APPGATE SDP: MAPPING TO DOD ZTA ADVANCED CONTROLS

This table details how Appgate SDP ZTNA features correspond to specific advanced 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 ADVANCED Controls Appgate v.10

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL	APPGATE PARTIAL
1.2.3	Rule Based Dynamic Access Pt. 2	DoD Organizations expand the development of rules for dynamic access decision making accounting for risk. Solutions used for dynamic access are integrated with cross pillar Machine Learning and Artificial Intelligence functionality enabling automated rule management.	Advanced Level ZT	Components and services are fully utilizing rules to enable dynamic access to applications and services; Technology utilized for Rule Based Dynamic Access supports integration with AI/ML tooling	User	X	
1.2.4	Enterprise Roles and Permissions Pt. 1	DoD Organizations federate remaining user and group attributes as appropriate to the Enterprise Identity, Credential and Access Management (ICAM) solution. The updated attribute set is used to create universal roles for Organizations to use. Core functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions are migrated to cloud services and/or environments enabling improved resilience and performance.	Advanced Level ZT	Component attribute and role data repository federatedwith enterprise ICAM; Cloud-based enterprise IdP can be used by cloud and on-premises applications; A standardized set of roles and permissions are created and aligned to attributes	User		X
1.2.5	Enterprise Roles and Permissions Pt. 2	DoD Organizations move all possible functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions to cloud environments. Enclave/DDIL environments local capabilities to support disconnected functions but ultimately are managed by the centralized Identity, Credential and Access Management (ICAM) solutions. Updated roles are now mandated for usage and exceptions are reviewed following a risk-based approach.	Advanced Level ZT	Majority of components utilize cloud IdP functionality Where possible on-prem IdP is decommissioned; Permissions and roles are mandated for usage when evaluating attributes	User		X
1.3.2	Alternative Flexible MFA Pt. 1	DoD Organization's Identity Provider (IdP) supports alternative methods of multi-factor authentication complying with Cyber Security requirements (e.g., FIPS 140-2, FIPS 197, etc.). Alternative tokens can be used for application-based authentication. Multi-Factor options support Biometric capability and can be managed using a self-service approach. Where possible multi-factor provider(s) is moved to cloud services instead of being hosted on-premise.	Advanced Level ZT	IdP provides user self-service alternative token; IdP provides alt token MFA for approved applications per policy	User	X	
1.3.3	Alternative Flexible MFA Pt. 2	Alternative tokens utilize user activity patterns from cross pillar activities such as "User Activity Monitoring (UAM) and User & Entity Behavior Analytics (UEBA)" to assist with access decision making (e.g., not grant access when pattern deviation occurs). This functionality is further extended onto Biometric enabled alternative tokens as well.	Advanced Level ZT	User Activity Patterns Implemented	User		X
1.4.3	Real Time Approvals & JIT/JEA Analytics Pt. 1	Identification of necessary attributes (Users, Groups, etc.) are automated and integrated into the Privileged Access Management (PAM) solution. Privilege access requests are migrated to the PAM solution for automated approvals and denials.	Advanced Level ZT	Identified accounts, applications, devices, and data of concern (of greatest risk to DoD mission); Using PAM tools, applied JIT/JEA access to high-risk accounts; Privileged access requests are automated as appropriate	User		X
1.4.4	Real Time Approvals & JIT/JEA Analytics Pt. 2	DoD Organizations integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with the Privileged Access Management (PAM) solution providing user pattern analytics for decision making.	Advanced Level ZT	UEBA or similar analytic system integrated with PAM tools for JIT/JEA account approvals'	User		X
1.5.3	Enterprise Identity Life-Cycle Management Pt. 2	DoD Organizations further integrate the critical automation functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions following the Enterprise Lifecycle Management process to enable Enterprise automation and analytics. Identity Lifecycle Management primary processes are integrated into the cloud-based Enterprise ICAM solution.	Advanced Level ZT	Integration w/ Critical IDM/IDP functions; Primary ILM functions are cloud based	User		X
1.5.4	Enterprise Identity Life-Cycle Management Pt. 3	DoD Organizations integrate remaining Identity Lifecycle Management processes with the Enterprise Identity, Credential and Access Management solution. Enclave/DDIL environments while still authorized to operate integrate with the Enterprise ICAM using local connectors to the cloud environment.	Advanced Level ZT	All ILM functions moved to cloud as appropriate; Integration with all IDM/IDP functions	User		X
1.6.2	User Activity Monitoring Pt. 1	DoD Organizations integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with Organizational Identity Providers (IdP) for extended visibility as needed. Analytics and data generated by UEBA and UAM for critical applications/services are integrated with the Just-in-Time and Just-Enough-Access solution improving decision making further.	Advanced Level ZT	UEBA is integrated with Org IDPs as appropriate; UEBA is integrated with JIT/JEA for critical services	User		X
1.6.3	User Activity Monitoring Pt. 2	DoD Organizations continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time and Just- Enough-Access solution.	Advanced Level ZT	UEBA/Entity Monitoring is integrated with JIT/JEA for all services	User		X
1.8.3	Continuous Authentication Pt. 1	DoD Organizations' applications/service utilize multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests required additional levels of authentication such as Multi-Factor Authentication (MFA) pushes to users.	Advanced Level ZT	Transaction authentication implemented per session based on security attributes	User		X

DoD ZTA Mapping to ADVANCED Controls Appgate v.10

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL	APPGATE PARTIAL
1.8.4	Continuous Authentication Pt. 2	DoD Organizations continue usage of transaction-based authentication to include integration such as user patterns.	Advanced Level ZT	Transaction authentication implemented per session based on security attributes	User	X	
1.9.2	Enterprise PKI/DP Pt. 2	DoD Organizations enable Biometric support in the Identity Provider (IdP) for mission/task-critical applications and services as appropriate. Biometric functionality is moved from Organizational solutions to the Enterprise. Organizational Multi-Factor (MFA) and Public Key Infrastructure (PKI) is decommissioned and migrated to the Enterprise as appropriate.	Advanced Level ZT	Critical Organizational Services Integrated w/ Biometrics; Decommission organizational MFA/PKI as appropriate in leu of enterprise MFA/PKI; Enterprise Biometric Functions Implemented	User		X
1.9.3	Enterprise PKI/DP Pt. 3	DoD Organizations integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor (MFA) tokens can be used.	Advanced Level ZT	All Organizational Services Integrate w/ Biometrics	User		X
2.1.4	Enterprise IDP Pt. 2	The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies adds additional dynamic attributes for NPEs such as location, usage patterns, etc.	Advanced Level ZT	Conditional device attributes are part of the IdP profile	Device	X	
2.2.2	Implement C2C/Compliance Based Network Authorization Pt. 2	DoD Organizations expand the deployment and usage of Comply to Connect to all supported environments required to meet ZT advanced functionalities. Comply to Connect teams integrate their solution(s) with the Enterprise IdP and Authorization Gateways to better manage access and authorizations to resources.	Advanced Level ZT	C2C is enforced in all supported environments; Advanced devices checks are completed and integrated with dynamic access (Enterprise IDP / ZTNA)	Device	X	
2.3.1	Entity Activity Monitoring Pt. 1	Using the developed User and Device baselines, DoD Organizations utilize the implemented User and Entity Behavioral Activity (UEBA) solution to integrate baselines. UEBA device attributes and baselines are available to be used for device authorization detections.	Advanced Level ZT	UEBA attributes are integrated for device baselining; UEBA attributes are available for usage with device access	Device		X
2.3.2	Entity Activity Monitoring Pt. 2	DoD Organizations utilize the User and Entity Behavioral Activity (UEBA) solution with network access solutions to mandate UEBA attributes (e.g., device health, logon patterns, etc.) for accessing environments and resources.	Advanced Level ZT	UEBA attributes are mandated for device access	Device		X
2.3.5	Fully Integrate Device Security Stack w/ C2C	DoD Organizations continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect for expanded access decision making data points. Comply to Connect analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	Advanced Level ZT	AppControl and FIM deployment is expanded to all necessary services/applications; Remaining data from Device Security tooling is implemented with C2C	Device		X
2.3.6	Enterprise PKI Pt. 1	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and device that do not support PKI certificates are marked for retirement and decommission starts.	Advanced Level ZT	Devices that are unable to have certificates are phased out and/or moved to minimal access environments; All devices and NPEs have certs installed for authentication in the Enterprise PKI	Device		X
2.3.7	Enterprise PKI Pt. 2	DoD Organizations utilize certificates for device authentication and machine to machine communications. Unsupported devices complete retirement and exceptions are approved using a risk based methodical approach.	Advanced Level ZT	Devices are required to authenticate to communicate with other services and devices	Device		X
2.4.3	Managed and Full BYOD & IoT Support Pt. 1	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for managed and approved devices to Mission and Operational Critical services/applications using dynamic access policies. BYOD and Internet of Things (IoT) devices are required to meet standard baseline checks before authorization.	Advanced Level ZT	Only BYOD and IOT devices that meet mandated configuration standards allowed to access resources; Critical Services require dynamic access for devices'	Device	X	
2.4.4	Managed and Full BYOD & IoT Support Pt. 2	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for unmanaged devices meeting device checks and standard baselines. All possible services/applications are integrated to allow access to managed devices. Unmanaged devices are integrated with services/applications based on risk driven methodical authorization approach.	Advanced Level ZT	All possible services require dynamic access for devices	Device	X	
2.7.3	Implement XDR Tools & Integrate w/ C2C Pt. 2	XDR solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk based methodical approach for continued operation. Extended analytics enabling ZT Advanced functionalities are integrated into the SIEM and other appropriate solutions.	Advanced Level ZT	Remaining integration points have been integrate as appropriate; Extended alerting and response is enabled with other Analytics tools at least using SIEM	Device	X	

DoD ZTA Mapping to ADVANCED Controls Appgate v.10

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL	APPGATE PARTIAL
3.2.4	Automate Application Security & Code Remediation Pt. 2	DoD Organizations modernize approaches to delivering internally developed and managed services following best practice approaches such as Microservices. These approaches will enable more resilient and secure architectures by allowing for quicker changes to code in each microservice as security issues are discovered. Further advancement security remediation activities continue across the DoD Enterprise with the inclusion of runtime security functions for containers as appropriate, automated vulnerable library updates and automated CI/CD approvals during the release process.	Advanced Level ZT	Secure API Gateway is operational and majority of API calls are passing through gateway; Services are provided following a Service Oriented Architecture (SOA); Security Remediation activities (e.g., runtime security, library updates, release approvals) are fully automated	Application & Workload		X
3.4.3	Enrich Attributes for Resource Authorization Pt. 1	Initial attributes from sources such as User and Entity Activity Monitoring, Micro-segmentation services, DLP and DRM are integrated into the Resource Authorization technology stack and policy. Any additional attributes for later integration are identified and planned. Attributes are used to create basic risk posture of users, NPEs and devices allowing for authorization decisions.	Advanced Level ZT	Most API calls are passing through the Secure API Gateway; Resource Authorization receives data from Analytics Engine; Authorization policies incorporate identified attributes in making authorization decisions; Attributes to be used for initial enrichment are identified; Identified attributes are assigned to resources and/or entities	Application & Workload		X
3.4.4	Enrich Attributes for Resource Authorization Pt. 2	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion.	Advanced Level ZT	Authorization policies incorporate confidence levels in making authorization decisions; Confidence levels for attributes are defined	Application & Workload	X	
3.4.5	REST API Micro-Segments	Using the DoD Enterprise approved API gateway(s), application calls are micro-segmented only allowing authenticated and authorized access to specific destinations (e.g., microservices). When possible, API Micro-Segmentation consoles are integrated and aware of other Micro- Segmentation consoles such as Software Defined Perimeter Controllers and/or Software Defined Networking Consoles.	Advanced Level ZT	Approved Enterprise APIs are Micro-Segmented appropriately	Application & Workload		
3.5.1	Continuous Authorization to Operate (ATO) Pt. 1	DoD Organizations utilize automation solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations. Where appropriate monitoring and testing is integrated with DevSecOps processes.	Advanced Level ZT	Controls derivation is standardized and ready for automation; Controls testing is integrated with DevSecOps processes and technology	Application & Workload		X
3.5.2	Continuous Authorization to Operate (ATO) Pt. 2	DoD Organizations fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboarding is used to monitor the status of authorizations and analytics are integrated with the responsible authorizing officials.	Advanced Level ZT	Controls testing is fully automated; Integration with standard IR and SOC operations is automated; Control derivation and applicability is fully automated; Dashboards are used to track continuing authorization status	Application & Workload		X
4.3.3	Manual Data Tagging Pt. 2	DoD organizational specific data level attributes are integrated into the manual data tagging process. DoD enterprise and organizations collaborate to decide which attributes are required to meet ZTA advanced functionality. Data level attributes for ZTA advanced functionality are standardized across the enterprise and incorporated	Advanced Level ZT	Manual data tagging is expanded to the program/org levels with specific attributes	Data		
4.3.4	Automated Data Tagging & Support Pt. 1	DoD Organizations use data loss prevention, rights management, and/or protection solutions to conduct scanning of data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.	Advanced Level ZT	Basic automation begins by scanning data repositories and applying tags	Data		X
4.3.5	Automated Data Tagging & Support Pt. 2	Remaining supported data repositories have basic and extended data tags which are applied using machine learning and artificial intelligence. Extended data tags are applied to existing repositories. Unsupported data repositories and data types are evaluated for decommissioning using a risk based methodical approach. Approved exceptions utilize manual data tagging approaches with data owners and/or custodians to manage tagging.	Advanced Level ZT	Full automation of data tagging is completed; Results of data tagging are fed into ML algorithms to develop AI driven data tagging	Data		X
4.4.5	Database Activity Monitoring	DoD Organizations procure, implement, and utilize Database Monitor solutions to monitor all databases containing regulated data types (CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are fed to the SIEM for monitoring and response. Analytics are fed into cross pillar activities such as "Enterprise Security Profile" and "Real Time Access" to better direct decision making.	Advanced Level ZT	Appropriate Database are being actively monitored; Monitoring technology is integrated with solutions such as SIEM, PDP and Dynamic Access Control mechanisms	Data		
4.4.6	Comprehensive Data Activity Monitoring	DoD Organizations expand monitoring of data repositories including databases as appropriate based on a methodical risk approach. Additional data attributes to meet the ZT Advanced functionalities are integrated into the analytics for additional integrations.	Advanced Level ZT	Data Activity monitoring mechanisms are integrated to provide a unified view of monitoring across data repositories; Appropriate integrations exist with solutions such as SIEM and PDP	Data		

DoD ZTA Mapping to ADVANCED Controls Appgate v.10

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL	APPGATE PARTIAL
4.5.4	DRM Enforcement via Data Tags and Analytics Pt. 2	Extended data repositories are protected with DRM and Protection solutions. DoD Organizations implement extended data tags applicable to organizations versus mandated enterprise. Data is encrypted in extended repositories using additional tags.	Advanced Level ZT	All applicable data repositories are protected using DRM; Data is encrypted using extended data tags from the org levels	Data		
4.5.5	DRM Enforcement via Data Tags and Analytics Pt. 3	DRM and Protection solutions integrate with AI and ML tooling for encryption, rights management and protection functions.	Advanced Level ZT	Analytics from ML/AI are integrated with DRM to better automate protections; Encryption protection is integrated with AI/ML and updated encryption methods are used as needed	Data		
4.6.3	DLP Enforcement via Data Tags and Analytics Pt. 2	Data loss prevention (DLP) solution is updated to include extended data tags based on parallel Automation activities.	Advanced Level ZT	Enforcement points have extended data tag attributes applied for additional prevention	Data		
4.6.4	DLP Enforcement via Data Tags and Analytics Pt. 3	Data loss prevention (DLP) solution is integrated with automated data tagging techniques to include any missing enforcement points and tags.	Advanced Level ZT	Automated tagging attributes are integrated with DLP and resulting metrics are used for ML	Data		
4.7.2	Integrate DAAS Access w/ SDS Policy Pt. 2	DoD Organizations implement the DAAS policy in an automated fashion.	Advanced Level ZT	Attribute based fine-grained DAAS Policy implemented in an automated fashion	Data		X
4.7.3	Integrate DAAS Access w/ SDS Policy Pt. 3	Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach should be taken to during implementation to measure results and adjust accordingly.	Advanced Level ZT	SDS is integrated with DAAS policy functionality; all data in all applications are protected with attribute based fine- grained DAAS policy	Data		X
4.7.5	Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2	Newly implemented SDS technology and/or functionalities are integrated with the Enterprise Identity Provider (IdP) following the integration plan. Identity attributes required to meet ZT Target functionalities are required for integration.	Advanced Level ZT	Complete integration with Enterprise IDP and SDS toolingto support all attribute based fine-grained DAAS access	Data		X
4.7.6	Integrate SDS Tool and/or Integrate with DRM Tool Pt. 1	Depending on the need for a Software Defined Storage tool, a new solution is implemented or an existing solution is identified meeting the functionality requirements to be integrated with DLP, DRM/Protection, and ML solutions.	Advanced Level ZT	If tooling is needed ensure there is supported integrations with DLP, DRM and ML tooling	Data		X
4.7.7	Integrate SDS Tool and/or Integrate with DRM Tool Pt. 2	DoD Organizations configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM/Protection infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	Advanced Level ZT	Integrate SDS infrastructure with existing DLP and DRM infrastructure	Data		
5.2.4	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.	Advanced Level ZT	Technical Refreshment/Technology Evolution; Provide Optimization/ Performance Controls	Network		
5.2.5	Real-Time Access Decisions	SDN Infrastructure utilizes cross Pillar data sources such as User Activity Monitoring, Entity Activity Monitoring, Enterprise Security Profiles and more for real-time access decisions. Machine learning is used to assist decision making based on advanced network analytics (full packet capture, etc.). Policies are consistently implemented across the Enterprise using unified access standards.	Advanced Level ZT	Analyze SIEM Logs with Analytics Engine to Provide Real- Time Policy Access Decisions; Support Sending Captured Packets, Data/Network Flows, and other Specific Logs for Analytics; Segment End-to-End Transport Network Flows; Audit Security Policies for Consistency across Enterprise; Protect Data-in-Transit During Coalition Information Sharing	Network		X
5.4.3	Process Micro-segmentation	DoD Organizations utilize existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Host- level processes are segmented based on security policies and access is granted using real-time access decision making.	Advanced Level ZT	Segment Host-Level Processes for Security Policies; Support Real-Time Access Decisions and Policy Changes; Support Offload of Logs for Analytics and Automation; Support Dynamic Deployment of Segmentation Policy	Network		
6.1.4	Enterprise Security Profile Pt. 2	The minimum number of Enterprise Security Profile(s) exist granting access to the widest range of DAAS across Pillars within the DoD Organizations. Mission/task organization profiles are integrated with the Enterprise Security Profile(s) and exceptions are managed in a risk based methodical approach.	Advanced Level ZT	Enterprise Profile(s) have been reduced and simplified to support widest array of access to DAAS; Where appropriate Mission/Task Critical profile(s) have been integrated and supported Organization profiles are considered the exception	Automatiion & Orchestration	X	
6.2.3	Enterprise Integration & Workflow Provisioning Pt. 2	DoD Organizations integrate remaining services to meet baseline requirements and advanced ZTA functionality requirements as appropriate per environment. Service provisioning is integrated and automated into workflows where required meeting ZTA target functionalities.	Advanced Level ZT	Services identified; Service provisioning is implemented	Automatiion & Orchestration		X

DoD ZTA Mapping to ADVANCED Controls Appgate v.10

ID#	ACTIVITY NAME	ASSOCIATED CAPABILITY	PHASE	OUTCOMES	WHICH PILLAR DOES THIS SUPPORT	APPGATE FULL	APPGATE PARTIAL
6.4.1	Implement AI Automation Tool	DoD Organizations identify areas of improvement based on existing machine learning techniques for Artificial Intelligence. AI solutions are identified, procured, and implemented using the identified areas as requirements.	Advanced Level ZT	Develop AI Tool Requirements; Procure and Implement AI Tools	Automatiion & Orchestration		
6.4.2	AI Driven by Analytics decides A&O modifications	DoD Organizations utilizing existing machine learning functions implement and use AI technology such as neural networks to drive automation and orchestration decisions. Decision making is moved to AI as much as possible freeing up human staff for other efforts. Utilizing historical patterns, AI will make anticipatory changes in the environment to better reduce risk.	Advanced Level ZT	AI is able to make changes to automated workflow activities	Automatiion & Orchestration		
6.5.3	Implement Playbooks	DoD organizations review all existing playbooks to identify for future automation. Existing manual and automated processes missing playbooks have playbooks developed. Playbooks are prioritized for automation to be integrated with the Automated Workflows activities covering Critical Processes. Manual processes without playbooks are authorized using a risk based methodical approach.	Advanced Level ZT	When possible automated playbooks based on automated workflows capability; Manual Playbooks are developed and implemented	Automatiion & Orchestration		X
6.7.3	Workflow Enrichment Pt. 3	DoD organizations use final enrichment data sources on basic and extended threat response workflows.	Advanced Level ZT	Enrichment data has been identified; Enrichment data is integrated into workflows	Automatiion & Orchestration		X
6.7.4	Automated Workflows	DoD organizations focus on automating Security Orchestration, Automation and Response (SOAR) functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk based approach.	Advanced Level ZT	Workflow processes are fully automated; Manual Processes have been identified; Remaining Processes are marked as exceptions and documented	Automatiion & Orchestration		X
7.2.3	Threat Alerting Pt. 3	Threat Alerting is expanded to include advanced data sources such as Extended Detection & Response (XDR), User & Entity Behavior Analytics (UEBA), and User Activity Monitoring (UAM). These advanced data sources are used to develop improved anomalous and pattern activity detections.	Advanced Level ZT	Identify Triggering Anomalous Events; Implement Triggering Policy	Visibility & Analytics		X
7.4.2	Baseline & Profiling Pt. 2	DoD Organizations expand baselines and profiles to include unmanaged and non-standard device types including Internet of Things (IoT) and Operational Technology (OT) through data output monitoring. These devices are again profiled based on standardized attributes and use cases. Analytics are updated to consider the new baselines and profiles accordingly enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.	Advanced Level ZT	Add threat profiles for IoT and OT devices; Develop and extend analytics; Extend threat profiles to individual users and devices	Visibility & Analytics		
7.4.3	UEBA Baseline Support Pt. 1	User & Entity Behavior Analytics (UEBA) within DoD Organizations expands monitoring to advanced analytics such as Machine Learning (ML). These results are in turn reviewed and fed back into the ML algorithms to improve detection and response.	Advanced Level ZT	Implement ML-based Analytics to detect anomalies	Visibility & Analytics		
7.4.4	UEBA Baseline Support Pt. 2	User & Entity Behavior Analytics (UEBA) within DoD Organizations completes it expansion by using traditional and machine learning (ML) based results to be fed into Artificial Intelligence (AI) algorithms. Initially AI based detections are supervised but ultimately using advanced techniques such as neural networks, UEBA operators are not part of the learning process	Advanced Level ZT	Implement ML-based Analytics to detect anomalies	Visibility & Analytics		
7.6.1	AI-enabled Network Access	DoD Organizations utilize the SDN Infrastructure and Enterprise Security Profiles to enable Artificial Intelligence (AI)/Machine Learning (ML) driven network access. Analytics from previous activities is used to teach the AI/ML algorithms improving decision making.	Advanced Level ZT	Network Access is AI driven based on environment analytics	Visibility & Analytics		X
7.6.2	AI-enabled Dynamic Access Control	DoD Organizations utilize previous rule based dynamic access to teach Artificial Intelligence (AI)/Machine Learning (ML) algorithms to make access decision to various resources. The "AI-enabled Network Access" activity algorithms are updated to enable broader decision making to all DAAS.	Advanced Level ZT	JIT/JEA are integrated with AI; Access is AI driven based on environment analytics	Visibility & Analytics		X

appgate