitted between remote users and the organization's systems is encrypted, preventing unauthorized access or interception of sensitive information. Appgate's approach to securing remote access sessions is designed to meet the highest standards of cryptographic strength, making it suitable for environments that require stringent confidentiality controls. Appgate's encryption configuration is highly customizable, allowing organizations to enforce the specific cryptographic standards required for their operational environment. This ensures that all remote access sessions are secured according to the sensitivity of the information being accessed, providing robust protection against potential threats.	For more information on how Appgate ensures remote access confidentiality, refer to the following sections in the Appgate Admin Guide: - **Encryption Configuration:** Refer to 'Encryption Configuration' for details on setting up mTLS, SPA, and FIPS-compliant encryption for secure remote access. - **Single Packet Authorization (SPA):** Review the 'Single Packet Authorization' section for configuring and managing SPA, which ensures that only authorized packets can initiate communication. - **Access Management:** Look at 'Access Management' for configuring secure remote access policies, including how encryption settings are applied. - **Logging and Auditing:** Check 'Logging and Auditing' for tracking and monitoring remote access sessions to ensure compliance with security policies.
AC.2.015	**Remote Access Routing** Route remote access via managed access control points. • NIST SP 800-171 Rev 2 3.1.14	Route remote access via managed access control points. **DISCUSSION** This control ensures that remote access to an organization's systems is managed through designated access control points, such as firewalls, gateways, or secure remote access servers. These control points enforce the organization's security policies, including authentication and authorization requirements, and monitor all remote access traffic for compliance with these policies. By routing remote access through managed control points, organizations can better protect their systems from unauthorized access.	Appgate routes remote access sessions through managed access control points by utilizing its Policy Decision Points (PDPs), known as Controllers, and Policy Enforcement Points (PEPs), known as Gateways. These components ensure that all remote access traffic is subject to the organization's security policies. The Controllers handle the authentication, authorization, and policy decision-making, while the Gateways enforce these decisions by controlling the network traffic according to the defined policies. Appgate's policy engine allows organizations to define specific routing rules based on user roles, device posture, and other contextual factors, ensuring that remote access is tightly controlled and compliant with security requirements. This architecture provides a secure and flexible framework for managing and monitoring all remote access sessions.	For more information on how Appgate manages remote access routing, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring routing policies for remote access, including setting up secure routes through Gateways. - **Controllers and Gateways:** Refer to 'Controller Configuration' and 'Gateway Configuration' for detailed guidance on setting up and managing the Controllers (PDPs) and Gateways (PEPs) to enforce remote access policies. - **Policy Engine:** Review the 'Policy Engine' section for configuring rules that dictate how remote access traffic is routed based on various contextual factors. - **Logging and Auditing:** Look at 'Logging and Auditing' for comprehensive guidance on monitoring and logging remote access routing activities to ensure they align with security policies.

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.3.021	**Privileged Remote Access** Authorize remote execution of privileged commands and remote access to security-relevant information. • NIST SP 800-171 Rev 2 3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information. **DISCUSSION** Privileged commands and access to security-relevant information are highly sensitive and can have significant security implications if accessed or executed remotely by unauthorized individuals. This control requires organizations to ensure that only authorized users with appropriate privileges can remotely execute privileged commands or access security-relevant information. Organizations must implement strong access control measures to mitigate risks associated with remote privileged access.	Appgate enforces strict access control policies for the remote execution of privileged commands and access to security-relevant information. The system ensures that only users with the appropriate privileges can execute such commands or access sensitive data remotely. All actions are logged and monitored, allowing organizations to track and audit the use of privileged access. By integrating with identity management systems and employing multi-factor authentication (MFA), Appgate adds additional layers of security to remote privileged access, ensuring that only authorized individuals can perform sensitive operations. Appgate's logging capabilities allow organizations to monitor and audit all privileged remote access activities, providing detailed records for compliance and security analysis. This comprehensive approach ensures that remote privileged access is both secure and accountable.	For more information on how Appgate manages privileged remote access, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring remote access policies for privileged users, including the setup of MFA and other conditions for privileged access. - **Role-Based Access Control (RBAC):** Refer to 'RBAC Configuration' for enforcing role-based access, ensuring that only users with the appropriate roles can execute privileged commands. - **Logging and Auditing:** Look at 'Logging and Auditing' for detailed guidance on tracking and monitoring the use of privileged remote access, ensuring all activities are recorded for compliance. - **Integration with Identity and Access Management (IAM) Systems:** Check the 'Identity Management Integration' section for how Appgate integrates with external IAM systems to manage privileged accounts and enforce access policies across the enterprise.
AC.2.011	**Wireless Access Authorization** Authorize wireless access prior to allowing such connections. • NIST SP 800-171 Rev 2 3.1.16	Authorize wireless access prior to allowing such connections. **DISCUSSION** Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication between the device and the network.	Appgate enables organizations to enforce stringent wireless access controls by integrating with existing identity and access management (IAM) systems, though it is important to note that Appgate does not rely on IAM for enforcing wireless access controls. The IAM provides authentication (Auth-N) and authorization (Auth-Z) details, such as roles, groups, or attributes about the user, which Appgate uses in its access decision process. Additionally, Appgate can enforce multi-factor authentication (MFA) independently of the IAM/IdP if needed. Appgate's capabilities allow it to detect the network name (SSID) and source IP, using this information to determine whether a user is attempting to connect from a wireless network. This information is then utilized in Appgate's decision-making process for access authorization. Furthermore, Appgate does not need to trust the underlying network transport since it creates mTLS and SPA-protected connections, ensuring that even if the wireless network is untrusted or contested, user traffic remains secure.	For more information on how Appgate protects wireless access, refer to the following sections in the Appgate Admin Guide: - **Cryptographic Mechanisms:** See 'Encryption Configuration' for details on setting up mTLS and SPA for secure wireless access. - **Access Management:** Refer to 'Access Management' for configuring wireless access policies. - **Logging and Auditing:** Look at 'Logging and Auditing' for tracking and monitoring wireless access events.

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AC.3.012	**Wireless Access Protection** Protect wireless access using authentication and encryption. • NIST SP 800-171 Rev 2 3.1.17	Protect wireless access using authentication and encryption. **DISCUSSION** This control ensures that wireless access to an organization's systems is secured using robust authentication and encryption mechanisms. Wireless networks are often targeted for attacks due to their susceptibility to unauthorized access. By implementing strong authentication protocols and encryption, organizations can protect the integrity and confidentiality of data transmitted over wireless networks, preventing unauthorized access and ensuring secure communications.	Appgate enforces strict control over the connection of mobile devices by using device posture checks, identity verification, and contextual data to ensure that only authorized and secure devices can access organizational systems. Appgate can detect the device type and use this information as part of the decision-making process, ensuring that access policies are applied based on the specific device being used. By integrating with mobile device management (MDM) solutions, Appgate ensures that mobile devices comply with security policies before granting access. This integration allows Appgate to enforce policies that take into account device posture, user roles, and other contextual factors, ensuring that only compliant devices are permitted to connect.	For more information on how Appgate controls mobile device connections, refer to the following sections in the Appgate Admin Guide: - **Device Posture and Device Claim Scripts:** See 'Device Claim Scripts' for configuring mobile device posture checks and detecting device type. - **Access Management:** Refer to 'Access Management' for setting up mobile device access policies. - **Logging and Auditing:** Look at 'Logging and Auditing' for monitoring and logging mobile device connections.
AC.3.020	**Mobile Device Connection** Control connection of mobile devices. • NIST SP 800-171 Rev 2 3.1.18	Control connection of mobile devices. **DISCUSSION** Mobile devices, including smartphones, tablets, and laptops, often access organizational systems remotely and can be used to process, store, or transmit Controlled Unclassified Information (CUI). This control requires organizations to establish policies and procedures for controlling the connection of mobile devices to organizational systems, ensuring that only authorized and secure devices are permitted to connect.	Appgate enforces strict control over the connection of mobile devices by using device posture checks, identity verification, and contextual data to ensure that only authorized and secure devices can access organizational systems. Appgate can detect the device type and the network name (SSID) and source IP, using this information as part of the decision-making process to determine access. This ensures that mobile devices comply with security policies before granting access. By integrating with mobile device management (MDM) solutions, Appgate enhances its ability to enforce security policies tailored to mobile devices, providing additional layers of control. Furthermore, Appgate's role-based access control (RBAC) and attribute-based access control (ABAC) allow organizations to define and enforce access policies based on user roles, device posture, and contextual information, ensuring secure access even over untrusted and contested networks.	For more information on how Appgate controls mobile device connections, refer to the following sections in the Appgate Admin Guide: - **Access Management:** Refer to 'Access Management' for setting up mobile device access policies. - **Logging and Auditing:** Look at 'Logging and Auditing' for monitoring and logging mobile device connections.
AC.3.022	**Encrypt CUI on Mobile** Encrypt CUI on mobile devices and mobile computing platforms. • NIST SP 800-171 Rev 2 3.1.19	Encrypt CUI on mobile devices and mobile computing platforms. **DISCUSSION** Mobile devices and mobile computing platforms are often used in environments where physical security is difficult to maintain. This control requires organizations to employ encryption to protect Controlled Unclassified Information (CUI) on mobile devices and platforms, ensuring that if the device is lost or stolen, the CUI remains secure and inaccessible to unauthorized users.	Appgate does not directly apply to the encryption of CUI on mobile devices. However, Appgate provides robust encryption for data in transit using FIPS-validated mTLS and Single Packet Authorization (SPA). These mechanisms ensure that CUI transmitted between mobile devices and organizational systems remains secure during transmission, protecting it from unauthorized access or interception. This capability is crucial for environments where mobile devices are used to access or transmit sensitive information, particularly when the network cannot be trusted.	For more information on how Appgate secures data in transit, refer to the following sections in the Appgate Admin Guide: - **Cryptographic Mechanisms:** See 'Encryption Configuration' for details on setting up mTLS and SPA. - **Access Management:** Refer to 'Access Management' for configuring secure access policies for mobile devices. - **Logging and Auditing:** Review 'Logging and Auditing' for monitoring encrypted data transmissions.
AC.2.006	**Portable Storage Use** Limit use of portable storage devices on external systems. • NIST SP 800-171 Rev 2 3.1.21	Limit use of portable storage devices on external systems. **DISCUSSION** Portable storage devices, such as USB drives and external hard drives, can introduce significant security risks when connected to external systems. This control requires organizations to limit the use of portable storage devices on external systems to reduce the risk of unauthorized access, data leakage, and the introduction of malware. Organizations should establish policies and procedures for the secure use of portable storage devices.	Appgate is not directly applicable to limiting the use of portable storage devices on external systems. This control is generally addressed through policies and procedures that restrict the use of such devices, combined with data loss prevention (DLP) tools that monitor and control data transfers to portable storage devices. However, Appgate can complement these efforts by providing secure access controls and monitoring capabilities for systems that handle sensitive data. Appgate's role in securing access to systems and monitoring data access can help ensure that portable storage devices are not used to improperly access or transfer sensitive information.	While Appgate is not directly applicable to limiting the use of portable storage devices, you can refer to the following sections in the Appgate Admin Guide for related access control measures: - **Access Management:** See 'Access Management' for configuring secure access policies. - **Logging and Auditing:** Look at 'Logging and Auditing' for monitoring access to systems that handle sensitive data.

DOMAIN: AWARENESS TRAINING

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AT.2.056	**Security Awareness Training** Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of applicable policies, standards, and procedures related to the security of organizational systems. • NIST SP 800-171 Rev 2 3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of applicable policies, standards, and procedures related to the security of organizational systems. **DISCUSSION** This control emphasizes the importance of making all personnel within an organization, including managers, system administrators, and users, aware of the security risks associated with their actions and the policies, standards, and procedures that must be followed to secure organizational systems. Security awareness training helps to reduce the risk of security breaches by educating employees about potential threats and the proper ways to mitigate them. Regular training ensures that everyone is informed about the latest security protocols and the consequences of non-compliance.	Appgate does not directly deliver security awareness training but can integrate with existing learning and training platforms to ensure that access to certain resources is contingent on the completion of required training. By using Appgate's policy engine, organizations can enforce access controls that check whether users have completed their security awareness training before allowing access to sensitive systems or data. Additionally, Appgate can be used to deliver a Message of the Day to inform users about security risks and organizational policies each time they log in. This approach ensures that users are regularly reminded of the importance of security and are informed of any updates to security policies.	For more information on how Appgate can integrate with training platforms and deliver messages to users, refer to the following sections in the Appgate Admin Guide: - **Policy Engine Configuration:** See the "Policy Engine" section for details on setting up conditions that require training completion before granting access. - **Message of the Day Configuration:** Refer to the "System Messages" or "Message of the Day" section for configuring daily security reminders or notifications.
AT.2.057	**Role-Based Security Training** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. • NIST SP 800-171 Rev 2 3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. **DISCUSSION** This control ensures that personnel who have specific information security responsibilities are adequately trained to carry out their duties. Role-based security training helps to ensure that employees understand the security requirements relevant to their specific job roles. By tailoring training to the responsibilities of each role, organizations can better manage security risks and ensure that security practices are applied consistently across different areas of the organization.	While Appgate does not directly provide role-based security training, it can be integrated with learning and training platforms to enforce access controls based on the completion of role-specific training. Appgate's policy-driven access management allows organizations to restrict access to sensitive applications or data until users have completed the necessary training tailored to their roles. Appgate can also deliver context-aware messages or notifications that remind users of the standards, policies, and procedures they must adhere to when accessing sensitive applications, further reinforcing the importance of role-based security training.	For more information on how Appgate enforces access controls based on role-specific training completion and delivers contextual messages, refer to the following sections in the Appgate Admin Guide: - **Policy-Based Access Control:** See "Access Management" for configuring role-specific access controls linked to training completion. - **Contextual Messaging:** Refer to the "System Messages" section for configuring notifications and messages that inform users of relevant policies before accessing sensitive applications.
AT.3.058	**Incident Response Training** Provide training in the use and management of security controls and procedures associated with incident response. • NIST SP 800-171 Rev 2 3.2.3	Provide training in the use and management of security controls and procedures associated with incident response. **DISCUSSION** This control focuses on the need to train personnel on how to effectively respond to security incidents. Incident response training ensures that employees understand the procedures and controls that should be followed during an incident to minimize damage and facilitate recovery. Regular training in incident response helps organizations prepare for potential security events and ensures that the response is efficient and effective, reducing the overall impact of an incident on the organization.	Appgate does not directly offer incident response training but can be used to enforce access controls that ensure users have completed incident response training before being granted access to certain security-relevant tools or systems. By integrating with an organization's training platform, Appgate can restrict access based on the status of training completion, ensuring that only trained personnel can access critical incident response systems. Furthermore, Appgate can deliver on-screen notifications or reminders that inform users of the procedures and security controls they need to follow during incident response, helping reinforce training and ensure compliance with organizational standards.	For more information on how Appgate supports access control enforcement linked to incident response training, refer to the following sections in the Appgate Admin Guide: - **Training Completion Verification:** See "Policy Engine" for details on configuring access restrictions based on incident response training status. - **Incident Response Notifications:** Refer to the "System Messages" or "Notifications" sections for setting up reminders and notifications related to incident response procedures and controls.

DOMAIN: AUDIT AND ACCOUNTABILITY

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AU.2.042	**System Auditing** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. • NIST SP 800-171 Rev 2 3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. **DISCUSSION** Audit logs are critical to identifying and responding to incidents of unauthorized access or other malicious activities. The ability to create and retain these logs ensures that organizations have the necessary data to monitor and analyze system activity, investigate incidents, and report on compliance with security policies.	Appgate provides robust system auditing capabilities by creating and retaining detailed audit logs that capture user activities, system events, and access control decisions. These logs are essential for monitoring, analyzing, and investigating system activity, particularly in detecting and responding to unauthorized access or suspicious behavior. Appgate's audit logs are configurable, allowing organizations to define what activities are logged based on their specific security and compliance requirements. Additionally, Appgate can integrate with SIEM systems to aggregate and analyze audit logs from multiple sources, enabling more comprehensive monitoring and quicker incident response. This integration ensures that all relevant data is available for detecting and investigating potential security incidents.	For more information on how Appgate handles system auditing, refer to the following sections in the Appgate Admin Guide: - **Logging and Auditing:** See 'Logging and Auditing' for details on configuring and managing system audit logs. - **Access Management:** Refer to 'Access Management' for configuring access to audit logs. - **Monitoring and Alerts:** Review 'Monitoring and Alerts' for setting up alerts related to audit logging. - **Security Information and Event Management (SIEM) Integration**: Refer to the 'SIEM Integration' section for information on forwarding Appgate logs to SIEM systems for centralized analysis and monitoring.
AU.2.041	**User Accountability** Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. • NIST SP 800-171 Rev 2 3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. **DISCUSSION** User accountability is essential to maintaining the integrity of organizational systems. By ensuring that every user action can be traced back to the individual responsible, organizations can deter malicious behavior and ensure that users are held accountable for their actions. This control is critical for enforcing policies and responding to security incidents.	Appgate ensures user accountability by uniquely identifying and tracing the actions of individual users through its comprehensive logging and auditing features. By capturing detailed logs of user activity, including access requests, entitlements, and actions taken within the system, Appgate enables organizations to hold users accountable for their actions. These logs are securely stored and can be reviewed to investigate incidents or verify compliance with security policies. Furthermore, Appgate's logs can be forwarded to SIEM systems, where they can be correlated with other data sources to provide a comprehensive view of user activity across the organization. This capability enhances the ability to detect and respond to insider threats and other security incidents by providing detailed visibility into user actions.	For more information on how Appgate ensures user accountability, refer to the following sections in the Appgate Admin Guide: - **Logging and Auditing:** See 'Logging and Auditing' for details on how user actions are logged and monitored. - **Access Management:** Refer to 'Access Management' for configuring user roles and access rights. - **Compliance Reporting:** Review 'Compliance Reporting' for how to generate reports that track user activity. - **Security Information and Event Management (SIEM) Integration:** Refer to the 'SIEM Integration' section for forwarding user activity logs to SIEM systems for enhanced monitoring and correlation.
AU.3.045	E**vent Review** Review and update logged events. • NIST SP 800-171 Rev 2 3.3.3	Review and update logged events. **DISCUSSION** Regular review of logged events is necessary to ensure that audit logs accurately reflect system activity and to identify any unauthorized or suspicious behavior. Organizations should establish processes for reviewing and updating event logs to ensure that they remain relevant and useful for monitoring, analysis, and investigation.	Appgate supports the regular review and update of logged events by providing tools that allow administrators to analyze audit logs, filter events, and update logging configurations as needed. This capability ensures that audit logs remain relevant and reflect the most critical system activities. By enabling regular event review, Appgate helps organizations maintain the integrity of their audit logs and ensures that they provide a reliable record of system activity. Additionally, Appgate's integration with SIEM systems allows for continuous monitoring and automated analysis of logged events. This integration helps organizations identify trends, detect anomalies, and quickly respond to potential security incidents.	For more information on how Appgate supports event review and updating, refer to the following sections in the Appgate Admin Guide: - **Logging and Auditing:** See 'Logging and Auditing' for details on reviewing and updating logged events. - **Event Management:** Refer to 'Event Management' for configuring event filters and logs. - **Compliance Reporting:** Review 'Compliance Reporting' for generating reports based on event logs. - **Security Information and Event Management (SIEM) Integration:** See 'SIEM Integration' for forwarding event logs to SIEM systems for continuous monitoring and automated analysis.

DOMAIN: AUDIT AND ACCOUNTABILITY (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AU.3.046	**Audit Failure Alerting** Alert in the event of an audit logging process failure. • NIST SP 800-171 Rev 2 3.3.4	Alert in the event of an audit logging process failure. **DISCUSSION** Audit logging is essential for maintaining the security and integrity of organizational systems. If the audit logging process fails, it could result in the loss of critical data needed for monitoring, analysis, and investigation. By alerting administrators to audit logging failures, organizations can take prompt action to address the issue and ensure that audit logs remain intact and available for review.	Appgate includes an alerting mechanism that notifies administrators in the event of an audit logging process failure. This feature is critical for ensuring that audit logs remain intact and available for analysis. By alerting administrators to any issues with the logging process, Appgate enables prompt action to be taken to resolve the problem and maintain the integrity of audit data. Appgate can also integrate with SIEM systems to enhance the visibility and response to audit logging failures. By forwarding alerts to a SIEM, organizations can automate responses and correlate these alerts with other events to quickly identify and mitigate the root cause of logging failures.	For more information on how Appgate handles audit failure alerting, refer to the following sections in the Appgate Admin Guide: - **Monitoring and Alerts:** See 'Monitoring and Alerts' for details on configuring alerts for audit logging failures. - **Logging and Auditing:** Refer to 'Logging and Auditing' for managing audit logs. - **Compliance Reporting:** Review 'Compliance Reporting' for tracking and responding to audit log issues. - **Security Information and Event Management (SIEM) Integration:** Refer to the 'SIEM Integration' section for information on forwarding audit failure alerts to SIEM systems for automated incident response.
AU.3.051	**Audit Correlation** Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. • NIST SP 800-171 Rev 2 3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. **DISCUSSION** The ability to correlate audit records from different sources and analyze them in a cohesive manner is critical for detecting and responding to security incidents. By integrating audit records from multiple systems and correlating the data, organizations can identify patterns of suspicious activity and respond more effectively to potential threats. This control ensures that audit records are not just collected but also analyzed in a way that provides meaningful insights into system behavior, enabling timely and informed responses to potential security breaches.	Appgate provides the ability to correlate audit records from different sources, enabling comprehensive analysis and reporting. This capability is essential for detecting and responding to security incidents, as it allows organizations to identify patterns of suspicious activity and investigate potential threats. By integrating audit records across systems, Appgate helps organizations respond more effectively to indications of unlawful or unauthorized activity. Additionally, Appgate's integration with SIEM systems enhances audit correlation by providing a centralized platform for analyzing logs from multiple sources. This allows for more effective identification of complex attack patterns and more comprehensive incident response.	For more information on how Appgate handles audit correlation, refer to the following sections in the Appgate Admin Guide: - **Logging and Auditing:** See 'Logging and Auditing' for correlating audit records. - **Event Management:** Refer to 'Event Management' for configuring audit correlations and analysis. - **Compliance Reporting:** Review 'Compliance Reporting' for reporting on correlated audit events. - **Security Information and Event Management (SIEM) Integration:** See the 'SIEM Integration' section for forwarding correlated audit logs to SIEM systems for enhanced analysis and incident response.
AU.3.052	**Reduction & Reporting** Provide audit record reduction and report generation to support on-demand analysis and reporting. • NIST SP 800-171 Rev 2 3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting. **DISCUSSION** Audit logs can generate large volumes of data, making it difficult to analyze and report on specific events. Audit record reduction and reporting tools help organizations to filter, reduce, and summarize audit data, making it easier to identify key events and generate reports for compliance and investigation purposes.	Appgate includes tools for audit record reduction and report generation, supporting on-demand analysis and reporting. These tools help organizations manage large volumes of audit data by filtering and summarizing key events, making it easier to identify critical incidents and generate reports for compliance and investigation purposes. Appgate's capabilities can be enhanced through integration with SIEM systems, which can automate the reduction and correlation of large datasets, enabling more efficient analysis and reporting. This integration ensures that the most relevant data is available for compliance and forensic investigations.	For more information on how Appgate handles audit record reduction and reporting, refer to the following sections in the Appgate Admin Guide: - **Logging and Auditing:** See 'Logging and Auditing' for details on reducing and summarizing audit records. - **Event Management:** Refer to 'Event Management' for configuring audit record filters and summaries. - **Compliance Reporting:** Review 'Compliance Reporting' for generating reports based on reduced audit data. - **Security Information and Event Management (SIEM) Integration:** See the 'SIEM Integration' section for forwarding reduced and summarized audit records to SIEM systems for enhanced reporting and analysis.

DOMAIN: AUDIT AND ACCOUNTABILITY (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
AU.2.043	**Authoritative Time Source** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. • NIST SP 800-171 Rev 2 3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. **DISCUSSION** Accurate time stamps are essential for correlating audit records across different systems and identifying the sequence of events. By synchronizing internal system clocks with an authoritative time source, organizations can ensure that all audit records contain accurate and consistent time stamps, making it easier to analyze and correlate events across multiple systems.	Appgate supports the synchronization of internal system clocks with an authoritative time source, ensuring that all audit logs contain accurate and consistent timestamps. This capability is essential for correlating events across systems and establishing an accurate timeline of activities, which is critical for incident investigation and response. Additionally, Appgate integrates with SIEM systems to ensure that synchronized timestamps are maintained across various security tools, facilitating better event correlation and analysis.	For more information on how Appgate handles time synchronization, refer to the following sections in the Appgate Admin Guide: - **Time Management:** See 'Time Management' for configuring synchronization with authoritative time sources. - **Logging and Auditing:** Refer to 'Logging and Auditing' for how time stamps are applied to audit records. - **Compliance Reporting:** Review 'Compliance Reporting' for ensuring that time synchronization is maintained.
AU.3.049	**Audit Protection** Protect audit information and audit logging tools from unauthorized access, modification, and deletion. • NIST SP 800-171 Rev 2 3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion. **DISCUSSION** Audit logs and logging tools are valuable resources for monitoring and analyzing system activity. If they are tampered with or deleted, it could compromise the organization's ability to detect and respond to security incidents. This control ensures that audit logs and logging tools are protected from unauthorized access and modification, helping to maintain the integrity and availability of audit data.	Appgate protects audit information and logging tools from unauthorized access, modification, and deletion by enforcing strict access control policies and providing secure storage for audit logs. This protection ensures that audit data remains intact and available for monitoring and investigation, helping to maintain the integrity of the audit process. Additionally, Appgate's integration with SIEM systems further ensures that audit logs are securely transmitted and stored, allowing for centralized monitoring and quick detection of any unauthorized access attempts.	For more information on how Appgate protects audit information, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for controlling access to audit logs. - **Secure Storage:** Refer to 'Secure Storage' for configuring secure storage for audit data. - **Logging and Auditing:** Review 'Logging and Auditing' for details on protecting audit logs from unauthorized access or modification.
AU.3.050	**Audit Management** Limit management of audit logging functionality to a subset of privileged users. • NIST SP 800-171 Rev 2 3.3.9	Limit management of audit logging functionality to a subset of privileged users. **DISCUSSION** Audit logging functionality is critical to maintaining the security and integrity of organizational systems. By limiting access to this functionality to a subset of privileged users, organizations can prevent unauthorized changes to audit settings, protect the integrity of audit logs, and ensure that logging remains consistent and reliable.	Appgate limits the management of audit logging functionality to a subset of privileged users, ensuring that only authorized individuals can modify logging settings or access audit logs. This control helps to protect the integrity of the audit process by preventing unauthorized changes to logging configurations and ensuring that audit data is consistently and accurately recorded. Furthermore, Appgate leverages Role-Based Access Control (RBAC) to enforce these restrictions, ensuring that only users with appropriate roles can manage audit logs and settings.	For more information on how Appgate manages audit logging functionality, refer to the following sections in the Appgate Admin Guide: - **Access Management:** See 'Access Management' for configuring privileged access to audit logs. - **Role-Based Access Control (RBAC):** Refer to 'RBAC Configuration' for limiting access to audit management. - **Logging and Auditing:** Review 'Logging and Auditing' for details on managing audit logs and functionality.

DOMAIN: CONFIGURATION MANAGEMENT

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
CM.2.061	**System Baselining** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. • NIST SP 800-171 Rev 2 3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. **DISCUSSION** Baseline configurations are essential to establishing and maintaining the secure state of an information system. These baselines provide a foundation for managing the security posture of an organization's systems by ensuring that only approved configurations are used.	Appgate provides robust capabilities for system baselining through both the SDP Operator and the management UI. The SDP Operator ensures that the configurations and deployments of Appgate's Secure Access systems align with predefined baseline configurations, managing the lifecycle of components and maintaining an inventory of all configurations. This is particularly useful in dynamic environments where automated enforcement is necessary. However, for environments where a DevOps/GitOps model is not required, administrators can utilize the management UI to manually configure and enforce baseline policies. This includes configuring the baseline settings for various system components, such as Controllers, Gateways, and Clients, ensuring that deviations are detected and reported. Integration: Appgate integrates with SIEM, IdP/IAM, and EDR systems, providing immediate detection and reporting of deviations from baseline configurations, thereby enhancing the overall security posture.	For more information on how Appgate handles system baselining, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for managing baselines within Kubernetes environments. - **Access Management:** Refer to 'Access Management' for configuring baseline policies. - **Logging and Auditing:** Review 'Logging and Auditing' for tracking baseline configurations.
CM.2.064	**Security Configuration Enforcement** Establish and enforce security configuration settings for information technology products employed in organizational systems. • NIST SP 800-171 Rev 2 3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems. **DISCUSSION** Security configuration settings provide a means to reduce the attack surface of organizational systems. By enforcing configuration settings, organizations can minimize the risk of unauthorized access and other security breaches. These settings should be established based on security best practices and should be regularly reviewed and updated.	Appgate enforces security configuration settings through both the SDP Operator and management UI. The SDP Operator is ideal for environments requiring automated and consistent enforcement of security policies across deployments. It manages and applies security configurations, ensuring they align with best practices and reducing the attack surface. For organizations not leveraging a DevOps/GitOps approach, administrators can use the management UI to manually enforce security settings on Controllers, Gateways, and Clients. This includes locking down unnecessary services, protocols, and ports on the appliances, configuring role-based access control (RBAC), and ensuring compliance with security policies. Integration: Appgate can integrate with NGFW, DLP, and other security tools to provide a comprehensive enforcement strategy across the network.	For more information on how Appgate enforces security configurations, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for managing and enforcing security configurations. - **Security Policies:** Refer to 'Security Policies' for configuring and enforcing security settings. - **Logging and Auditing:** Review 'Logging and Auditing' for monitoring security configurations.
CM.2.065	**System Change Management** Track, review, approve or disapprove, and log changes to organizational systems. • NIST SP 800-171 Rev 2 3.4.3	Track, review, approve or disapprove, and log changes to organizational systems. **DISCUSSION** Change management is critical for maintaining the security and stability of organizational systems. By tracking and reviewing changes, organizations can ensure that modifications do not introduce new vulnerabilities or compromise existing security controls. Change logs provide a record of all changes made to systems.	Appgate facilitates comprehensive system change management through both the SDP Operator and the management UI. The SDP Operator offers automated tracking, reviewing, and approving changes, ensuring that any alterations are logged and analyzed for potential security impacts. Administrators can also manually manage and log changes using the management UI, which is particularly useful in smaller or less dynamic environments. This capability ensures that all changes are documented, approved, and that their impact on the security posture is fully understood. Integration: Appgate's integration with SIEM and DLP systems enables real-time monitoring of changes and generates alerts for unauthorized modifications, thereby enhancing the security of the change management process.	For more information on how Appgate handles system change management, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for tracking and managing changes within Kubernetes. - **Change Management:** Refer to 'Change Management' for logging and reviewing system changes. - **Logging and Auditing:** Review 'Logging and Auditing' for maintaining an audit trail of system changes.

DOMAIN: *CONFIGURATION MANAGEMENT (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
CM.2.066	**Security Impact Analysis** Analyze the security impact of changes prior to implementation. • NIST SP 800-171 Rev 2 3.4.4	Analyze the security impact of changes prior to implementation. **DISCUSSION** Security impact analysis is critical for understanding the potential risks associated with changes to organizational systems. By analyzing the security impact of changes before implementation, organizations can identify and mitigate potential vulnerabilities, ensuring that changes do not compromise the security of the system.	Appgate supports security impact analysis through its comprehensive change management capabilities, which include both the SDP Operator and the management UI. The SDP Operator can simulate the impact of changes on the system's security posture, allowing organizations to identify potential risks and address them proactively before the changes are implemented. This feature is particularly beneficial in environments that require automated and continuous integration of security checks. In addition, the management UI provides administrators with tools to manually assess the security impact of changes, offering flexibility in environments where a DevOps/GitOps approach may not be required. This allows for detailed configuration and impact analysis before any changes are made. Integration: Appgate can also integrate with SIEM, EDR, and other security tools to correlate changes with potential security events, providing a deeper understanding of the security impact and enhancing the overall security monitoring process.	For more information on how Appgate supports security impact analysis, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for simulating and analyzing the impact of system changes. - **Change Management:** Refer to 'Change Management' for processes related to assessing the security impact of changes. - **Risk Assessment:** Review 'Risk Assessment' for evaluating potential risks associated with changes.
CM.3.067	**Access Restrictions for Change** Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. • NIST SP 800-171 Rev 2 3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. **DISCUSSION** Access restrictions are essential for ensuring that only authorized individuals can make changes to organizational systems. By enforcing physical and logical access restrictions, organizations can prevent unauthorized changes and protect the integrity of their systems.	Appgate enforces access restrictions for changes through a combination of its role-based access control (RBAC) and change management features available in both the SDP Operator and the management UI. The RBAC system ensures that only authorized users can make changes to the system, while the SDP Operator logs all changes for audit purposes, providing an additional layer of control and oversight. For environments not using a DevOps/GitOps model, the management UI allows for granular control and configuration of access restrictions, ensuring that only those with proper authorization can modify critical system components. This reduces the risk of unauthorized changes and helps maintain the integrity of the system. Integration: Appgate's integration with IAM and SIEM systems enhances visibility and control over change activities, ensuring compliance with security policies and enabling real-time monitoring and alerts for unauthorized modifications.	For more information on how Appgate enforces access restrictions for changes, refer to the following sections in the Appgate Admin Guide: - **Role-Based Access Control (RBAC):** See 'RBAC Configuration' for controlling access to system changes. - **SDP Operator Overview:** Refer to 'SDP Operator' for managing and logging access to changes. - **Access Management:** Review 'Access Management' for enforcing access controls during changes.
CM.2.062	**Least Functionality** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. • NIST SP 800-171 Rev 2 3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. **DISCUSSION** Least functionality involves limiting system functionality to only what is necessary for operational requirements. By doing so, organizations reduce the attack surface of their systems, minimizing the potential for exploitation by malicious actors. This principle is critical for maintaining the security and resilience of organizational systems.	Appgate adheres to the principle of least functionality by enabling organizations to configure their systems to provide only the necessary capabilities. Through the SDP Operator, organizations can disable unnecessary features and services, ensuring that only essential functions are active, thereby reducing the attack surface. Additionally, the management UI allows for granular configuration to disable or restrict nonessential functionality directly on the Controller, Gateway, and other appliances without requiring a full DevOps/GitOps setup. This flexibility ensures that even in traditional environments, Appgate can enforce the least functionality principle effectively. Integration: Appgate can also integrate with system hardening and security policy frameworks to enforce least functionality across various components of the IT environment, further bolstering security measures.	For more information on how Appgate adheres to the principle of least functionality, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for disabling unnecessary functions and services. - **System Hardening:** Refer to 'System Hardening' for configuring systems with only essential capabilities. - **Security Policies:** Review 'Security Policies' for defining and enforcing the least functionality principle. - **Logging and Auditing:** Refer to 'Logging and Auditing' for monitoring and enforcing least functionality configurations.

DOMAIN: CONFIGURATION MANAGEMENT (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
CM.3.068	**Nonessential Functionality** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. • NIST SP 800-171 Rev 2 3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. **DISCUSSION** Nonessential functionality increases the attack surface of a system by providing more opportunities for attackers to exploit vulnerabilities. By disabling or restricting these nonessential elements, organizations can reduce the risk of unauthorized access and other security breaches.	Appgate enforces the principle of least functionality through multiple avenues. Using the SDP Operator, organizations can automate the restriction or disabling of nonessential functions, programs, ports, protocols, and services within their environment, especially in a DevOps/GitOps configuration as code model. For environments that do not require such an approach, the Appgate management UI allows administrators to manually configure the system to lock down interfaces, disable services like SSH and Prometheus, and restrict specific ports and protocols on the appliances, including the Controller and Gateway. This flexibility ensures that organizations can maintain a secure and minimalistic operational footprint, regardless of their specific deployment model.	For more information on how Appgate restricts nonessential functionality, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for managing and disabling nonessential functions and services. - **System Hardening:** Refer to 'System Hardening' for configuring systems with only essential capabilities. - **Security Policies:** Review 'Security Policies' for defining and enforcing nonessential functionality restrictions. - **Management UI Configuration:** Refer to 'Management UI Configuration' for settings related to locking down interfaces, services, and ports/protocols on Appgate appliances.
CM.3.069	**Application Execution Policy** Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. • NIST SP 800-171 Rev 2 3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. **DISCUSSION** Application execution policies are essential for controlling the software that can run on organizational systems. By using deny-by-exception or permit-by-exception policies, organizations can prevent unauthorized or potentially harmful software from executing.	Appgate supports the application execution policy by providing both deny-by-exception (blacklisting) and permit-by-exception (whitelisting) controls. Through the SDP Operator, these policies can be enforced in environments using a DevOps/GitOps approach, ensuring strict control over which applications can be executed within the environment. For environments not utilizing the SDP Operator, Appgate's management UI allows for similar control over software execution policies. Administrators can define which applications are authorized to run on the system, reducing the risk of malicious or unauthorized software being executed.	For more information on how Appgate enforces application execution policies, refer to the following sections in the Appgate Admin Guide: - **SDP Operator Overview:** See 'SDP Operator' for configuring deny-by-exception and permit-by-exception policies. - **Application Control:** Refer to 'Application Control' for managing which software can be executed within the environment. - **Security Policies:** Review 'Security Policies' for defining and enforcing application execution rules. - **Management UI Configuration:** Refer to 'Management UI Configuration' for setting up application execution policies without the SDP Operator.
CM.2.063	**User-Installed Software** Control and monitor user-installed software. • NIST SP 800-171 Rev 2 3.4.9	Control and monitor user-installed software. **DISCUSSION** User-installed software can introduce vulnerabilities or conflict with existing security policies. By controlling and monitoring the installation of software by users, organizations can ensure that only approved software is used, reducing the risk of introducing security threats into the environment.	Appgate offers comprehensive controls for managing and monitoring user-installed software through device posture checks and device claims. These device claims can be configured to inspect the presence of specific installed applications, registry keys, and running processes, ensuring that only compliant devices are granted access to the network. This approach allows organizations to enforce policies that restrict the use of unauthorized or vulnerable software, significantly reducing the risk of security threats. For organizations looking to adopt a configuration-as-code model, the SDP Operator can be used to automate and enforce these controls, ensuring that all endpoints meet the required security standards. The management UI also provides administrators with the ability to monitor and control user-installed software without requiring the SDP Operator, making it suitable for environments that do not require a full DevOps or GitOps approach.	For more information on how Appgate controls and monitors user-installed software, refer to the following sections in the Appgate Admin Guide: - **Device Claims and Posture Checks:** See 'Device Claims Configuration' for setting up checks on installed applications, registry keys, and running processes. - **Role-Based Access Control (RBAC):** Refer to 'RBAC Configuration' for controlling software installation based on user roles. - **SDP Operator Overview:** For environments using the SDP Operator, refer to 'SDP Operator' for automating device claims and software monitoring. - **Management UI Configuration:** For manual monitoring and control of user-installed software, see 'Management UI Configuration'. - **Logging and Auditing:** Review 'Logging and Auditing' for tracking software installation activities and ensuring compliance with security policies.

DOMAIN: IDENTIFICATION AND AUTHENTICATION

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
IA.3.083	**Multifactor Authentication** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. • NIST SP 800-171 Rev 2 3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. **DISCUSSION** Multifactor authentication (MFA) provides an additional layer of security by requiring multiple forms of verification before granting access. This reduces the likelihood of unauthorized access, even if one factor (e.g., a password) is compromised.	Appgate supports multifactor authentication (MFA) through integration with identity providers and the use of multiple factors for verifying user identity. Appgate can enforce MFA for both privileged and non-privileged accounts, ensuring that users must authenticate using at least two different factors before accessing critical systems. This provides an additional layer of security, reducing the risk of unauthorized access, even if a user's password is compromised.	For more information on how Appgate supports multifactor authentication, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring MFA with external identity providers. - **Access Policies:** Refer to 'Access Policies' for enforcing MFA for privileged and non-privileged accounts. - **Authentication Methods:** Review 'Authentication Methods' for details on setting up MFA within the Appgate platform.
IA.3.084	**Replay-Resistant Authentication** Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. • NIST SP 800-171 Rev 2 3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. **DISCUSSION** Replay-resistant authentication mechanisms help protect against replay attacks, where an attacker intercepts and retransmits authentication data to gain unauthorized access.	Appgate employs replay-resistant authentication mechanisms by leveraging secure authentication protocols that include one-time passwords and cryptographic challenges. These mechanisms ensure that authentication data cannot be reused by an attacker, thereby protecting against replay attacks. By integrating with secure identity providers and enforcing the use of replay-resistant authentication methods, Appgate enhances the security of network access for both privileged and non-privileged accounts.	For more information on how Appgate employs replay-resistant authentication, refer to the following sections in the Appgate Admin Guide: - **Authentication Protocols:** See 'Authentication Protocols' for configuring replay-resistant methods. - **Identity Providers (IdPs) and Integration:** Refer to 'Identity Provider Integration' for using one-time passwords and cryptographic challenges. - **Security Policies:** Review 'Security Policies' for enforcing replay-resistant authentication.
IA.3.085	**Identifier Reuse** Prevent reuse of identifiers for a defined period. • NIST SP 800-171 Rev 2 3.5.5	Prevent reuse of identifiers for a defined period. **DISCUSSION** Identifier reuse can allow attackers to leverage previously compromised identifiers for unauthorized access. By preventing the reuse of identifiers, organizations can reduce the risk of unauthorized access and ensure that each identifier is unique and secure for a specified period.	Appgate assists in preventing identifier reuse by managing user identifiers through its integration with identity providers. The system can enforce policies that prevent the reuse of identifiers for a defined period, ensuring that once an identifier is no longer in use, it cannot be reissued or reused within the organization. This helps to maintain the integrity and security of user identities within the system.	For more information on how Appgate prevents identifier reuse, refer to the following sections in the Appgate Admin Guide: - **Identity Management:** See 'Identity Management' for managing user identifiers and preventing reuse. - **Identity Providers (IdPs) Integration:** Refer to 'Identity Provider Integration' for enforcing identifier reuse policies. - **Access Policies:** Review 'Access Policies' for setting and enforcing identifier reuse restrictions.
IA.3.086	**Identifier Handling** Disable identifiers after a defined period of inactivity. • NIST SP 800-171 Rev 2 3.5.6	Disable identifiers after a defined period of inactivity. **DISCUSSION** Identifier handling is crucial to maintaining the security of user accounts. By disabling identifiers after a period of inactivity, organizations can reduce the risk of unauthorized access using old or inactive accounts.	Appgate enforces identifier handling by automatically disabling user accounts that have been inactive for a specified period. This helps to ensure that old or unused accounts do not become a target for unauthorized access. The system's integration with identity providers allows for seamless management of user identities, including the enforcement of inactivity policies.	For more information on how Appgate handles identifier management, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring inactivity policies with external identity providers. - **Access Policies:** Refer to 'Access Policies' for enforcing inactivity-based identifier handling. - **Identity Management:** Review 'Identity Management' for details on managing user identifiers and disabling inactive accounts.

DOMAIN: *IDENTIFICATION AND AUTHENTICATION (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
IA.2.078	**Password Complexity** Enforce a minimum password complexity and change of characters when new passwords are created. • NIST SP 800-171 Rev 2 3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created. **DISCUSSION** Password complexity is critical to preventing unauthorized access. By enforcing rules around password complexity, including length, character types, and frequency of change, organizations can make it more difficult for attackers to guess or crack passwords.	Appgate supports password complexity requirements by integrating with identity providers that enforce complex password policies. Through its role-based access control (RBAC) and policy enforcement capabilities, Appgate ensures that users must comply with predefined password complexity standards when accessing systems. This reduces the risk of password-based attacks by ensuring that all passwords meet the necessary security criteria.	For more information on how Appgate supports password complexity, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring password complexity with external identity providers. - **Access Policies:** Refer to 'Access Policies' for enforcing password complexity requirements. - **Authentication Methods:** Review 'Authentication Methods' for details on setting up password policies within the Appgate platform.
IA.2.079	**Password Reuse** Prohibit password reuse for a specified number of generations. • NIST SP 800-171 Rev 2 3.5.8	Prohibit password reuse for a specified number of generations. **DISCUSSION** Password reuse is a common security weakness that can be exploited by attackers. By prohibiting the reuse of passwords, organizations can ensure that users do not recycle old passwords, which might have been compromised.	Appgate helps to enforce password reuse policies by working in conjunction with identity providers that track password history and prevent the reuse of previous passwords. This ensures that users create new, unique passwords when they change their credentials, thereby reducing the risk of compromised passwords being reused.	For more information on how Appgate supports password reuse policies, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring password reuse policies with external identity providers. - **Access Policies:** Refer to 'Access Policies' for enforcing password reuse prevention. - **Authentication Methods:** Review 'Authentication Methods' for details on setting up password policies within the Appgate platform.
IA.2.080	**Identification and Authentication** Uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). • NIST SP 800-171 Rev 2 3.5.1	Uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). **DISCUSSION** Identification and authentication are critical for ensuring that only authorized users can access organizational systems. By uniquely identifying and authenticating each user, organizations can prevent unauthorized access and protect sensitive information from compromise.	Appgate ensures the unique identification and authentication of organizational users through its robust identity management features. Appgate integrates with identity providers (IdPs) and leverages multiple identity attributes, such as username, group membership, and device posture, to uniquely identify and authenticate users. This process ensures that only authorized users can access the system, and all authentication events are logged for audit purposes.	For more information on how Appgate handles identification and authentication, refer to the following sections in the Appgate Admin Guide: - **Identity Management:** See 'Identity Management' for configuring user authentication. - **Integration with Identity Providers (IdPs):** Refer to 'IdP Integration' for details on integrating with identity providers. - **Logging and Auditing:** Review 'Logging and Auditing' for monitoring authentication events.
IA.2.081	**Multi-Factor Authentication for Local and Network Access** Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. • NIST SP 800-171 Rev 2 3.5.3	Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. **DISCUSSION** Multi-factor authentication (MFA) adds an additional layer of security by requiring users to present two or more forms of identification before gaining access. This control is essential for protecting privileged accounts, which are often targeted by attackers, as well as non-privileged accounts that may still provide access to sensitive information.	Appgate supports multi-factor authentication (MFA) for both local and network access by integrating with various MFA providers. Appgate's policies can enforce MFA for privileged accounts and can also require MFA for non-privileged accounts when accessing the network. This additional layer of security helps prevent unauthorized access, especially to sensitive resources that are protected by Appgate's secure access solutions.	For more information on how Appgate supports multi-factor authentication, refer to the following sections in the Appgate Admin Guide: - **Multi-Factor Authentication (MFA):** See 'MFA Configuration' for setting up MFA for local and network access. - **Access Policies:** Refer to 'Access Policies' for enforcing MFA requirements. - **Integration with Multi-Factor Authentication (MFA) Providers:** Review 'MFA Provider Integration' for connecting with external MFA services.

DOMAIN: IDENTIFICATION AND AUTHENTICATION (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
IA.2.082	**Replay Resistant** Authentication Mechanisms Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. • NIST SP 800-171 Rev 2 3.5.7	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. **DISCUSSION** Replay-resistant authentication mechanisms protect against attacks where an adversary intercepts and reuses authentication credentials. By employing such mechanisms, organizations can ensure that authentication credentials cannot be reused by attackers to gain unauthorized access to their systems.	Appgate employs replay-resistant authentication mechanisms by using secure cryptographic protocols for authentication processes. The system leverages mutual TLS (mTLS) and single-packet authorization (SPA) to ensure that authentication credentials cannot be intercepted and reused by attackers. This replay resistance is crucial for maintaining the integrity of authentication processes and preventing unauthorized access.	For more information on how Appgate employs replay-resistant authentication, refer to the following sections in the Appgate Admin Guide: - **Mutual TLS (mTLS):** See 'mTLS Configuration' for setting up secure cryptographic authentication. - **Single-Packet Authorization (SPA):** Refer to 'SPA Configuration' for configuring replay-resistant mechanisms. - **Security Protocols:** Review 'Security Protocols' for ensuring authentication integrity.

DOMAIN: INCIDENT RESPONSE

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
IR.2.092	**Incident Handling** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. • NIST SP 800-171 Rev 2 3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. **DISCUSSION** Incident handling is essential for minimizing the impact of security incidents on organizational systems. By establishing a robust incident-handling capability, organizations can quickly detect, analyze, and respond to incidents, reducing the potential damage and ensuring a swift recovery.	Appgate provides robust incident-handling capabilities by integrating with security information and event management (SIEM) systems, enabling real-time detection, analysis, and response to security incidents. Appgate's logging and auditing features allow organizations to monitor user activities and system events, facilitating quick identification and containment of incidents. Appgate also supports automated response actions, such as blocking or isolating compromised systems, to minimize the impact of security incidents.	For more information on how Appgate supports incident handling, refer to the following sections in the Appgate Admin Guide: - **Incident Management:** See 'Incident Management' for configuring and managing incident-handling procedures. - **Logging and Auditing:** Refer to 'Logging and Auditing' for monitoring and responding to security incidents. - **Security Information and Event Management (SIEM) Integration:** Review 'SIEM Integration' for connecting with security information and event management systems.
IR.3.098	Incident Reporting Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. • NIST SP 800-171 Rev 2 3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. **DISCUSSION** Incident reporting is a critical component of an organization's incident response strategy. By tracking, documenting, and reporting incidents, organizations can ensure that the appropriate stakeholders are informed and can take the necessary actions to address the incident. This process also helps organizations to meet regulatory requirements for incident reporting.	Appgate enables comprehensive incident reporting by providing detailed logs and audit trails of all security events and user activities. These logs can be forwarded automatically to SIEM systems or other incident reporting tools for further analysis and reporting. Appgate's integration with incident management platforms allows organizations to track and document incidents effectively, ensuring that all relevant stakeholders are informed and appropriate actions are taken.	For more information on how Appgate supports incident reporting, refer to the following sections in the Appgate Admin Guide: - **Incident Reporting:** See 'Incident Reporting' for generating and forwarding incident reports. - **Logging and Auditing:** Refer to 'Logging and Auditing' for capturing detailed logs of security events. - **Security Information and Event Management (SIEM) Integration:** Review 'SIEM Integration' for reporting incidents to external authorities.

DOMAIN: INCIDENT RESPONSE (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
IR.3.099	**Incident Response Testing** Test the organizational incident response capability. • NIST SP 800-171 Rev 2 3.6.3	Test the organizational incident response capability. **DISCUSSION** Regular testing of incident response capabilities is necessary to ensure that the organization is prepared to respond effectively to security incidents. By conducting tests, organizations can identify weaknesses in their response plans and make improvements to enhance their overall security posture.	Appgate supports regular testing of incident response capabilities by allowing organizations to simulate security incidents and assess the effectiveness of their response plans. The platform's integration with testing and simulation tools enables organizations to evaluate their incident response procedures in a controlled environment, identify gaps, and make necessary improvements to their incident response strategies.	For more information on how Appgate supports incident response testing, refer to the following sections in the Appgate Admin Guide: - **Incident Response Testing:** See 'Incident Response Testing' for simulating and assessing response capabilities. - **Logging and Auditing:** Refer to 'Logging and Auditing' for capturing test results and identifying improvements. - **Incident Management:** Review 'Incident Management' for making updates to response plans based on testing outcomes.

DOMAIN: MAINTENANCE

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MA.2.111	**Perform Maintenance** Perform maintenance on organizational systems. • NIST SP 800-171 Rev 2 3.7.1	Perform maintenance on organizational systems. DISCUSSION Regular maintenance is necessary to ensure that organizational systems operate effectively and securely. Proper maintenance activities help to prevent system failures, mitigate risks, and ensure that security controls continue to function as intended.	Appgate ensures the reliable and secure execution of system maintenance through comprehensive backup, high availability (HA), and restore functionalities, complemented by the SDP Operator's GitOps and CI/CD capabilities. Appgate's HA architecture ensures that critical components, such as Controllers and Gateways, are continuously available and resilient against failures, thereby minimizing downtime during maintenance activities. Regular backups are scheduled to create consistent snapshots of system states, ensuring that data integrity is maintained, and allowing for rapid recovery in case of unexpected issues. The SDP Operator further enhances maintenance processes by enabling GitOps and CI/CD practices. Through GitOps, all configuration changes and updates are tracked and managed via version-controlled repositories, ensuring that every change is documented and can be rolled back if necessary. CI/CD pipelines automate the deployment of these changes, ensuring that maintenance tasks are carried out efficiently and securely, with minimal manual intervention. This combination of HA, backup, restore, and automated deployment processes ensures that Appgate systems remain secure and operational during all phases of maintenance.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **High Availability (HA):** Refer to the 'High Availability' section for details on configuring and managing HA to ensure continuous service availability during maintenance. - **Backup and Restore:** See the 'Backup and Restore' section for instructions on scheduling regular backups and restoring system components. - **SDP Operator - GitOps and CI/CD:** Review the 'SDP Operator' documentation for details on implementing GitOps and CI/CD pipelines to manage and automate maintenance tasks.

DOMAIN: *MAINTENANCE (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MA.2.112	**System Maintenance Control** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. • NIST SP 800-171 Rev 2 3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. **DISCUSSION** Controlling the tools, techniques, and personnel involved in maintenance activities is critical to maintaining system security. By implementing strict controls, organizations can prevent unauthorized access and ensure that maintenance activities do not introduce vulnerabilities into the system.	Appgate enforces strict control over system maintenance through a combination of its high availability (HA) architecture, automated backup and restore capabilities, and the advanced features of the SDP Operator. By leveraging HA, Appgate ensures that maintenance can be performed without disrupting critical services, as redundant systems take over seamlessly during updates or repairs. The SDP Operator's GitOps functionality allows all maintenance-related changes to be managed through a version-controlled repository, where only authorized and verified changes are applied to the system. This ensures that all updates are consistent, traceable, and compliant with organizational policies. Additionally, CI/CD pipelines automate the deployment process, reducing the risk of human error and ensuring that maintenance tasks are executed efficiently and securely. These combined practices guarantee that only validated changes are implemented, with full visibility and control over the maintenance process.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **High Availability (HA):** Refer to the 'High Availability' section for managing redundant systems to facilitate seamless maintenance without service disruption. - **Backup and Restore:** See the 'Backup and Restore' section for guidance on safeguarding system integrity during maintenance through regular backups. - **SDP Operator - Access Control and Automation:** Review the 'SDP Operator' section for managing system maintenance through GitOps and CI/CD, ensuring controlled and automated updates.
MA.3.115	**Equipment Sanitization** Ensure equipment removed for off-site maintenance is sanitized of any CUI. • NIST SP 800-171 Rev 2 3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI. **DISCUSSION** Sanitizing equipment before it is removed from an organization's premises ensures that controlled unclassified information (CUI) is not exposed to unauthorized individuals. This control is essential for protecting sensitive information when equipment is sent off-site for maintenance or repair.	While Appgate does not handle the physical sanitization of CUI from devices, it plays a crucial role in securing data within its managed virtual infrastructure. Appgate ensures that all sensitive information is protected through encrypted backups and secure data handling practices before any infrastructure components are decommissioned or removed from the environment. Using the SDP Operator, administrators can automate the decommissioning of Appgate components within a Kubernetes environment, ensuring that all data is securely backed up and that any sensitive configurations are properly managed through GitOps practices. This approach ensures that all changes, including data handling during decommissioning, are documented, version-controlled, and compliant with security policies. While physical device sanitization requires additional tools and procedures outside of Appgate's scope, the platform ensures that any data associated with its virtual infrastructure is handled securely and appropriately before off-site maintenance.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Backup and Restore:** Refer to the 'Backup and Restore' section for procedures to securely back up data before decommissioning virtual infrastructure components. - **Data Encryption:** See the 'Data Encryption' section for details on securing CUI within Appgate-managed environments prior to component removal. - **SDP Operator - Decommissioning:** Review the 'SDP Operator' section for best practices in automating the secure decommissioning of infrastructure, including handling sensitive data.
MA.3.116	**Media Inspection** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. • NIST SP 800-171 Rev 2 3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. **DISCUSSION** Media used for diagnostic and test purposes can introduce malicious code into an organization's systems if not properly inspected. By checking media for malware before use, organizations can prevent the introduction of security risks during maintenance activities.	Appgate's platform enhances security during maintenance activities by ensuring that any media used within its infrastructure is thoroughly checked for malware and other security threats. While Appgate does not directly manage physical media inspection, its secure logging and monitoring capabilities allow administrators to track the use of media in the system. For organizations using Appgate within a Kubernetes environment, the SDP Operator can automate the scanning and inspection processes for media used within containers and virtual environments, ensuring that all media complies with security policies before being utilized.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Logging and Auditing:** Review 'Logging and Auditing' for tracking media use and inspection processes. - **SDP Operator - Automation:** See 'SDP Operator' for automating the scanning of media within containers and virtual environments.

DOMAIN: MAINTENANCE (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MA.2.113	**Nonlocal Maintenance** Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. • NIST SP 800-171 Rev 2 3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. **DISCUSSION** Nonlocal maintenance provides significant advantages, such as remote troubleshooting and updates, but also poses security risks if not properly managed. Requiring multifactor authentication (MFA) and ensuring that connections are terminated immediately after use are essential to maintaining the security of organizational systems during remote maintenance.	Appgate supports secure nonlocal maintenance by enforcing multifactor authentication (MFA) for all remote access sessions. Appgate's SDP Operator further enhances this by allowing for automated, secure connections to be established for maintenance purposes, with all activities logged and monitored. The platform ensures that once maintenance is complete, all remote sessions are automatically terminated, reducing the risk of unauthorized access. The integration with CI/CD pipelines via the SDP Operator also allows for the secure and automated deployment of updates, ensuring that maintenance activities are performed consistently and securely.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Multi-Factor Authentication (MFA):** See 'Access Management' for configuring MFA for remote access. - **SDP Operator - Secure Connections:** Review 'SDP Operator' for automating and securing remote maintenance sessions. - **Logging and Termination:** Refer to 'Logging and Auditing' for tracking and terminating remote sessions post-maintenance.
MA.2.114	**Maintenance Personnel** Supervise the maintenance activities of maintenance personnel without required access authorization. • NIST SP 800-171 Rev 2 3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization. **DISCUSSION** Supervising maintenance personnel who do not have the necessary access authorization ensures that they do not gain unauthorized access to sensitive information or systems. This control helps to prevent accidental or deliberate security breaches during maintenance operations.	Appgate enforces strict supervision of maintenance personnel through Role-Based Access Control (RBAC) and comprehensive logging. The platform ensures that only authorized personnel have access to sensitive systems, while maintenance personnel without required access authorization are closely monitored. This supervision is enhanced through the SDP Operator, which automates the enforcement of access policies and monitors all maintenance activities. In the event that unauthorized access is attempted, the system generates alerts, and corrective actions are automatically enforced to prevent security breaches.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Role-Based Access Control (RBAC):** See 'Access Management' for controlling access based on roles. - **SDP Operator - Supervision:** Review 'SDP Operator' for automating the enforcement of access policies during maintenance. - **Logging and Alerting:** Refer to 'Logging and Auditing' for monitoring maintenance activities and responding to unauthorized access attempts.

DOMAIN: MEDIA PROTECTION

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MP.2.119	**Media Protection** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. • NIST SP 800-171 Rev 2 3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. **DISCUSSION** Proper physical and digital protection of media containing Controlled Unclassified Information (CUI) is crucial to prevent unauthorized access. This includes securing media in locked environments and using encryption for digital storage.	Appgate SDP's primary function focuses on controlling and securing access to networked resources and applications that may store or process CUI, rather than directly managing the physical or digital media itself. Through policies that enforce role-based access controls (RBAC) and network segmentation, Appgate ensures that only authorized users and devices can access applications and services where CUI might be stored. This helps prevent unauthorized access to CUI within the networked environment. For organizations that integrate Appgate with endpoint management or DLP (Data Loss Prevention) solutions, there can be enhanced protections, such as ensuring that endpoints comply with security policies before accessing network resources. However, Appgate itself does not manage or control physical media such as disks or paper documents.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Access Management:** Refer to 'Access Management' for configuring RBAC to control access to applications handling CUI. - **Network Segmentation:** See 'Network Segmentation' for isolating critical applications and services. - **Integration with Endpoint Management:** Review options for integrating Appgate with endpoint security solutions.

DOMAIN: *MEDIA PROTECTION (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MP.2.120	**Media Access** Limit access to CUI on system media to authorized users. • NIST SP 800-171 Rev 2 3.8.2	Limit access to CUI on system media to authorized users. **DISCUSSION** Limiting access to system media that contains CUI is essential to ensuring that only authorized personnel can view or modify this information. This applies to both physical access to the media and logical access within systems.	Appgate SDP controls access to network-based resources and applications where CUI may reside, ensuring that only authenticated and authorized users can connect to these resources. While Appgate cannot directly control who accesses physical media, it enforces strict network access policies based on user identity, device posture, and other contextual factors, helping to safeguard CUI within applications. Appgate's role-based access controls (RBAC) and policy-driven security ensure that only authorized users can access applications that store or manage CUI, reducing the risk of unauthorized access. This is particularly effective in environments where CUI is processed or stored in cloud or networked applications.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Role-Based Access Control (RBAC) Implementation:** Refer to 'RBAC Configuration' for setting up role-based access controls. - **Policy Enforcement:** See 'Policy Management' for defining and enforcing security policies. - **Secure Access Controls:** Review 'Secure Access' for implementing conditional access based on user identity and device posture.
MP.3.122	**Media Markings** Mark media with necessary CUI markings and distribution limitations. • NIST SP 800-171 Rev 2 3.8.4	Mark media with necessary CUI markings and distribution limitations. **DISCUSSION** Properly marking media that contains CUI is essential for ensuring that all users who handle the media understand the sensitivity of the information and the appropriate distribution limitations.	Appgate SDP does not have the capability to mark or label physical media with CUI markings. However, within its scope of network security and access management, Appgate can help enforce policies that ensure only authorized users can access networked resources where CUI is stored or processed. Appgate's integration capabilities can extend to work with DLP (Data Loss Prevention) systems or other security solutions that might handle labeling or marking of digital files with CUI tags. In such cases, Appgate's access control can ensure that only users or systems with the correct permissions can access these marked files, providing an additional layer of security around CUI.	For more information on how Appgate supports system maintenance, refer to the following sections in the Appgate Admin Guide: - **Integration with Data Loss Prevention (DLP) Systems:** See 'Integration Options' for connecting Appgate with DLP solutions. - **Access Control Policies:** Refer to 'Policy Enforcement' for controlling access to applications handling CUI-labeled files. - **Secure Access Management:** Review how Appgate enforces secure access to network resources where CUI is processed.
MP.3.125	**Portable Storage Encryption** The organization implements cryptographic mechanisms to protect the confidentiality and integrity of information at rest on all media storage devices, ensuring that sensitive information is safeguarded against unauthorized access or tampering when stored. • NIST SP 800-171 Rev 2 3.8.6	Employ cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during storage. **DISCUSSION** The use of cryptographic mechanisms, such as encryption, is essential for protecting the confidentiality of Controlled Unclassified Information (CUI) when it is stored on digital media. Encryption helps prevent unauthorized access to sensitive data by ensuring that even if the media is compromised or accessed by unauthorized individuals, the information remains unreadable without the proper decryption key. The implementation of this control ensures that CUI is protected from disclosure and maintains its integrity during storage, reducing the risk of data breaches or leaks. Organizations must select cryptographic mechanisms that are appropriate for the sensitivity of the information and comply with federal standards or industry best practices.	Appgate does not directly manage the control of removable media. However, Appgate's microsegmentation and role-based access control (RBAC) can ensure that even if removable media is used, the data accessible through Appgate remains secure by enforcing strict access policies and monitoring data transfers. Additionally, access can be restricted to trusted devices only, reducing the risk of unauthorized data transfers via removable media.	For more information on how Appgate handles access controls and data protection, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring trusted devices and access controls. - **Access Policies:** Refer to 'Access Policies' for enforcing RBAC and data access restrictions. - **Logging and Monitoring:** Review 'Logging and Monitoring' for tracking data transfers and access attempts.

DOMAIN: *MEDIA PROTECTION (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
MP.2.121	**Removable Media** Control the use of removable media on system components. • NIST SP 800-171 Rev 2 3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse. **DISCUSSION** Media sanitization and destruction ensure that CUI is not inadvertently disclosed during the reuse or disposal process.	Appgate does not provide direct media sanitization capabilities. However, it ensures that only authorized users can access network resources that may contain CUI, reducing the risk of unauthorized handling of sensitive data. Additionally, Appgate's logging capabilities can track attempts to access or transfer CUI, providing a layer of oversight and control.	For more information on how Appgate handles access controls and data integrity, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for managing user access to sensitive data. - **Access Policies:** Refer to 'Access Policies' for configuring access restrictions to CUI-containing media. - **Logging and Monitoring:** Review 'Logging and Monitoring' for tracking access and ensuring compliance.
MP.3.123	**Shared Media** Prohibit the use of portable storage devices when such devices have no identifiable owner. • NIST SP 800-171 Rev 2 3.8.10	Protect the confidentiality of CUI at rest. **DISCUSSION** This requirement ensures that CUI stored on system components remains protected from unauthorized access, especially during periods of inactivity.	Appgate employs FIPS-validated mTLS to encrypt data in transit, but encryption of data at rest is typically managed by other systems. However, Appgate ensures secure access to encrypted data through its zero-trust network access (ZTNA) policies. Appgate enforces strict user access controls and continuously monitors access to sensitive data to prevent unauthorized access or leakage.	For more information on how Appgate manages secure access to encrypted data, refer to the following sections in the Appgate Admin Guide: - **Encryption and Security**: See 'Encryption Policies' for details on how Appgate enforces encryption in transit. - **Access Policies:** Refer to 'Access Policies' for enforcing user access controls to CUI. - **Monitoring and Compliance:** Review 'Monitoring and Compliance' for continuous oversight of data access.
RE.2.138	**Protect Backups** Protect the confidentiality of backup CUI at storage locations. • NIST SP 800-171 Rev 2 3.8.9	Conduct regular backup of CUI. **DISCUSSION** Ensuring regular backups of CUI protects against loss due to system failures, data corruption, or other incidents that may impact the availability of the information.	Appgate does not directly manage the backup process, but it ensures that backup systems are securely accessed through its zero-trust policies. The integration of Appgate with SIEM and other monitoring tools helps ensure that any access to backup data is securely logged and monitored to prevent unauthorized access.	For more information on how Appgate supports secure backup processes, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for restricting access to backup systems. - **Security Information and Event Management (SIEM) Integration:** Review 'SIEM Integration' for details on monitoring and logging access to backup data. - **Compliance Monitoring:** Refer to 'Compliance Monitoring' for ensuring secure and compliant access to backup resources.

DOMAIN: PERSONNEL SECURITY

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
PS.2.127	**Personnel Screening** Screen individuals prior to authorizing access to organizational systems containing CUI. • NIST SP 800-171 Rev 2 3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI. **DISCUSSION** Screening processes ensure that individuals who may pose a risk to the organization are identified and mitigated before they are granted access to CUI.	Appgate does not directly manage personnel screening but ensures that only authorized and authenticated users can access systems containing CUI. This is enforced through integration with Identity Providers (IdP) which may include screening attributes as part of the user profile. Appgate enforces access policies based on these profiles.	For more information on how Appgate integrates with Identity Providers and manages access, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring user authentication and attributes. - **Access Policies:** Refer to 'Access Policies' for enforcing access controls based on user profiles. - **User Authentication:** Review 'User Authentication' for detailed processes on how Appgate handles user access.
PS.2.128	**Personnel Termination** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. • NIST SP 800-171 Rev 2 3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. **DISCUSSION** This control ensures that access to CUI is properly managed when employees leave the organization or are transferred to different roles to prevent unauthorized access.	Appgate supports personnel termination and transfer processes by ensuring that once a user's access is revoked or modified, the changes are immediately propagated throughout the network. Appgate's token-based architecture ensures that user sessions are terminated or adjusted in real-time to reflect changes in access status, preventing unauthorized access to CUI.	For more information on how Appgate manages access changes during personnel actions, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for enforcing access controls based on personnel status. - **Session Management:** Refer to 'Session Management' for details on how Appgate manages active sessions during access changes. - **Token Revocation:** Review 'Token Revocation' for immediate enforcement of access changes.
PS.2.127	**Personnel Screening** Screen individuals prior to authorizing access to organizational systems containing CUI. • NIST SP 800-171 Rev 2 3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI. **DISCUSSION** Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.	Appgate does not directly manage personnel screening but ensures that only authorized and authenticated users can access systems containing CUI. This is enforced through integration with Identity Providers (IdP) which may include screening attributes as part of the user profile. Appgate enforces access policies based on these profiles.	For more information on how Appgate integrates with Identity Providers and manages access, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring user authentication and attributes. - **Access Policies:** Refer to 'Access Policies' for enforcing access controls based on user profiles. - **User Authentication:** Review 'User Authentication' for detailed processes on how Appgate handles user access.
PS.L2-3.9.1	**Personnel Screening** Screen individuals prior to authorizing access to organizational systems containing CUI. • NIST SP 800-171 Rev 2 3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI. **DISCUSSION** Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.	Appgate does not directly manage personnel screening but ensures that only authorized and authenticated users can access systems containing CUI. This is enforced through integration with Identity Providers (IdP) which may include screening attributes as part of the user profile. Appgate enforces access policies based on these profiles.	For more information on how Appgate integrates with Identity Providers and manages access, refer to the following sections in the Appgate Admin Guide: - **Identity Providers (IdPs) and Integration:** See 'Identity Provider Integration' for configuring user authentication and attributes. - **Access Policies:** Refer to 'Access Policies' for enforcing access controls based on user profiles. - **User Authentication:** Review 'User Authentication' for detailed processes on how Appgate handles user access.

DOMAIN: PHYSICAL PROTECTION

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
PE.2.135	**Monitor Facility** Protect and monitor the physical facility and support infrastructure for organizational systems. • NIST SP 800-171 Rev 2 3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems. **DISCUSSION** Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.	Appgate does not directly address the control of monitoring physical facilities. However, Appgate's capabilities can complement physical security measures by enforcing strict network access controls based on Geo-Location, Network Location, and IP Addresses. These factors can be used in Appgate policies to ensure that only authorized users can access network resources and applications, providing an additional layer of security that is responsive to the physical location of the user.	For more information on how Appgate can complement physical access monitoring, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for details on configuring access controls based on Geo-Location and Network Location. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for setting up real-time notifications based on user location and network conditions. - **Integration with Physical Security:** Review 'Physical Security Integration' for integrating Appgate with existing physical security systems.
PE.3.136	**Alternative Work Sites** Enforce safeguarding measures for CUI at alternate work sites. • NIST SP 800-171 Rev 2 3.10.6	Enforce safeguarding measures for CUI at alternate work sites. **DISCUSSION** Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.	Appgate does not directly enforce safeguarding measures for physical alternate work sites. Nonetheless, Appgate can enhance security by applying policies based on Geo-Location, Network Location, and IP Addresses, ensuring that only authorized users from recognized locations can access CUI. This approach ensures that the security measures are adaptive to the user's physical and network environment, thereby safeguarding CUI when accessed from alternate locations.	For more information on how Appgate enforces security at alternate work sites, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring location-based access controls using Geo-Location and Network Location. - **Remote Work Support:** Refer to 'Remote Work' for best practices in supporting secure remote access. - **Monitoring and Alerts:** Review 'Monitoring and Alerts' for setting up real-time notifications based on user and network location.

DOMAIN: RISK ASSESSMENT

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
RM.2.141	**Risk Assessments** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. • NIST SP 800-171 Rev 2 3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. **DISCUSSION** Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.	Appgate does not directly manage risk assessments but plays a key role in mitigating identified risks by enforcing Zero Trust principles across network access. Appgate policies can be configured based on risk scores, IP addresses, device posture, and other factors, such as determining device health, including whether a system has vulnerable software or unpatched systems. By continuously monitoring network activities and enforcing dynamic access controls, Appgate helps ensure that only authorized and verified entities can access critical resources, reducing the overall risk to the organization.	For more information on how Appgate supports risk management, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for details on configuring risk-based access controls. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for setting up real-time notifications based on risk assessment results. - **Risk-Based Authentication:** Review 'Risk-based Authentication' for enforcing access controls based on risk levels.
RM.2.142	**Vulnerability Scan** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. • NIST SP 800-171 Rev 2 3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. **DISCUSSION** Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.	Appgate does not directly perform vulnerability scans but can be integrated with other vulnerability management tools to enhance security posture. Appgate's capabilities include determining device health, such as identifying unpatched systems or vulnerable processes running on a device, which can be used to restrict access to network resources. By leveraging Appgate's Zero Trust policies, you can ensure that only authorized devices and users can access systems, minimizing the potential attack surface. Additionally, Appgate can enforce compliance by restricting access to vulnerable systems until they are patched or otherwise secured, based on integration with vulnerability scanning results.	For more information on how Appgate integrates with vulnerability management, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for details on restricting access to vulnerable systems based on device health. - **Integration with Vulnerability Scanners:** Review 'Vulnerability Management Integration' for details on integrating Appgate with vulnerability scanning tools. - **Monitoring and Compliance:** Refer to 'Monitoring and Compliance' for ensuring continuous oversight of system vulnerabilities.

DOMAIN: RISK ASSESSMENT (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
RM.2.143	**Vulnerability Remediation** Remediate vulnerabilities in accordance with risk assessments. • NIST SP 800-171 Rev 2 3.11.3	Remediate vulnerabilities in accordance with risk assessments. **DISCUSSION** Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.	Appgate does not directly remediate vulnerabilities but supports the remediation process by ensuring that access to vulnerable systems is controlled and monitored. Appgate can determine device health, including the presence of vulnerable software or unpatched systems, and enforce policies that limit access to affected systems. This ensures that only authorized personnel can apply necessary patches or mitigations, preventing the exploitation of known vulnerabilities during the remediation process, and protecting critical assets until full remediation is achieved.	For more information on how Appgate supports vulnerability remediation, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for details on enforcing access restrictions during remediation efforts based on device health. - **Incident Response:** Review 'Incident Response' for coordinating remediation activities with access controls. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for setting up real-time notifications during the remediation process.

DOMAIN: SECURITY ASSESSMENT

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
CA.2.158	**Security Control Assessment** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. • NIST SP 800-171 Rev 2 3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. **DISCUSSION** Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures.	Appgate does not directly assess security controls but can provide real-time insights into network access and activity, which is crucial for assessing the effectiveness of security controls. By enforcing Zero Trust principles, Appgate ensures that only authorized users and devices have access to organizational resources, thereby supporting the overall security assessment process. Additionally, Appgate's logging and monitoring capabilities allow for continuous evaluation of access policies and their impact on security.	For more information on how Appgate supports security assessments, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring security controls that align with assessment requirements. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for setting up real-time notifications based on security control assessments. - **Security Information and Event Management (SIEM) Integration**: Review 'SIEM Integration' for details on how Appgate integrates with security information and event management systems to provide comprehensive security assessment data.
CA.2.159	**Plan of Action** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. • NIST SP 800-171 Rev 2 3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. **DISCUSSION** The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.	Appgate does not directly develop plans of action but supports the implementation of corrective measures by restricting access to vulnerable systems until they are secured. Through its policy-based access controls, Appgate ensures that only compliant devices and users can access critical resources, thereby aiding in the reduction of vulnerabilities. By integrating with existing remediation processes, Appgate helps enforce plans of action effectively.	For more information on how Appgate supports the implementation of plans of action, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring access controls that support remediation efforts. - **Incident Response:** Refer to 'Incident Response' for coordinating plans of action with access control measures. - **Monitoring and Alerts:** Review 'Monitoring and Alerts' for setting up real-time notifications during the remediation process.

DOMAIN: SECURITY ASSESSMEN (CONT)

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
CA.3.161	**Security Control Monitoring** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. • NIST SP 800-171 Rev 2 3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. **DISCUSSION** Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations.	Appgate does not directly monitor security controls but enhances continuous monitoring efforts by enforcing strict access controls based on device posture, RBAC/ABAC, and other contextual factors. By leveraging real-time monitoring and dynamic access policies, Appgate ensures that security controls remain effective over time. Additionally, Appgate's integration with security information and event management (SIEM) systems provides comprehensive visibility into network activities, supporting ongoing security control monitoring.	For more information on how Appgate enhances security control monitoring, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring continuous monitoring controls. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for setting up real-time notifications and integrating with SIEM systems. - **Device Health Checks:** Review 'Device Health' for ensuring that only compliant devices can access network resources.
CA.2.157	**System Security Plan** Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. • NIST SP 800-171 Rev 2 3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. **DISCUSSION** System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls.	Appgate does not directly manage system security plans but complements them by enforcing access policies that align with the security requirements documented in these plans. Appgate's capabilities in device health assessment, user authentication, and network segmentation ensure that the security controls outlined in the system security plan are effectively implemented and maintained. By providing detailed logging and audit trails, Appgate supports the periodic updates and assessments required for system security plans.	For more information on how Appgate complements system security plans, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring access controls that align with system security plans. - **System Security Plan Integration:** Review 'System Security Integration' for details on how Appgate supports the implementation of security requirements documented in security plans. - **Monitoring and Compliance:** Refer to 'Monitoring and Compliance' for ensuring continuous oversight of system security plan implementation.

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SC.3.180	**Security Engineering** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. • NIST SP 800-171 Rev 2 3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. **DISCUSSION** Organizations apply secure engineering principles throughout the system development life cycle to effectively mitigate risks associated with the operation of organizational systems. Organizations use well-defined security engineering principles and established security practices for the development, implementation, and integration of secure systems.	Appgate does not directly perform security engineering but significantly enhances security through its Zero Trust Network Access (ZTNA) principles. Appgate enables a multi-dimensional identity profile, where access is granted based on a combination of user, device, application, and contextual risk. This identity/data/device-centric approach ensures that only verified users and devices interact with critical resources, aligning security practices with modern engineering principles. Furthermore, Appgate's SPA (Single Packet Authorization) technology cloaks the enterprise edge, making critical services undiscoverable to potential adversaries, thus reducing the attack surface.	For more information on how Appgate supports secure system design, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring secure access controls based on security engineering principles. - **System Operation:** Refer to 'System Operation' for details on how Appgate integrates with secure software development and engineering processes. - **Single Packet Authorization (SPA):** Review the 'SPA' section for understanding how Appgate hides critical services behind an invisible layer, enhancing overall security.

DOMAIN: *SYSTEM AND COMMUNICATIONS PROTECTION (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SC.3.181	**Role Separation** Separate user functionality from system management functionality. • NIST SP 800-171 Rev 2 3.13.3	Separate user functionality from system management functionality. **DISCUSSION** System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.	Appgate's approach to role separation is comprehensive, addressing both user and administrative access. Appgate allows for the creation of multiple admin roles with specific privileges, enabling a strict separation of duties among administrators. For example, different administrative roles can be configured to manage specific areas, such as policy management, user management, or audit logs, with privileges tailored to those responsibilities. Similarly, user access is tightly controlled through policies that define what resources and systems a user can access, based on their role and device posture. By implementing this dual-layer control—segregating user access from administrative functions—Appgate mitigates the risk of privilege escalation and unauthorized access. The combination of these controls ensures that system management functionalities are not accessible to standard users and that administrative actions are strictly regulated, supporting compliance with this control.	For more information on how Appgate enforces role separation for both user and administrative access, refer to the following sections in the Appgate Admin Guide: - **Admin Roles:** See 'Admin Roles' for configuring administrative privileges and enforcing role-based access controls. - **User Access Management:** Review 'User Access Management' for configuring user-specific access controls and policies. - **Using Policies:** Refer to 'Using Policies' for details on assigning and managing admin roles and user access via policies.
SC.3.182	**Shared Resource Control** Prevent unauthorized and unintended information transfer via shared system resources. • NIST SP 800-171 Rev 2 3.13.4	Prevent unauthorized and unintended information transfer via shared system resources. **DISCUSSION** Shared resources within a system may unintentionally allow information transfer between users, such as through shared memory or storage. Security controls are necessary to prevent such unintended information flows, ensuring that data is accessed only by authorized users.	While Appgate does not directly prevent unauthorized information transfer via shared system resources, it excels in enforcing policies that restrict access to these resources based on metadata tags, user roles, and device health. This data-centric approach allows Appgate to use metadata tags for policy alignment, replacing traditional static ACLs with dynamic controls that better reflect the security posture of the environment. By microsegmenting users and employing multi-tunneling technology, Appgate ensures that unauthorized information transfer is minimized, supporting compliance with this control.	For more information on how Appgate controls shared resource access, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for enforcing access controls to shared resources. - **Microsegmentation:** Review 'Microsegmentation' for ensuring secure communication within the network. - **Security Specifications:** Refer to 'Security Specifications' for details on how Appgate's policies prevent unauthorized information transfer.
SC.3.183	**Network Communication by Exception** Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). • NIST SP 800-171 Rev 2 3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). **DISCUSSION** Organizations control inbound and outbound network traffic to prevent unauthorized access or communication. By default, all traffic is denied unless explicitly allowed, minimizing the attack surface and reducing the risk of unauthorized network access.	Appgate enforces network communication by exception through its Zero Trust Network Access (ZTNA) architecture, where all network traffic is denied by default unless explicitly permitted by policy. Appgate allows organizations to create finely tuned access policies based on user roles, device posture, and contextual information, ensuring that only authorized traffic is allowed. This capability is enhanced by Appgate's use of Single Packet Authorization (SPA), which cloaks network resources, making them undiscoverable to unauthorized users. This approach significantly reduces the attack surface by ensuring that only legitimate, authenticated, and authorized requests can traverse the network.	For more information on how Appgate enforces network communication by exception, refer to the following sections in the Appgate Admin Guide: - **Access Policies:** See 'Access Policies' for configuring traffic control based on exception rules. - **Single Packet Authorization (SPA):** Review the 'SPA' section to understand how Appgate cloaks network resources to reduce the attack surface. - **System Operation:** Refer to 'System Operation' for details on managing inbound and outbound traffic controls.

DOMAIN: *SYSTEM AND COMMUNICATIONS PROTECTION (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SC.3.184	**Split Tunneling** Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). • NIST SP 800-171 Rev 2 3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). **DISCUSSION** Split tunneling creates a security risk by allowing remote devices to communicate with both internal organizational systems and external networks simultaneously. This can lead to unauthorized data exfiltration or exposure to external threats. Organizations prevent split tunneling to ensure secure remote access.	Appgate effectively mitigates the risks associated with split tunneling by enforcing strict access controls that prevent remote devices from establishing unauthorized connections. Appgate's multi-tunneling technology ensures that all traffic from remote devices is securely routed through the appropriate network segments, preventing simultaneous connections to external and internal networks. This capability, combined with continuous device posture assessments, ensures that only compliant and secure devices can maintain network connectivity, thereby protecting against data exfiltration and exposure to external threats.	For more information on how Appgate mitigates split tunneling risks, refer to the following sections in the Appgate Admin Guide: - **Multi-Tunneling:** See 'Multi-Tunneling' for details on how Appgate manages network traffic for remote devices. - **Device Posture:** Review 'Device Posture' for continuous monitoring and enforcement of device compliance. - **Security Specifications:** Refer to 'Security Specifications' for ensuring secure network access and routing.
SC.3.185	**Data in Transit** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. • NIST SP 800-171 Rev 2 3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. **DISCUSSION** Cryptography is used to protect CUI during transmission across networks, ensuring that sensitive information is not exposed to unauthorized parties. This control is particularly important when transmitting data over public or untrusted networks.	Appgate provides robust protection for data in transit by implementing mutual TLS (mTLS) 1.3, ensuring that both the client and server authenticate each other before any data is transmitted. This bidirectional authentication, combined with FIPS-validated cryptographic algorithms, ensures that all communications are securely encrypted, preventing unauthorized disclosure of CUI during transmission. Additionally, Appgate's Single Packet Authorization (SPA) technology further enhances security by requiring a cryptographically secure single packet to authenticate and authorize access to the network. This mechanism ensures that only legitimate, authenticated traffic is allowed, significantly reducing the risk of data interception or unauthorized access.	For more information on how Appgate protects data in transit, refer to the following sections in the Appgate Admin Guide: - **Encryption Policies:** See 'Encryption Policies' for configuring mTLS 1.3 and other cryptographic mechanisms for data protection. - **Federal Information Processing Standards (FIPS)-Validated Cryptography:** Review 'FIPS Validation' for details on Appgate's compliance with cryptographic standards. - **Single Packet Authorization (SPA):** Refer to 'SPA' for understanding how Appgate secures network access and protects data in transit.
SC.3.186	**Connections Termination** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. • NIST SP 800-171 Rev 2 3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. **DISCUSSION** Terminating network connections after a session ends or after a period of inactivity reduces the risk of unauthorized access. This control ensures that sessions are not left open, which could be exploited by unauthorized users.	Appgate enforces connection termination policies by ensuring that network sessions are automatically terminated after a defined period of inactivity or when the session ends. This is crucial for preventing unauthorized access that might occur if sessions remain open after use. Appgate's policies can be configured to align with specific inactivity timeouts, ensuring that only authorized and active sessions are maintained. Continuous monitoring and dynamic session management enable the system to immediately terminate sessions if unauthorized activity is detected, protecting the integrity of the network and minimizing potential security risks.	For more information on how Appgate manages connection termination, refer to the following sections in the Appgate Admin Guide: - **Session Management:** See 'Session Management' for configuring inactivity timeouts and session termination policies. - **Access Policies:** Review 'Access Policies' for integrating session management with access controls. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for setting up real-time notifications and automated session termination.
SC.3.187	**Key Management** Establish and manage cryptographic keys for cryptography employed in organizational systems. • NIST SP 800-171 Rev 2 3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems. **DISCUSSION** Cryptographic keys are critical to the security of cryptographic operations. Organizations must ensure that keys are generated, stored, and managed securely to prevent unauthorized access or use.	Appgate supports key management through its integration with cryptographic services that manage key generation, distribution, and storage. Appgate enables the use of both internally generated CA certificates and externally generated root certificates. The initial Controller in a Collective creates a CA certificate with a 10-year lifetime, and organizations can generate or upload the next CA certificate as needed. This ensures that all cryptographic operations within Appgate are securely executed, with the option to integrate external certificates for enhanced security. By aligning with established key management practices, Appgate helps minimize the risk of key compromise and ensures that encryption keys used in its operations are securely handled.	For more information on how Appgate integrates with key management systems, refer to the following sections in the Appgate Admin Guide: - **Cryptographic Integration:** See 'Cryptographic Integration' for details on how Appgate works with key management services and manages CA certificates. - **Certificate Management:** Review 'Internal Certificates' and 'Add Certificate' for configuring and managing CA certificates. - **Federal Information Processing Standards (FIPS) Validation:** Refer to 'FIPS Validation' for ensuring compliance with cryptographic standards.

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SC.3.177	**CUI Encryption** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. • NIST SP 800-171 Rev 2 3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. **DISCUSSION** FIPS-validated cryptographic algorithms provide assurance that CUI is protected using standards-compliant encryption. Organizations use FIPS-validated cryptography to ensure the confidentiality of CUI during storage and transmission.	Appgate provides robust encryption for CUI by employing FIPS-validated cryptographic algorithms across its network. This includes mutual TLS 1.3 for data in transit and other encryption standards for data at rest. Appgate's encryption policies are fully configurable, allowing organizations to enforce the highest levels of cryptographic protection for sensitive data. The system also supports the use of external root CA certificates, offering flexibility in managing encryption credentials. This approach ensures that CUI remains confidential during both transmission and storage, aligning with the stringent requirements of this control.	For more information on how Appgate enforces encryption for CUI, refer to the following sections in the Appgate Admin Guide: - **Federal Information Processing Standards (FIPS)-Validated Cryptography:** See 'FIPS Validation' for details on Appgate's compliance with cryptographic standards. - **Encryption Policies:** Review 'Encryption Policies' for configuring encryption for data in transit and at rest. - **Security Specifications:** Refer to 'Security Specifications' for a comprehensive overview of how Appgate secures CUI through encryption.
SC.2.178	**Collaborative Device Control** Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. • NIST SP 800-171 Rev 2 3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. **DISCUSSION** Collaborative computing devices, such as microphones or cameras, should not be remotely activated without the knowledge of users. This control prevents unauthorized remote activation, ensuring that users are aware of any active devices in their vicinity.	Appgate enhances collaborative device control by integrating with device posture checks and access policies to ensure that collaborative computing devices, such as microphones and cameras, are not remotely activated without explicit authorization. Appgate's security framework ensures that any attempt to activate such devices remotely is detected and blocked unless the action is compliant with predefined policies. Additionally, Appgate provides visibility into device status, ensuring that users are aware of any active devices in their vicinity, thus preventing unauthorized remote activation.	For more information on how Appgate enhances collaborative device control, refer to the following sections in the Appgate Admin Guide: - **Device Posture:** See 'Device Posture' for configuring checks that prevent unauthorized remote activation of devices. - **Access Policies:** Review 'Access Policies' for enforcing collaborative device control through policy management. - **Monitoring and Alerts:** Refer to 'Monitoring and Alerts' for real-time notifications related to collaborative device use.
SC.3.188	**Mobile Code** Control and monitor the use of mobile code. • NIST SP 800-171 Rev 2 3.13.13	Control and monitor the use of mobile code. **DISCUSSION** Mobile code refers to software programs that can be transmitted across networks and executed on a remote system. Organizations must control and monitor the use of mobile code to prevent the introduction of malicious code or unauthorized actions within the system.	Appgate does not directly control mobile code but plays a critical role in monitoring and enforcing policies related to its use. By integrating with endpoint security solutions, Appgate ensures that only authorized and verified mobile code can be executed within the network. This is achieved through strict access controls, continuous monitoring, and real-time policy enforcement, which together minimize the risk of introducing malicious code or unauthorized actions within the system.	For more information on how Appgate monitors and controls mobile code, refer to the following sections in the Appgate Admin Guide: - **Endpoint Integration:** See 'Endpoint Integration' for configuring policies that control the execution of mobile code. - **Access Policies:** Review 'Access Policies' for managing access to resources based on mobile code execution. - **Security Specifications:** Refer to 'Security Specifications' for details on monitoring and controlling code execution within the network.
SC.3.189	**Voice over Internet Protocol** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. • NIST SP 800-171 Rev 2 3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. **DISCUSSION** VoIP technologies transmit voice communications over IP networks, which may introduce security risks. Organizations must implement controls to monitor and secure VoIP communications, ensuring that they are not intercepted or compromised.	Appgate secures VoIP communications by enforcing strict access controls and using cryptographic protocols to protect voice data transmitted over IP networks. Appgate's policy-based access management ensures that only authorized users can initiate and participate in VoIP sessions. Furthermore, Appgate supports the use of FIPS-validated cryptographic algorithms to encrypt VoIP traffic, preventing interception and ensuring the confidentiality and integrity of voice communications.	For more information on how Appgate secures VoIP communications, refer to the following sections in the Appgate Admin Guide: - **Voice Over Internet Protocol (VoIP) Security:** See 'VoIP Security' for configuring secure VoIP communication protocols. - **Encryption Policies:** Review 'Encryption Policies' for applying cryptographic protection to VoIP traffic. - **Access Policies:** Refer to 'Access Policies' for managing and controlling VoIP access within the network.

DOMAIN: *SYSTEM AND COMMUNICATIONS PROTECTION (CONT)*

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SC.3.190	**Communications Authenticity** Protect the authenticity of communications sessions. • NIST SP 800-171 Rev 2 3.13.15	Protect the authenticity of communications sessions. **DISCUSSION** Ensuring the authenticity of communications sessions helps protect against impersonation attacks. Organizations must implement mechanisms to verify the identity of parties involved in a communication session, ensuring that sessions are not compromised.	Appgate protects the authenticity of communication sessions by implementing mutual TLS (mTLS) 1.3, which ensures that both parties in a communication session are authenticated before any data exchange occurs. This mutual authentication prevents impersonation attacks and ensures that only legitimate parties can participate in a session. Additionally, Appgate's use of Single Packet Authorization (SPA) adds an extra layer of security by verifying the authenticity of connection requests before granting access to the network, thereby safeguarding the integrity of communication sessions.	For more information on how Appgate protects the authenticity of communication sessions, refer to the following sections in the Appgate Admin Guide: - **Mutual TLS (mTLS):** See 'mTLS' for configuring mutual TLS 1.3 for communication sessions. - **Single Packet Authorization (SPA):** Review 'SPA' for understanding how Appgate secures the authenticity of connection requests. - **Security Specifications:** Refer to 'Security Specifications' for a comprehensive overview of how Appgate ensures the authenticity of communications.
SC.3.191	**Data at Rest** Protect the confidentiality of CUI at rest. • NIST SP 800-171 Rev 2 3.13.16	Protect the confidentiality of CUI at rest. **DISCUSSION** CUI stored on organizational systems must be protected from unauthorized access. This control requires organizations to implement security measures to ensure that CUI remains confidential, even when it is stored on devices or media.	Appgate protects the confidentiality of CUI at rest by enforcing FIPS-validated cryptographic mechanisms. Data at rest within the Appgate environment is encrypted using strong cryptographic algorithms, ensuring that CUI is protected from unauthorized access even if the physical media is compromised. Appgate's encryption policies are fully configurable, allowing organizations to enforce specific encryption standards that align with their security requirements. This approach ensures that sensitive data remains confidential, adhering to the stringent requirements of this control.	For more information on how Appgate protects CUI at rest, refer to the following sections in the Appgate Admin Guide: - **Federal Information Processing Standards (FIPS)-Validated Cryptography:** See 'FIPS Validation' for details on Appgate's compliance with cryptographic standards for data at rest. - **Encryption Policies:** Review 'Encryption Policies' for configuring encryption standards for data at rest. - **Security Specifications:** Refer to 'Security Specifications' for a comprehensive overview of how Appgate secures CUI stored on devices and media.

DOMAIN: SYSTEM AND INFORMATION INTEGRITY

CMMC Control Number	CMMC Control Description	NIST SP 800-171 Rev 2	Appgate SDP Control Mapping	Appgate SDP Admin Guide Reference
SI.2.214	**Security Alerts & Advisories** Monitor system security alerts and advisories and take action in response. • NIST SP 800-171 Rev 2 3.14.3	Monitor system security alerts and advisories and take action in response. **DISCUSSION** Security alerts and advisories can come from a variety of sources, including external organizations (e.g., US-CERT), internal monitoring systems, and other external sources. Organizations need to monitor these alerts and advisories to identify potential threats and take appropriate action.	Appgate enhances security monitoring by integrating with system security alerts and advisories. Appgate's platform can be configured to respond to various security alerts from internal and external sources. By incorporating these alerts into its access policies and monitoring framework, Appgate ensures that appropriate actions are taken automatically in response to identified threats. This proactive approach helps organizations stay ahead of potential threats and maintain a secure operational environment.	For more information on how Appgate handles security alerts and advisories, refer to the following sections in the Appgate Admin Guide: - **Monitoring and Alerts:** See 'Monitoring and Alerts' for configuring responses to security alerts. - **Access Policies:** Review 'Access Policies' for integrating security advisories into policy enforcement. - **Security Specifications:** Refer to 'Security Specifications' for a comprehensive overview of Appgate's monitoring capabilities.
SI.2.216	**Monitor Communications for Attacks** Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. • NIST SP 800-171 Rev 2 3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. **DISCUSSION** Monitoring inbound and outbound communications traffic for signs of attacks is crucial to detecting and responding to potential security threats. This monitoring helps identify malicious activity early and provides the information necessary to take defensive action.	Appgate provides comprehensive monitoring of communications traffic to detect attacks and potential indicators of compromise. Through its Zero Trust architecture, Appgate continuously monitors all network traffic, both inbound and outbound, using advanced threat detection techniques. This monitoring is combined with strict access controls to ensure that only legitimate traffic is allowed, and any suspicious activity is flagged for further investigation. By integrating with SIEM systems, Appgate enhances the detection and response capabilities of the organization, helping to prevent and mitigate attacks.	For more information on how Appgate monitors communications for attacks, refer to the following sections in the Appgate Admin Guide: - **Threat Detection:** See 'Threat Detection' for configuring monitoring of inbound and outbound traffic. - **Access Policies:** Review 'Access Policies' for managing and controlling communications traffic. - **Security Information and Event Management (SIEM) Integration:** Refer to 'SIEM Integration' for enhancing threat detection and response capabilities.
SI.2.217	**Identify Unauthorized Use** Identify unauthorized use of organizational systems. • NIST SP 800-171 Rev 2 3.14.7	Identify unauthorized use of organizational systems. **DISCUSSION** Detecting unauthorized use of organizational systems is critical to maintaining security. Unauthorized use can indicate potential security breaches or misuse of resources, and it is important to identify and address these issues promptly.	Appgate plays a critical role in identifying unauthorized use of organizational systems by enforcing strict access controls and continuously monitoring user activity. Appgate's Zero Trust approach ensures that only authorized users can access network resources, and any deviations from expected behavior are immediately flagged. Additionally, Appgate's logging and monitoring capabilities provide detailed insights into user activity, allowing organizations to quickly identify and respond to unauthorized access attempts, thereby maintaining the integrity of their systems.	For more information on how Appgate identifies unauthorized use, refer to the following sections in the Appgate Admin Guide: - **User Activity Monitoring:** See 'User Activity Monitoring' for tracking and identifying unauthorized access attempts. - **Access Policies:** Review 'Access Policies' for enforcing strict controls on system access. - **Security Specifications:** Refer to 'Security Specifications' for a detailed overview of Appgate's monitoring and logging capabilities.

Appgate SDP Fully Authorized to Operate with the DoD

Appgate SDP has been fully vetted and is operational across numerous DoD branches. This includes the Space Force, Marine Corps, Navy, Air Force, Platform One, and Cloud Native Access Point (CNAP), along with key entities such as U.S. Cyber Command, the Joint Warfighting Capabilities Assessment (JWCA), and the Unified Platform. This widespread adoption underscores Appgate SDP's robust security and effectiveness in meeting the stringent requirements of diverse DoD environments.

Authorized to Operate at IL6

Appgate SDP is authorized to operate at DoD Impact Level 6 (IL6), the highest classification for safeguarding sensitive information, from classified up to secret.

NIAP Common Criteria EAL

Appgate SDP is the only ZTNA solution to achieve NIAP Common Criteria certification with Evaluation Assurance Level 4 augmentation, meeting the most stringent internationally recognized security requirements for government agencies.

CtF for Platform One

Appgate SDP has been granted a Certificate to Field (CtF) for Platform One, signifying its accreditation to operate as a mission-critical application within specific DoD environments.

U.S. Military Command Pen Tested

Appgate SDP has undergone rigorous penetration testing by U.S. Cyber Command, Army Cyber and Air Force Cyber, earning a high-mission impact and low-risk rating.

FIPS 140-2

Appgate SDP is compliant with the Federal Information Processing Standard (FIPS) 140-2, meeting NIST requirements for cryptographic modules, ensuring the robust security of sensitive data.

NCCoE Contributor

Appgate is a select contributor to the NCCoE at NIST, collaborating on the Center's "Implementing a Zero Trust Architecture" project and how-to guides.

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.

appgate