APPGATE SDP: MAPPING TO DOD ZTA TARGET CONTROLS

This table details how Appgate SDP ZTNA features correspond to specific target controls defined by the by the U.S. Department of Defense (DoD) Zero Trust Architecture (ZTA) framework. This mapping demonstrates Appgate SDP's adherence to mandated federal industry standards and provides a clear overview of how the solution addresses key security requirements outlined by the DoD.

DoD ZTA Mapping to TARGET Controls Appgate v.10.0

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE
1.1.1	Inventory User	1.1 User Inventory	Target Level ZT	Identified Managed Regular Users; Identified Managed Privileged Users; Identified applications using their own user account management for non-administrative and administrative accounts	User	X
1.2.1	Implement App Based Permissions per Enterprise	1.2 Conditional User Access	Target Level ZT	Enterprise roles/attributes needed for user authorization to application functions and/or data have been registered with enterprise ICAM; DoD Enterprise ICAM has self-service attribute/role registration service that enables application owners to add attributes or use existing enterprise attributes; Privileged activities are fully migrated to PAM	User	X
1.2.2	Enterprise Roles and Permissions Pt. 2	Rule Based Dynamic Access Pt1	Target Level ZT	Access to application's/service's functions and/or data are limited to users with appropriate enterprise attributes; All possible applications use JIT/JEA permissions for administrative users	User	X
1.3.1	Organizational MFA/IDP	1.3 Multi-Factor Authentication (MFA)	Target Level ZT	Component is using IdP with MFA for critical applications/services; Components have implemented an Identity Provider (IdP) that enables DoD PKI multifactor authentication; Organizational Standardized PKI for critical services	User	X
1.4.1	Implement System and Migrate Privileged Users Pt1	1.4 Privileged Access Management (PAM)	Target Level ZT	Privilege Access Management (PAM) tooling is implemented; applications and devices that support and do not support PAM tools identified; Applications that support PAM, now use PAM for controlling emergency/built-in accounts	User	X
1.4.2	Implement System and Migrate Privileged Users Pt2	1.4 Privileged Access Management (PAM)	Target Level ZT	Privileged activities are migrated to PAM and access is fully managed	User	X
1.5.1	Organizational Identity Life-Cycle Management	1.5 Identity Federation & User Credentialing	Target Level ZT	Standardized Identity Lifecycle Process	User	X
1.5.2	Enterprise Identity Life-Cycle Management Pt1	1.5 Identity Federation & User Credentialing	Target Level ZT	Automated Identity Lifecycle Processes; Integrated with Enterprise ICAM process and tools	User	X
1.6.1	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling	1.6 Behavioral, Contextual ID, and Biometrics	Target Level ZT	UEBA and UAM functionality is implemented for Enterprise IDP	User	X
1.7.1	Deny User by Default Policy	1.7 Least Privileged Access	Target Level ZT	Applications updated to deny by default to functions/data requiring specific roles/attributes for access; Reduced default permissions levels are implemented; Applications/services have reviewed/audited all privileged users and removed those users who do not need that level of access; Applications' identify functions and data requiring specific roles/attributes for access	User	X
1.8.1	Single Authentication	1.8 Continuous Authentication	Advanced Level ZT	Authentication implemented across applications per session	User	X
1.8.2	Periodic Authentication	1.8 Continuous Authentication	Advanced Level ZT	Authentication implemented multiple times per session based on security attributes	User	X
1.9.1	Enterprise PKI/IDP Pt1	1.9 Integrated ICAM Platform	Advanced Level ZT	Components are using IdP with MFA for all applications/services; Organizational MFA/PKI integrated with Enterprise MFA/PKI; Organizational Standardized PKI for all services	User	X
2.1.1	Device Health Tool Gap Analysis	2.1 Device Inventory	Advanced Level ZT	Manual inventory of devices is created per organization w/ owners	Device + Network/ Environment	X
2.1.2	NPE/PKI, Device under Management	2.1 Device Inventory	Advanced Level ZT	Non-person entities are managed via Org PKI and Org IDP	Device + Network/ Environment	X
2.1.3	Enterprise IDP Pt1	2.1 Device Inventory	Advanced Level ZT	NPEs including devices are integrated with Enterprise IDP	Device	
2.2.1	Implement C2C/Compliance Based Network Authorization Pt1	2.2 Device Detection and Compliance	Advanced Level ZT	NPEs including devices are integrated with Enterprise IDP	Device	X

DoD ZTA Mapping to TARGET Controls Appgate v.10.0

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL
2.3.3	Implement Application Control & File Integrity Monitoring (FIM) Tools	2.3 Device Authorization w/ Real Time Inspection	Target Level ZT	AppControl and FIM tooling is implemented on all critical services/applications; EDR tooling covers maximum amount of services/applications; AppControl and FIM data is sent to C2C as needed	Device	X
2.3.4	Integrate NextGen AV Tools with C2C	2.3 Device Authorization w/ Real Time Inspection	Target Level ZT	Critical NextGen AV data is being sent to C2C for checks ; NextGen AV tooling is implemented on all critical services/applications	Device	X
2.4.1	Deny Device by Default Policy	2.4 Remote Access	Target Level ZT	Components can block device access by default to resources (apps/data) and explicitly allow compliant devices per policy; Remote Access is enabled following a "deny device by default policy" approach	Device	X
2.4.2	Managed and Limited BYOD & IOT Support	2.4 Remote Access	Target Level ZT	All applications require dynamic permissions access for devices; BYOD and IOT device permissions are baselined and integrated with Enterprise IDP	Device	X
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	Target Level ZT	Components can confirm if devices meet minimum compliance standards or not; Components have asset management, vulnerability, and patching systems with APIs that will enable integration across the systems	Device	X
2.6.1	Implement UEDM or equivalent Tools	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	Components can confirm if devices meet minimum compliance standards or not; Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoD enterprise; Components asset management systems can programmatically, i.e., API, provide device compliance status and if it meets minimum standards	Device	X
2.6.2	Enterprise Device Management Pt1	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	Manual inventory is integrated with an automated management solution for critical services; Enable ZT Device Management (from any location with or without remote access)	Device	X
2.6.3	Enterprise Device Management Pt2	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	Manual inventory is integrated with an automated management solution for all services	Device	X
2.7.1	Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Advanced Level ZT	Endpoint Detection & Response Tooling is implemented ; Critical EDR data is being sent to C2C for checks; NextGen AV tooling covers maximum amount of services/applications	Device	X
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Advanced Level ZT	Integration Points have been identified per Capability; Riskiest integration points have been integrated w/ XDR; Basic alerting is in place with SIEM and/or other mechanisms	Device	X
3.1.1	Application/Code Identification	3.1 Application Inventory	Advanced Level ZT	Component has identified applications and classified as either legacy, virtualized on-premises, and cloud hosted	Applications and Workloads	X
3.1.2	Resource Authorization Pt1	3.4 Resource Authorization & Integration	Advanced Level ZT	Resource Authorization Gateway is in place for external facing applications; Resource Authorization policy integrated with identity and device; Enterprise-wide Guidance on conversion standards are communicated to stakeholders	Applications and Workloads	X
3.1.3	Resource Authorization Pt2	3.4 Resource Authorization & Integration	Advanced Level ZT	Resource Authorization gateway is utilized for all applications; Resource Authorization is integrated with DevSecOps and CI/CD for automated functions	Applications and Workloads	X
3.2.1	Build DevSecOps Software Factory Pt1	3.2 Secure Software Development & Integration	Advanced Level ZT	Developed Data/Service Standards for DevSecOps; CI/CD Pipeline is fully functional and tested successfully; Vulnerability Management program is officially in place and operating	Applications and Wrokloads + Automation & Orchestration	X
3.2.2	Build DevSecOps Software Factory Pt2	3.2 Secure Software Development & Integration	Advanced Level ZT	Development of applications is migrated to CI/CD pipeline; Continual validation process/technology is implemented and in use; Development of applications is migrated to DevSecOps process and technology	Applications and Wrokloads + Automation & Orchestration	X
3.2.3	Automate Application Security & Code Remediation Pt1	3.2 Secure Software Development & Integration	Advanced Level ZT	Secure API Gateway is operational and majority of API calls are passing through gateway; Application Security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps	Applications and Workloads & Network / Environment	X

DoD ZTA Mapping to TARGET Controls Appgate v.10.0

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL
3.3.1	Approved Binaries/Code	3.3 Software Risk Management	Target Level ZT	Supplier sourcing risk evaluated and identified for approved sources; Repository and update channel established for use by development teams; Bill of Materials is created for applications identify source, supportability and risk posture; Industry standard (DIB) and approved vulnerability databases are pulled in to be used in DevSecOps	Applications and Workloads	
3.3.2	Vulnerability Management Program Pt1	3.3 Software Risk Management	Target Level ZT	Vulnerability Management Team is in place w/ appropriate stakeholder membership; Vulnerability Management policy and process is in place and agreed to w/ stakeholders; Public source of vulnerabilities are being utilized for tracking	Applications and Workloads	X
3.3.3	Vulnerability Management Program Pt2	3.3 Software Risk Management	Target Level ZT	Controlled (e.g., DIB, CERT) sources of vulnerabilities are being utilized for tracking; Vulnerability management program has a process for accepting external/public disclosures for managed services	Applications and Workloads	X
3.3.4	Continual Validation	3.3 Software Risk Management	Target Level ZT	Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned; Continual validation tools are implemented and applied to code in the CI/CD pipeline; Code requiring continuous validation is identified and validation criteria are established	Applications and Wrokloads + Automation & Orchestration	X
3.4.1	SDC Resource Authorization Pt1	3.4 Resource Authorization & Integration	Target Level ZT	Applications unable to be updated to use approved binaries/code are marked for retirement and transition plans are created; Identified applications without approved binaries and code are updated to use approved binaries/code; Enterprise-wide Guidance on conversion standards are communicated to stakeholders	Applications and Workloads	X
3.4.2	SDC Resource Authorization Pt2	3.4 Resource Authorization & Integration	Target Level ZT	Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned	Applications and Workloads	X
4.1.1	Data Analysis	4.1 Data Catalog Risk Alignment	Target Level ZT	The service catalog is updated with data types for each application and service based on data classification levels	Data / Applications and Workloads	X
4.2.1	Define Data Tagging Standards	4.2 DoD Enterprise Data Governance	Target Level ZT	Enterprise data classification and tagging standards are developed; Organizations align to enterprise standards and begin implementation	Data / Applications and Workloads	X
4.2.2	Interoperability Standards	4.2 DoD Enterprise Data Governance	Target Level ZT	Formal standards are in place by the Enterprise for the appropriate data standards	Data / Applications and Workloads	X
4.2.3	Network Asset Discovery & Optimization	DoD Organizations automate network asset discovery through the SDN infrastructure limiting access to devices based on risk based methodical approaches. Optimization is conducted based on the SDN analytics to improve overall performance along with provide necessary approved access to resources.	Target Level ZT	Technical Refreshment/Technology Evolution; Provide Optimization/Performance Controls	Data	X
4.3.1	Implement Data Tagging & Classification Tools	4.3 Data Labeling and Tagging	Target Level ZT	A requirement of Data classification and tagging tools must include integration and/or support of Machine Learning (ML); Data classification and tagging tools are implemented at org and enterprise levels	Data / Applications and Workloads	X
4.3.2	Manual Data Tagging Pt1	4.3 Data Labeling and Tagging	Advanced Level ZT	Manual data tagging begins at the enterprise level with basic attributes	Data / Applications and Workloads	X
4.4.1	DLP Enforcement Point Logging and Analysis	4.4 Data Monitoring and Sensing	Advanced Level ZT	Enforcement points are identified; Standardized Logging schema is enforced at the enterprise and org levels	Data / Applications and Workloads	
4.4.2	DRM Enforcement Point Logging and Analysis	4.4 Data Monitoring and Sensing	Advanced Level ZT	Enforcement points are identified; Standardized Logging schema is enforced at the enterprise and org levels	Data / Applications and Workloads	

DoD ZTA Mapping to TARGET Controls Appgate v.10.0

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL
4.4.3	File Activity Monitoring Pt1	4.4 Data Monitoring and Sensing	Target Level ZT	Data and files of critical classification are actively being monitored; Basic Integration is in place with monitoring system such as the SIEM	Data	
4.4.4	File Activity Monitoring Pt2	4.4 Data Monitoring and Sensing	Target Level ZT	Data and files of all regulated classifications are actively being monitored; Extended integrations are in place as appropriate to further manage risk	Data	
4.5.1	Implement DRM and Protection Tools Pt1	4.5 Data Encryption & Rights Management	Target Level ZT	DRM and protection tools are enabled for high risk data repositories with basic protections	Data	
4.5.2	Implement DRM and Protection Tools Pt2	4.5 Data Encryption & Rights Management	Target Level ZT	DRM and protection tools are enabled for possible repositories	Data	
4.5.3	DRM Enforcement via Data Tags and Analytics Pt1	4.5 Data Encryption & Rights Management	Target Level ZT	Data Tags are integrated with DRM and monitored repositories are expanded; Based on data tags, data is encrypted at rest	Data	
4.6.1	Implement Enforcement Points	4.6 Data Loss Prevention (DLP)	Target Level ZT	Identified enforcement points have DLP tool deployed and set to monitor mode with standardized logging	Data	
4.6.2	DLP Enforcement via Data Tags and Analytics Pt1	4.6 Data Loss Prevention (DLP)	Target Level ZT	Enforcement Points to set to prevent mode integrating the logging schema and manual tags	Data	
4.7.1	Integrate DAAS Access w/ SDS Policy Pt1	4.7 Data Access Control	Target Level ZT	DAAS policy is developed w/ enterprise and org level support; SDS Integration plan is developed to support DAAS policy	Data & Network / Environment	X
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	4.7 Data Access Control	Target Level ZT	Integration plan with SDS is developed to support existing DAAS access	Data & Network / Environment	X
5.1.1	Define Granular Control Access Rules & Policies Pt1	5.1 Data Flow Mapping	Target Level ZT	Provide Technical Standards; Develop Concept of Operations; Identify Communities of Interest	Network / Environment + Applications and Workloads	X
5.1.2	Define Granular Control Access Rules & Policies Pt2	5.1 Data Flow Mapping	Advanced Level ZT	Define Data Tagging Filters for API Infrastructure	Network / Environment + Applications and Workloads	X
5.2.1	Define SDN APIs	5.2 Software Defined Networking (SDN)	Target Level ZT	SDN APIs are standardized and implemented; APIs are functional for AuthN Decision Point, App Delivery Control Proxy and Segmentation Gateways	Network/Environment	
5.2.2	Implement SDN Programable Infrastructure	5.2 Software Defined Networking (SDN)	Target Level ZT	Implemented Application Delivery Control Proxy; Established SIEM Logging Activities; Implemented User Activity Monitoring (UAM); Integrated with Authentication Decision Point; Implemented Segmentation Gateways	Network/Environment	
5.2.3	Segment Flows into Control, Management, and Data Planes	5.2 Software Defined Networking (SDN)	Target Level ZT	IPv6 Segmentation; Enable Automated NetOps Information Reporting; Ensure Configuration Control Across Enterprise; Integrated with SOAR	Network/Environment	
5.3.1	Datacenter Macro segmentation	5.3 Macro Segmentation	Target Level ZT	Log Actions to SIEM; Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Analyze Activities with Analytics Engine	Network/Environment	X
5.3.2	B/C/P/S Macro segmentation	5.3 Macro Segmentation	Target Level ZT	Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Log Actions to SIEM; Analyze Activities with Analytics Engine; Leverage SOAR to Provide RT Policy Access Decisions	Network/Environment	X
5.4.1	Implement Micro segmentation	5.4 Micro Segmentation	Target Level ZT	Accept Automated Policy Changes; Implement API Decision Points; Implement NGF/Micro FW/Endpoint Agent in Virtual Hosting Environment	Network / Environment + Applications and Workloads	X
5.4.2	Application & Device Micro segmentation	5.4 Micro Segmentation	Target Level ZT	Assign Role, Attribute, & Condition Based Access Control to User & Devices; Provide Privileged Access Management Services; Limit Access on Per Identity Basis for User & Device; Create Logical Network Zones; Support Policy Control via REST API	Network / Environment + Applications and Workloads	X

DoD ZTA Mapping to TARGET Controls Appgate v.10.0

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL
5.4.4	Protect Data In Transit	5.4 Micro Segmentation	Target Level ZT	Protect Data In Transit During Coalition Information Sharing; Protect Data in Transit Across System High Boundaries; Integrate Data In Transit Protection Across Architecture Components	Network / Environment + Applications and Workloads	X
6.1.1	Policy Inventory & Development	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	Policies have been collected in reference to applicable compliance and risk (e.g. RMF, NIST); Policies have been reviewed for missing Pillars and Capabilities per the ZTRA; Missing areas of policies are updated to meet the capabilities per ZTRA	Automation & Orchestration + Applications and Workloads	X
6.1.2	Organization Access Profile	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	Organization scoped profile(s) are created to determine access to DAAS using capabilities from User, Data, Network, and Device pillars; Initial enterprise profile access standard is developed for access to DAAS ; When possible the organization profile(s) utilizes enterprise available services in the User, Data, Network and Device pillars; Organization Mission/Task critical profile(s) are created	Automation & Orchestration	X
6.1.3	Enterprise Security Profile Pt1	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	Enterprise Profile(s) are created to access DAAS using capabilities from User, Data, Network and Device Pillars; Non-mission/task critical organization profile(s) are integrated with the enterprise profile(s) using a standardized approach	Automation & Orchestration	X
6.2.1	Task Automation Analysis	6.2 Critical Process Automation	Target Level ZT	Automatable tasks are identified; Tasks are enumerated	Automation & Orchestration	X
6.2.2	Enterprise Integration & Workflow Provisioning Pt1	6.2 Critical Process Automation	Target Level ZT	Implement full enterprise integration; Identify key integrations; Identify recovery and protection requirements	Automation & Orchestration / Applications and Workloads	X
6.3.1	Implement Data Tagging & Classification ML Tools	6.3 Machine Learning	Target Level ZT	Implemented data tagging and classification tools are integrated with ML tools	Automation & Orchestration	
6.5.1	Response Automation Analysis	6.5 Security Orchestration, Automation & Response (SOAR)	Target Level ZT	Automatable response activities are identified; Response activities are enumerated	Automation & Orchestration / Applications and Workloads	X
6.5.2	Implement SOAR Tools	6.5 Security Orchestration, Automation & Response (SOAR)	Target Level ZT	Develop requirements for SOAR tool; Procure SOAR tools	Automation & Orchestration / Applications and Workloads	X
6.6.1	Tool Compliance Analysis	6.6 API Standardization	Target Level ZT	API status is determined compliance or non-compliance to API standards; Tools to be used are Identified	Automation & Orchestration / Applications and Workloads	X
6.6.2	Standardized API Calls & Schemas Pt1	6.6 API Standardization	Target Level ZT	Initial calls and schemas are implemented; Non-compliant tools are replaced	Automation & Orchestration / Applications and Workloads	X
6.6.3	Standardized API Calls & Schemas Pt2	6.6 API Standardization	Target Level ZT	All calls and schemas are implemented	Automation & Orchestration / Applications and Workloads	X
6.7.1	Workflow Enrichment Pt1	6.7 Security Operations Center (SOC) & Incident Response (IR)	Target Level ZT	Threat events are identified; Workflows for threat events are developed	Automation & Orchestration / Applications and Workloads	X
7.1.1	Scale Considerations	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	Sufficient infrastructure in place; Distributed environment established; Sufficient bandwidth for network traffic	Visibility & Analytics	X
7.1.2	Log Parsing	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	Standardized log formats; Rules developed for each log format	Visibility & Analytics	X
7.1.3	Log Analysis	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	Develop analytics per activity; Identify activities to analyze	Visibility & Analytics	X
7.2.1	Threat Alerting Pt1	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Rules developed for threat correlationtraffic	Visibility & Analytics	X
7.2.2	Threat Alerting Pt2	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Develop analytics to detect deviations	Visibility & Analytics	X

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL
7.2.4	Asset ID & Alert Correlation	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Rules developed for asset ID based responses	Visibility & Analytics	X
7.2.5	User/Device Baselines	7.2 Security Information and Event Management (SIEM)	Target Level ZT	Identify user and device baselines	Visibility & Analytics	X
7.3.1	Implement Analytics Tools	7.3 Common Security and Risk Analytics	Target Level ZT	Develop requirements for analytic environment; Procure and implement analytic tools	Visibility & Analytics	X
7.3.2	Establish User Baseline Behavior	7.3 Common Security and Risk Analytics	Target Level ZT	Identify users for baseline; Establish ML-based baselines	Visibility & Analytics / Automation & Orchestration / Applications and Workloads	X
7.4.1	Baseline & Profiling Pt1	7.4 User and Entity Behavior Analytics	Target Level ZT	Develop analytics to detect changing threat conditions; Identify user and device threat profiles	Visibility & Analytics / Automation & Orchestration / Applications and Workloads	X
7.5.1	Cyber Threat Intelligence Program Pt1	7.5 Threat Intelligence Integration	Target Level ZT	Cyber Threat Intelligence team is in place with critical stakeholders; Public and Baseline CTI feeds are being utilized by SIEM for alerting; Basic integration points exist with Device and Network enforcement points (e.g., NGAV, NGFW, NG-IPS)	Visibility & Analytics	
7.5.2	Cyber Threat Intelligence Program Pt2	7.5 Threat Intelligence Integration	Target Level ZT	Cyber Threat Intelligence team is in place with extended stakeholders as appropriate; Controlled and Private feed are being utilized by SIEM and other appropriate Analytics tools for alerting and monitoring; Integration is in place for extended enforcement points within the Device, User, Network and Data pillars (UEBA, UAM)	Visibility & Analytics	