Compliance Series

Cybersecurity Maturity Model Certification (CMMC v2.0)

Using the Netskope Platform to Protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)

TABLE OF CONTENTS

INTRODUCTION

The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity framework designed by the United States Department of Defense (DoD) to ensure that DoD contractors and subcontractors adequately safeguard the confidentiality, integrity, and availability of information supplied to them by the DoD.

The CMMC is largely derived from the National Institute of Standards and Technology's Special Publication 800-171 Revision 2 (NIST 800-171), with some additional requirements pulled from the Federal Acquisition Regulation Clause 52.204-21 and the Defense Federal Acquisition Regulation Supplement Clause 252.204-7012.

Compliance with the CMMC framework is necessary to protect two kinds of information defined by the DoD:

Federal Contract Information (FCI): information provided by or generated for the federal government under contract, which is not intended for public release; and

Controlled Unclassified Information (CUI): information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

HOW TO USE THIS GUIDE

This guide consists of 14 tables corresponding to the 14 domains of the NIST 800-171 Framework that form the basis for the CMMC model. Each row in each table consists of a CMMC identifier, the practice statement associated with that CMMC identifier, a description of how Netskope's products help achieve compliance with the practice statement, and a list of relevant Netskope products.

Remember that CMMC identifiers adhere to the following format: DD.L#-REQ, where DD refers to the two-letter abbreviation of the relevant NIST 800-171 domain, L# is the level number (1 or 2 in this version, but stay tuned for level 3, which will be coming out next year), and REQ refers to the specific NIST 800-171 requirement number.

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
Public Cloud Security	Public Cloud Security
Zero Trust Network Access	ZTNA Next
Cloud Security Posture Management	CSPM
SaaS Security Posture Management	SSPM
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)	Borderless SD-WAN Secure SD-WAN Endpoint SD-WAN Wireless SD-WAN IoT Intelligent AccessI
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

The following table will break down each requirement, mapping specific Netskope products and use cases to individual regulatory requirements. Only the requirements relevant to Netskope controls have been included, all other requirements have been omitted.

ACCESS CONTROL

CMMC Identifier	Practice Statement	Netskope Response	Products
AC.L1-3.1.1: Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).	Netskope's security solutions encompass various tools for comprehensive cloud and network protection. Netskope's CASB detects both managed and unmanaged apps and cloud services, facilitating the identification of vendors requiring contractual safeguards. Similarly, the Next-Generation Secure Web Gateway (NG-SWG) offers app and cloud service inventory. Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms to prevent misconfigurations and data exfiltration, integrating with Cloud Ticket Orchestrator for alerting and automated remediation. SaaS Security Posture Management (SSPM) oversees SaaS functions, preventing misconfigurations, and also integrates with Cloud Ticket Orchestrator for automated responses, converting past misconfigurations into new security rules. Netskope's ZTNA Next ensures secure, zero-trust access to private apps, with end-to-end encryption and integration with third-party authentication providers. It logs access attempts and enforces policies on login failures. Device Intelligence identifies and segments both managed and unmanaged devices, using AI/ML to establish behavioral baselines, detect anomalies, and apply access controls. It integrates with incident response tools for generating alerts based on organizational criteria.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • ZTNA Next • Device Intelligence • CTO
AC.L1-3.1.2: Transaction and Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Netskope's suite of solutions, including CASB, NGSWG, DLP, and ZTNA-Next, all support Role-Based Access Control (RBAC) to help organizations enforce access management policies. These policies are based on the principle of least privilege, ensuring that users have only the minimum level of access necessary for their roles.	• CASB • NG-SWG • DLP • ZTNA Next
AC.L2-3.1.3: Control CUI Flow	Control the flow of CUI in accordance with approved authorizations.	Netskope offers comprehensive security solutions through its CASB and NG-SWG, empowered by a machine learning-driven Data Loss Prevention (DLP) engine. This DLP protects sensitive data across web, cloud, and endpoint devices, applying context-aware policies and real-time actions like obfuscation and encryption. It supports role-based access control, facilitates incident response, ensures backup integrity, and provides detailed logging for continuous monitoring and forensic investigations.	• CASB • NG-SWG • Cloud Firewall • DLP • ZTNA Next • Advanced Analytics • Advanced UEBA

CMMC Identifier	Practice Statement	Netskope Response	Products
		The CASB component enforces the principle of least privilege in access management, while NG-SWG integrates with identity providers to extend SSO/MFA protections. NG-SWG monitors user activities for anomalies and applies granular policy controls, requiring additional authentication or suggesting safer alternatives when risky behavior is detected. It also generates detailed logs and alerts to enhance incident response and aid regulatory compliance. Netskope's Cloud Firewall secures web and cloud application traffic, detecting and mitigating DNS attacks without backhauling traffic. Meanwhile, its Advanced User Entity and Behavior Analytics use ML-based models and a User Confidence Index to detect insider threats, adapt controls, and recommend training. Advanced Analytics maps data flows and assesses cloud risks, offering admins detailed insights into security trends and potential threats..	
AC.L2-3.1.4: Separation of Duties	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. It scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to automate alerts and remediation efforts. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors mission-critical SaaS functions to prevent misconfigurations and ensure proper data usage. SSPM provides step-by-step remediation instructions, integrates with the Cloud Ticket Orchestrator for automated issue resolution, and allows previously detected misconfigurations to be converted into new security rules for ongoing improvement.	• Public Cloud Security • CSPM • SSPM • CTO
AC.L2-3.1.5: Least Privilege	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Netskope's CASB monitors and logs SaaS and IaaS activities, applying real-time data loss prevention controls, such as requiring business justifications for risky actions, or referring users for further training. It supports Role-Based Access Control (RBAC) based on the principle of least privilege. Cloud Security Posture Management continuously monitors IaaS platforms to prevent misconfigurations, ensures compliance with organizational policies and standards, and integrates with Cloud Ticket Orchestrator for automated remediation of security flaws. SaaS Security Posture Management similarly monitors mission-critical SaaS functions and integrates with the Cloud Ticket Orchestrator, converting findings into new security rules. The NG-SWG integrates with third-party identity providers for SSO/MFA, decodes activities, detects anomalies, and enforces granular policy controls. It can generate reports and alerts for SIEM tools and supports non-repudiation of user actions. ZTNA Next provides secure remote access to private apps, uses end-to-end encryption, applies granular access controls, logs access attempts, and enforces RBAC based on zero trust principles.	• CASB • NG-SWG • Public Cloud Security • CSPM • ZTNA Next • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
AC.L2-3.1.6: Non- Privileged Account Use	Use non-privileged accounts or roles when accessing nonsecurity functions.	Netskope's CASB provides comprehensive activity monitoring and logging for SaaS and IaaS services, capturing user, device, instance, and action details. It offers real-time activity-level and data loss prevention controls, enabling not just action blocking but also requiring business justifications for risky actions or delivering policy training. Netskope's NG-SWG integrates with NISTcompliant identity providers to extend SSO/MFA across web and cloud-based apps, logging over 100 inline activities. It establishes a user activity baseline to detect anomalies and applies granular policy controls based on activity nature, data type, or app instance. NG-SWG's context-aware controls can handle risky behaviors by enforcing multi-factor authentication, notifying users of policy violations, suggesting safer alternatives, or directing them to cybersecurity training. It generates customizable reports and alerts for integration with SIEM tools, aiding incident response and ensuring nonrepudiation of user actions through detailed logging. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NISTcompliant third-party identity providers to support secure authentication, 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. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts.	• CASB • NG-SWG • ZTNA
AC.L2-3.1.7: Privileged Functions	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor mission-critical IaaS and SaaS platforms, respectively. Both systems aim to prevent misconfigurations, ensuring compliance with organizational policies, regulatory requirements, and industry standards. CSPM focuses on preventing data exfiltration by routinely scanning cloud storage buckets, while SSPM provides step-by-step instructions for correcting misconfigurations. Both solutions integrate with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation efforts. Additionally, SSPM enables conversion of previously detected misconfigurations into new security rules, enhancing overall protection.	• Public Cloud Security • CSPM • SSPM • CTO
AC.L2-3.1.8: Unsuccess- ful Logon Attempts	Limit unsuccessful logon attempts.	ZTNA Next logs all access attempts and enforces organizational policies on failed login attempts.	• ZTNA Next

CMMC Identifier	Practice Statement	Netskope Response	Products
AC.L2-3.1.9: Privacy & Security Notices	Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.	Netskope's product suite enhances cybersecurity and data privacy by communicating and tracking policy acknowledgments, and facilitating awareness and training through pop-up banners and coaching pages. These tools notify employees of potential policy breaches, request justifications for risky actions, and refer users to third-party vendors for further training. ZTNA Next by Netskope offers secure remote access to private apps hosted on-premise or in the cloud from any device. It integrates with NISTcompliant third-party identity providers for secure authentication, uses end-to-end encryption to protect data, and employs granular controls based on zero trust principles to limit access and privileges. ZTNA Next also logs all access attempts and enforces organizational policies on failed login attempts..	• All products • ZTNA Next
AC.L2-3.1.10: Session Lock	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Netskope's products do not map to this requirement.	
AC.L2-3.1.11: Session Termination	Terminate (automatically) user sessions after a defined condition.	Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NISTcompliant third-party identity providers to support secure authentication, 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. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts.	• ZTNA
AC.L2-3.1.12: Control Remote Access	Monitor and control remote access sessions.	Netskope's NG-SWG integrates with NISTcompliant third-party identity providers to extend SSO/MFA across web and cloud-based apps, both managed and unmanaged. It decodes and logs over 100 inline activities to establish a user activity baseline for detecting anomalies. It then applies granular policy controls based on activity, data, or app instances. Beyond basic "allow" or "block" rules, NG-SWG uses context-aware controls to handle risky behavior by requiring multi-factor authentication, notifying users of policy violations, or recommending safer alternatives and cybersecurity training. It generates customizable reports and alerts for SIEM tool integration, aiding incident response and ensuring non-repudiation of actions. Netskope's ZTNA Next facilitates secure remote access to on-prem and cloud-hosted private apps from any device. It integrates with NIST-compliant identity providers for secure authentication, employs end-to-end encryption, and enforces zero trust principles with granular access controls. ZTNA Next logs all access attempts and upholds organizational policies for failed login attempts.	• NG-SWG • ZTNA Next

CMMC Identifier	Practice Statement	Netskope Response	Products
AC.L2-3.1.13: Remote Access Confidentiality	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NISTcompliant third-party identity providers to support secure authentication, 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. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts.	- ZTNA
AC.L2-3.1.14: Remote Access Routing	Route remote access via managed access control points.	Netskope's ZTNA Next offers remote access to both on-premises and cloud-hosted private applications from any device and location. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing highavailability 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.	- ZTNA Next - SD-WAN
AC.L2-3.1.15: Privileged Remote Access	Authorize remote execution of privileged commands and remote access to securityrelevant information.	Netskope's ZTNA Next offers remote access to private, on-prem, or cloud-hosted applications from any device, anywhere. It integrates with NISTcompliant third-party identity providers for secure authentication, uses end-to-end encryption to protect data in use and in motion, and enforces granular access controls based on zero trust principles. ZTNA Next logs all access attempts and can enforce policies on failed login attempts, ensuring robust security and compliance.	- ZTNA Next
AC.L2-3.1.16: Wireless Access Authorization	Authorize wireless access prior to allowing such connections.	Netskope's products do not map to this requirement.	
AC.L2-3.1.17: Wireless Access Protection	Protect wireless access using authentication and encryption.	Netskope's ZTNA Next offers secure remote access to on-premises or cloud-hosted private applications from any device and location. It integrates with NIST-compliant third-party identity providers for secure authentication and employs end-to-end encryption to protect data both in use and in motion. ZTNA Next adheres to zero trust principles by applying granular access controls and privileges. Additionally, it logs all access attempts and enforces organizational policies regarding failed login attempts.	- ZTNA Next
AC.L2-3.1.18: Mobile Device Connection	Control connection of mobile devices.	Netskope's NG-SWG integrates with NISTcompliant identity providers to extend SSO/MFA across various services, decoding and logging over 100 activities to detect anomalous behavior and apply policy controls. It can prompt additional authentication or user notifications as needed. Alerts and reports can be integrated into SIEM tools for incident response and ensure user action nonrepudiation. Borderless SD-WAN extends the network perimeter to any user or device globally, using Netskope's New Edge network for high-availability connectivity and uniform policy enforcement, adaptive to user context, location, and device specifics. ZTNA Next offers secure remote access to private applications from any device, employing NISTcompliant identity providers for authentication, endto- end encryption, and granular access control based on zero trust principles, logging all access attempts.	- NG-SWG - SD-WAN - ZTNA Next - Device Intelligence

CMMC Identifier	Practice Statement	Netskope Response	Products
		Device Intelligence identifies and classifies all devices connecting to the network, isolating risky ones. Its AI/ ML engine establishes normal behavior baselines, detects anomalies, and enforces granular controls. It also integrates with incident response tools to generate security alerts.	
AC.L2-3.1.20: External Connections	Verify and control/limit connections to and use of external information systems.	Netskope evaluates SaaS applications using its Cloud Confidence Index (CCI), assessing each vendor's security, audit capabilities, legal, and privacy concerns. Netskope's CASB (Cloud Access Security Broker) provides real-time monitoring and control for SaaS and IaaS activities, applying data loss prevention (DLP) measures. Its DLP engine, featuring machine learning and context-aware policies, secures organizational data across various environments by obfuscating, encrypting, or blocking sensitive data. It also supports role-based access, incident response, and forensic investigations. Netskope's ZTNA Next offers remote access to private apps with end-to-end encryption, integrating with NIST-compliant identity providers for secure authentication and applying zero trust principles. Logs of access attempts and enforcement of policies on failed logins ensure additional security.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • DLP • ZTNA Next
AC.L2-3.1.21: Portable Storage Use	Limit use of portable storage devices on external systems.	Netskope's CASB (Cloud Access Security Broker) and NG-SWG (Next-Generation Secure Web Gateway) feature a robust Data Loss Prevention (DLP) engine. This engine offers comprehensive monitoring and protection for endpoint data in use, including the capability to control USB storage devices.	• CASB • NG-SWG • DLP
AC.L2-3.1.22: Control Public Information	Limit use of portable storage devices on external systems.	Netskope's CASB (Cloud Access Security Broker) and NG-SWG (Next-Generation Secure Web Gateway) feature a robust Data Loss Prevention (DLP) engine. This engine offers comprehensive monitoring and protection for endpoint data in use, including the capability to control USB storage devices.	• CASB • NG-SWG • DLP

AWARENESS AND TRAINING

CMMC Identifier	Practice Statement	Netskope Response	Products
AT.L2-3.2.1: Role-Based Risk Awareness	Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.	Netskope's NG-SWG integrates with NIST-compliant identity providers, extending Single Sign-On (SSO) and Multi-Factor Authentication (MFA) across various web and cloud apps. It decodes over 100 inline activities and establishes user activity baselines to detect anomalous behavior, applying granular policy controls. Beyond simple "allow" or "block" rules, NGSWG's context-aware controls can escalate MFA, notify users of potential policy violations, suggest safer alternatives, or direct users to cybersecurity training. It generates customizable reports and alerts, feeds data into SIEM tools for incident response, and supports non-repudiation of user actions. The advanced User Entity and Behavior Analytics (UEBA) employs multiple ML-based anomalydetection models and includes a User Confidence Index (UCI), a dynamic risk score for users. UCI helps adapt policies, recommend security training, and mitigate insider threats, and can share insider threat information through Netskope's Cloud Risk Exchange.	• NG-SWG • Advanced UEBA
AT.L2-3.2.2: Role-Based Training	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Netskope's Cloud Access Security Broker (CASB) monitors and logs activities in SaaS and IaaS services, capturing information on users, devices, instances, and actions. It applies real-time activity and data loss prevention controls, which may include requesting business justifications for risky actions or providing policy training instead of merely blocking actions. Netskope's Next-Gen Secure Web Gateway (NGSWG) integrates with NIST-compliant identity providers, extending SSO/MFA to both managed and unmanaged web and cloud-based apps. It decodes and logs over 100 inline activities, establishing a baseline to detect anomalies and enforce granular policy controls based on activity, data transmission, or specific app instances. NG-SWG's context-aware controls go beyond simple "allow" or "block" rules, responding to risky or anomalous behavior by requiring enhanced MFA, notifying users of potential policy violations, requesting justifications for risky actions, suggesting safer alternatives, or referring users to cybersecurity training. Additionally, NG-SWG can generate customizable reports and alerts for integration with SIEM tools, aiding incident response, and providing detailed event logging to ensure nonrepudiation of user actions.	• CASB • NG-SWG
AT.L2-3.2.3: Insider Threat Awareness	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Netskope's Standard User Entity and Behavior Analytics (UEBA) monitors user activities across web and cloud applications, establishing normal behavior baselines and detecting anomalies through sequential rules. It adjusts access and privileges based on user behavior risk and deviations from these baselines. The Advanced UEBA adds more machine-learning-based anomaly detection models and features a User Confidence Index (UCI), which is a dynamic risk score for each user. This advanced version adapts policies, recommends security training to mitigate insider threats, and integrates with Netskope's Cloud Exchange to share insider threat information.	• CASB • NG-SWG • UEBA • Advanced UEBA

AUDIT AND ACCOUNTABILITY

CMMC Identifier	Practice Statement	Netskope Response	Products
AU.L2-3.3.1: System Auditing	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.	Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor IaaS and SaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory policies. Both CSPM and SSPM can integrate with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation. The Cloud Firewall enforces security policies for web and cloud egress traffic, disrupts various DNS attacks, and integrates with SIEM tools for better incident response. ZTNA Next provides secure remote access to private apps, with end-to-end encryption and granular access controls based on zero trust principles. Netskope's Advanced Analytics maps data from NGSWG & CASB and categorizes data flows across web and cloud services, providing insights into cloud risk and security trends. The Cloud Log Shipper exports logs from various Netskope tools to an organization's SIEM system, while Cloud Ticket Orchestrator automates service ticket creation and incident response workflows. Cloud Ticket Orchestrator, part of Netskope's Cloud Exchange, enhances the efficiency of incident handling and enforcing access controls.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • SSPM • ZTNA Next • Advanced Analytics • CLS • CTO
AU.L2-3.3.2: User Accountability	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	Netskope provides comprehensive security solutions for SaaS, IaaS, and private applications. Its CASB monitors and logs user activities, applying real-time controls to prevent data loss and enforce policies through actions like requesting business justifications for risky actions or providing training. The NG-SWG decodes and logs over a hundred inline activities, sets baselines for user behavior to detect anomalies, and applies granular policy controls. Rather than just blocking actions, it can require multi-factor authentication or suggest safer alternatives in response to risky behavior. ZTNA Next ensures secure remote access to private apps, integrating with NIST-compliant identity providers, using end-to-end encryption, and enforcing zero trust principles. It logs all access attempts and enforces policies on failed logins, securing data and activities across multiple platforms.	• CASB • NG-SWG • ZTNA Next
AU.L2-3.3.3: Event Review	Review and update logged events.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and data exfiltration, ensuring compliance with organizational, regulatory, and industry standards. It integrates with Netskope's Cloud Ticket Orchestrator for alerting and automated remediation. Similarly, SaaS Security Posture Management (SSPM) monitors SaaS functions, providing step-by-step remediation instructions and converting detected misconfigurations into new security rules. Netskope's Cloud Firewall enforces security policies on egress traffic and disrupts DNS attacks while integrating event logs with SIEM tools for incident response. ZTNA Next offers secure remote access to private apps with zero trust principles, NIST-compliant authentication, and access logging.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • SSPM • ZTNA Next • Advanced Analytics • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
		Advanced Analytics maps data flows, assesses cloud risk, and tracks security trends. The Cloud Ticket Orchestrator automates incident response workflows and role-based access controls as part of Netskope's Cloud Exchange.	
AU.L2-3.3.4: Audit Failure Alerting	Alert in the event of an audit logging process failure.	Netskope's Cloud Log Shipper exports event and alert logs from various tools, including NG-SWG, CASB, ZTNA Next, Cloud Firewall, and Cloud and SaaS Security Posture Management, to an organization's SIEM or other incident response tools.	• CLS
AU.L2-3.3.5: Audit Correlation	Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor IaaS and SaaS platforms to prevent misconfigurations, ensure compliance with access management policies and standards, and secure data. CSPM also scans cloud storage to prevent data exfiltration and both systems integrate with Netskope's Cloud Ticket Orchestrator for automated remediation. The Cloud Firewall applies security policies to egress traffic and inspects DNS queries to prevent attacks, integrating logs with SIEM tools for incident response. ZTNA Next secures remote access to private apps using end-to-end encryption and zero trust principles, while mapping data flows and assessing cloud risks via Advanced Analytics. Cloud Log Shipper exports logs from Netskope tools to SIEM, and Cloud Risk Exchange normalizes and enforces adaptive controls on assessed risks. Cloud Threat Exchange allows real-time sharing of threat indicators among customers and partners. The Cloud Ticket Orchestrator automates incident response workflows, role-based access controls, and integrates within the Cloud Exchange platform.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • SSPM • ZTNA Next • Advanced Analytics • CLS • CRE • CTE • CTO
AU.L2-3.3.6: Reduction & Reporting	Provide audit record reduction and report generation to support ondemand analysis and reporting.	Netskope's suite of security tools provides comprehensive monitoring and protection for organizations' cloud and web assets. Cloud Security Posture Management (CSPM) continuously oversees IaaS and SaaS platforms for misconfigurations and compliance with policies and regulations, preventing data misuse and exfiltration. It integrates with Cloud Ticket Orchestrator for automated alerts and remediation. Netskope's Next-Gen Secure Web Gateway (NGSWG) integrates with NIST-compliant identity providers to extend single sign-on (SSO) and multifactor authentication (MFA) across various apps, detecting anomalous user activity and applying context-aware controls to mitigate risks. Its event logging assists in incident response and user action accountability. The Cloud Firewall ensures secure egress traffic, defends against attacks like DDoS, and supports integration with SIEM tools. SaaS Security Posture Management (SSPM) mitigates misconfigurations in mission-critical SaaS functions, offering step-by-step remediation and integrating with Cloud Ticket Orchestrator.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • SSPM • UEBA • ZTNA Next • Advanced Analytics • Device Intelligence • CLS • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
		User Entity and Behavior Analytics (UEBA) and ZTNA Next provide advanced monitoring and secure remote access, respectively, adjusting controls based on risk and integrating with identity providers. Device Intelligence identifies and isolates risky devices, leveraging AI/ML for behavior baselining, while Advanced Analytics maps data flows and assesses cloud risks. Netskope's Cloud Log Shipper exports comprehensive event logs to incident response tools, and the Cloud Ticket Orchestrator automates incident response workflows and enforces role-based access controls. This orchestrator is part of Netskope's Cloud Exchange, enhancing the organization's incident response and recovery plans.	
AU.L2-3.3.7: Authoritative Time Source	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Netskope's products do not map to this requirement.	
AU.L2-3.3.8: Audit Protection	Protect audit information and audit logging tools from unauthorized access, modification and deletion.	Netskope's Data Loss Prevention (DLP) engine leverages machine learning to protect sensitive data across web, cloud applications, and devices. The DLP enforces role-based access, ensures backup integrity, and supports forensic investigations. Cloud Security Posture Management and SaaS Security Posture Management continually monitor and prevent misconfigurations in IaaS and SaaS platforms, integrating with Cloud Ticket Orchestrator for automated remediation. The Cloud Firewall applies security policies to web and cloud traffic, preventing DNS attacks and integrating with SIEM tools. ZTNA Next offers secure remote access with zero trust principles, logging all access attempts. Advanced Analytics maps data flows and assesses cloud risk, providing insights into security trends. Finally, Cloud Ticket Orchestrator automates incident response by generating service tickets and enforcing role-based access controls, enhancing Netskope's overall security posture.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • DLP • SSPM • ZTNA Next • Advanced Analytics • CTO
AU.L2-3.3.9: Audit Management	Limit management of audit logging functionality to a subset of privileged users.	Netskope offers comprehensive security solutions focused on role-based access control, least privilege principles, and continuous monitoring across various cloud environments. Cloud Security Posture Management (CSPM) ensures mission-critical IaaS and SaaS platforms adhere to compliance and access management policies, automating remediation efforts through integration with Netskope's Cloud Ticket Orchestrator. The Next-Generation Secure Web Gateway (NGSWG) and Cloud Firewall protect against data exfiltration and DNS attacks, while also providing policy enforcement and incident response integration. The Data Loss Prevention (DLP) and Zero Trust Network Access (ZTNA Next) solutions reinforce secure access and privilege limitations, with ZTNA Next offering end-to-end encrypted remote access and detailed logging.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • DLP • SSPM • ZTNA Next • Advanced Analytics • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
		Advanced Analytics maps and assesses data flow and cloud application usage, providing insights for enhanced security. Netskope's Cloud Ticket Orchestrator automates incident response and enforces access controls, supporting overall security management and policy adherence across all integrated platforms.	

CONFIGURATION MANAGEMENT

CMMC Identifier	Practice Statement	Netskope Response	Products
CM.L2-3.4.1: System Baselining	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.	Netskope's Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing both managed and unmanaged apps and cloud services. Cloud Security Posture Management (CSPM) continuously monitors mission-critical IaaS platforms to prevent misconfigurations and data exfiltration, integrating with the Cloud Ticket Orchestrator for alerts and automated remediation. SaaS Security Posture Management (SSPM) similarly monitors SaaS functions, providing remediation instructions and integrating with the Cloud Ticket Orchestrator. Netskope's Next-Generation Secure Web Gateway (NG-SWG) integrates with identity providers for SSO/MFA across web and cloud apps, and it can detect and log multiple activities to monitor for anomalous behavior, applying granular policy controls and generating reports for incident response. Finally, Netskope's Device Intelligence classifies devices connecting to the network and uses AI/ML to detect anomalies, applying access controls in line with zero trust principles and generating alerts for incident response.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Device Intelligence • CTO
CM.L2-3.4.2: Security Configuration Enforcement	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) tools continuously monitor an organization’s critical IaaS and SaaS platforms, respectively, to prevent misconfigurations and ensure compliance with access management policies and regulatory standards. Both CSPM and SSPM scan for data exfiltration risks and automate remediation efforts by integrating with Netskope's Cloud Ticket Orchestrator, which generates alerts and service tickets. Additionally, detected misconfigurations can be turned into new security rules. Netskope's Device Intelligence solution identifies and classifies all devices connected to the network, including unmanaged ones, and segregates risky devices into different network segments. Its AI/ML engine establishes a baseline of normal device behavior and detects anomalies, allowing for granular access controls based on zero trust principles. Device Intelligence also integrates with incident response tools to generate tailored security alerts.	• Public Cloud Security • CSPM • SSPM • Device Intelligence • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
CM.L2-3.4.3: System Change Management	Track, review, approve or disapprove and log changes to organizational systems.	Netskope's Cloud Confidence Index (CCI) scores SaaS applications based on various criteria, such as security policies, certifications, and legal concerns, to help organizations assess the risk of their use. Netskope’s Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with policies and standards. CSPM also scans cloud storage to prevent data exfiltration and integrates with Netskope’s Cloud Ticket Orchestrator for automated remediation. Similarly, Netskope’s SaaS Security Posture Management (SSPM) monitors SaaS functions for misconfigurations, provides remediation instructions, and can automate responses through integration with Cloud Ticket Orchestrator. SSPM allows for the conversion of detected misconfigurations into new rules, enhancing security over time.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CTO
CM.L2-3.4.4: Security Impact Analysis	Analyze the security impact of changes prior to implementation.	Netskope evaluates SaaS applications through its Cloud Confidence Index (CCI), assessing risk based on security policies, certifications, audit capabilities, and legal and privacy concerns. Cloud Security Posture Management continuously monitors IaaS platforms, ensuring compliance with organizational policies and regulatory standards to prevent misconfigurations and data exfiltration. Netskope's SaaS Security Posture Management similarly monitors SaaS functions to prevent deviations from policies and standards. It provides alerts with remediation instructions. Both CSPM and SSPM integrate with the Cloud Ticket Orchestrator to automate fixes.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CTO
CM.L2-3.4.5: Access Restrictions for Change	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	Netskope offers comprehensive security solutions for web, cloud, and private applications through in-line controls, identifying and managing different instances of cloud applications across development, testing, and production environments. Its CASB (Cloud Access Security Broker) monitors and logs activities in SaaS and IaaS services, applying real-time data loss prevention and activity-level controls, which can include business justifications or policy training. Netskope's Cloud Security Posture Management (CSPM) prevents misconfigurations in IaaS platforms and scans cloud storage to avoid data exfiltration, integrating with Cloud Ticket Orchestrator for alerts and remediation automation. Similarly, its SaaS Security Posture Management (SSPM) addresses misconfigurations in SaaS functions, offering remediation instructions and integration with Cloud Ticket Orchestrator. Finally, Netskope’s Borderless SD-WAN extends network security to any user or device globally, utilizing the New Edge network to ensure highavailability connectivity and enforce policy controls with continuous adaptive trust.	• All products • CASB • Public Cloud Security • CSPM • SD-WAN • SSPM • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
CM.L2-3.4.6: Least Functionality	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Netskope's Cloud Access Security Broker (CASB) enables real-time monitoring and logging of activities in SaaS and IaaS services, tracking details on users, devices, instances, and actions. It allows activity-level and data loss prevention controls, offering capabilities such as blocking actions, requiring business justifications, or providing policy training. Netskope's Cloud Security Posture Management (CSPM) continuously oversees IaaS environments to prevent misconfigurations and ensure compliance with organizational policies and regulatory standards. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerting and automated remediation. Netskope's SaaS Security Posture Management (SSPM) performs similar functions for SaaS applications, continuously monitoring for misconfigurations and ensuring compliance. SSPM provides step-by-step instructions for fixing issues and can generate service tickets to automate remediation. Misconfigurations found can be turned into new security rules to enhance protective measures.	• CASB • Public Cloud Security • CSPM • SSPM • CTO
CM.L2-3.4.7: Nonessential Functionality	Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.	Netskope's Cloud Security Posture Management (CSPM) safeguards mission-critical IaaS platforms by preventing misconfigurations and ensuring compliance with organizational and regulatory standards. CSPM integrates with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation, and routinely scans cloud storage to prevent data exfiltration. The SaaS Security Posture Management (SSPM) similarly monitors SaaS functions, offering step-by-step remediation guidance and integration with Cloud Ticket Orchestrator to generate service tickets and automate fixes. SSPM can convert detected misconfigurations into new security rules. Netskope's Public Cloud Security Advanced Data Loss Prevention (DLP) scans IaaS storage for hidden malware. Netskope's Remote Browser Isolation protects against risky websites by containing potential threats in a secure, cloud-based sandbox. Advanced User Entity and Behavior Analytics (UEBA) utilizes machine learning models to detect anomalies and assign dynamic risk scores to users, aiding in adaptive policy enforcement and insider threat mitigation. Advanced Threat Protection layers comprehensive malware detection techniques on top of Standard Threat Protection, which defends against known and new malware, phishing, and web threats through integration with various Netskope security tools. SkopeAI enhances Netskope DLP by using machine learning to identify and secure unstructured data and detect various sophisticated cyber threats quickly.	• CASB • NG-SWG • Public Cloud Security • CSPM • RBI • SSPM • Advanced DLP • Advanced Threat Protection • Advanced UEBA • Threat Protection • CTO • SkopeAI

CMMC Identifier	Practice Statement	Netskope Response	Products
CM.L2-3.4.8: Application Execution Policy	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-byexception (whitelisting) policy to allow the execution of authorized software.	Netskope's CASB helps with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and cataloging both managed and unmanaged apps and cloud services in the IT environment. It assesses their criticality based on usage and risk levels. Netskope's NG-SWG integrates with NISTcompliant third-party identity providers, extending SSO/MFA to various web and cloudbased apps and services. It decodes and logs over 100 activities, establishes user activity baselines to detect anomalies, and applies granular policy controls based on activity type, data nature, or app instance. Beyond simple "allow" or "block" rules, NG-SWG's contextaware controls can require additional authentication, notify users of potential policy violations, suggest safer alternatives, or direct users to just-in-time cybersecurity training. It also generates customizable reports and alerts that feed into the organization's SIEM tool for improved incident response, and its detailed event logging helps assert non-repudiation of user actions.	• CASB • NG-SWG
CM.L2-3.4.9: User-Installed Software	Control and monitor userinstalled software.	Netskope's Cloud Access Security Broker (CASB) and Next-Gen Secure Web Gateway (NG-SWG) offer comprehensive monitoring, logging, and control for SaaS, IaaS, and web services. CASB tracks user activities and devices, employing real-time data loss prevention that can request business justification or provide policy training. NG-SWG integrates with third-party identity providers, supports SSO/MFA for cloud apps, and monitors user activities to detect anomalies, applying contextaware controls such as stepped-up authentication or policy notifications. Both solutions log detailed events and can interface with SIEM tools for better incident response. Additionally, Advanced Threat Protection includes capabilities like deobfuscation, recursive file unpacking, and multi-stage sandboxing to combat new malware. Netskope's Device Intelligence identifies and segments all devices, whether managed or unmanaged, applying AI/ML to detect anomalies and enforce zero trust principles. This device-level intelligence can also generate alerts and integrate with incident response tools, enhancing overall network security.	• CASB • NG-SWG • Advanced Threat • Protection Device Intelligence

IDENTIFICATION AND AUTHENTICATION

CMMC Identifier	Practice Statement	Netskope Response	Products
IA.L1-3.5.1: Identification	Identify information system users, processes acting on behalf of users or devices.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms to prevent misconfigurations and ensure compliance with policies and standards. CSPM scans cloud storage to prevent data exfiltration, generates alerts, and automates remediation via Cloud Ticket Orchestrator integration. Netskope's SaaS Security Posture Management (SSPM) similarly monitors critical SaaS functions, alerts on deviations, provides remediation steps, and automates mitigation through integration with Cloud Ticket Orchestrator. Detected misconfigurations can be turned into new security rules. Netskope's Next-Generation Secure Web Gateway (NG-SWG) integrates with third-party identity providers, extends SSO/MFA across apps, logs activities, and detects anomalies. NG-SWG applies granular policies and context-aware controls, such as requiring stepped-up MFA or suggesting safer alternatives, and its detailed event logging supports non-repudiation and incident response. Netskope ZTNA Next offers secure remote access to private apps, integrates with identity providers for authentication, uses end-to-end encryption, and enforces zero trust policies with detailed logging of access attempts.	• NG-SWG • Public Cloud Security • CSPM • SSPM • ZTNA Next • CTO
IA.L1-3.5.2: Authentication	Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.	Netskope's Next-Generation Secure Web Gateway (NG-SWG) integrates with NISTcompliant identity providers, extending SSO/MFA across web and cloud apps, and detecting anomalous user behavior through granular policy controls. NG-SWG enforces context-aware security measures and can trigger multi-factor authentication or user notifications based on risky actions, integrating with SIEM tools for incident response. Netskope's ZTNA Next provides secure remote access to private apps, integrating with third-party identity providers and applying zero trust principles through end-to-end encryption and granular access controls. ZTNA Next logs access attempts and enforces policies on failed logins. Netskope's Cloud Security Posture Management (CSPM) ensures the security of IaaS platforms by monitoring for and preventing misconfigurations and data exfiltration, adhering to organizational policies and regulations. CSPM integrates with the Cloud Ticket Orchestrator for automated alerts and remediation. Netskope's SaaS Security Posture Management (SSPM) ensures the security of SaaS functions by monitoring misconfigurations and generating automated remediation efforts through integration with the Cloud Ticket Orchestrator. SSPM can convert misconfigurations into new security rules. Netskope Device Intelligence identifies and classifies all devices on the network, detecting anomalies and applying zero trust security controls. It can integrate with incident response tools to generate alerts based on predefined criteria.	• NG-SWG • Public Cloud Security • CSPM • SSPM • ZTNA Next • Device Intelligence • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
IA.L2-3.5.3: Multifactor Authentication	Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Netskope's NG-SWG integrates with NISTcompliant identity providers, extending SSO/MFA across web and cloud apps. It decodes over 100 inline activities, developing a user activity baseline to detect anomalies and applying granular policy controls based on activity or data nature. NG-SWG goes beyond simple "allow" or "block" rules with contextaware controls that can require additional authentication, notify users of policy violations, suggest safer alternatives, or refer users for cybersecurity training. It generates customizable reports and alerts for SIEM tools and provides detailed event logging to support non-repudiation of actions. Netskope's ZTNA Next offers remote access to on-prem or cloud-hosted private apps from any device. It integrates with NIST-compliant identity providers for secure authentication, employs end-to-end encryption, and applies zero trust principles to limit access based on granular controls. ZTNA Next logs all access attempts and enforces policies on failed logins.	• NG-SWG • ZTNA Next
IA.L2-3.5.4: Replay- Resistant Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Netskope's ZTNA Next offers remote access to on-premises or cloud-hosted private applications from any device, anywhere. It integrates with third-party, NIST-compliant identity providers for secure authentication. The solution uses end-to-end encryption to protect data in use and in motion and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next also logs all access attempts and enforces organizational policies regarding failed login attempts.	• ZTNA Next
IA.L2-3.5.4: Replay- Resistant Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Netskope's ZTNA Next offers remote access to on-premises or cloud-hosted private applications from any device, anywhere. It integrates with third-party, NIST-compliant identity providers for secure authentication. The solution uses end-to-end encryption to protect data in use and in motion and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next also logs all access attempts and enforces organizational policies regarding failed login attempts.	• ZTNA Next
IA.L2-3.5.5: Identifier Reuse	Prevent the reuse of identifiers for a defined period.	Netskope's ZTNA Next enables secure remote access to private apps hosted on-premises or in the cloud, from any device and location. It integrates with NIST-compliant third-party identity providers for secure authentication. ZTNA Next employs end-to-end encryption to protect data both in use and in transit, and incorporates granular controls to limit access and privileges based on zero trust principles. It logs all access attempts and can enforce policies on failed login attempts to enhance security.	• ZTNA Next
IA.L2-3.5.6: Identifier Handling	Disable identifiers after a defined period of inactivity	Netskope's products do not map to this requirement.	• ZTNA Next
IA.L2-3.5.7: Password Complexity	Enforce a minimum password complexity and change of characters when new passwords are created.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with access management policies, regulatory, and industry standards. It routinely scans cloud storage buckets to prevent data exfiltration. Integration with Netskope's Cloud Ticket Orchestrator enables it to send alerts and automate remediation efforts.	• Public Cloud Security • CSPM • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
IA.L2-3.5.8: Password Reuse	Prohibit password reuse for a specified number of generations.	Netskope's ZTNA Next offers secure remote access to private applications, whether onpremises or cloud-hosted, from any device, anywhere. It integrates with NIST-compliant third-party identity providers for secure authentication and employs end-to-end encryption to safeguard data in use and transit. Utilizing zero trust principles, ZTNA Next enforces granular controls to restrict access and privileges. It also logs all access attempts and can enforce organizational policies on failed login attempts.	• ZTNA Next
IA.L2-3.5.9: Temporary Passwords	Allow temporary password use for system logons with an immediate change to a permanent password	Netskope's ZTNA Next offers secure remote access to private applications hosted onpremises or in the cloud from any location and device. It integrates with third-party identity providers that comply with NIST standards for secure authentication. The solution employs end-to-end encryption to protect data both in use and in transit, and enforces zero trust principles with granular access and privilege controls. ZTNA Next also logs all access attempts and can enforce organizational policies related to failed login attempts.	• ZTNA Next
IA.L2-3.5.10: Cryptographically - Protected Passwords	Store and transmit only cryptographically-protected passwords.	Netskope's Cloud Access Security Broker (CASB) and Next-Generation Secure Web Gateway (NG-SWG) leverage an advanced Data Loss Prevention (DLP) engine to ensure robust security for organizational data across various environments, including web, cloud applications, and endpoint devices. This DLP system employs machine learning to identify, classify, and protect sensitive information based on organizational and regulatory criteria. It utilizes context-aware policies considering users, devices, apps, networks, and actions to safeguard data in real-time by obfuscating, encrypting, or restricting actions as necessary. Additionally, Netskope's DLP enforces rolebased data access during incident response and recovery, maintains backup integrity, and stores log files in dedicated repositories, enabling continuous monitoring and facilitating forensic investigations.	• CASB • NG-SWG • DLP
IA.L2-3.5.11: Obscure Feedback	Obscure feedback of authentication information.	Netskope’s Cloud Confidence Index (CCI) scores SaaS applications, providing details to assess the risk of using each vendor's services based on security policies, certifications, audit capabilities, and legal/privacy concerns. Cloud Security Posture Management system continuously monitors mission-critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. This includes routine scans of cloud storage to prevent data exfiltration. Additionally, it integrates with Netskope’s Cloud Ticket Orchestrator to automate alerts and remediation efforts.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • CTO

INCIDENT RESPONSE

CMMC Identifier	Practice Statement	Netskope Response	Products
IR.L2-3.6.1: Incident Handling	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.	Netskope provides robust security features including a CASB that generates and exports alerts to an organization's Security Incident and Event Management (SIEM) tool for automated incident response and recovery. Event logs support lessons learned and progress reports. The NG-SWG integrates with NIST-compliant identity providers to extend SSO/MFA across web and cloud apps, logging over 100 activities to detect anomalies and enforce granular policy controls. It can respond to risky behavior by requiring additional authentication, notifying users of violations, suggesting safer alternatives, or referring them for just-in-time training. Customizable thresholds in NG-SWG generate reports and alerts fed into the SIEM for incident response, with detailed logging aiding in nonrepudiation. The Cloud Log Shipper exports event and alert logs from various Netskope tools to the SIEM, while the Cloud Ticket Orchestrator automates service ticket creation and workflows in response to security alerts, enforcing role-based access controls and supporting the incident response plan.	• CASB • NG-SWG • CLS • CTO
IR.L2-3.6.2: Incident Reporting	Track, document and report incidents to designated officials and/or authorities both internal and external to the organization.	Netskope's CASB can generate alerts and export them to the organization's SIEM tool for automated incident response and recovery, while event logs support lessons learned and progress reporting. The NG-SWG integrates with NIST-compliant identity providers, extending SSO/MFA across various apps and services. It logs over 100 inline activities to detect anomalies, applying granular policy controls. Beyond simple rules, NG-SWG's context-aware controls respond to risky behavior, potentially requiring additional authentication, user notifications, or thirdparty cybersecurity training. It also generates customizable alerts for SIEM integration, aiding in incident response and non-repudiation. Netskope's Cloud Log Shipper exports logs from NGSWG, CASB, ZTNA Next, Cloud Firewall, and other tools to the organization's SIEM or incident response tool. The Cloud Ticket Orchestrator automates service ticket creation and workflows in response to security alerts, supporting automated incident response and role-based access controls.	• CASB • NG-SWG • CLS • CTO
IR.L2-3.6.3: Incident Response Testing	Test the organizational incident response capability.	Netskope's CASB (Cloud Access Security Broker) and Next-Generation Secure Web Gateway (NG-SWG) both excel in identifying and inventorying managed and unmanaged apps and cloud services. This capability is crucial for determining the scope and preparing an effective incident response plan. Both solutions provide precise, consistent, and reproducible response measures and metrics, which are essential for testing the effectiveness of these plans.	• CASB • NG-SWG

MAINTENANCE

CMMC Identifier	Practice Statement	Netskope Response	Products
MA.L2-3.7.1: Perform Maintenance	Perform maintenance on organizational systems.	Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational, regulatory, and industry standards. It routinely scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) provides similar monitoring for SaaS functions, offering alerts with remediation instructions and integration with the Cloud Ticket Orchestrator for automated response. Misconfigurations can be transformed into rules to enhance security over time. Netskope's ZTNA Next offers secure remote access to private apps, integrating with NIST-compliant identity providers for authentication, using end-to-end encryption, and applying zero trust principles with granular access controls. It logs all access attempts and enforces policies on login failures.	• Public Cloud Security • CSPM • SSPM • ZTNA Next • CTO
MA.L2-3.7.2: System Maintenance Control	Provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.	Netskope's products do not map to this requirement	
MA.L2-3.7.3: Equipment Sanitization	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Netskope's products do not map to this requirement.	
MA.L2-3.7.4: Media Inspection	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Netskope's products do not map to this requirement.	
MA.L2-3.7.5: Nonlocal Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Netskope's Borderless SD-WAN extends an organization's network to any user on any device, anywhere, ensuring high-availability connectivity to web and cloud applications through the global New Edge network. It enforces consistent policy controls with adaptive trust based on criteria such as user, location, and device. Netskope's ZTNA Next offers remote access to onprem or cloud-hosted private apps from any device, utilizing third-party identity providers for secure authentication, end-to-end encryption, and granular control based on zero trust principles. ZTNA Next logs access attempts and enforces policies on login attempts. Additionally, it supports Role-Based Access Control to align with the principle of least privilege.	• SD-WAN • ZTNA Next
MA.L2-3.7.6: Maintenance Personnel	Supervise the maintenance activities of personnel without required access authorization.	Netskope's products do not map to this requirement.	

MEDIA PROTECTION

CMMC Identifier	Practice Statement	Netskope Response	Products
MP.L1-3.8.1: Media Protection	Protect (e.g., physically control and securely store) system media containing Federal Contract Information, both paper and digital.	Netskope's Cloud Access Security Broker (CASB) and Next-Generation Secure Web Gateway (NGSWG) offer robust data security via Data Loss Prevention (DLP) engine. This tool safeguards data in use, transit, or at rest across web, cloud apps, and endpoint devices. Utilizing machine learning, it identifies and protects sensitive data per organizational and regulatory requirements, applying real-time context-aware policies based on user, device, app, network, and action to secure data, such as by encrypting files or blocking actions. The DLP also facilitates role-based access, backup integrity, and continuous monitoring for incident response and forensic investigations. The NG-SWG integrates with NIST-compliant identity providers for enhanced SSO/MFA across web and cloud services. It monitors over 100 inline activities to detect anomalies, applying granular policy controls based on activity or app instance. Beyond simple "allow" or "block" rules, it can prompt multi-factor authentication, request a business justification for risky actions, offer safer alternatives, or direct users to cybersecurity training. Configurable to generate actionable alerts and reports, NG-SWG's detailed logging supports incident response and nonrepudiation of user actions.	• CASB • NG-SWG • DLP
MP.L2-3.8.2: Media Access	Limit access to CUI on system media to authorized users.	Netskope's CASB and NG-SWG utilize an advanced Data Loss Prevention (DLP) engine to safeguard organizational data in various states—whether in use, in transit, or at rest—across the web, cloud applications, and endpoint devices. The DLP leverages machine learning to identify, classify, and protect sensitive data according to organizational or regulatory requirements. Contextaware policies that consider users, devices, apps, networks, and actions are employed in real time to protect data, for example, by encrypting files or blocking certain actions. It also supports role-based access during incident response, ensures backup integrity, and facilitates continuous monitoring and forensic investigations. Additionally, Netskope's CASB, NG-SWG, and ZTNA-Next enforce role-based access control in line with the principle of least privilege, thereby supporting organizational access management policies.	• CASB • NG-SWG • DLP • ZTNA Next
MP.L2-3.8.3: Media Disposal	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.	Netskope's products do not map to this requirement.	
MP.L2-3.8.4: Media Markings	Mark media with necessary CUI markings and distribution limitations..	Netskope's CASB and NG-SWG leverage a robust Data Loss Prevention (DLP) engine to safeguard organizational data across web, cloud applications, and endpoint devices. Utilizing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data in real time depending on organizational or regulatory needs. It employs context-	• CASB • NG-SWG • DLP

CMMC Identifier	Practice Statement	Netskope Response	Products
		aware policies that consider users, devices, apps, networks, and actions to protect data by obfuscating personal data, encrypting sensitive files, or blocking specific actions. The DLP also supports role-based data access for incident response, ensures backup integrity, and maintains log files in specialized repositories for continuous monitoring and forensic investigations.	
MP.L2-3.8.5: Media Accountability	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Netskope's products do not map to this requirement.	
MP.L2-3.8.6: Portable Storage Encryption	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Netskope's CASB (Cloud Access Security Broker) and NG-SWG (Next-Generation Secure Web Gateway) leverage a powerful Data Loss Prevention (DLP) engine. This engine offers monitoring and protection for endpoint data usage, including the ability to control USB storage devices.	• CASB • NG-SWG • DLP
MP.L2-3.8.7: Removable Media	Control the use of removable media on system components.	Netskope's CASB and NG-SWG feature a robust Data Loss Prevention (DLP) engine that monitors and protects endpoint data in use. This protection includes controls for USB storage devices, ensuring comprehensive data security. In addition, Netskope's Device Intelligence identifies and classifies all devices connecting to the network, segmenting risky devices. Utilizing AI and machine learning, it establishes a baseline of normal device behavior, detects anomalies, and enforces granular access controls aligned with zero trust principles. Device Intelligence integrates with incident response tools to generate security alerts based on predefined criteria.	• CASB • NG-SWG • DLP • Device Intelligence
MP.L2-3.8.8: Shared Media	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Netskope's CASB and NG-SWG feature a robust Data Loss Prevention (DLP) engine that monitors and protects endpoint data in use. This protection includes controls for USB storage devices, ensuring comprehensive data security.	• CASB • NG-SWG • DLP
MP.L2-3.8.9: Protect Backups	Protect the confidentiality of backup CUI at storage locations.	Netskope's Cloud Access Security Broker (CASB) and Next-Generation Secure Web Gateway (NGSWG) utilize an advanced Data Loss Prevention (DLP) engine to secure organizational data across web activities, cloud applications, and endpoint devices. Netskope's DLP enforces role-based data access during incident response, maintains backup integrity, and stores log files in dedicated repositories, supporting continuous monitoring, internal audits, and regulatory investigations.	• CASB • NG-SWG • DLP

PHYSICAL AND ENVIRONMENTAL PROTECTION

While Netskope's products do not provide physical and environmental security tools, the Netskope platform provides logging and reporting, access management controls, and user and entity behavior analytics that complement the organization's physical security controls.

PERSONNEL SECURITY

CMMC Identifier	Practice Statement	Netskope Response	Products
PS.L2-3.9.1: Screen Individuals	Screen individuals prior to authorizing access to organizational systems containing CUI.	Netskope's products do not map to this requirement.	
PS.L2-3.9.2: Personnel Actions	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Netskope offers various tools to support organizational access management policies based on the principle of least privilege. Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with regulatory standards, while also scanning cloud storage to prevent data exfiltration. CSPM integrates with Netskope's Cloud Ticket Orchestrator for alert automation and remediation. The Next-Gen Secure Web Gateway (NG-SWG) and SaaS Security Posture Management (SSPM) similarly prevent misconfigurations and ensure intended data use, with SSPM offering step-by-step remediation and integration for automated ticket generation. Netskope's Data Loss Prevention (DLP) and ZTNANext tools also support role-based access control, enhancing overall security.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • CTO

RISK ASSESSMENT

CMMC Identifier	Practice Statement	Netskope Response	Products
RA.L2-3.11.1: Risk Assessments	Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI.	Netskope offers a comprehensive suite of security solutions for cloud services. The Cloud Confidence Index (CCI) rates SaaS applications on various security criteria. Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor IaaS and SaaS environments for misconfigurations and deviations from policies, providing alerts and automated remediation through Cloud Ticket Orchestrator integration. CSPM also scans cloud storage to prevent data exfiltration, while SSPM helps convert detected issues into new security rules.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • RBI • SSPM

CMMC Identifier	Practice Statement	Netskope Response	Products
		Remote Browser Isolation is a feature of Netskope's Next-Generation Secure Web Gateway (NG-SWG), isolating risky websites in a secure container to prevent malware infections. Advanced User Entity and Behavior Analytics (UEBA) uses machine learning for anomaly detection and includes a User Confidence Index to assess and mitigate insider threats, sharing insights via the Cloud Risk Exchange. Netskope's Advanced Analytics tracks data flows and cloud app usage, assessing risks and identifying security trends through a dashboard. Standard Threat Protection combats known and new malware, offers phishing detection, and integrates with various Netskope tools and threat intelligence feeds for a layered security approach.	• Advanced Analytics • Advanced UEBA • Threat Protection • CTO
RA.L2-3.11.2: Vulnerability Scan	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations, ensuring compliance with organizational policies and industry standards, and scans cloud storage to prevent data exfiltration. CSPM integrates with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation. Netskope's SaaS Security Posture Management (SSPM) performs similar monitoring for SaaS functions, providing step-by-step remediation instructions and integration with the Cloud Ticket Orchestrator for automated service tickets. SSPM can also convert detected misconfigurations into new security rules, enhancing overall security. Netskope's ZTNA Next offers secure remote access to private apps from any device, using NISTcompliant identity providers for authentication, endto- end encryption, and zero trust-based access controls. It logs all access attempts and enforces policies on failed logins. Netskope's Device Intelligence catalogs and classifies all network-connected devices, segments at-risk devices, and uses AI/ML to establish normal behavior patterns. It detects anomalies, applies zero trust access controls, and integrates with incident response tools for security alerts based on organizational criteria.	• Public Cloud Security • CSPM • SSPM • ZTNA Next • Device Intelligence • CTO
RA.L2-3.11.3: Vulnerability Remediation	Remediate vulnerabilities in accordance with risk assessments.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations, ensuring compliance with organizational policies and industry standards, and scans cloud storage to prevent data exfiltration. CSPM integrates with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation. Netskope's SaaS Security Posture Management (SSPM) performs similar monitoring for SaaS functions, providing step-by-step remediation instructions and integration with the Cloud Ticket Orchestrator for automated service tickets. SSPM can also convert detected misconfigurations into new security rules, enhancing overall security.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • Advanced UEBA • Device Intelligence • Threat Protection • CTO

SECURITY ASSESSMENT

CMMC Identifier	Practice Statement	Netskope Response	Products
CA.L2-3.12.1: Security Control Assessment	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Netskope enforces organizational policies and aids communication via pop-up banners to notify employees of potential policy violations. It prepares organizations for security tests by inventorying unmanaged apps and devices, assigning risk-based scores. Netskope's Cloud Confidence Index assesses SaaS application risks based on vendor security policies and other criteria. Netskope's CASB and NG-SWG, with a Data Loss Prevention (DLP) engine, safeguard data across web, cloud apps, and devices using machine learning. The DLP enforces role-based access, maintains backup integrity, and ensures compliance through real-time data protection. The CASB aids asset inventory, risk management, and automates incident response via integration with security tools. Cloud Security Posture Management continuously monitors IaaS platforms, preventing misconfigurations and data exfiltration. Integrating with Netskope's Cloud Ticket Orchestrator, it automates remediation. Similarly, SaaS Security Posture Management prevents misconfigurations in SaaS functions and enhances security through automated alerts and remediation. Public Cloud Security, Advanced DLP, Remote Browser Isolation, and ZTNA Next provide additional layers of protection by securing access to apps and isolating risky sites. Advanced Threat Protection identifies sophisticated malware, while Advanced Analytics and Threat Protection map data flows, assess cloud risks, and offer real-time security against known and new threats. Proactive Digital Experience Management ensures optimal user experience from endpoints to the cloud.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • DLP • RBI • SSPM • ZTNA Next Advanced • Analytics Advanced • DLP Advanced • Threat Protection • Device Intelligence • Threat Protection • CTO • P-DEM
CA.L2-3.12.2: Plan of Action	Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Netskope's CASB supports asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and inventorying both managed and unmanaged apps and cloud services in an organization's IT ecosystem, assessing their criticality based on usage and risk levels. This helps determine the scope of contingency plans and their testing. Netskope’s Cloud Security Posture Management (CSPM) continuously monitors mission-critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. It scans cloud storage buckets to prevent data exfiltration and integrates with Cloud Ticket Orchestrator to send alerts and automate remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) continuously monitors mission-critical SaaS functions to prevent misconfigurations, ensuring compliance and proper usage. SSPM provides step-by-step remediation instructions and integrates with Cloud Ticket Orchestrator to generate service tickets and automate fixes. Additionally, previously detected misconfigurations can be converted into new security rules to enhance protection.	• CASB • Public Cloud Security • CSPM • SSPM • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
CA.L2-3.12.3: Security Control Monitoring	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Netskope enforces organizational policies via pop-up banners and coaching pages, notifying employees of potential infringements. It scores SaaS applications in its Cloud Confidence Index (CCI) for risk assessment, covering security, privacy, and more. Netskope's CASB and NG-SWG feature a Data Loss Prevention (DLP) engine using machine learning to secure data across web, cloud, and devices, enforcing role-based access and backing up data integrity. SaaS Security Posture Management (SSPM) prevents misconfigurations and integrates with Cloud Ticket Orchestrator for automated remediation. Advanced DLP scans for malware in IaaS Storage. Remote Browser Isolation and ZTNA Next enhance security for web interactions and remote app access. Standard Threat Protection guards against known and new malware through machine learning and integration with various security tools. Advanced Threat Protection offers multi-layered defense against malware. Device Intelligence monitors network devices, identifying risky behavior and enhancing network segmentation. Advanced Analytics maps data flows and assesses cloud risks. Cloud Risk Exchange normalizes risk scores from third-party tools, while Cloud Threat Exchange shares threat indicators. Proactive Digital Experience Management oversees user experience and automates troubleshooting.	• All products • CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • DLP • RBI • SSPM • ZTNA Next • Advanced Analytics • Advanced DLP • Advanced Threat Protection • Device Intelligence • Threat Protection • CRE • CTE • CTO • P-DEM
CA.L2-3.12.4: System Security Plan	Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.	Netskope's Cloud Access Security Broker (CASB) and Next-Gen Secure Web Gateway (NG-SWG) feature a Data Loss Prevention (DLP) engine that ensures robust security for organizational data across web, cloud applications, and endpoints. The DLP, powered by machine learning, identifies, classifies, and safeguards sensitive data based on organizational or regulatory requirements. It employs context-aware policies that consider users, devices, apps, networks, and actions to protect data in realtime, including obfuscation, encryption, or action blocking. This engine supports role-based data access during incident response, ensures backup integrity, and maintains log files for continuous monitoring and investigations. Additionally, SkopeAI enhances the DLP by providing deep contextual awareness and rapid detection of unstructured data, diverse attacks, polymorphic malware, novel phishing domains, zero-day threats, and malicious web content, surpassing traditional DLP capabilities.	• CASB • NG-SWG • DLP • SkopeAI

SYSTEM AND COMMUNICATIONS PROTECTION

CMMC Identifier	Practice Statement	Netskope Response	Products
SC.L1-3.13.1: Boundary Protection	Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Netskope's Borderless SD-WAN extends network perimeters to users on any device, anywhere, by steering traffic through its global New Edge network. This ensures high-availability connectivity to web and cloud applications while enforcing consistent policy controls based on user, location, device, and other criteria. Netskope's Cloud Firewall secures egress traffic to web and cloud applications across all ports and protocols without needing to redirect traffic to onpremise security stacks. It protects against DDoS, man-in-the-middle, and DNS attacks by examining queries for malicious activity. Event logs from Netskope's Cloud Firewall can be integrated with SIEM tools for effective incident response and recovery.	• Cloud • Firewall • SD-WAN
SC.L1-3.13.2: Security Engineering	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Netskope aids organizations in establishing a secure network architecture aligned with industry-standard cybersecurity and data privacy practices. This defense-in-depth strategy ensures each security layer functions independently, reducing risk to operations, assets, individuals, and third parties. The platform helps design, implement, and modify secure systems and services. Netskope offers various security solutions, including a layered structure that minimizes interactions between security layers. Borderless SD-WAN extends network perimeters to any user, device, or location, steering traffic through the global New Edge network for highavailability connectivity and consistent policy enforcement. This system adapts controls based on context-specific criteria. Additionally, Netskope's ZTNA Next provides secure remote access to private apps, integrating with NISTcompliant identity providers for authentication. It employs end-to-end encryption to protect data and enforces zero trust principles with granular access controls. ZTNA Next also logs all access attempts and enforces policies for failed logins, ensuring robust security for remote applications.	• All products • SD-WAN • ZTNA Next
SC.L2-3.13.3: Role Separation	Separate user functionality from system management functionality.	Netskope's Borderless SD-WAN extends the network perimeter to any user on any device globally, by routing traffic through the high-availability New Edge network for seamless access to web and cloud applications. It enforces uniform policy controls using adaptive trust based on user, location, device, and other context-specific factors. Netskope's ZTNA Next offers remote access to private apps hosted on-premises or in the cloud, ensuring secure authentication via third-party identity providers compliant with NIST standards. It employs end-to-end encryption, applies granular access controls based on zero trust principles, logs all access attempts, and enforces organizational policies for failed logins.	• SD-WAN • ZTNA Next

CMMC Identifier	Practice Statement	Netskope Response	Products
SC.L2-3.13.4: Shared Resource Control	Prevent unauthorized and unintended information transfer via shared system resources.	Netskope's CASB and NG-SWG solutions, powered by Netskope's Data Loss Prevention (DLP) engine, offer comprehensive security for organizational data across the web, cloud applications, and endpoint devices. Utilizing machine learning, the DLP identifies, classifies, and protects sensitive data based on organizational and regulatory standards. It applies context-aware policies that account for user, device, app, network, and action information to protect data in real time, which can include obfuscation, encryption, or blocking actions. It also enforces role-based data access, maintains backup integrity, and keeps log files in dedicated repositories for ongoing monitoring and forensic investigations. SkopeAI enhances the DLP engine with deep contextual awareness, effectively identifying and protecting unstructured data such as images. It also excels in detecting various attacks, polymorphic malware, novel phishing domains, zero-day threats, and malicious web content with superior speed and accuracy.	• CASB • NG-SWG • DLP • SkopeAI
SC.L2-3.13.5; Public-Access System Separation	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Netskope's Borderless SD-WAN extends network perimeters to any user, device, or location, leveraging Netskope's global New Edge network for highavailability connectivity to web and cloud applications. It enforces uniform policies with adaptive trust based on context-specific criteria such as user, location, and device. Netskope's Cloud Firewall secures egress traffic to the web and cloud applications across all ports and protocols without backhauling to on-prem security stacks. It mitigates DDoS, man-in-the-middle, and DNS attacks by inspecting queries for malicious or suspicious domains. Event logs from Netskope's Cloud Firewall can integrate with the organization's SIEM tool for enhanced incident response and recovery.	• Cloud • Firewall • SD-WAN
SC.L2-3.13.6: Network Communication by Exception	Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).	Netskope's Cloud Firewall secures outbound traffic to the web and cloud applications across all ports and protocols, eliminating the need to route traffic through on-premises security systems. It protects against DDoS, man-in-the-middle, and DNS attacks by inspecting domain queries for threats. Additionally, event logs from Netskope's Cloud Firewall can be integrated with the organization's SIEM tool to aid in incident response and recovery.	• Cloud • Firewall
SC.L2-3.13.7: Split Tunneling	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (e.g., split tunneling).	Netskope's Borderless SD-WAN extends network perimeter capabilities to any user on any device, anywhere, by routing traffic through its global New Edge network. This ensures high-availability connectivity to web and cloud applications and enforces policy controls with adaptive trust based on user context, location, device, and app instance. Netskope's ZTNA Next offers remote access to onpremise or cloud-hosted private apps from any device, integrating with NIST-compliant identity providers for secure authentication. It uses end-to-end encryption for data security, applies granular control limits based on zero trust principles, logs all access attempts, and enforces policies related to failed login attempts.	• SD-WAN • ZTNA Next

CMMC Identifier	Practice Statement	Netskope Response	Products
SC.L2-3.13.8: Data in Transit	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Netskope's Comprehensive Security Suite includes CASB and NG-SWG, both utilizing a robust Data Loss Prevention (DLP) engine. The DLP engine employs machine learning for real-time identification, classification, and protection of sensitive data across web, cloud applications, and endpoint devices. Context-aware policies, considering users, devices, apps, and networks, help in data protection via encryption, obfuscation, or blocking actions. It also supports role-based access, ensures backup integrity, and facilitates continuous monitoring for incident response and forensic investigations. Netskope's NG-SWG integrates with NIST-compliant identity providers for secure SSO/MFA across web and cloud services. It decodes and logs numerous inline activities, detecting anomalies through user activity baselines. Granular policy controls address risky behaviors via multi-factor authentication, policy violation notifications, safer alternatives, or just-in-time training referrals. NG-SWG also generates customizable reports and alerts for SIEM tools, aiding in incident response and non-repudiation. Netskope's ZTNA Next ensures secure remote access to private apps with end-to-end encryption and zero trust principles, integrating with NIST-compliant identity providers for secure authentication. It logs all access attempts and enforces policies on failed logins, providing granular access control for enhanced security.	• CASB • NG-SWG • DLP • SkopeAI
SC.L2-3.13.9: Connections Termination	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Netskope's Borderless SD-WAN extends network perimeters to any user on any device, ensuring highavailability connectivity and consistent policy enforcement via its global New Edge network. It offers continuous adaptive trust using context-specific criteria like user and location. Netskope's ZTNA Next enables remote access to private apps from any device, integrating with NISTcompliant identity providers for secure authentication. It uses end-to-end encryption, applies granular access controls based on zero trust principles, and logs all access attempts, enforcing organizational policies on failed logins.	• SD-WAN • ZTNA Next
SC.L2-3.13.10: Key Management	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Netskope's products do not map to this requirement.	

CMMC Identifier	Practice Statement	Netskope Response	Products
SC.L2-3.13.11: CUI Encryption	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Netskope's Cloud Access Security Broker (CASB) and Next-Gen Secure Web Gateway (NG-SWG) feature an advanced Data Loss Prevention (DLP) engine designed to secure organizational data across web traffic, cloud applications, and endpoint devices. Leveraging machine learning, Netskope's DLP identifies, classifies, and protects sensitive data according to organizational and regulatory standards. Context-aware policies enhance real-time protection by considering users, devices, applications, networks, and actions, enabling measures like data obfuscation, file encryption, or action blocking. Additionally, Netskope's DLP enforces role-based data access during incidents, ensures backup integrity, and maintains logs in designated repositories for continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP
SC.L2-3.13.12: Collaborative Device Control	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Netskope Device Intelligence detects and categorizes all devices, both managed and unmanaged, on an organization's network. It segments these devices to isolate potential risks. Using AI and ML, it establishes a baseline of normal behavior, identifies anomalies, and enforces detailed access controls aligned with zero trust principles. Additionally, it integrates with incident response tools to trigger security alerts based on the organization's predefined criteria.	• Device Intelligence
SC.L2-3.13.13: Mobile Code	Control and monitor the use of mobile code.	Netskope Device Intelligence identifies and classifies all devices, both managed and unmanaged, connected to an organization's network. It segments devices to isolate risky ones and uses AI/ML to establish a baseline of normal behavior, detect anomalies, and enforce detailed access and activity controls based on zero trust principles. Additionally, it integrates with incident response tools to generate security alerts based on predefined criteria.	• Device Intelligence
SC.L2-3.13.14: Voice Over Internet Protocol	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Netskope's CASB and NG-SWG offer extensive data security through the Data Loss Prevention (DLP) engine, safeguarding data across web, cloud applications, and endpoint devices. Utilizing machine learning, Netskope's DLP identifies and protects sensitive data based on organizational and regulatory needs. Real-time protection is enforced via contextaware policies that consider user, device, app, network, and action details. The DLP also supports role-based access control, incident response, backup integrity, and continuous monitoring for forensic investigations. Netskope's NG-SWG integrates with NIST-compliant identity providers, extending SSO/MFA across web and cloud services. It logs over a hundred inline activities and establishes user behavior baselines to detect anomalies. The NG-SWG applies detailed policy controls, such as requiring multi-factor authentication for risky activities or alerting users of policy violations. It can produce customizable reports and alerts for SIEM tools and detailed event logs for non-repudiation of user actions.	• CASB • NG-SWG • DLP

CMMC Identifier	Practice Statement	Netskope Response	Products
SC.L2-3.13.15: Communications Authenticity	Protect the authenticity of communications sessions.	Netskope's NG-SWG integrates with NIST-compliant third-party identity providers, extending SSO/MFA across web and cloud apps. It decodes and logs over 100 inline activities, establishing user activity baselines to detect anomalies and applying detailed policy controls. These controls can notify users when they are about to commit a policy violation, require a stepped-up multi-factor authentication, request a business justification for risky actions, or suggest safer alternatives. The NG-SWG also generates customizable reports and feeds data into the organization's SIEM for incident response, providing non-repudiation of user actions. Netskope's Borderless SD-WAN extends network perimeters to any user/device globally. It routes traffic through Netskope's New Edge network, ensuring highavailability connectivity and uniform policy enforcement with adaptive trust based on user, location, and other contextual criteria. Netskope's ZTNA Next offers remote access to private apps via any device, integrating with NIST-compliant identity providers for secure authentication, and employing end-to-end encryption. It enforces zerotrust principles with granular access controls, logs all access attempts, and manages organizational policies on login failures.	• NG-SWG • SD-WAN • ZTNA Next
SC.L2-3.13.16: Data at Rest	Protect the confidentiality of CUI at rest.	Netskope Device Intelligence identifies, catalogs, and classifies all devices, both managed and unmanaged, connected to an organization's network. It groups these devices into network segments to isolate those deemed risky. Using its AI/ML engine, Device Intelligence establishes a baseline of normal device behavior and detects anomalies. It applies granular access and activity controls adhering to zero trust principles. Additionally, it can integrate with an organization's incident response tools to generate security alerts based on predefined criteria.	• Device Intelligence

SYSTEM AND INFORMATION INTEGRITY

CMMC Identifier	Practice Statement	Netskope Response	Products
SI.L1-3.14.1: Flaw Remediation	Identify, report and correct information and information system flaws in a timely manner.	Netskope's Cloud Confidence Index (CCI) evaluates the risk of using SaaS applications by examining criteria such as security policies, certifications, audit capabilities, and legal concerns. Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure compliance with access policies and industry standards, actively scanning cloud storage to prevent data exfiltration. CSPM's integration with Cloud Ticket Orchestrator facilitates automated alerts and remediation efforts.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
		Additionally, Netskope’s SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations and ensure compliance. SSPM provides detailed remediation instructions and integrates with Cloud Ticket Orchestrator to automate alert-driven service tickets and corrective actions. It also allows for the conversion of detected misconfigurations into new security rules, enhancing overall security.	
SI.L1-3.14.2: Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Netskope's Public Cloud Security can be enhanced with Advanced DLP, which scans IaaS Storage for hidden malware, providing robust cloud protection. The Remote Browser Isolation feature in Netskope's NG-SWG secures access to risky websites by isolating them in a cloud-based sandbox, preventing malware from infecting the organization's network. Standard Threat Protection guards against known malware and uses machine learning for new threats, offering real-time phishing detection and web filtering. Advanced Threat Protection extends the capabilities of Standard Threat Protection by using deobfuscation, recursive file unpacking, and multistage sandboxing to detect new malware. Netskope integrates these threat protection tools with its Cloud Threat Exchange and other Intelligent Security Service Edge tools, such as Cloud Firewall and User Entity and Behavior Analytics, to provide layered security. SkopeAI, leveraging machine learning, enhances the DLP engine by enabling deep contextual awareness to analyze and protect unstructured data like images. It excels in detecting various attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content, delivering superior speed and accuracy.	• NG-SWG • Public Cloud Security • RBI • Advanced DLP • Advanced Threat • Protection Threat • Protection SkopeAI
SI.L1-3.14.3: Update Malicious Code Protection	Monitor system security alerts and advisories and take action in response.	Netskope's Cloud Risk Exchange integrates risk scores for users, devices, and apps from third-party vendors like Crowdstrike and ServiceNow. It normalizes these scores based on organizational policies and enforces adaptive controls to mitigate risks posed by the most dangerous users, apps, and devices. Cloud Threat Exchange is a near real-time tool that facilitates bi-directional sharing of threat indicators such as malicious URLs and file hashes among Netskope customers and technology partners. It can automatically sync these indicators with an organization's SIEM tool to enhance threat detection and response. Cloud Ticket Orchestrator automates the creation of service tickets and workflows in response to security alerts, significantly streamlining incident response and recovery processes. It also enforces role-based access controls for involved teams.	• CRE • CTE • CTO

CMMC Identifier	Practice Statement	Netskope Response	Products
SI.L1-3.14.4: System & File Scanning	Update malicious code protection mechanisms when new releases are available.	Netskope's Public Cloud Security, enhanced with Advanced DLP, scans IaaS Storage for hidden malware to protect cloud environments. Its Remote Browser Isolation feature, part of Netskope's NGSWG, securely isolates risky websites in a cloudbased container, ensuring malware is contained and cannot infect the network. Netskope Device Intelligence identifies and classifies all devices connecting to the network, isolating risky ones. Its AI/ML engine establishes a normal behavior baseline to detect anomalies and apply zero-trust access controls, integrating with incident response tools for security alerts. Standard Threat Protection safeguards against known and new malware using machine learning, phishing detection, corroborative sandboxing, and web filtering. It integrates with Netskope's Cloud Threat Exchange and other security tools such as Remote Browser Isolation, Cloud Firewall, and User Entity and Behavior Analytics, providing a comprehensive, layered defense-in-depth security solution. Advanced Threat Protection goes beyond Standard Threat Protection by employing deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware.	• NG-SWG • Public Cloud Security • RBI • Advanced DLP • Advanced Threat Protection • Device Intelligence • Threat Protection
SI.L2-3.14.5: Security Alerts & Advisories	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.	Netskope's NG-SWG offers Remote Browser Isolation to securely contain risky web activities in a cloud-based sandbox, thwarting malware from infecting networks. Standard Threat Protection shields against known malware with machine learning capabilities for new threats, provides real-time phishing detection, corroborative sandboxing, and web filtering. Netskope's threat protection integrates with Cloud Threat Exchange and other security tools for a comprehensive defense approach. Advanced Threat Protection enhances Standard Threat Protection by adding deobfuscation, recursive file unpacking, and multi-stage sandboxing to counteract new malware. Device Intelligence identifies and classifies networkconnected devices, segments risky ones, and leverages AI/ML to detect anomalies and apply zero trust-based controls. It can also trigger security alerts through integration with incident response tools. SkopeAI enhances the DLP engine's ability to understand and protect unstructured data, including images, and excels in detecting various sophisticated attacks, polymorphic malware, novel phishing domains, zero-day threats, and malicious web content, delivering rapid and accurate threat detection.	• NG-SWG • RBI • Advanced Threat Protection • Device Intelligence • Threat Protection • SkopeAI

CMMC Identifier	Practice Statement	Netskope Response	Products
SI.L2-3.14.6: Monitor Communication s for Attacks	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Netskope's NG-SWG integrates with third-party identity providers to extend SSO/MFA across web and cloud apps, detecting anomalous behavior and applying granular policy controls. It can enforce context-aware rules like stepped-up MFA and just-intime cybersecurity training, and generates detailed logs for SIEM integration and non-repudiation. Netskope's Cloud Firewall applies security policies to egress traffic without backhauling and disrupts attacks by inspecting DNS queries, integrating logs with SIEM for incident response. Standard Threat Protection guards against malware and phishing, integrating with threat feeds and other security tools for a defense-in-depth approach. Advanced Threat Protection enhances malware detection with deobfuscation, recursive unpacking, and multi-stage sandboxing. Device Intelligence identifies and classifies networkconnected devices, using AI/ML to create behavioral baselines and apply zero trust principles.	• NG-SWG • Cloud Firewall • Advanced Threat Protection • Device Intelligence • Threat Protection
SI.L2-3.14.7: Identify Unauthorized Use	Identify unauthorized use of organizational systems	Netskope's Cloud Log Shipper exports event and alert logs from various Netskope tools, such as NGSWG, CASB, ZTNA Next, and more, to an organization's SIEM or incident response tool. The Cloud Risk Exchange aggregates risk scores for users, devices, and applications from third-party vendors like Crowdstrike and ServiceNow, normalizes these scores based on organizational policies, and enforces adaptive controls to mitigate risks. Similarly, the Cloud Threat Exchange enables near real-time bidirectional sharing of threat indicators, including malicious URLs and file hashes, among Netskope customers and partners, and can also automatically share this information with a SIEM tool.	• NG-SWG • CASB • ZTNA-Next • CLS • CRE • CTE

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 is 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 global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.