netskope

Compliance Series

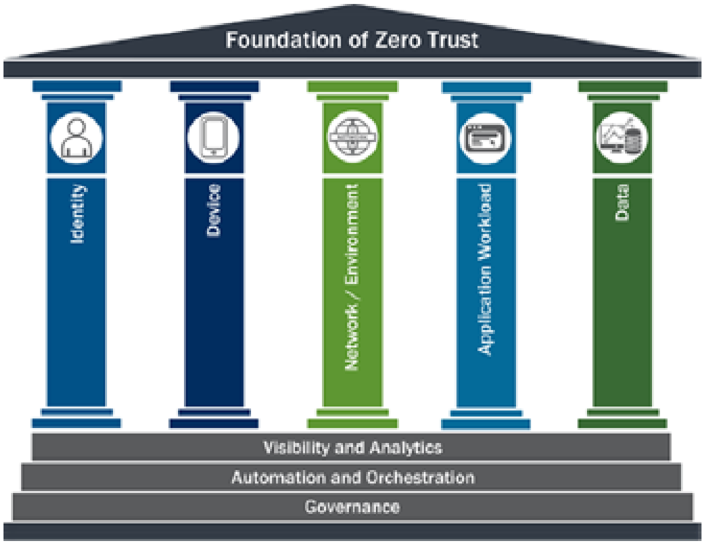
Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model 2.0 (CISA ZTMM 2.0)

Control Mapping to Netskope Products

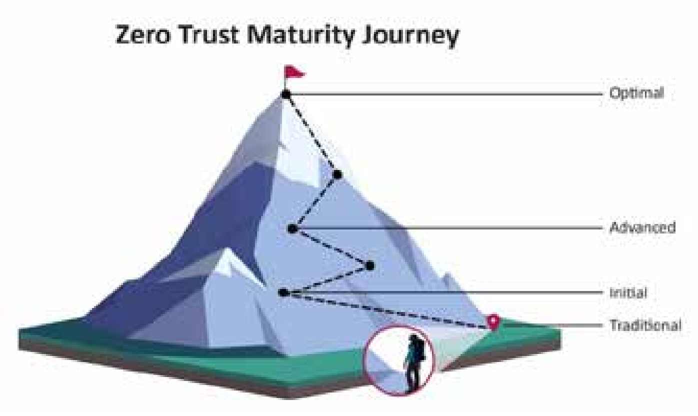
TABLE OF CONTENTS

The Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model (CISA ZTMM) is a framework for helping organizations gradually shift their operations in the direction of a cybersecurity posture that fully embraces zero trust principles. It consists of five "pillars": Identity, Devices, Networks, Applications and Workloads, and Data. The five pillars are supported by three sets of "cross-cutting capabilities"—Visibility and Analytics, Automation and Orchestration, and Governance.

Each pillar consists of a set of functions. For example, the first function of the Identity pillar is Authentication. In turn, each function is broken down into "maturity levels," which begin at **Traditional** and progress through **Initial** and **Advanced** until they reach **Optimal**. Each cross-cutting capability is also broken down by maturity levels.



Source: CISA Zero Trust Maturity Model 2.0



Source: CISA Zero Trust Maturity Model 2.0

Each table in this guide corresponds to one of the five ZTMM pillars, with a final table for the three cross-cutting capabilities. The tables are further broken down by function and maturity level, along with a description of Netskope products and capabilities and an indication of the maturity level they satisfy or support.

The Netskope platform can help support Optimal compliance with 40 out of 40 functions depending on the product used and the policy configuration and automation applied. With the Netskope platform in place, organizations can further progress their zero trust maturity journey.

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

Industry Terminology	Netskope Product Line/Abbreviation
Security Access Service Edge	SASE
Security Service Edge	SSE
Next Gen Secure Web Gateway	NG-SWG
Cloud Access Security Broker	CASB
Zero Trust Network Access	ZTNA Next
SaaS Security Posture Management	SSPM
Data Security Posture Management	CSPM
Data Loss Prevention	DLP (Standard & Advanced)
Firewall as a Service	Cloud Firewall
Reporting and Analytics	Advanced Analytics
Threat Intelligence	Threat Protection (Standard & Advanced)
Remote Browser Isolation	RBI
Artificial Intelligence Security	SkopeAI
Software-Defined Wide Area Network (SD-WAN)	SD-WAN Secure SD-WAN SD-WAN for Endpoint Wireless SD-WAN IoT Intelligent Access
Threat/Risk Sharing	Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

1. IDENTITY

Function	Maturity Level	Netskope Controls	Products
Authentication	Traditional: Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.	Netskope products can extend existing agencies SAML (SSO/MFA) across web, managed and unmanaged apps and cloud services, and continuously validates user identities through granular, context-aware policies. NG-SWG, CASB, and Private Access can detect more than 100 inline actions within cloud services and SaaS applications and support secure remote access, 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's User Confidence Index (UCI), a feature of Netskope's Advanced User and Entity Behavior Analytics (UEBA), to determine what is permitted. Furthermore, Netskope's SaaS Security Posture Management continuously monitors essential SaaS applications for access misconfigurations, and offers step-by-step instructions for remediation. It also integrates with Netskope's Cloud Ticket Orchestrator for automated remediation, and converts remediated configurations into new security rules.	• NG-SWG • CASB • Private Access • SSPM • UEBA • CTO
	Initial: Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).		
	Advanced: Agency begins to authenticate all identities using phishing-resistant MFA and attributes, including initial implementation of password-less MFA via FIDO222 or PIV.		
	Optimal: Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.		
Identity Stores	Traditional: Agency only uses self managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Netskope NG-SWG, CASB, and Private Access provide auditing and verification of user identities and credentials. By integrating with third-party identity providers like Okta and Ping to extend SSO/MFA across the web and managed and unmanaged cloud services, the Netskope platform facilitates the secure integration of identity stores across all partners and environments. Furthermore, the Netskope platform also provides detailed event logging that captures user identity, organizational unit, device, app instance, and actions performed, such as upload, download, delete, or share. This detailed level of logging can assist organizations in asserting non-repudiation of user actions in web, cloud, and on-prem applications. Finally, Netskope's SaaS Security Posture Management provides security configuration, auditing, compliance, and company checks for user identities in cloud services and managed SaaS apps.	• NG-SWG • CASB • Private Access • SSPM
	Initial: Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign On).		
	Advanced: Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.		
	Optimal: Agency securely integrates their identity stores across all partners and environments as appropriate.		

Function	Maturity Level	Netskope Controls	Products
Risk Assessments	Traditional: Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised). Initial: Agency determines identity risk using manual methods and static rules to support visibility. Advanced: Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities. Optimal: Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.	Netskope's User and Entity Behavior Analytics (UEBA) tracks user behavior and sets baselines to detect anomalies. The Advanced UEBA uses multiple ML-based models to offer a dynamic, risk-based User Confidence Index, aiding in insider threat detection and adapting security policies in real time. Netskope's CASB, NG-SWG, and Private Access provide real-time monitoring, logging, and activity-level controls on SaaS and IaaS services, enabling data loss prevention and establishing user behavior baselines to detect anomalies and apply context-aware controls such as advanced authentication or policy training. Private Access affords access only to those apps or services the user needs, and uses context-aware controls to continuously verify user identity Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope to IdP services to automatically restrict access in the event of an incident..	• NG-SWG • CASB • UEBA • Private Access • CRE
Access Management	Traditional: Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts. Initial: Agency authorizes access, including for privileged access requests, that expires with automated review. Advanced: Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources. Optimal: Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.	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. This is based on zero trust principles. 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 • SSPM • Device Intelligence

Function	Maturity Level	Netskope Controls	Products
Visibility and Analytics Capability	Traditional: Agency collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.	Netskope's Advanced Analytics allows organizations to perform automated analysis on trends in activity and support policy automation. Netskope's User and Entity Behavior Analytics (UEBA) analyzes user behavior and sets baselines to detect anomalies. The Advanced UEBA uses multiple ML-based models to offer a dynamic User Confidence Index, aiding in insider threat detection and adapting security policies accordingly. Netskope's NG-SWG and CASB can decode and log over 100 inline user actions (such as share, edit, delete, upload, download, etc.) across web and cloud services. Cloud Exchange can be leveraged to extend and share activity data across an ecosystem of network and security tools. Moreover, event logs and alerts can be exported to the organization's SIEM or SOAR tools using Netskope's Cloud Log Shipper, and the Cloud Ticket Orchestrator can automate incident response and remediation efforts. Threat protection and DLP components are also used to identify activities that may be malicious such as intentionally downloading malicious code or attempting to exfiltrate data.	• NG-SWG • CASB • Threat Protection • DLP • Advanced Analytics • UEBA • Cloud Exchange • CLS • CTO
	Initial: Agency collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.		
	Advanced: Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.		
	Optimal: Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.		
Automation and Orchestration Capability	Traditional: Agency manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review.	Netskope's User and Entity Behavior Analytics includes the User Confidence Index, which leverages machine learning to develop a baseline of normal behavior for each user, as well as assess the riskiness of each user's behavior. Anomalous or excessively risky behavior can trigger real-time adjustment to access privileges, as well as referring users for training on cyber hygiene or organizational policy. Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope to IdP services to automatically restrict access in the event of an incident. The Netskope platform integrates with third-party identity providers like Okta, Ping, Google, and Microsoft to manage secure and secret authentication, including support for SAML, SSO, and MFA. 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's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• NG-SWG • CASB • UEBA • Cloud Exchange • CLS • CTO • CRE
	Initial: Agency manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities.		
	Advanced: Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.		
	Optimal: Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.		

Function	Maturity Level	Netskope Controls	Products
Governance Capability	Traditional: Agency implements identity policies (authentication, credentials, access, lifecycle, etc.) with enforcement via static technical mechanisms and manual review.	Netskope products extend SSO/MFA across the web as well as managed and unmanaged apps and cloud services. NG-SWG and CASB enforce role based access control (RBAC) that offers segregation of duties and areas of responsibility for the administration of networks and cloud, web, and private applications. And Private Access allows end-to-end encryption for remote users connecting to managed apps. Private Access affords access only to those apps or services the user needs, and uses context-aware controls to continuously verify user identity. Netskope's User and Entity Behavior Analytics includes the User Confidence Index, which leverages machine learning to develop a baseline of normal behavior for each user, as well as assess the riskiness of each user's behavior. Anomalous or excessively risky behavior can trigger real-time adjustment to access privileges, as well as referring users for training on cyber hygiene or organizational policy. Netskope's SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's SD-WAN, traffic is steered through Netskope's global New Edge Network, allowing enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more.	• NG-SWG • CASB • Advanced Analytics • SD-WAN • Private Access • UEBA
	Initial: Agency defines and begins implementing identity policies for enterprise-wide enforcement with minimal automation and manual updates.		
	Advanced: Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.		
	Optimal: Agency implements and fully automates enterprise-wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.		

2. DEVICES

Function	Maturity Level	Netskope Controls	Products
Policy Enforcement and Compliance Monitoring	Traditional: Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Netskope's CASB, NG-SWG, and Private Access can identify device posture and limit or control access to services based on this posture. Netskope's SSPM continuously monitors an organization's SaaS platforms, and can alert when configuration deviates from the baseline This is relevant to this control if the SaaS service identifies as a virtual asset. Netskope Device Intelligence can be leveraged to identify hardware (including IoT, OT, and traditional devices) and manage devices and connectivity, useful for rogue or EOL devices.	• NG-SWG • CASB • SSPM • Device Intelligence
	Initial: Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.		
	Advanced: Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.		
	Optimal: Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.		
Asset and Supply Chain Risk Management	Traditional: Agency does not track physical or virtual assets in an enterprise-wide or cross-vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Netskope's CASB and NG-SWG provide a real-time catalog of apps and cloud services in the organization's IT environment, and the Cloud Confidence Index (CCI) assigns each app a risk-based score. Together, these capabilities can help the organization identify critical cloud applications and service providers. CCI also provides 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. Organizations can change the default CCI score by giving more or less weight to different criteria based on their importance to the organization, and then compare apps side by side to determine which better meets the organization's compliance needs. Policies can also be customized to block apps, or certain actions within apps, based on their CCI score.	• NG-SWG • CASB • CCI • SSPM
	Initial: Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework (e.g., NIST SCRM.)		
	Advanced: Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.		

Function	Maturity Level	Netskope Controls	Products
	Optimal: Agency has a comprehensive, at- or near real-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.	Using SaaS Security Posture Management, improvements can be recommended prior to go-live of any new service, and continuous monitoring can be performed to ensure that the organization's SaaS services maintain secure configurations.	
Resource Access	Traditional: Agency does not require visibility into devices or virtual assets used to access resources.	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. IT and Security teams are able to map communication and data flows to an exceptional degree of accuracy. Netskope will not only map where data is flowing, including for company and personal app instances, but also provide the necessary controls to contain data flows when unmanaged devices are being used and unmanaged services are being adopted by end-users. Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope to device and endpoint security solutions to automatically restrict access in the event of an incident.	• NG-SWG • CASB • Private Access • DLP • Device Intelligence • CRE • Advanced Analytics
	Initial: Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.		
	Advanced: Agency's initial resource access considers verified device or virtual asset insights.		
	Optimal: Agency's resource access considers real-time risk analytics within devices and virtual assets.		
Device Threat Protection	Traditional: Agency manually deploys threat protection capabilities to some devices.	Netskope NG-SWG Advanced Threat Protection provides anti-malware detection, bare-metal and cloud sandboxing, and ML-based detection to detect and prevent malicious code being executed. It also provides pre-execution analysis and heuristics for more than 3,500 file format families for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types. Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope to device and endpoint security solutions to automatically restrict access in the event of an incident. Netskope's Remote Browser Isolation ensures no malicious code is executed in an organization's environment. RBI works by executing web server code in cloud storage containers, and reproducing the resulting webpage as an interactive pixel-rendered image. RBI ensures no executable code makes it from a web server to an end-user's system, essentially creating an "air gap," ensuring complete safety for viewing webpages browsed through RBI.	• NG-SWG • CASB • Advanced Threat Protection • RBI
	Initial: Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.		
	Advanced: Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.		
	Optimal: Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.		

Function	Maturity Level	Netskope Controls	Products
Visibility and Analytics Capability	Traditional: Agency uses a physically labeled inventory and limited software monitoring to review devices on a regular basis with some manual analysis.	Netskope's Device Intelligence maintains a current catalog of all managed and unmanaged devices connected to the organization's network, while Netskope's CASB can identify all managed and unmanaged apps and cloud services in use in the organization. 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. This helps build user and device baselines that can be leveraged to detect anomalies and alert on potential security incidents. NG-SWG and CASB also use an advanced DLP engine to identify and protect organizational data at rest, in transit, or in use across web, cloud apps, and endpoint devices. Advanced Analytics gives administrators visibility into where and how data flows to and from devices and applications and can aid in detecting anomalies.	• NG-SWG • CASB • Private Access • DLP • Device Intelligence • Advanced Analytics • UEBA
	Initial: Agency uses digital identifiers (e.g., interface addresses, digital tags) alongside a manual inventory and endpoint monitoring of devices when available. Some agency devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk.		
	Advanced: Agency automates both inventory collection (including endpoint monitoring on all standard user devices, e.g., desktops and laptops, mobile phones, tablets, and their virtual assets) and anomaly detection to detect unauthorized devices.		
	Optimal: Agency automates status collection of all network connected devices and virtual assets while correlating with identities, conducting endpoint monitoring, and performing anomaly detection to inform resource access. Agency tracks patterns of provisioning and/or deprovisioning of virtual assets for anomalies.	Netskope's Advanced User and Entity Behavior Analytics includes the User Confidence Index, which leverages machine learning to develop a baseline of normal behavior for each user, as well as assess the riskiness of each user's behavior. Anomalous or excessively risky behavior can trigger real-time adjustment to access privileges, as well as referring users for training on cyber hygiene or organizational policy.	
Automation and Orchestration Capability	Traditional: Agency manually provisions, configures, and/or registers devices within the enterprise.	Netskope's Device Intelligence provides a continuously updated catalog of managed and unmanaged devices connected to the organization's network, and can calculate baseline risk scores for devices. Devices can then be isolated in network microsegments, and combined with features like the User Confidence Index and the Cloud Confidence Index can be leveraged to design real-time policies that restrict access to unsanctioned apps, or risky actions within apps. NG-SWG and CASB provide a continuously updated log of devices connecting to apps and services in use in the organization's IT ecosystem. Netskope integrates with organizational SIEM or SOAR tools, and event or alert logs can be leveraged to generate service tickets and automate workflows for remediating access rules. Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope platform to device and endpoint security solutions to automatically restrict access in the event of an incident.	• CASB • NG-SWG • Device Intelligence • UEBA • CRE
	Initial: Agency begins to use tools and scripts to automate the process of provisioning, configuration, registration, and/or deprovisioning for devices and virtual assets.		
	Advanced: Agency has implemented monitoring and enforcement mechanisms to identify and manually disconnect or isolate noncompliant (vulnerable, unverified certificate; unregistered mac address) devices and virtual assets.		
	Optimal: Agency has fully automated processes for provisioning, registering, monitoring, isolating, remediating, and deprovisioning devices and virtual assets.		

Function	Maturity Level	Netskope Controls	Products
Governance Capability	Traditional: Agency sets some policies for the lifecycle of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.	Netskope Device Intelligence can be leveraged to identify hardware (including IoT, OT, and traditional devices) and manage devices and connectivity, useful for rogue or EOL devices. NG-SWG and CASB provide a continuously updated log of devices connecting to apps and services in use in the organization's IT ecosystem. Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope platform to device and endpoint security solutions to automatically restrict access in the event of an incident.	• Device Intelligence • CASB • NG-SWG • CRE
	Initial: Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.		
	Advanced: Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.		
	Optimal: Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.		

3. NETWORKS

Function	Maturity Level	Netskope Controls	Products
Network Segmentation	Traditional: Agency defines their network architecture using large perimeter/macrosegmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels). Initial: Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least-function principles, and a transition toward service-specific interconnections. Advanced: Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress microperimeters and service-specific interconnections. Optimal: Agency network architecture consists of fully distributed ingress/egress microperimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.	Netskope's SD-WAN provides site-to-site connectivity including options to segment networks and environments and manage logical access. Netskope Private Access protects private networks through a Zero Trust model. This ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN). Netskope's FWaaS provides firewall policies for egress traffic across ports and protocols for users and offices. Netskope's Remote Browser Isolation ensures no malicious code is executed in an organization's environment. RBI works by executing web server code in cloud storage containers, and reproducing the resulting webpage as an interactive pixel-rendered image.	• SD-WAN • Private Access • FWaaS • RBI
Network Traffic Management	Traditional: Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g., application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission-critical applications. Initial: Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments Advanced: Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring. Optimal: Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.	Netskope's NG-SWG and CASB continuously monitor the organization's network, identifying all managed and unmanaged apps and cloud services in use in the IT ecosystem, and characterizing them by usage and risk score. This helps organizations determine which apps and services are most critical to their operations. Netskope can also identify and categorize all organizational data across web and cloud traffic. Private Access, Device Intelligence, and the Cloud Confidence Index can be jointly leveraged to enforce dynamic zero trust policies across the network from devices to services. Netskope DEM can help identify user experience issues with networks and services such as ISP and CSP issues including network devices in the path of connectivity such as routers. Netskope's SD-WAN extends the organization's security perimeter to any user on any device, anywhere. Traffic steered to Netskope's NewEdge Network can be subjected to a uniform set of security policies..	• NG-SWG • CASB • CCI • Private Access • Device Intelligence • SD-WAN • DEM

Function	Maturity Level	Netskope Controls	Products
Traffic Encryption	Traditional: Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Netskope NG-SWG and CASB ensure best practice SSL/TLS encryption is applied. Organizations can choose to use their own keys (BYOK) to ensure secure server/service encryption is maintained. Netskope's Private Access offers secure remote access to private apps across devices, integrating with third-party identity providers for secure authentication, end-to-end encryption for data security, and granular controls following zero trust principles. Netskope's SD-WAN extends the organization's security perimeter to any device, anywhere. Traffic is steered through Netskope's NewEdge Network, allowing uniform enforcement of security policies. It also provides options to segment networks and environments and manage logical access.	• NG-SWG • CASB • Private Access • SD-WAN
	Initial: Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications, to formalize key management policies, and to secure server/service encryption keys.		
	Advanced: Agency ensures encryption for all applicable internal and external traffic protocols, manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.		
	Optimal: Agency continues to encrypt traffic as appropriate, enforces least-privilege principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.		
Network Resilience	Traditional: Agency configures network capabilities on a case-by case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Netskope's products support resilience requirements in both normal and adverse conditions, including the ability to both scale up and scale down on demand. Netskope's NewEdge private cloud network implements a high-availability, cloud-based architecture, allowing operations to continue in the event of a failure at any node with an uptime availability SLA of 99.999%. In addition, Netskope SD-WAN offers hot standby at remote sites to help achieve resilience requirements at remote locations. Remote users can securely access sanctioned apps using Netskope's Private Access.	• NG-SWG • CASB • SD-WAN • Private Access
	Initial: Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.		
	Advanced: Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.		
	Optimal: Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.		

Function	Maturity Level	Netskope Controls	Products
Visibility and Analytics Capability	Traditional: Agency incorporates limited boundary-focused network monitoring capabilities with minimal analysis to start developing centralized situational awareness.	The Netskope platform can assist monitoring for network events across the ecosystems of networks, public cloud, SaaS, and devices. Events are created across a suite of products and can be assessed by either Digital Experience Monitoring or FWaaS, or SD-WAN depending on the event and traffic profile. The same approach is taken for web, cloud, and on-prem apps and services. Advanced Analytics can also be used to assess trends and assist in identifying potential adverse events and anomalies. Cloud Exchange can be leveraged to extend and share event data across the ecosystem of network and security tools.	• CASB • NG-SWG • DEM • FWaaS • SD-WAN • Advanced Analytics • Cloud Exchange
	Initial: Agency employs network monitoring capabilities based on known indicators of compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.		
	Advanced: Agency deploys anomaly-based network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.		
	Optimal: Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.		
Automation and Orchestration Capability	Traditional: Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Netskope's products are fully agile without the need for dedicated hardware and include the ability to both scale up and scale down on demand. Policies can be managed manually or automated using APIs to manage configuration. Management of policies and configuration can be aligned to change management processes including the use of role-based access control (RBAC) to manage changes within the administration console. Policies can be set based on time-based parameters and can be reported on and exported for automated reviews.	• NG-SWG • CASB • Private Access • FWaaS • SD-WAN
	Initial: Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.		
	Advanced: Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.		
	Optimal: Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.		

Function	Maturity Level	Netskope Controls	Products
Governance Capability	Traditional: Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Netskope's SD-WAN provides site-to-site connectivity including options to segment networks and environments and manage logical access. Netskope Private Access protects private networks through a Zero Trust model. This ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN). Private Access, NG-SWG, and CASB integrate with third-party identity providers like Okta and Ping to extend SSO/MFA across web and cloud-based apps and services. With granular and adaptive policy controls, the Netskope platform can build a baseline of normal user and device behavior, and can adjust privileges in real time in response to risky or anomalous events.	• NG-SWG • CASB • SD-WAN • Private Access
	Initial: Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.		
	Advanced: Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.		
	Optimal: Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.		

4. APPLICATION AND WORKLOADS

Function	Maturity Level	Netskope Controls	Products
Application Access	Traditional: Agency authorizes access to applications primarily based on local authorization and static attributes. Initial: Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration. Advanced: Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least-privilege principles. Optimal: Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.	Netskope products provide granular and adaptive policy controls, with the ability to allow or block specific activities within an application, demand a business justification or stepped-up MFA for risky actions, or suggest a safer alternative. These controls ensure that access control permissions are not granted excessively and adhere to the principle of least privilege. Netskope's UEBA builds a baseline of normal user behavior, as well as assigning each user a User Confidence Index based on the riskiness of their use of IT resources. Access privileges can be adjusted in real time when it detects behavior that deviates from the baseline, or when the UCI score dips too low. For remote users, Private Access furnishes secure access only to those sanctioned apps that have been provisioned to the user, and not to the rest of the internal network, as occurs with a VPN. This prevents lateral movement by malicious actors. 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. Not only can Netskope products be configured to secure activity to web, SaaS, IaaS, and egress traffic from on-network and remote users, but they also secure app and cloud service activity to the extent that specific user actions (such as share, edit, delete, upload, download, etc.) within cloud apps are recorded. Netskope's unique ability to decode inline unpublished API calls and JSON streams allow it to secure user activity in real time across apps and cloud services, including by instance (i.e., company vs. personal). Cloud Risk Exchange (CRE) allows for risk signals to be shared continuously across a series of platforms including sharing signals from Netskope platform to device and endpoint security solutions to automatically restrict access in the event of an incident.	• NG-SWG • CASB • Private Access • UEBA • CRE • Advanced Analytics

Function	Maturity Level	Netskope Controls	Products
Application Threat Protections	Traditional: Agency threat protections have minimal integration with application workflows, applying general-purpose protections for known threats.	Netskope products support creation and ingestion of Cyber Threat Intelligence (CTI) and can detect and block activity that is considered malicious. Netskope's predefined conditions, rules, and machine-learning technology, including Advanced Threat Protection, User and Entity Behavior Analytics (UEBA), and DLP, assist in providing context to event information. 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. APIs are provided for sandboxing and retrospective hunting, and the various modules of Netskope's Cloud Exchange perform threat intel sharing, log export, risk score exchange, and workflow automation. Furthermore, MITRE ATT&CK analysis is incorporated into sandboxing reports. Netskope's UEBA builds a baseline of normal user behavior, detecting anomalies that may indicate a compromised device or the actions of a malicious insider. Netskope's SaaS Security Posture Management continuously monitors the organization's SaaS apps for any misconfigured access controls. Discovered misconfigurations can generate alerts that are exported to the organization's SIEM tool via Netskope's Cloud Log Shipper, and Netskope's Cloud Ticket Orchestrator can automate remediation efforts.	• NG-SWG • CASB • Advanced Threat Protection • Advanced DLP • UEBA • Cloud Exchange • SSPM • CLS • CTO
	Initial: Agency integrates threat protections into mission-critical application workflows, applying protections against known threats and some application-specific threats.		
	Advanced: Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.		
	Optimal: Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.		

Function	Maturity Level	Netskope Controls	Products
Accessible Applications	Traditional: Agency makes some mission-critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Netskope's security solutions, 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. Private Access additionally provides secure remote access to private apps hosted on-prem or in the cloud, integrating with NIST-compliant identity providers for authentication. It employs end-to-end encryption to secure data and enforces granular access controls, ensuring that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN). Netskope's SD-WAN permits network segmentation and allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's SD-WAN, traffic is steered through Netskope's global New Edge Network, allowing high-availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more.	• NG-SWG • CASB • Private Access • DLP • SD-WAN
	Initial: Agency makes some of their applicable mission-critical applications available over open public networks to authorized users with need via brokered connections.		
	Advanced: Agency makes most of their applicable mission-critical applications available over open public network connections to authorized users as needed.		
	Optimal: Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.		
Secure Application Development and Deployment Workflow	Traditional: Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Netskope can be used to manage access to apps and services used during SDLC, i.e., GitHub, Public Cloud, etc. 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. Netskope's Private Access, SD-WAN, and FWaaS capabilities support network segmentation to provide secure access to development environments, and Private Access ensures that remote users access only the applications they have been provisioned and do not gain remote access to the rest of the internal network.	• NG-SWG • CASB • DLP • Private Access • SD-WAN • FWaaS
	Initial: Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least-privilege principles.		
	Advanced: Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.		
	Optimal: Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.		

Function	Maturity Level	Netskope Controls	Products
Application Security Testing	Traditional: Agency performs application security testing prior to deployment, primarily via manual testing methods.	Netskope's NG-SWG and CASB 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's SaaS Security Posture Management (SSPM) monitors critical SaaS functions to avoid misconfigurations and ensure alignment with policies and standards. SSPM provides detailed remediation instructions and can also integrate with the Cloud Ticket Orchestrator to automate service ticket generation and remediation. Detected misconfigurations can be turned into new rules to enhance security.	• NG-SWG • CASB • SSPM
	Initial: Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.		
	Advanced: Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.		
	Optimal: Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.		
Visibility and Analytics Capability	Traditional: Agency performs some performance and security monitoring of mission-critical applications with limited aggregation and analytics.	The Netskope platform identifies and categorizes managed and unmanaged applications in the organization's IT ecosystem. Netskope can export event logs to the organization's SIEM or SOAR tools for further analysis. It also continuously monitors organizational SaaS apps for misconfigurations. Netskope's Advanced Analytics can track data flows across web and cloud services, and its Advanced DLP scans cloud storage buckets to prevent data exfiltration and identify malware.	• NG-SWG • CASB • SSPM • Advanced Analytics
	Initial: Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.		
	Advanced: Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.		
	Optimal: Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.		
Automation and Orchestration Capability	Traditional: Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Netskope NG-SWG and CASB can identify cloud applications in use and help determine hosting location and access provisioning. SaaS Security Posture Management monitors critical SaaS functions to prevent misconfigurations and ensure compliant usage. SSPM provides step-by-step remediation instructions and can integrate with the Cloud Ticket Orchestrator to automate ticket generation and remediation. Detected misconfigurations can be converted into new rules to enhance security.	• NG-SWG • CASB • SSPM • CTO
	Initial: Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.		
	Advanced: Agency automates application configurations to respond to operational and environmental changes.		
	Optimal: Agency automates application configurations to continuously optimize for security and performance.		

Function	Maturity Level	Netskope Controls	Products
Governance Capability	Traditional: Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	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. Netskope's SaaS Security Posture Management monitors an organization's critical SaaS apps for misconfigurations. Alerts can be exported to the organization's SIEM tool via Netskope's Cloud Ticket Orchestrator for automated remediation.	• NG-SWG • CASB • Private Access • SSPM • CTO
	Initial: Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).		
	Advanced: Agency implements tiered, tailored policies enterprise-wide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.		
	Optimal: Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.		

5. DATA

Function	Maturity Level	Netskope Controls	Products
Data Inventory Management	Traditional: Agency manually identifies and inventories some agency data (e.g., mission-critical data).	Netskope products offer controls to identify and protect organizational data across web and cloud applications, cloud infrastructure, on-prem servers, and endpoint devices. These controls can be used to create an inventory of information assets across managed and unmanaged devices using DLP discovery controls. Netskope's DLP and DSPM can scan cloud storage buckets to identify data assets. They can be configured to alert on DLP/DSPM violations and take corrective actions such as revoking sharing permissions or encrypting a file. Netskope's DLP engine 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. With the continuous adoption of SaaS apps and cloud services for data hosting and storage, Netskope is also able to enforce real-time protections on data in motion to unsanctioned, user-adopted Shadow IT applications.	• NG-SWG • CASB • DLP • DSPM
	Initial: Agency begins to automate data inventory processes for both on-premises and in cloud environments, covering most agency data, and begins to incorporate protections against data loss.		
	Advanced: Agency automates data inventory and tracking enterprise-wide, covering all applicable agency data, with data loss prevention strategies based upon static attributes and/or labels.		
	Optimal: Agency continuously inventories all applicable agency data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.		
Data Categorization	Traditional: Agency employs limited and ad hoc data categorization capabilities.	Netskope's NG-SWG and CASB offer controls to identify categorized data and metadata and can associate policies to protect this information. In addition, Netskope can apply controls around uncategorized data and metadata based on its DLP/DSPM engine, including fingerprinting and natural language processing. These controls can be leveraged to implement file-level policies that grant or restrict access based on the type of data identified. Netskope's industry-leading DLP engine leverages AI/ML capabilities to analyze many different categories of data identifiers, including over 3,000 pre-defined identifiers, exact data matching, optical character recognition, and more, to achieve the most comprehensive data protection with the lowest degree of error possible. Netskope can be integrated with classification/labeling tools to apply classification labels to data.	• NG-SWG • CASB • DLP • DSPM
	Initial: Agency begins to implement a data categorization strategy with defined labels and manual enforcement mechanisms.		
	Advanced: Agency automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.		
	Optimal: Agency automates data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.		

Function	Maturity Level	Netskope Controls	Products
Data Availability	Traditional: Agency primarily makes data available from on-premises data stores with some off-site backups.	The Netskope platform supports secure access to backups through redundant pathways. Netskope's Private Access, SD-WAN, and FWaaS capabilities support network segmentation to ensure backups are stored and transported in a secure environment. And Netskope's SD-WAN offers resilient, high-availability connectivity. Netskope's DSPM can identify data posture including detail of data availability, how often it is used, and details on availability and criticality of data including any risks associated with the data such as permission issues. In addition, Netskope offers legal hold capabilities that allow for the preservation of data in a forensic repository for legal requirements.	• NG-SWG • CASB • DLP • DSPM
	Initial: Agency makes some data available from redundant, highly available data stores (e.g., cloud) and maintains off-site backups for on-premises data.		
	Advanced: Agency primarily makes data available from redundant, highly available data stores and ensures access to historical data.		
	Optimal: Agency uses dynamic methods to optimize data availability, including historical data, according to user and entity needs.		
Data Access	Traditional: Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls.	Netskope products provide granular and adaptive policy controls, with the ability to allow or block specific activities depending on the applicable DLP rule(s), demand a business justification or stepped-up MFA for risky actions, or suggest a safer alternative. These controls ensure that access control permissions are not granted excessively and adhere to the principle of least privilege. For remote users, Private Access furnishes secure access only to those sanctioned apps that have been provisioned to the user, and not to the rest of the internal network, as occurs with a VPN. This prevents lateral movement by malicious actors. 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. Not only can Netskope products be configured to secure activity to web, SaaS, IaaS, and egress traffic from on-network and remote users, but they also secure app and cloud service activity to the extent that specific user actions (such as share, edit, delete, upload, download, etc.) within cloud apps are recorded. Netskope's unique ability to decode inline unpublished API calls and JSON streams allow it to secure user activity in real time across apps and cloud services, including by instance (i.e., company vs. personal).	• NG-SWG • CASB • DLP • DSPM • Private Access • UEBA
	Initial: Agency begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.		
	Advanced: Agency automates data access controls that consider various attributes such as identity, device risk, application, data category, etc., and are time limited where applicable.		
	Optimal: Agency automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.		

Function	Maturity Level	Netskope Controls	Products
		Netskope’s Advanced UEBA builds a baseline of normal user behavior, as well as assigning each user a User Confidence Index based on the riskiness of their use of IT resources. Access privileges can be adjusted in real time when it detects behavior that deviates from the baseline, or when the UCI score dips too low. Finally, Netskope’s Data Security Posture Management and SaaS Security Posture Management continuously monitor the organization’s platforms and SaaS apps for access misconfigurations and data posture, and can prevent configuration drift and ensure that access permissions remain within organization-defined parameters.	
Data Encryption	Traditional: Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Netskope’s CASB and NG-SWG leverage a powerful Data Loss Prevention (DLP) and Data Security Posture Management (DSPM) engines to secure organizational data across web, cloud applications, and endpoints. This DLP/DSPM engine 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's Private Access provides remote access to on-prem or cloud-hosted private apps from any device, anywhere, including secure access to key management stores. Private Access uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles.	• NG-SWG • CASB • DLP • DSPM • Private Access
	Initial: Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission-critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys.		
	Advanced: Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).		
	Optimal: Agency encrypts data in use where appropriate, enforces least-privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.		
Visibility and Analytics Capability	Traditional: Agency has limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes.	Netskope's 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.	• NG-SWG • CASB • DLP • DSPM • Advanced Analytics
	Initial: Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some automated analysis and correlation.		
	Advanced: Agency maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and begins to employ predictive analytics.		

Function	Maturity Level	Netskope Controls	Products
	Optimal: Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and continuous security posture assessment.	Furthermore, Netskope's DLP/DSPM engine can be used to identify data through discovery and identify last access date. This is helpful in identifying the lifecycle of data and offer data lineage reporting.	
Automation and Orchestration Capability	Traditional: Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	The Netskope platform can assist organizations in automating all phases of data lifecycle management. Its industry-leading DLP/DSPM engine identifies and classifies organizational data across the web as well as managed and unmanaged cloud apps and services, and managed and unmanaged devices. It protects data at rest and in use with a uniform set of policies, and can identify data through discovery and last access date. Discovered misconfigurations and DLP/DSPM violations can trigger alerts that can be exported to the organization's SIEM or SOAR tools via Netskope's Cloud Ticket Orchestrator, automating remediation efforts and incident response.	• NG-SWG • CASB • DLP • DSPM • CTO
	Initial: Agency uses some automated processes to implement data lifecycle and security policies.		
	Advanced: Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.		
	Optimal: Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.		
Governance Capability	Traditional: Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Netskope's NG-SWG and CASB can discover and classify managed and unmanaged apps and cloud services and their associated data in the organization's IT ecosystem, and enforce role-based access controls to protect data in use, in transit, and at rest. Netskope's DLP/DSPM engine 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/DSPM program is easy to maintain.	• NG-SWG • CASB • DLP • DSPM
	Initial: Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.		
	Advanced: Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.		
	Optimal: Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.		

6. CROSS-CUTTING CAPABILITIES

Function	Maturity Level	Netskope Controls	Products
Visibility and Analytics	Traditional: Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	The Netskope platform generates transaction log data across web, cloud, on-prem and devices, summarizing activity and reporting on this activity continuously. Advanced Analytics maps activity 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. 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's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• NG-SWG • CASB • Advanced Analytics • Cloud Exchange • CTO
	Initial: Agency begins to automate the collection and analysis of logs and events for mission-critical functions and regularly assesses processes for gaps in visibility.		
	Advanced: Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.		
	Optimal: Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.		
Automation and Orchestration	Traditional: Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Netskope's NG-SWG, CASB, and Security Posture Management (DSPM/SSPM) capabilities continuously monitor SaaS apps and data to ensure adherence to updated policy configurations. By integrating data from various security tools, and generating relevant alerts and security tickets, Netskope's Cloud Exchange makes it easier to derive lessons learned and implement policy changes in 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.	• NG-SWG • CASB • SSPM • DSPM • Cloud Exchange • CTO
	Initial: Agency begins automating orchestration and response activities in support of mission-critical functions.		
	Advanced: Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.		
	Optimal: Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.		

Function	Maturity Level	Netskope Controls	Products
Governance	Traditional: Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Netskope's platform is optimized to apply dynamic policies and controls based on risk scores across user, device, application/workload, and data using a combination of available controls. In addition, the platform can leverage Netskope's cloud exchange to share signals (threat = CTE or risk = CRE) with other integrated services such as identity, endpoint, SIEM/SOAR, email, etc, security services. Finally, Netskope can support governance reporting on policy violations and decisions based on contextual information including predicted trends.	• NG-SWG • CASB • Private Access • SSPM • DSPM • Cloud Exchange • Advanced Analytics
	Initial: Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.		
	Advanced: Agency implements tiered, tailored policies enterprise-wide and leverages automation where possible to support enforcement. Access policy decisions incorporate contextual information from multiple sources.		
	Optimal: Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.		

Disclaimer

The content provided has been created to the best of Netskope's ability and knowledge. However, Netskope cannot guarantee the accuracy, completeness, or timeliness of the information. Netskope are not liable for any errors or omissions in the content, and readers are encouraged to verify the information independently. The use of this content is at the reader's own risk, and Netskope shall not be held responsible for any consequences resulting from reliance on the provided information.

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.