netskope

Compliance Series

DoD Zero Trust Architecture

Control Mapping to Netskope Products

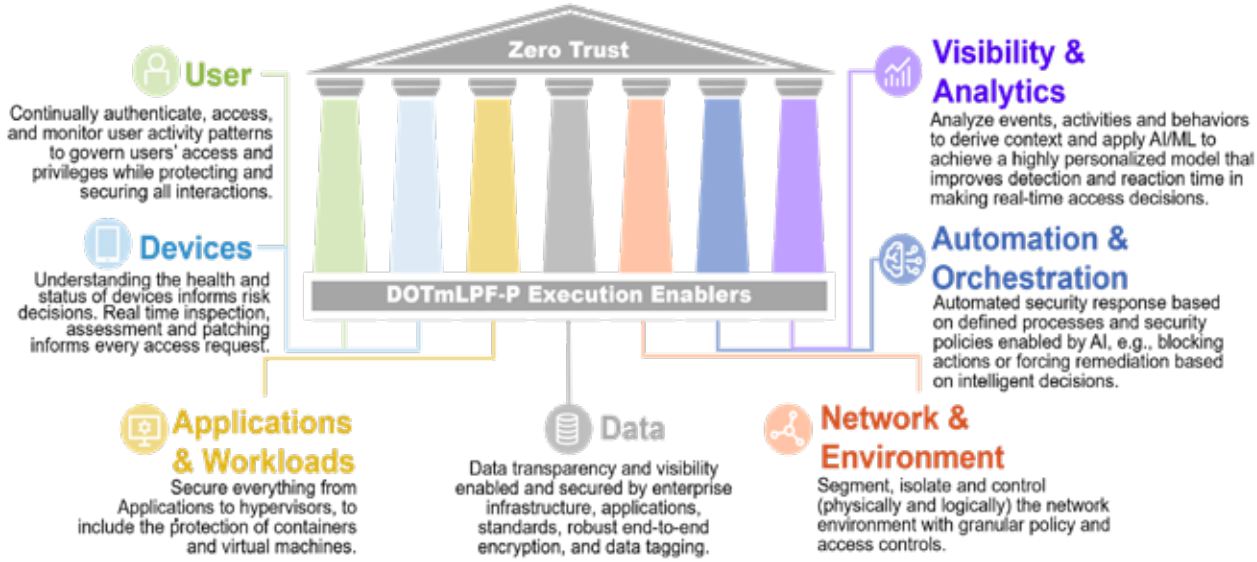
TABLE OF CONTENTS

INTRODUCTION	3
USER	5
DEVICE	13
APPLICATION AND WORKLOAD	18
DATA	23
NETWORK AND ENVIRONMENT	30
AUTOMATION AND ORCHESTRATION	33
VISIBILITY AND ANALYTICS	39

INTRODUCTION

This mapping guide aligns Netskope products and capabilities with the U.S. Department of Defense Zero Trust Capability Execution Roadmap.[1] That Roadmap is based on the DoD's Zero Trust Reference Architecture, part of the DoD's strategy to "infuse ZT principles" into all its digital resources and operations.

The Zero Trust Architecture rests on seven "pillars" that interconnect and support one another, with each pillar consisting of core "capabilities" and supporting "activities." The central pillar and ultimate goal of any ZT strategy is the protection of organizational Data. The other pillars relate to Users, Devices, Workloads, Networks, Visibility and Analytics, and Automation and Orchestration.



As its name suggests, the roadmap contemplates a journey toward increasing integration of zero trust principles and capabilities. Therefore, each pillar is broken down into Target-level capabilities and Advanced capabilities. Each of these capabilities is further subdivided into supporting activities.

This guide consists of seven tables, one for each pillar of the DoD's Zero Trust Architecture. Each table breaks down the pillar's capabilities and supporting activities, and includes a description of how Netskope's products meet the requirements. The DoD Zero Trust Capability Execution Roadmap (COA 1) is available here.

[1]https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTExecutionRoadmap.pdff

Note the following acronyms and/or aliases for the Netskope products:

Industry Terminology	Netskope Product Line/Abbreviation
Security access service edge	Netskope One SASE (SASE)
Security service edge	Netskope One SSE (SSE)
Next-gen secure web gateway	Netskope One Next Gen SWG (NG-SWG)
Cloud access security broker	Netskope One CASB (CASB)
Private access	Netskope One Private Access (Private Access)
SaaS security posture management	Netskope One SSPM (SSPM)
Data loss prevention	Netskope One DLP (DLP)
Firewall as a service	Netskope One FWaaS (FWaaS)
Reporting and analytics	Netskope One Advanced Analytics (Advanced Analytics)
Threat intelligence	Netskope One Threat Protection
Remote browser isolation	Netskope One RBI
Artificial intelligence security	Netskope One SkopeAI (SkopeAI)
Software-defined wide area network (SD-WAN)	Netskope One SD-WAN (SD-WAN) Netskope One SD-WAN for Endpoint (SD-WAN for Endpoint)
Threat/risk-sharing	Netskope Cloud Threat Exchange (CTE) Netskope Cloud Risk Exchange (CRE)
IT/IoT/OT security	Netskope One Device Intelligence (Device Intelligence)
Digital experience management	Netskope One DEM (DEM)
Data security posture management	Netskope One DSPM (DSPM)
Enterprise browser	Netskope One Enterprise Browser (Enterprise Browser)
User & entity behavior analytics	Netskope One UEBA (UEBA)
Third-party risk management/supply chain	Cloud Confidence Index (CCI)
User risk metrics	User Confidence Index (UCI)

1. USER

Capability	Activity	Netskope Controls	Products
1.1 User Inventory Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.	**1.1.1 User Inventory** DoD Organizations establish and update a user inventory manually if needed, preparing for automated approach in later stages. Accounts both centrally managed by an IdP/ICAM and locally on systems will be identified and inventoried. Privileged accounts will be identified for future audit and both standard and privileged user accounts local to applications and systems will be identified for future migration and/or decommission.	The Netskope One platform can be used to inventory all users connecting to the organization's network, as well as all managed and unmanaged applications and cloud services in use in the organization's IT ecosystem. The Netskope One platform also supports role based access controls for privileged and regular users, and can adjust privileges in real time based on user behavior with granular, context-aware controls that assess the riskiness of user actions and respond accordingly to protect organizational networks and data.	• All products
1.2 Conditional User Access Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role-based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	**1.2.1 App-Based Permission.** The DoD enterprise working with the Organizations establishes a basic set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete enterprise standard. The enterprise Identity, Credential and Access Management (ICAM) solution is enabled for self-service functionality for adding/updating attributes within the solution. Remaining Privileged Access Management (PAM) activities are fully migrated to PAM solution.	Netskope products, including its Netskope One Next Gen SWG (NG -SWG), , Netskope One CASB (CASB), and Netskope One Private Access (Private Access), can audit and verify user identities and credentials. Netskope also integrates with third-party identity providers like Okta and Ping to provision and manage user accounts, and to ensure secure authentication for remote and on-prem users. Netskope One SSPM (SSPM) detects and facilitates remediation of misconfigurations in the organization's SaaS apps, ensuring access management controls remain within organization-defined parameters.	• NG-SWG • CASB • Private Access • SSPM
	1.2.2 Rule-Based Dynamic Access I DoD Organizations utilize the rules from the "Periodic Authentication" activity to build basic rules enabling and disabling privileges dynamically. High-risk user accounts utilize the PAM solution to move to dynamic privileged access using Just-In-Time access and JustEnough-Administration methods.	Netskope NG-SWG, CASB, and Private Access provide detailed logging of all web, cloud, and on-prem access activity by users, including inline app and cloud service API-level. Netskope One UEBA (UEBA) can use this data, in combination with sequential anomaly rules across apps and cloud services, in order to detect and block risky actions.	• NG-SWG • CASB • Private Access • UEBA
	1.2.3 Rule-Based Dynamic Access II 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.	Netskope UEBA deploys machine-learning algorithms to detect anomalous behavior, and assigns each user a User Confidence Index (UCI) based on the riskiness of their actions. UCI can be leveraged to create adaptive access controls that adjust privileges in real time.	• UEBA • UCI

Capability	Activity	Netskope Controls	Products
	1.2.4 Enterprise Roles and Permissions I 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.	The Netskope One platform supports role based access control, and integrates with third-party identity providers like Okta and Ping to ensure secure authentication for remote or on-prem users. Netskope SD-WAN and SASE architecture facilitate the migration of identity and access management controls to the cloud, allowing uniform enforcement of granular, context-aware policies to all users and devices connecting to the organization's network.	• SASE • SD-WAN
	1.2.5 Enterprise Roles and Permissions II 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 utilize 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.	Netskope SD-WAN, FWaaS, and Private Access support network segmentation to create enclave/DDIL environments. Netskope UEBA provides a User Confidence Index (UCI) that assigns each user a dynamic, risk-based score, which can be leveraged to adjust access privileges. And Netskope Cloud Risk Exchange allows organizations to share data about risky users, devices, and applications.	• SD-WAN • FWaaS • Private Access • UEBA • UCI • Cloud Exchange
1.3 Multifactor Authentication This capability initially focuses on developing an organization focused MFA provider and Identity Provider to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical piece to this capability. At the later maturity levels alternative and flexible MFA tokens can be used to provide access for standard and external users.	**1.3.1 Organizational MFA/IDP** DoD Organizations procure and implement a centralized Identity Provider (IdP) solution and Multi-Factor (MFA) solution. The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well enabling key pairs to be signed by the trusted root certificate authorities. Mission/Task-Critical applications and services are utilizing the IdP and MFA solution for management of users and groups.	Netskope products integrate with third-party identity providers like Okta and Ping to extend SSO/MFA across web, managed and unmanaged apps, and cloud services, and can detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. When an action is detected, such as an upload of company data to a non-managed cloud service or application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user. Adaptive policy controls can also leverage Netskope Cloud Confidence Index (CCI) ratings for apps and Netskope User Confidence Index (UCI) risk scoring for the user to determine what is permitted. Netskope One Device Intelligence can also monitor IoT, OT, and traditional devices for authentication.	• NG-SWG • CASB • Private Access • CCI • UEBA • UCI • Device Intelligence
	1.3.2 Alternative Flexible MFA I 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.		

Capability	Activity	Netskope Controls	Products
	1.3.3 Alternative Flexible MFA II 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.		
1.4 Privileged Access Management The capability focuses on removal of permanent administrator/ elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.	**1.4.1 Implement System and Mitigate Privileged Users I** DoD Organizations procure and implement a Privileged Access Management (PAM) solution that supports all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that easily integrate with PAM solutions are transitioned over to using solution versus static and direct privileged permissions.	Netskope zero trust SASE architecture supports all critical privileged use cases. NG-SWG, CASB, and Private Access integrate with third-party identity providers to provision and manage identities and credentials. And Netskope SSPM continuously monitors the organization's SaaS applications for misconfigured access controls.	• NG-SWG • CASB • Private Access • SSPM
	1.4.2 Implement System and Mitigate Privileged Users II DoD Organizations utilize the inventory of supported and unsupported Applications/ Services for integration with privileged access management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support PAM solution.	Netskope products provide detailed reports and interactive dashboards that inventory, categorize, assign risk scores to, and show the usage of more than 85,000 cloud applications in use within the enterprise, including SaaS and public cloud services. Netskope can also identify, inventory, and enforce real-time controls for unmanaged applications (i.e., end-user adopted SaaS applications that have not been officially onboarded by IT, also known as Shadow IT). The insights provided by these tools make it easier to identify and migrate away from applications and services whose risk profiles are not aligned with the organization's requirements for privileged users.	• CASB • CCI

Capability	Activity	Netskope Controls	Products
	1.4.3 Real Time Approvals and JIT/JEA Analytics I 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.	Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. When access to a cloud service or SaaSapplication is granted, administrators can differentiate between personal, third-party, and corporate-owned instances of the same managed app and adjust policy controls accordingly. Activity controls can be implemented for both corporate-owned devices for web, SaaS, Shadow IT, and IaaS/PaaS, as well as personal devices accessing corporate-managed apps and cloud services. Netskope Private Access ensures that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access and inbound access rules.	• NG-SWG • CASB • Private Access • SSPM • Device Intelligencel
	1.4.4 Real Time Approvals and JIT/JEA Analytics II 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.	Netskope products can detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. When an action is detected, such as an upload of company data to a non-managed cloud service or application, adaptive policy controls can leverage Netskope Cloud Confidence Index (CCI) ratings for apps and Netskope User Confidence Index (UCI) risk scoring for the user to determine what is permitted.	• NG-SWG • CASB • Private Access • CCI • Advanced UEBA • UCI

Capability	Activity	Netskope Controls	Products
1.5 Identity Federation and User Credentialing The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard organizational IDP/IDM solution. Once completed the capability shifts to establishing an Enterprise ILM process/ solution either through a single solution or identity federation.	**1.5.1 Organization Identity Life-Cycle Management** DoD Organizations establish a process for life cycle management of users both privileged and standard. Utilizing the Organizational Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Any users who fall outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	Netskope NG-SWG, CASB, and Private Access provide auditing and verification of user identities and credentials. Netskope SSPM also provides security configuration, auditing, compliance, and company checks for user identities in managed SaaS apps.	• NG-SWG • CASB • Private Access • SSPM
	1.5.2 Enterprise Identity Life-Cycle Management I The DoD Enterprise works with Organizations to review and align the existing Identity Lifecycle Processes, policy, and standards. A finalized agreed upon policy and supporting process are developed and followed by the DoD Organizations. Utilizing the centralized or federated Identity Provider (IdP) and Identity & Access Management (IdAM) solutions, DoD Organizations implement the Enterprise Lifecycle Management process for the maximum number of identities, groups, and permissions. Exceptions to the policy are managed in a risk based methodical approach.	Netskope integrates with third-party identity providers like Okta and Ping to provision, manage, and deprovision users and groups as needed. Netskope One SD-WAN and SASE architecture allows uniform enforcement of granular, adaptive policy controls to all users and devices connecting to the organization's network from anywhere. Netskope SSPM continuously monitors the organization's managed SaaS apps to ensure that access controls do not drift from organization-defined parameters.	• SASE • SD-WAN • SSPM
	1.5.3 Enterprise Identity Life-Cycle Management II 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.		
	1.5.4 Enterprise Identity Life-Cycle Management III 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.		

Capability	Activity	Netskope Controls	Products
1.6 Behavioral, Contextual ID, and Biometrics Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	**1.6.1 Implement UEBA Tooling** DoD Organizations procure and implement User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed enabling future usage in decision making. **1.6.2 User Activity Monitoring I** 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. **1.6.3 User Activity Monitoring II** 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 JustEnough-Access solution.	Netskope products can detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. Netskope UEBA can use this data, in combination with sequential anomaly rules across apps and cloud services, to build a baseline of normal behavior for each user, to alert on anomalous behavior, and to detect and block risky actions. Netskope UEBA deploys machine-learning algorithms to detect anomalous behavior, and assigns each user a User Confidence Index (UCI) based on the riskiness of their actions. UCI can be leveraged to create adaptive access controls that adjust privileges in real time.	• NG-SWG • CASB • Private Access • UEBA • UCI
1.7 Least Privileged Access DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoD Application Owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organization DAAS is audited and removed when unneeded.	**1.7.1 Deny User by Default Policy** DoD Organizations audit internal user and group usage for permissions and revoke permissions when possible. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible static privileged users are decommissioned or reduced permissions preparing for future rule/dynamic based access.	Netskope identifies and inventories all users and applications in the organization's IT ecosystem, and scores them by risk and usage. Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. Netskope SSPM continuously monitors the organization's managed SaaS apps to prevent access controls from drifting away from organization-defined policies.	• NG-SWG • CASB • Private Access • SSPM

Capability	Activity	Netskope Controls	Products
1.8 Continuous Authentication The DoD organizations and overall enterprise will methodically move towards continuous attribute based authentication. Initially the capability focuses on standardizing legacy single authentication to an organizationally approved IDP with users and groups. The second stage adds in based rule based (time) authentication and ultimately matures to Continuous Authentication based on the application/ software activities and privileges requested.	**1.8.1 Single Authentication** DoD Organizations employ basic authentication processes to authenticate users and NPEs at least once per session (e.g., logon). Importantly, users being authenticated are managed by the parallel activity "Organizational MFA/IDP" with the Organizational Identity Provider (IdP) versus using application/service-based identities and groups. **1.8.2 Periodic Authentication** DoD Organizations enable period authentication requirements for applications and services. Traditionally these are based on duration and/or duration timeout but other period based analytics can be used to mandate re-authentication of user sessions.. **1.8.3 Continuous Authentication I** 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. **1.8.4 Continuous Authentication II** DoD Organizations continue usage of transaction-based authentication to include integration such as user patterns.	Netskope products integrate with third-party identity providers like Okta and Ping to extend SSO/MFA across web and cloud applications. Netskope decodes numerous activities, allowing it to create a baseline of normal behavior for each user, and detect anomalous or risky actions. This ongoing, real-time analysis constitutes a kind of continuous authentication of each user in accordance with zero trust principles. It can also be leveraged to require periodic re-authentication, such as requesting a stepped-up MFA before performing a risky action.	• NG-SWG • CASB • Private Access • DLP • UEBA • SSPM

Capability	Activity	Netskope Controls	Products
1.9 Integrated ICAM Platform DoD organizations and overall enterprise employ enterprise-level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CA's.	**1.9.1 Enterprise PKI/IDP I** The DoD Enterprise works with Organizations to implement Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) which can then be trusted by Organizations to build Intermediate CA's off. The Identity Provider solution may either be a single solution or federated set of Organizational IdPs with standard level of access across Organizations and standardized set of attributes. Organizations' IdPs and PKI Certificated Authorities are integrated with the Enterprise IdP and PKI solutions.	Netskope One platform does not map to this requirement.	
	1.9.2 Enterprise KPI/IDP II 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.	Netskope One platform extends SSO/MFA across web and managed and unmanaged cloud apps and services, by integrating with third-party identity providers like Okta and Ping, who can also enforce biometric authentication in accordance with organizational requirements.	• NG-SWG • CASB • Private Access
	1.9.3 Enterprise KPI/IDP III DoD Organizations integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor (MFA) tokens can be used.		

2. DEVICE

Capability	Activity	Netskope Controls	Products
2.1 Device Inventory DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/ vulnerability status and others to enable successor activities.	**2.1.1 Device Help Tool Gap Analysis** DoD Organizations develop a manual inventory of devices within the environment. Device attributes tracked in the inventory enable functionality outlined in the ZTA target level.	Netskope Device Intelligence offers organizations the ability to produce an inventory of hardware on their network, including IoT, OT, and traditional devices.	• Device Intelligence
	2.1.2 NPE/PKI Device Under Management DoD Organizations utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Additional other Non-Person Entities (NPEs) that support x509 certificates are assigned in the PKI and/or IdP systems.	Netskope One platform does not map to this requirement.	
	2.1.3 Enterprise IDP I The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies integrates NonPerson Entities (NPEs) such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or exempted using a risk based methodical approach.	Netskope's Device Intelligence can assist with authenticating hardware connected to the organization's network, as well as identifying vulnerable operating systems and browsers. This capability is useful for identifying rogue or unsupported devices .	• Device Intelligence
	2.1.4 Enterprise IDP II 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.		
2.2 Device Detection and Compliance DoD organizations employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C).	**2.2.1 Implement C2C/Compliance Based Network Authorization I** The DoD Enterprise working with the Organizations develops a policy, standard and requirements for Comply to Connect. Once agreement is reached, solution procurement is started, a vendor(s) is selected, and implementation begins with base level functionality in ZT Target environments (low risk). Base level checks are implemented in the new Comply to Connection solution enabling the ability to meet ZTA target functionalities.	Netskope Device Intelligence catalogs all managed and unmanaged devices on the network, isolates risky devices, and uses AI/ML to establish normal device behavior and detect anomalies. It applies granular controls to enforce zero trust principles, and integrates with incident response tools to trigger security alerts based on organizational criteria.	• Device Intelligence

Capability	Activity	Netskope Controls	Products
	2.2.2 Implement C2C/Compliance Based Network Authorization II 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.		
2.3 Device Authorization with Real Time Inspection DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.	**2.3.1 Entity Activity Monitoring I** 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.	Netskope User and Entity and Behavior Analytics (UEBA) tracks user behavior and sets baselines to detect anomalies. Netskope UEBA uses multiple ML-based models to offer a dynamic User Confidence Index (UCI), aiding in insider threat detection and adapting security policies accordingly. UCI is calculated from alerts fed in from many other Netskope products, including Device Intelligence—that can identify devices using vulnerable browsers or operating systems, or NG-SWG, CASB, or Private Access, that can log and alert on failed login attempts.	• NG-SWG • CASB • UEBA • Device Intelligence • Private Access
	2.3.2 Entity Activity Monitoring II 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.		
	2.3.3 Implement App Control and FIM Tools DoD Organizations procure and implement File Integrity Monitoring (FIM) and Application Control solutions. FIM continues development and expansion of monitoring in the Data Pillar. Application Control is deployed to low-risk environments in a monitor only mode establishing baseline allowances. Application control teams being integrated with the Enterprise and Organization PKI environments utilize certificates for application allowances. NextGen AV covers all possible services and applications.	Netskope security solutions, including CASB and NG-SWG, utilize a Data Loss Prevention (DLP) engine that provides file integrity monitoring across various environments such as web, cloud applications, and endpoint devices. Netskope CASB helps organizations identify and categorize cloud apps by usage and risk score. Netskope One FWaaS provides uniform enforcement of security policies for web and cloud traffic, and Private Access ensures remote users only have access to approved applications. Netskope One Threat Protection safeguards against known and new malware, phishing, and web threats, using machine-learning and corroborative sandboxing. It integrates with threat intelligence feeds and other Netskope tools like Netskope One RBI and FWaaS to offer a comprehensive, layered security solution. Netskope Device Intelligence identifies all devices connecting to the organization's network and can isolate risky devices in network microsegments.	• NG-SWG • CASB • DLP • FWaaS • SSPM • Threat Protection • Cloud Exchange • Device Intelligence • RBI
	2.3.4 Integrate NextGen AV Tools with C2C DoD Organizations procure and implement Next Generation Anti-Virus & Anti-Malware solutions as needed. These solutions are integrated with the initial deployment of Comply to Connect for baseline status checks of signatures, updates, etc.		

Capability	Activity	Netskope Controls	Products
	2.3.5 Fully Integrate Device Security Stack with 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.	Netskope's Device Intelligence identifies all devices connecting to the organization's network, and can isolate risky devices in network microsegments.	
	2.3.6 Enterprise PKI I The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and devices that do not support PKI certificates are marked for retirement and decommission starts.	The Netskope One platform does not map to these requirements.	
	2.3.7 Enterprise PKI II 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.		
2.4 Remote Access DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.	**2.4.1 Deny Device by Default Policy** DoD Organizations block all unmanaged remote and local device access to resources. Compliant managed devices are provided risk based methodical access following ZTA target level concepts.	Netskope NG-SWG integrates with third-party identity providers like Okta and Ping to extend SSO/MFA across web and cloud apps and services. Netskope Device Intelligence provides a complete picture of all devices connected to the organization's network. It analyzes hundreds of device parameters to generate unique device identifiers and authenticity ratings, grouping similar devices together for uniform policy enforcement. Device Intelligence also uses machine-learning to recognize anomalous behavior and offers insights and analytics about device-level risks, threats, and best practices for threat mitigation. It dynamically groups devices within network microsegments to isolate risky devices and prevent lateral movement by threat actors. Netskope CASB identifies all cloud apps and services in use in the organization's IT ecosystem, and categorizes them by usage and risk level, allowing organizations to assess which services/ applications are most critical to their day-to-day operations .	• NG-SWG • CASB • Private Access • SD-WAN • Device Intelligence
	2.4.2 Managed and Limited BYOD and IOT Support DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP, enabling user and device-based authorization are supported. Device access for all applications requires dynamic access policies.		
	2.4.3 Managed and Full BYOD and IOT Support I 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.		

Capability	Activity	Netskope Controls	Products
	2.4.4 Managed and Full BYOD and IOT Support II 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.	Private Access allows secure access to managed cloud applications, with end-to-end encryption, for remote users. Granular and adaptive controls adjust access privileges based on user, device type, app instance, and other risk-based criteria. Netskope Endpoint SD-WAN and Security Secure Service Edge (SSE) extend reliable and secure network access to managed and unmanaged devices, using granular, context-aware controls that authorize access on the basis of continuously adaptive trust.	
2.5 Partially and Fully Automated Asset Vulnerability, and Patch Management DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed.	**2.5.1 Implement Asset, Vulnerability, and Patch Management Tools** DoD Organizations implement solution(s) for managing assets/devices configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, etc.) teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	Netskope Device Intelligence can assist with authenticating hardware connected to the organization's network, as well as identifying vulnerable operating systems and browsers.	• Device Intelligence
2.6 Unified Endpoint Management (UEM) and Mobile Device Management (MDM) DoD organizations establish a centralized UEM solution that provides the choices of agent and/or agentless management of computer and mobile devices to a single console regardless of device location. DoD-issued devices can be remotely managed and security policies are enforced.	**2.6.1 Implement UEDM or Equivalent Tools** DoD Organizations will work closely with the "Implement Asset, Vulnerability, and Patch Management tools" activity to procure and implement a Unified Endpoint and Device Management (UEDM) solution ensuring that requirements are integrated with the procurement process. Once a solution is procured the UEDM team(s) ensure that critical ZT target functionalities such as minimum compliance, asset management, and API support are in place. **2.6.2 Enterprise Device Management I** DoD Organizations migrate the manual device inventory to an automated approach using the Unified Endpoint and Device Management solution. Approved devices are able to be managed regardless of location. Devices part of critical services are mandated to be managed by the Unified Endpoint and Device Management solution supporting automation.	Netskope Private Access provides secure access for remote users to managed cloud apps and services. Private Access ensures that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access and inbound access rules. Netskope's Endpoint SD-WAN and SSE extend reliable and secure network access to managed and unmanaged devices, using granular, context-aware controls that authorize access on the basis of continuously adaptive trust. Netskope Device Intelligence provides a complete picture of all devices connected to the organization's network. It analyzes hundreds of device parameters to generate unique device identifiers and authenticity ratings, grouping similar devices together for uniform policy enforcement.	• Private Access • SD-WAN • Device Intelligence

Capability	Activity	Netskope Controls	Products
	2.6.3 Enterprise Device Management II DoD Organizations migrate the remaining devices to Enterprise Device Management solution. EDM solution is integrated with risk and compliance solutions as appropriate.	Device Intelligence also uses machine-learning to recognize anomalous behavior and offers insights and analytics about device-level risks, threats, and best practices for threat mitigation. It dynamically groups devices within network microsegments to isolate risky devices and prevent lateral movement by threat actors. Device Intelligence integrates with SIEM tools for automated incident response and remediation.	
2.7 Endpoint and Extended Detection and Response (EDR & XDR) DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	**2.7.1 Implement EDR Tools and Integrate with C2C** DoD Organizations procure and implement Endpoint Detection and Response (EDR) solution(s) within environments. EDR is protecting, monitoring, and responding to malicious and anomalous activities enabling ZT Target functionality and is sending data to the Comply to Connection solution for expanded device and user checks.	Netskope Cloud Exchange can be integrated with EDR and XDR solutions. Netskope Cloud Log Shipper can export cloud and web logs, share threat intelligence, and automate service tickets based on alerts.	• Cloud Exchange
	2.7.2 Implement XDR Tools and Integrate with C2C I DoD Organizations procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities are identified and prioritized based on risk. The riskiest of these integration points are actioned and integration is started. EDR continues coverage of endpoints to include the maximum number of services and applications as part of the XDR implementation. Basic analytics are sent from the XDR solution stack to the SIEM.		
	2.7.3 Implement XDR Tools and Integrate with C2C II 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.		

3. APPLICATION AND WORKLOAD

Capability	Activity	Netskope Controls	Products
3.1 Application Inventory System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/ CISO/CIO shall be utilized within the system owner's purview.	**3.1.1 Application Code Identification** DoD Organizations create an inventory of approved applications and code (e.g., source code, libraries, etc.). Each organization will track the supportability (i.e., active, legacy, etc.) and hosted location (i.e., cloud, on-premise, hybrid, etc.) at least in the inventory.	Netskope products provide detailed reports and interactive dashboards that inventory, categorize, assign risk scores to, and show the usage of more than 85,000 cloud applications in use within the enterprise including SaaS and Public Cloud services. Netskope can also identify, inventory, and enforce real-time control for unmanaged applications (i.e., end-user adopted SaaS applications that have not been officially onboarded by IT, also known as Shadow IT).	• CASB • CCI
3.2 Software Development and Integration Foundational software and application security processes and infrastructure are established following Zero Trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.	**3.2.1 Build DevSecOps Software Factory I** The DoD enterprise creates the foundational standards for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across DoD organizations able to meet future Application Security requirements. An enterprise-wide Vulnerability Management program is integrated with the CI/CD pipelines following the Vulnerability Management Program activities.	The Netskope platform supports secure software development at all stages of the CI/CD pipeline. Netskope can be used to manage access to apps and services used during SDLC (i.e., GitHub, public cloud, etc.). With instance awareness, services can also be managed to separate dev, test, and production environments.	• NG-SWG • CASB • Private Access • FWaaS
	3.2.2 Build DevSecOps Software Factory II DoD Organizations will use their approved CI/ CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.		

Capability	Activity	Netskope Controls	Products
	3.2.3 Automate Application Security and Code Remediation I A standardized approach to application security including code remediation is implemented across the DoD enterprise. Part one (1) of this activity includes the integration of a Secure API gateway with applications utilizing API or similar calls. Code reviews are conducted in a methodical approach and standardized protections for containers and their infrastructure are in place. Additionally, any serverless functions where the 3rd party manages the infrastructure such as Platform as a Service utilize adequate serverless security monitoring and response functions. Code Reviews, Container and Serverless security functions are integrated into the CI/CD and/or DevSecOps process as appropriate.	Netskope can be used to continuously assess and protect movement of source code including the use of proprietary source code in Generative AI services. And Netskope offers reverse proxy capabilities to protect development environments hosted on cloud infrastructure and cloud applications. Netskope offers inline controls that can block, notify, or allow employees access to web, cloud or private application information assets. Netskope is also instance aware and can identify different instances of cloud applications including applications used for development, testing, and production environments and apply data protection rules to ensure separation of environments.	• NG-SWG • CASB • Private Access • DLP
	3.2.4 Automate Application Security and Code Remediation II 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.		
3.3 Software Risk Management DoD organizations establish software/ application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	**3.3.1 Approved Binaries/Code** The DoD enterprise uses best practice approaches to manage approved binaries and code in a methodical approach. These approaches will include supplier sourcing risk management, approved repository usage, bill of materials supply chain risk management, and industry standard vulnerability management.	The Netskope platform can assist with supply chain discovery and risk management. Netskope CASB identifies all managed and unmanaged apps and cloud services in the organization's IT ecosystem, and categorizes them by usage and risk. The Cloud Confidence Index scores over 85,000 apps and cloud services based on dozens of risk factors including known vulnerabilities, enterprise readiness, auditability, privacy policies, and regulatory compliance.	• CASB • CCI
	3.3.2 Vulnerability Management Program I The DoD Enterprise works with Organizations to establish and manage a Vulnerability Management program. The program includes a policy and standards agreed upon by all Organizations. The developed program includes at a minimum the track and management of public vulnerabilities based on DoD applications/ services.	Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements. Netskope CASB can audit web, and cloud applications, and provide metadata to understand if suppliers are using underlying cloud infrastructure to support supply chain discovery.	• CASB • Cloud Exchange

Capability	Activity	Netskope Controls	Products
	Organizations establish a vulnerability management team with key stakeholders where vulnerabilities are discussed and managed following the Enterprise policy and standards.	Netskope also offers reverse proxy capabilities to protect cloud applications along with Netskope Private Access to manage suppliers' access to organizational assets. Netskope Cloud Exchange supports discovery and disclosure of vulnerabilities. Netskope Cloud Risk Exchange (CRE) allows sharing of risk signals for individual users, devices, web, and cloud services with other security solutions. Further, Netskope Cloud Threat Exchange (CTE) enables bidirectional threat intelligence sharing. This can be integrated with both open- and closed-source intelligence feeds, ensuring that up-to-date threat intelligence is in the Netskope One platform.	
	3.3.3 Vulnerability Management Program II Processes are established at the DoD Enterprise level for managing the disclosure of vulnerabilities in DoD maintained/operated services both publicly and privately accessible. DoD Organizations expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB, CERT, and others.		
	3.3.4 Continual Validation DoD Organizations will implement a continual validation approach for application development where parallel deployment is conducted and integrated with an approved environment level (e.g., UAT, Prod). Applications unable to integrate continual validation into their CI/CD process are identified and exceptions are provided as needed using a methodical approach.	Netskope can be used to continuously assess and protect movement of source code including the use of proprietary source code in generative AI services. Netskope offers inline controls that can block, notify, or allow employees access to web, cloud or private application information assets. Netskope is also instance aware and can identify different instances of cloud applications including applications used for development, testing, and production environments and apply data protection rules to ensure separation of environments.	• NG-SWG • CASB • Private Access • DLP
3.4 Resource Authorization and Integration DoD establishes a standardized resource authorization gateway for authorizations via the CI/CD pipelines in a risk approach that reviews the User, Device and Data security posture. Authorizations utilize a programmatic (e.g., Software Defined) approach in a live/production environment. Attributes are enriched utilizing other pillar activities and the API and Authorization gateway. Approved enterprise APIs are micro-segmented using authorizations..	**3.4.1 Resource Authorization I** The DoD Enterprise standardizes on resource authorization approaches (e.g., Software Defined Perimeter) with the organizations. At a minimum the resource authorization gateways will be integrated with identities and devices. Organizations deploy approved resource authorization gateways and enable for external facing applications/services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.	Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. When access to a cloud service or cloud application is granted, administrators can differentiate between personal, third-party, and corporate-owned instances of the same managed app and adjust policy controls accordingly. Activity controls can be implemented for both corporate-owned devices for web, SaaS, Shadow IT, and IaaS/PaaS, as well as personal devices accessing corporate-managed apps and cloud services. Netskope Private Access ensures that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access and inbound access rules.	• NG-SWG • CASB • Private Access • Device Intelligence
	3.4.2 Resource Authorization II Resource authorization gateways are used for all possible applications/ services. Applications unable to utilize gateways are either decommissioned or excepted using a risk based methodical approach. Authorizations are further integrated with the CI/CD pipeline for automated decision making.		

Capability	Activity	Netskope Controls	Products
	3.4.3 SDC Resource Authorization I The DoD Enterprise provides a standardized approach for code based compute management (i.e., Software Defined Compute) following industry best practices. Using risk-based approaches baselines are created using the approved set of code libraries and packages. DoD Organizations work with the approved code/binaries activities to ensure that applications are identified which can and cannot support the approach. Applications which can support a modern software based configuration and management approaches are identified and transitioning begins. Applications which cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	Netskope CASB can identify and categorize all apps and cloud services in use in the organization's IT ecosystem, and its Cloud Confidence Index provides a risk-based score to assist organizations in determining whether use of a given app or service comports with organization-defined policy. Netskope FWaaS, Private Access, and SD-WAN support network microsegmentation to segregate resources into production, testing, or live environments. Netskope SSPM continuously monitors an organization's SaaS apps for vulnerabilities and misconfigurations.	• CASB • CCI • Private Access • Cloud Firewall • SD-WAN • SSPM
	3.4.4 SDC Resource Authorization II Applications which support software-based configuration and management have been transitioned to a production/live environment and are in normal operations. Where possible applications which cannot support software-based configuration and management are decommissioned.		
	3.4.5 Enrich Attributes for Resource Authorization I 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.	Netskope UEBA uses machine-learning to develop a baseline for each user's normal behavior, and includes the User Confidence Index (UCI) that scores each user based on the riskiness of their actions. Netskope Device Intelligence also creates a baseline for each device's behavior and can isolate risky devices in network microsegments. Netskope Cloud Confidence Index provides a risk-based score to over 85,000 apps and cloud services that may be in use in the organization's IT environment. The Netskope One platform integrates these and other risk factors into a suite of granular and adaptive policy controls that can adjust access privileges in real time based on the level of risk.	• NG-SWG • CASB • CCI • Private Access • Advanced UEBA • Device Intelligence
	3.4.6 Enrich Attributes for Resource Authorization II 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.		

Capability	Activity	Netskope Controls	Products
	3.4.7 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.	Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. Netskope FWaaS, SD-WAN, and Private Access support network microsegmentation, and Device Intelligence can segregate risky devices into dedicated microsegments.	• NG-SWG • CASB • Private Access • FWaaS • SD-WAN • Device Intelligence
3.5 Continuous Monitoring and Ongoing Authorizations DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate.	**3.5.1 Continuous Authorization to Operate (ATO) I** 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.	Netskope SSPM monitors SaaS applications, preventing misconfigurations, and offers step-by-step remediation instructions. It integrates with Netskope Cloud Ticket Orchestrator (CTO) for automated remediation and converts detected misconfigurations into new security rules.	• SSPM • CTO
	3.5.2 Continuous Authorization to Operate (ATO) II 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.		

4. DATA

Capability	Activity	Netskope Controls	Products
4.1 Data Catalog Risk Alignment Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access.	**4.1.1 Data Analysis** DoD Organizations update the service and application catalog(s) with data classifications. Data tags are also added to each service and application.	Netskope offers controls to identify labeled classified data and metadata and can associate policies to protect this information. In addition, Netskope can apply controls around unclassified data and metadata based on Netskope One DLP including fingerprinting and natural language processing.	• CASB • NG-SWG • DLP
4.2 DoD Enterprise Data Governance DoD establishes enterprise data labeling/tagging and DAAS access control/ sharing policies (e.g., SDS policy) that are enforceable. Developed enterprise standards ensure an appropriate level of interoperability between DoD Organizations.	**4.2.1 Define Data Tagging Standards** The DoD Enterprise works with organizations to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.	Netskope CASB and NG-SWG leverage a powerful DLP engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine-learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. It ensures real-time data protection through measures like obfuscation, encryption, and action blocking.	• NG-SWG • CASB • DLP
	4.2.2 Interoperability Standards The DoD Enterprise collaborating with the organizations develops interoperability standards integrating mandatory Data Rights Management (DRM) and Protection solutions with necessary technologies to enable ZT target functionality.	Netskope DLP is fully integrated into the entire cloud platform, ensuring that both data at rest and data in transit are protected by the same set of policies and workflows. This ensures that policy is easy to implement and the DLP program is easy to maintain. In addition to creating custom DLP rules, administrators can also select from over 30 predefined DLP profiles based on common industry standards and regulatory frameworks.	• DLP
	4.2.3 Develop SDS Policy The DoD enterprise working with organizations establishes a software defined storage (SDS) policy and standards based on industry best practices. DoD organizations evaluate current data storage strategy and technology for implementation of SDS. Where appropriate storage technology is identified for SDS implementation.	Netskope DLP can be configured to hold certain transaction log data in dedicated repositories for forensics or compliance purposes. Netskope Advanced DLP can discover and classify organizational data at rest in cloud storage services like AWS, Azure, and Google Cloud. It can also discover malware in cloud storage buckets, and integrates with incident response tools to automate remediation.	• Advanced DLP

Capability	Activity	Netskope Controls	Products
4.3 Data Labeling and Tagging Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy. As phases advance automation is used to meet scaling demands and provide better accuracy.	**4.3.1 Implement Data Tagging and Classification Tools** DoD Organizations utilize the enterprise standard and requirements to implement data tagging and classification solution(s). Organizations ensure that future ML and AI integrations are supported by solutions through DoD enterprise requirements. **4.3.2 Manual Data Tagging I** Using the DoD Enterprise data tagging and classification policy and standards, manual tagging starts using basic data level attributes to meet ZT target functionality. **4.3.3 Manual Data Tagging II** 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. **4.3.4 Automated Data Tagging and Support I** 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. **4.3.5 Automated Data Tagging and Support II** 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.	Netskope security solutions, including CASB and NG-SWG, utilize the industry's most comprehensive DLP to discover and classify organizational data across various environments such as web, cloud applications, and endpoint devices. Netskope DLP leverages machine-learning to identify data and classify it according to both customized, organizational profiles as well as predefined profiles for common regulatory frameworks such as GDPR, HIPAA, or PCI-DSS. Netskope Advanced DLP scans IaaS data repositories across AWS, Azure, and Google Cloud for both sensitive data and malware. It also utilizes machine-learning with deep object-level classification capabilities to identify and tag organizational data according to organization-defined profiles. Netskope One Advanced Analytics also supports data tagging efforts by tracking the movement of organizational data across web and cloud environments. Finally, Netskope Cloud Exchange allows the above tools to generate and send alerts to the organization's SIEM or SOAR tools via the Cloud Log Shipper and Cloud Ticket Orchestrator. These tools integrate with cloud services such as Jira, ServiceNow, and other to automate remediation efforts and incident response.	• NG-SWG • CASB • DLP • Advanced DLP • Advanced Analytics • Cloud Exchange

Capability	Activity	Netskope Controls	Products
4.4 Data Monitoring and Sensing Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.	**4.4.1 DLP Enforcement Point Logging and Analysis** DoD Organizations identify data loss prevention (DLP) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Netskope security solutions, including CASB and NG-SWG, utilize the industry's most comprehensive Data Loss Prevention (DLP) engine to discover and classify organizational data across various environments such as web, cloud applications, and endpoint devices. SkopeAI enhances Netskope DLP with machine-learning classifiers, including optical character recognition, to identify and protect unstructured data such as images.	• NG-SWG • CASB • DLP • Skope AI
	4.4.2 DRM Enforcement Point Logging and Analysis DoD Organizations identify data rights management (DRM) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Netskope products are able to characterize SaaS, IaaS, and web usage across an entire enterprise including remote access connections to on-prem apps and services. This includes the monitoring of non- corporate devices accessing corporate SaaS applications and users accessing non-corporate SaaS applications from IT-managed devices. Netskope Device Intelligence catalogs and assigns risk scores to all managed and unmanaged devices connecting to the organization's network. Risky devices can be segregated in network microsegments. And Netskope Advanced Analytics allows organizations to track data flows across the organization, including to web and cloud services.	• NG-SWG • CASB • Private Access • Device Intelligence • Advanced Analytics
	4.4.3 File Activity Monitoring I DoD Organizations utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with basic data attributes to accomplish ZT Target functionality.	The Netskope One platform generates transaction log data across web, cloud, on prem, and device summarizing activity and reporting on this activity continuously. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• NG-SWG • CASB • Private Access • DLP • Cloud Exchange
	4.4.4 File Activity Monitoring II DoD Organizations utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.		

Capability	Activity	Netskope Controls	Products
	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.	Netskope products can protect organizational data stored in cloud-based infrastructure. Event logs and alerts can be exported to the organization's SIEM tool via Netskope Cloud Log Shipper, a feature of Netskope Cloud Exchange. The Netskope One platform also includes the ability to perform data loss prevention scans, which can alert on DLP violations and take corrective action. Netskope products can be configured to automatically revoke sharing permissions or encrypt a file, for example, if a file containing sensitive information is being shared excessively.	• CASB • DLP • Cloud Exchange • CLS
	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.		
4.5 Data Encryption and Rights Management DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection.	**4.5.1 Implement DRM and Protection Tools I** DoD Organizations procure and implement DRM and Protection solution(s) as needed following the DoD Enterprise standard and requirements. Newly implemented DRM and protection solution(s) are implemented with high risk data repositories using ZTA target level protections.	The Netskope One platform can identify and classify organizational data across web, cloud services, and endpoint devices. Granular and adaptive policy controls adjust privileges in real time based on risk. Netskope also integrates with DRM solutions like Box and Microsoft Purview Information Protection to enforce policies relating to content classification, access control, content encryption, file level security, and file level marking.	• All products
	4.5.2 Implement DRM and Protection Tools II DRM and protection coverage is expanded to cover all in scope data repositories. Encryption keys are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification.		
	4.5.3 DRM Enforcement via Data Tags and Analytics I Data rights management (DRM) and protection solutions are integrated with basic data tags defined by the DoD Enterprise standard. Initial data repositories are monitored and have protect and response actions enabled. Data at rest is encrypted in repositories.	Netskope CASB and NG-SWG leverage a powerful Data Loss Prevention (DLP) engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine-learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. It ensures real-time data protection through measures like obfuscation, encryption, and action blocking. Netskope also integrates with DRM solutions like Box and Microsoft Purview Information Protection to enforce policies relating to content classification, access control, content encryption, file level security, and file level marking security, and file level marking.	• NG-SWG • CASB • DLP
	4.5.4 DRM Enforcement via Data Tags and Analytics II 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.		

Capability	Activity	Netskope Controls	Products
	4.5.5 DRM Enforcement via Data Tags and Analytics III DRM and Protection solutions integrate with AI and ML tooling for encryption, rights management and protection functions..		
4.6 Data Loss Prevention DoD organizations utilize the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially the DLP solution is put into a "monitor only" mode to limit business impact and later using analytics is put into a "prevent" mode. Extended data tag attributes are used to feed the DLP solution and lastly integrate with ML and AI.	**4.6.1 Implement Enforcement Points** Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. DLP solution is set to “monitor-only” and/or “learning” mode limiting impact. DLP solution results are analyzed, and policy is fine tuned to manage risk to an acceptable level.	Netskope CASB and NG-SWG leverage a powerful data loss prevention (DLP) engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine-learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. It ensures real-time data protection through measures like obfuscation, encryption, and action blocking.	• NG-SWG • CASB • DLP
	4.6.2 DLP Enforcement via Data Tags and Analytics I Data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Basic data tags are utilized for DLP solution and logging schema is integrated.	Netskope NG-SWG and CASB can discover and classify managed and unmanaged apps and cloud services in the organization’s IT ecosystem, and enforce role-based access controls to protect data in use, in transit, and at rest. Netskope Advanced Analytics maps data flows across web and cloud services, assesses cloud risks, and categorizes data by its sensitivity. It also provides a dashboard for administrators to track security trends, including app usage, threats detected, policies triggered, and the number of affected users. Netskope DLP is fully integrated into the entire cloud platform, ensuring that data in use, at rest, and in transit are protected by the same set of policies and workflows. This ensures that policy is easy to implement and the DLP program is easy to maintain. Netskope SSPM continuously monitors organizations’ SaaS apps for security misconfigurations. Discovered misconfigurations and DLP violations can trigger alerts that can be exported to the organization’s SIEM or SOAR tools via Netskope Cloud Ticket Orchestrator, automating remediation efforts and incident response.	• NG-SWG • CASB • Advanced Analytics • DLP • SSPM • CTO
	4.6.3 DLP Enforcement via Data Tags and Analytics II Data loss prevention (DLP) solution is updated to include extended data tags based on parallel Automation activities.		
	4.6.4 DLP Enforcement via Data Tags and Analytics III Data loss prevention (DLP) solution is integrated with automated data tagging techniques to include any missing enforcement points and tags.		

Capability	Activity	Netskope Controls	Products
4.7 Data Access Control DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	**4.7.1 Integrate DAAS Access with SDS Policy I** Utilizing the DoD enterprise SDS policy, organizational DAAS policy is developed with intended integration in mind. SDS implementation guide is developed by DoD organizations due to environment specific nature. **4.7.2 Integrate DAAS Access with SDS Policy II** DoD Organizations implement the DAAS policy in an automated fashion. **4.7.3 Integrate DAAS Access with SDS Policy III** Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach should be taken during implementation to measure results and adjust accordingly.	Netskope NG-SWG can decode and log more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, upload, download, post, and delete. This visibility allows the organization to build a baseline of normal behavior for users and devices. Granular and adaptive policy controls can then give organizations the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. Activity controls can be implemented for both corporate-owned devices for web, SaaS, Shadow IT, and IaaS/PaaS, as well as personal devices accessing corporate-managed apps and cloud services. Netskope Private Access ensures that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access and inbound access rules. Finally, Netskope CSPM and SSPM continuously monitor the organization's IaaS platforms and SaaS apps for access misconfigurations, preventing configuration drift and ensuring that access permissions remain within organization-defined parameters.	• NG-SWG • CASB • DLP • Private Access • UEBA • Device Intelligence
	4.7.4 Integrate SDS Solution(s) and Policy with Enterprise IDP I DoD Organizations develop an integration plan using the SDS policy and technology/ functionality with the enterprise Identity Provider (IdP) solution.. **4.7.5 Integrate SDS Solution(s) and Policy with Enterprise IDP II** 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.	The Netskope One platform integrates with third-party identity providers like Okta, Ping, Google, and Microsoft to manage secure and secret authentication, extending SSO/MFA across web, managed and unmanaged apps, and cloud services. The Netskope One platform can also detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. When an action is detected, such as an upload of company data to a non-managed cloud service or application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user. Adaptive policy controls can also leverage Netskope Cloud Confidence Index (CCI) ratings for apps and Netskope User Confidence Index (UCI) risk scoring for the user to determine what is permitted.	• NG-SWG • CASB • Private Access • CCI • UEBA • UCI • Device Intelligence

Capability	Activity	Netskope Controls	Products
	4.7.6 Integrate SDS Tool and/or Integrate with DRM I 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.	Netskope CASB and NG-SWG leverage a powerful data loss prevention (DLP) engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine-learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. Netskope DLP is fully integrated into the entire cloud platform, ensuring that data in use, at rest, and in motion are protected by the same set of policies and workflows. This ensures that policy is easy to implement and the DLP program is easy to maintain.	• NG-SWG • CASB • DLP
	4.7.7 Integrate SDS Solution(s) and Policy with Enterprise IDP II 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.		

5. NETWORK AND ENVIRONMENT

Capability	Activity	Netskope Controls	Products
5.1 Data Flow Mapping DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.	**5.1.1 Define Granular Control Access Rules and Policies I** The DoD Enterprise working with the Organizations creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies as well ensure future supportability. Once agreed upon, DoD Organizations will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels.	Netskope Advanced Analytics maps data flows across web and cloud services, assesses cloud risks, and categorizes data by its sensitivity. It also provides a dashboard for administrators to track security trends, including app usage, threats detected, policies triggered, and the number of affected users. Advanced Analytics can also be used to assess trends and assist in identifying potential adverse events and anomalies. Netskope products, including NG-SWG, CASB, and Private Access, provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. Moreover, Netskope SaaS Security Posture Management (SSPM) continuously monitors the organization's SaaS apps for misconfigurations, ensuring that access controls remain within organization-defined parameters. Netskope SD-WAN extends the organization's security perimeter to any user on any device, anywhere. Traffic steered to Netskope NewEdge Network can be subjected to a uniform set of DLP and security policies.	• Advanced Analytics • NG-SWG • CASB • Private Access • SSPM • DLP • SD-WAN
	5.1.2 Define Granular Control Access Rules and Policies II DoD Organizations utilize data tagging and classification standards to develop data filters for API access to the SDN Infrastructure. API Decision Points are formalized within the SDN architecture and implemented with non-mission/task critical applications and services.		
5.2 Software Defined Networking DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real time decision making for access to resources.	**5.2.1 Define SDN APIs** The DoD Enterprise works with the Organizations to define the necessary APIs and other programmatic interfaces to enable Software Defined Networking (SDN) functionalities. These APIs will enable Authentication Decision Point, Application Delivery Control Proxy and Segmentation Gateways automation.	Netskope SD-WAN supports network segmentation, and extends the organization's security perimeter to any user on any device, anywhere. Traffic steered to Netskope NewEdge Network can be subjected to a uniform set of security policies. The Netskope One platform generates transaction log data across web, cloud, on prem, and device summarizing activity and reporting on this activity continuously. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms). Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• SD-WAN
	5.2.2 Implement SDN Programmable Infrastructure Following the API standards, requirements and SDN API functionalities, DoD Organizations will implement Software Defined Networking (SDN) infrastructure to enable automation tasks. Segmentation Gateways and Authentication Decision Points are integrated into the SDN infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.		

Capability	Activity	Netskope Controls	Products
	5.2.3 Segment Flows into Control Management and Data Plan Network infrastructure and flows are segmented either physically or logically into control, management, and data planes. Basic segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure is automatically fed into Operations Centers and analytics tools.		
	5.2.4 Network Asset Discovery and 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.		
	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.		
5.3 Macro Segmentation DoD organizations establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.	**5.3.1 Datacenter Macro Segmentation** DoD Organizations implement data center focused macrosegmentation using traditional tiered (web, app, db) and/or service based architectures. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	Netskope Private Access, FWaaS, and SD-WAN support network segmentation. Private Access also uses granular and adaptive controls to enforce security and privacy policies by ensuring remote users only have access to private apps they have been provisioned, can only carry out authorized actions within those apps, and may be required to re-authenticate where risky or anomalous behavior indicates a potential security incident. Netskope UEBA and Device Intelligence provide further support, enabling the organization to isolate risky users or devices in real time based on behavioral attributes.	• Private Access • FWaaS • SD-WAN • UEBA • Device Intelligence
	5.3.2 B/C/P/S Macro Segmentation DoD Organizations implement base, camp, post, and station macrosegmentation using logical network zones limiting lateral movement. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.		

Capability	Activity	Netskope Controls	Products
5.4 Micro Segmentation DoD organizations define and document network segmentation based on identity and / or application access in their virtualized and/ or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly where possible organizations will utilize host-level process micro segmentation.	**5.4.1 Implement Micro Segmentation** DoD Organizations implement Micro-Segmentation infrastructure into SDN environments enabling basic segmentation of service components (e.g., web, app, db), ports and protocols. Basic automation is accepted for policy changes including API decision making. Virtual hosting environments implement micro-segmentation at the host/container level.	Netskope Private Access, FWaaS, and SD-WAN support network segmentation. Private Access also uses granular and adaptive controls to enforce security and privacy policies by ensuring remote users only have access to private apps they have been provisioned, can only carry out authorized actions within those apps, and may be required to re-authenticate where risky or anomalous behavior indicates a potential security incident. Furthermore, Netskope SSE, including its CASB, NG-SWG, DLP, and Private Access, all support role based access control (RBAC) to enforce organizational access management policies based on the principle of least privilege.	• NG-SWG • CASB • DLP • Private Access • FWaaS • SD-WAN
	5.4.2 Application & Device Micro Segmentation DoD Organizations utilize Software Defined Networking (SDN) solution(s) to establish infrastructure meeting the ZT Target functionalities – logical network zones, role, attribute and conditional based access control for user and devices, privileged access management services for network resources, and policy-based control on API access.		
	5.4.3 Process Micro Segmentation DoD Organizations utilize existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Hostlevel processes are segmented based on security policies and access is granted using real-time access decision making.	Netskope Private Access, and UEBA provide real-time security controls that can isolate risky users or devices in network microsegments based on organization-defined criteria.	• Private Access • UEBA
	5.4.4 Protect Data in Transit Based on the data flow mappings and monitoring, policies are enabled by DoD Organizations to mandate protection of data in transit. Common use cases such as Coalition Information Sharing, Sharing Across System Boundaries and Protection across Architectural Components are included in protection policies.	Netskope Private Access, FWaaS, and SD-WAN support network microsegmentation.	• Private Access • SD-WAN • FWaaS

6. AUTOMATION AND ORCHESTRATION

Capability	Activity	Netskope Controls	Products
6.1 PDP and Orchestration DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	**6.1.1 Policy Inventory & Development** The DoD Enterprise works with the Organizations to catalog and inventory existing Cyber Security policies and standards. Policies are updated and created in cross pillar activities as needed to meet critical ZT Target functionality.	Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Netskope SD-WAN enables organizations to extend their network perimeter to any user on any device, anywhere, utilizing Netskope global NewEdge Network for high-availability connectivity to web and cloud applications. It ensures uniform policy controls and adaptive trust based on specific criteria like user, location, and device. Furthermore, Netskope SSPM continuously monitors the organization's SaaS apps, ensuring access controls' consistent adherence with organizational policy. Netskope FWaaS enforces security policies on egress traffic and disrupts DNS attacks while integrating event logs with SIEM tools for incident response.	• NG-SWG • CASB • DLP • SD-WAN • SSPM • FWaaSI
	6.1.2 Organization Access Profile DoD Organizations develop basic access profiles for mission/task and non-mission/task DAAS access using the data from the User, Data, Network, and Device pillars. The DoD Enterprise works with the Organizations to develop an Enterprise Security Profile using the existing Organizational security profiles to create a common access approach to DAAS. A phased approach can be used in organizations to limit risk to mission/task critical DAAS access once the security profile(s) are created.	The Netskope platform supports role based access controls for privileged and regular users, and can adjust privileges in real time based on user behavior with granular, context-aware controls that assess the riskiness of user actions and respond accordingly to protect organizational networks and data. Moreover, Netskope SSPM continuously monitors the organization's SaaS applications for misconfigurations, ensuring that access controls remain within organization-defined parameters. Netskope FWaaS enforces security policies on egress traffic and disrupts DNS attacks while integrating event logs with SIEM tools for incident response.	• NG-SWG • CASB • Private Access • SSPM • FWaaS

Capability	Activity	Netskope Controls	Products
	6.1.3 Enterprise Security Profile I The Enterprise Security profile covers the User, Data, Network and Device pillars initially. Existing Organizational Security Profiles are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Netskope SD-WAN enables organizations to extend their network perimeter to any user on any device, anywhere, utilizing Netskope global NewEdge Network for high-availability connectivity to web and cloud applications. It ensures uniform policy controls and adaptive trust based on specific criteria like user, location, and device. Furthermore, Netskope SSPM continuously monitors the organization's SaaS apps, ensuring access controls' consistent adherence with organizational policy Netskope FWaaS enforces security policies on egress traffic and disrupts DNS attacks while integrating event logs with SIEM tools for incident response.	• NG-SWG • CASB • DLP • SD-WAN • SSPM • FWaaS
	6.1.4 Enterprise Security Profile II 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.		
6.2 Critical Process Automation DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.	**6.2.1 Task Automation Analysis** DoD Organizations identify and enumerate all task activities that can be executed both manually and in an automated fashion. Task activities are organized into automated and manual categories. Manual activities are analyzed for possible retirement.	The Netskope One platform makes it easy to implement cybersecurity policies, as well as automate the process of detecting and remediating any deviations from established policy. For example, Netskope CASB and NG-SWG can detect both managed and unmanaged apps in use in the organization's IT ecosystem, and its Cloud Confidence Index can assign them risk scores that can be calibrated to the organization's specific risk tolerances. Netskope UEBA assigns users a User Confidence Index based on the riskiness of each user's behavior. Both the CCI and UCI can be leveraged to automatically block access to certain apps, or certain actions within an app. Private Access provides secure access for remote users to private applications. Using zero trust principles, Private Access applies granular and adaptive controls to continuously and automatically and adjust access privileges in real time. The Netskope One platform generates transaction log data across web, cloud, on prem, and device summarizing activity and reporting on this activity continuously. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently.	• All products
	6.2.2 Enterprise Integration & Workflow Provisioning I The DoD enterprise establishes baseline integrations within the Security Orchestration, Automation and Response solution (SOAR) required to enable target level ZTA functionality. DoD organizations identify integration points and prioritize key ones per the DoD enterprise baseline. Critical integrations occur meeting key services enabling recovery and protection capabilities.		
	6.2.3 Enterprise Integration & Workflow Provisioning II 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.		

Capability	Activity	Netskope Controls	Products
		Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real-time.	
6.3 Machine Learning DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	**6.3.1 Implement Data Tagging & Classification ML Tools** DoD Organizations utilize existing Data Tagging and Classification standards and requirements to procure machine-learning solution(s) as needed. machine-learning solution(s) is implemented in organizations and existing tagged and classified data repositories are used to establish baselines. machine-learning solution(s) applies data tags in a supervised approach to continually improve analysis.	The Netskope One platform can help identify any ML-based apps or cloud services currently in use in the organization's IT ecosystem. It can also assist in procurement decisions. Netskope Cloud Confidence Index scores apps and cloud services, including ML-based apps, according to risk The Netskope One platform also includes data protection capabilities to include the improvement of labeling, classifying, and categorizing data consumed by AI systems. In addition, data can be automatically labeled or fingerprinted to determine if it's training, validation data, or from a testing data set. Additional controls include limiting data if it is shared from a specific geographical location or if contextual and/or behavioral changes have taken effect through its lifecycle. Netskope Threat Protection uses ML and AI to detect new forms of malware, while Device Intelligence uses ML and AI to establish a baseline for devices connecting to the organization's network, detect anomalies, and segregate risky devices in network microsegments. Netskope UEBA also uses ML and AI to build a baseline of normal behavior for each user, and computes a User Confidence Index (UCI) that can be leveraged to automatically adjust privileges in response to risky or anomalous behavior.	• NG-SWG • CASB • DLP • Advanced Threat Protection • UEBA • UCI • GenAI Security

Capability	Activity	Netskope Controls	Products
6.4 Artificial Intelligence DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.	**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.	Netskope SSE incorporates AI into many of its components. For example, Netskope UEBA uses AI to build a baseline of normal user behavior in order to detect anomalies and adjust access privileges based on risk. And its DLP uses AI to identify and classify not just many common, predefined types of data, but also allows customers to train the DLP to recognize customized classifiers for enhanced, tailored data protection. Finally, event logs and alerts generated by Netskope AI-powered tools can be exported to the organization's SIEM or SOAR tools to facilitate automated incident response and remediation. In addition, Netskope products can assess and evaluate new risks from cloud-based services during evaluation or PoC stage of procurement. Using Netskope SSPM or even CCI for cloud services, improvements can be recommended prior to procurement or go-live of new service. Ongoing, continuous security checks can also be performed.	• NG-SWG • CASB • DLP • CCI • SSPM • UEBA
	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.	The Netskope One platform leverages a powerful DLP engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine-learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. Moreover, Netskope leverages machine-learning and artificial intelligence to help identify new anomalies or security events based on previous incidents.	• All products
6.5 Security Orchestration, Automation, and Response DoD organizations achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability	**6.5.1 Response Automation Analysis** DoD Organizations identify and enumerate all response activities that are executed both manually and in an automated fashion. Response activities are organized into automated and manual categories. Manual activities are analyzed for possible retirement.	The Netskope One platform generates transaction log data across web, cloud, onprem, and devices, summarizing activity and reporting on this activity continuously. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently.	• All products

Capability	Activity	Netskope Controls	Products
management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	**6.5.2 Implement SOAR Tools** DoD enterprise working with Organizations develops a standard set of requirements for security orchestration, automation, and response (SOAR) tooling to enable target level ZTA functions. DoD Organizations use approved requirements to procure and implement SOAR solution. Basic infrastructure integrations for future SOAR functionality is completed..	Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real-time.	• Cloud Exchange • CLS • CTO
	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.	The Netskope One platform does not map to this requirement.	
6.6 API Standardization DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.	**6.6.1 Tool Compliance Analysis** Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise programmatic interface standard and requirements. Any additional tooling or solutions are identified to support the programmatic interface standards and requirements.	Netskope products score SaaS applications in its Cloud Confidence Index (CCI) and provide many important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	• CASB • CCI
	6.6.2 Standardized API Calls & Schemas I The DoD enterprise works with organizations to establish a programmatic interface (e.g., API) standard and requirements as needed to enable target ZTA functionalities. DoD Organizations update programmatic interfaces to the new standard and mandate newly acquired/ developed tools to meet the new standard. Tools unable to meet the standard are allowed by exception using a risk based methodical approach.	The Netskope One platform does not map to these requirements.	
	6.6.3 Standardized API Calls & Schemas II DoD Organizations complete the migration to the new programmatic interface standard. Tools marked for decommission in the previous activity are retired and functions are migrated to modernized tools. Approved schemas are adopted based on the DoD Enterprise standard/ requirements.		

Capability	Activity	Netskope Controls	Products
6.7 SOC and Incident Response In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	**6.7.1 Workflow Enrichment I** DoD Enterprise works with organizations to establish a cybersecurity incident response standard using industry best practices such as NIST. DoD Organizations utilize the enterprise standard to determine incident response workflows. External sources of enrichment are identified for future integration.	Netskope products can help with incident report creation, providing context to improve triage response times and mitigation through reporting and Advanced Analytics. Netskope products can integrate with the customer's SIEM via near real-time transaction event streaming, Cloud Log Shipper, and SOAR tools with Netskope Cloud Ticket Orchestrator (CTO), which can generate alerts or tickets based on incident notifications from Netskope. Reports can be directly generated on notification from SIEM and SOAR systems and investigated via the Netskope console.	• SASE • Advanced Analytics • Cloud Exchange
	6.7.2 Workflow Enrichment II DoD organizations identify and establish extended workflows for additional incident response types. Initial enrichment data sources are used for existing workflows. Additional enrichment sources are identified for future integrations.		
	6.7.3 Workflow Enrichment III DoD organizations use final enrichment data sources on basic and extended threat response workflows.		
	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.	The Netskope One platform can enforce security policies defined by the organization. It generates event and alert logs that can be exported to the organization's SOAR tool to facilitate automated incident response. Netskope Cloud Ticket Orchestrator (CTO) allows customers to map customer alerts, events, and log data into whatever format is required to facilitate automated workflows in ServiceNow, Jira, and PagerDuty, or notifications in Slack, Teams, Email, etc. Initiating incident recovery is supported across the Netskope SASE service stack including SSE and SD-WAN services, enabling organizations to recover quickly without the need to replace hardware or services impacted by the incident.	• NG-SWG • CASB • DLP • Cloud Exchange • CTO • Advanced Analytics

7. VISIBILITY AND ANALYTICS

Capability	Activity	Netskope Controls	Products
7.1 Log All Traffic DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	**7.1.1 Scale Considerations** DoD Organizations conduct analysis to determine current and future needs of scaling. Scaling is analyzed following common industry best practice methods and ZT Pillars. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DPR) groups to determine distributed environment needs in emergencies and as organizations grow.	Netskope NewEdge Network implements a high-availability cloud-based architecture, allowing operations to continue in the event of a failure at any node including the ability to both scale up and scale down on demand. The Netskope platform also allows IT admins to audit web and cloud usage, and define policies to ensure logs are centrally managed. Netskope SSPM continuously monitors the organization's SaaS apps to guard against security misconfigurations. Alerts generated by SSPM can be exported to the organization's SIEM tool via Netskope Cloud Log Shipper, and Netskope Cloud Ticket Orchestrator can be leveraged to generate service tickets and automate remediation efforts.	• All products • SSPM • CLS • CTO
	7.1.2 Log Parsing DoD Organizations identify and prioritize log and flow sources (e.g., Firewalls, Endpoint Detection & Response, Active Directory, Switches, Routers, etc.) and develop a plan for collection of high priority logs first then low priority. An open industry-standard log format is agreed upon at the DoD Enterprise level with the Organizations and implemented in future procurement requirements. Existing solutions and technologies are migrated to the format on a continual basis.	The Netskope One platform generates transaction log data across web, cloud, on prem, and device, summarizing activity and reporting on this activity continuously. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently. Netskope Cloud Log Shipper can export events and alert logs directly to the organization's SIEM tool to support log parsing.	• All products • CLS
	7.1.3 Log Analysis Common user and device activities are identified and prioritized based on risk. Activities deemed the most simplistic and risky have analytics created using different data sources such as logs. Trends and patterns are developed based on the analytics collected to look at activities over longer periods of time.	Netskope NG-SWG, CASB, and Private Access can decode and log more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, upload, download, post, and delete. This visibility allows the organization to build a baseline of normal behavior for users and devices, which can then be leveraged to detect anomalies and alert on potential security incidents.	• NG-SWG • CASB • Private Access

Capability	Activity	Netskope Controls	Products
7.2 Security Information and Event Management (SIEM) Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines, etc.).	**7.2.1 Threat Alerting I** DoD Organizations utilize existing Security Information and Event Management (SIEM) solutions to develop basic rules and alerts for common threat events (malware, phishing, etc.). Alerts and/or rule firings are fed into the parallel "Asset ID & Alert Correlation" activity to begin automation of responses.	Netskope Advanced Threat Protection can detect external malware/ ransomware from web and cloud services and can analyze to block in real time. Netskope provides detailed analysis of the malware type, which can help organizations understand the types of threats and threat actors impacting their organization. Netskope Cloud Threat Exchange (CTE) and Cloud Risk Exchange (CRE) can keep an organization up to date with respect to particular cyber threats (including IoCs, malicious URLs, and malicious file hashes), and overall risk scores for users, devices, and apps in an ICT ecosystem. Netskope products can be configured to collate and report on events and generate alerts on a series of suspicious events. Netskope has built-in ticketing systems, log analysis, forensic reporting, and advanced analytics capabilities to help an organization in the event of a security incident. Netskope products can help with incident report creation, providing context to improve triage response times and mitigation through reporting and Advanced Analytics.	• NG-SWG • CASB • Private Access • Advanced Threat Protection • Advanced Analytics • GenAI Security • Cloud Exchange • UEBA • Device Intelligence
	7.2.2 Threat Alerting II DoD Organizations expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats.		
	7.2.3 Threat Alerting III 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.		
	7.2.4 Asset ID & Alert Correlation DoD Organizations develop basic correlation rules using asset and alert data. Response to common threat events (e.g., malware, phishing, etc.) are automated within the Security Information and Event Management (SIEM) solution.	Netskope products can integrate with the customer's SIEM via near real-time transaction event streaming, Cloud Log Shipper, and SOAR tools with Netskope Cloud Ticket Orchestrator (CTO), which can generate alerts or tickets based on incident notifications from Netskope. Reports can be directly generated on notification from SIEM and SOAR systems and investigated via the Netskope console.	
	7.2.5 User/Device Baselines DoD Organizations develop user and device baseline approaches based on DoD Enterprise standards for the appropriate pillar. Attributes utilized in baselining are pulled from the enterprise wide standards developed in cross pillar activities.	Netskope UEBA uses machine-learning to develop a baseline for each user's normal behavior, and includes the User Confidence Index that scores each user based on the riskiness of their actions. Netskope Device Intelligence also creates a baseline for each device's behavior and can isolate risky devices in network microsegments.	• UEBA • Device Intelligence

Capability	Activity	Netskope Controls	Products
7.3 Common Security and Risk Analysis Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	**7.3.1 Implement Analytics Tools** DoD Organizations procure and implement basic Cyber-focused analytics tools. Analytics development is prioritized based on risk and complexity looking for easy impactful analytics first. Continued analytics development focuses on Pillar requirements to better meet reporting needs.	Netskope Advanced Analytics maps organizational data flows, categorizing data by sensitivity and assessing cloud app risks. Its dashboard tracks security trends, including apps accessed, threats detected, policies triggered, and users impacted.	• Advanced Analytics
	7.3.2 Establish User Baseline Behavior Utilizing the analytics developed for users and devices in a parallel activity, baselines are established in a technical solution. These baselines are applied to an identified set of users based on risk initially and then expanded to the larger DoD Organization user base. The technical solution used is integrated with machine-learning functionality to begin automation.	Netskope UEBA employs machine-learning models to detect anomalies. It includes the User Confidence Index (UCI), a risk score based on user behavior, which helps adapt policies, controls, and recommend security training to mitigate insider threats. The UCI can also integrate with Netskope Cloud Exchange to share insider threat information across platforms. Netskope Device Intelligence identifies and categorizes all managed and unmanaged devices connecting to the organization's network, and also creates a baseline for each device's behavior.	• UEBA • Device Intelligence
7.4 User & Entity Behavior Analytics (UEBA) DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	**7.4.1 Baseline & Profiling I** Utilizing the analytics developed for users and devices in a parallel activity, common profiles are created for typical user and device types. Analytics taken from baselining are updated to look at larger containers, profiles.	Netskope UEBA employs advanced machine-learning models to detect anomalies. It includes the User Confidence Index (UCI), a risk score based on user behavior, which helps adapt policies and controls, and recommends security training to mitigate insider threats. The UCI can also integrate with Netskope Cloud Exchange to share insider threat information across platforms. Netskope Device Intelligence identifies and categorizes all managed and unmanaged devices connecting to the organization's network, and also creates a baseline for each device's behavior and can isolate risky devices in network microsegments.	• UEBA • UCI • Device Intelligence
	7.4.2 Baseline & Profiling II 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 responses. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.		

Capability	Activity	Netskope Controls	Products
	7.4.3 UEBA Baseline Support I 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.	Netskope UEBA employs advanced machine-learning models to detect anomalies. It includes the User Confidence Index (UCI), a risk score based on user behavior, which helps adapt policies and controls, and recommends security training to mitigate insider threats. The UCI can also integrate with Netskope Cloud Exchange to share insider threat information across platforms.	• UEBA • UCI
	7.4.4 UEBA Baseline Support II 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.		
7.5 Threat Intelligence Integration Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM.	**7.5.1 Cyber Threat Intelligence Program I** The DoD Enterprise works with the Organizations to develop aCyber Threat Intelligence (CTI) program policy, standard and process. Organizations utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI Teams integrate common feeds of data with the Security Information and Event Management (SIEM) for improved alerting and response. Integrations with Device and Network enforcement points (e.g., Firewalls, Endpoint Security Suites, etc.) are created to conduct basic monitoring of CTI driven data.	Netskope Cloud Threat Exchange is a tool for near real-time threat ingestion, curation, and sharing. It enables Netskope customers and partners to bidirectionally share indicators of compromise (IoCs) like malicious URLs and file hashes, and can be configured to automatically share IoCs with an organization's SIEM tool.	• Cloud Exchange • CTE
	7.5.2 Cyber Threat Intelligence Program II DoD Organizations expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Authenticated, private and controlled CTI data feeds are integrated into Security Information and Event Management (SIEM) and enforcement points from the Device, User, Network and Data pillars.		

Capability	Activity	Netskope Controls	Products
7.6 Automated Dynamic Policies DoD Organization ML & AI solutions dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	**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.	Netskope Private Access allows secure access to managed cloud applications, with end-to-end encryption, for remote users. Granular and adaptive controls adjust access privileges based on user, device type, app instance, and other risk-based criteria. Netskope Device Intelligence catalogs all managed and unmanaged devices on the network, isolates risky devices, and uses AI/ML to establish normal device behavior and detect anomalies. It applies granular controls to enforce zero trust principles, and integrates with incident response tools to trigger security alerts based on organizational criteria. Netskope SSE and SD-WAN for Endpoint extend reliable and secure network access to managed and unmanaged devices, using granular, context-aware controls that authorize access on the basis of continuously adaptive trust.	• Private Access • Device Intelligence • SD-WAN
	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 decisions to various resources. The “AI-enabled Network Access” activity algorithms are updated to enable broader decision making to all DAAS.	Netskope NG-SWG, CASB, and Private Access provide detailed logging of all web, cloud and on-prem access activity by users, including inline app and cloud service API-level. Netskope UEBA can use this data, in combination with sequential anomaly rules across apps and cloud services, in order to detect and block risky actions. Netskope UEBA deploys machine-learning algorithms to detect anomalous behavior, and assigns each user a User Confidence Index (UCI) based on the riskiness of their actions. UCI can be leveraged to create adaptive access controls that adjust privileges in real time.	• NG-SWG • CASB • Private Access • UEBA

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs. Visit netskope.com.