netskope

White Paper

How the Netskope Platform can assist with NIST CSF capability

The NIST Cyber Security Framework (CSF) integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity capability. It has become the recognized de facto industry standard.

The Framework not only helps organizations understand their cybersecurity risks (threats, vulnerabilities, and impacts), but how to reduce these risks with customized measures. The Framework also helps them respond to and recover from cybersecurity incidents, prompting them to analyze root causes and consider how they can make improvements.

THE FRAMEWORK CORE

The framework core defines the activities you need to do to attain different cybersecurity results. This is further divided into four different elements:

Functions: The five functions outlined in the NIST Cybersecurity Framework are identify, detect, respond, protect, and recover. These are your most basic cybersecurity tasks.

Categories: For each of the five functions, there are categories that are actually specific challenges or tasks that you must carry out. For instance, in order to protect (function) your systems, you must implement software updates, install antivirus and antimalware programs, and have access control policies in place.

Subcategories: These are the tasks or challenges associated with each category. For instance, in implementing software updates (category), you must be sure that all Windows machines have auto-updates turned on.

Informative sources: These are the documents/manuals that detail specific tasks for users on how to do things. For instance, you should have a document that would detail how auto-updates are enabled for Windows machines.

This document maps to the NIST Cyber Security Framework (CSF) version 1.1.

IMPLEMENTATION TIERS

The NIST Cybersecurity Framework specifies four implementation tiers. This would help you know at what level of compliance you are in. The higher the tier, the more compliant you are.

Netskope has produced these artifacts to assist customers to understand how the Netskope platform contributes to an organization's ability to strengthen and mature their capabilities with respect to the NIST CSF. Specifically, each subcategory has been analyzed indicating how, if applicable (not all sub-categories are applicable), the Netskope platform will support an organization on this journey.

Color	ID	Description
	Complete	Addresses all of the subcategory
	Contribute	Provides a significant contribution to addressing the subcategory
	Inform	Outputs of the Netskope suite provide insights and information to help address the subcategory
	N/A	Does not address the subcategory

	Identify	Protect	Detect	Respond	Recover	Total
Complete	2	8	0	0	0	**10**
Contribute	11	15	13	8	0	**47**
Inform	3	3	3	2	0	**11**
N/A	13	13	2	6	6	**40**
Subcategory total	**29**	**39**	**18**	**16**	**6**	**108**

SNAPSHOT

Identify	Protect	Detect	Respond	Recover
ID.AM-1	PR.AC-1	DE.AE-1	RS.RP-1	RC.RP-1
ID.AM-2	PR.AC-2	DE.AE-2	RS.CO-1	RC.IM-1
ID.AM-3	PR.AC-3	DE.AE-3	RS.CO-2	RC.IM-2
ID.AM-4	PR.AC-4	DE.AE-4	RS.CO-3	RC.CO-1
ID.AM-5	PR.AC-5	DE.AE-5	RS.CO-4	RC.CO-2
ID.AM-6	PR.AC-6	DE.CM-1	RS.CO-5	RC.CO-3
ID.BE-1	PR.AC-7	DE.CM-2	RS.AN-1	
ID.BE-2	PR.AT-1	DE.CM-3	RS.AN-2	
ID.BE-3	PR.AT-2	DE.CM-4	RS.AN-3	
ID.BE-4	PR.AT-3	DE.CM-5	RS.AN-4	
ID.BE-5	PR.AT-4	DE.CM-6	RS.AN-5	
ID.GV-1	PR.AT-5	DE.CM-7	RS.MI-1	
ID.GV-2	PR.DS-1	DE.CM-8	RS.MI-2	
ID.GV-3	PR.DS-2	DE.DP-1	RS.MI-3	
ID.GV-4	PR.DS-3	DE.DP-2	RS.IM-1	
ID.RA-1	PR.DS-4	DE.DP-3	RS.IM-2	
ID.RA-2	PR.DS-5	DE.DP-4		
ID.RA-3	PR.DS-6	DE.DP-5		
ID.RA-4	PR.DS-7			
ID.RA-5	PR.DS-8			
ID.RA-6	PR.IP-1			
ID.RM-1	PR.IP-2			
ID.RM-2	PR.IP-3			
ID.RM-3	PR.IP-4			
ID.SC-1	PR.IP-5			
ID.SC-2	PR.IP-6			
ID.SC-3	PR.IP-7			
ID.SC-4	PR.IP-8			
ID.SC-5	PR.IP-9			
	PR.IP-10			
	PR.IP-11			
	PR.IP-12			
	PR.MA-1			
	PR.MA-2			
	PR.PT-1			
	PR.PT-2			
	PR.PT-3			
	PR.PT-4			
	PR.PT-5			

Function	Category	Subcategory	Netskope reference	Coverage
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Netskope does not map to this subcategory	N/A
		ID.AM-2: Software platforms and applications within the organization are inventoried	Netskope provides detailed reports and interactive dashboards that categorize, risk score, and show the usage of thousands of applications in use within the enterprise. As of this writing, Netskope will aid in the inventory and categorization of more than 55,000 applications. It is of critical importance to note that Netskope identifies, inventories, and enforces real-time control for unmanaged applications (end-user adopted SaaS applications that have not been officially onboarded by IT, otherwise known as Shadow IT). Netskope also provides policy controls by app instance (e.g., company vs personal) for managed apps.	Contribute
		ID.AM-3: Organizational communication and data flows are mapped	Netskope is able to characterize SaaS, IaaS, and web usage across an entire enterprise. This includes the monitoring of non-corporate devices accessing corporate SaaS applications and users accessing non-corporate SaaS applications from IT-managed devices. With Netskope in place, security teams are able to map communication and data flows to an exceptional degree of accuracy. Netskope will not only map where data is flowing, including for company and personal app instances, but also provide the necessary controls to contain data flows when unmanaged devices are being used and unmanaged services are being adopted by end-users.	Contribute
		ID.AM-4: External information systems are catalogued	Netskope NG-SWG and CASB solutions, both key components of the Netskope Intelligent Security Service Edge (SSE) can detect and catalogue external, unmanaged SaaS applications (Shadow IT) with an unmatched degree of accuracy. This ensures that all non-managed SaaS applications, including personal instances of Google Drive or Dropbox, can be catalogued.	Complete
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Netskope can enforce conditional access policies to resources based on user, location, service, activity, device type, operating system, and access method. Organizations can use these detailed conditional access policies to tailor access to SaaS applications and internally published applications via Netskope Private Access. In addition, Netskope can give priority traffic, rate-limit the bandwidth usage, enforce access based on applications, devices, and user groups using Netskope Borderless SD-WAN.	Contribute
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Netskope does not map to this subcategory	N/A
		ID.BE-2: The organization's place in critical infrastructure and its industry sector are identified and communicated	Netskope does not map to this subcategory	N/A
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Netskope does not map to this subcategory	N/A
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Netskope Borderless SD-WAN supports high availability/resilience to access critical SaaS applications, by enabling failover to alternate connectivity links at sub-second upon blackout/ brownout.	Contribute
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Netskope Borderless SD-WAN supports high availability/resilience to access critical SaaS applications, by enabling failover to alternate connectivity links at sub-second upon blackout/ brownout.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
IDENTIFY (ID)	**Governance (ID. GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	User notifications can pop up in real time when a user violates a policy. This ensures the user is educated on organizational policy in real time and prevents the incident from occurring. This enforcement mechanism is extremely valuable to security teams, as it provides immediate feedback to the user upon a policy violation and can block the activity before it completes. There is a high degree of flexibility in this mechanism, as Netskope provides the ability to warn users before a potential violation occurs, or block them entirely from carrying out the action, or provide real-time coaching, suggest safer alternatives, or collect justification for an activity.	Contribute
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Netskope does not map to this subcategory	N/A
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Netskope Security Posture Management (SPM) solutions are available for cloud services (CSPM) and managed SaaS applications (SSPM), giving visibility and control over cloud service security settings to manage them according to legal, regulatory, and company policy requirements. Netskope's Cloud Confidence Index (CCI) also provides a risk-based score for SaaS applications, incorporating assessments based on privacy policies and regulatory compliance. This can help organizations understand and manage regulatory requirements related to SaaS applications, both managed and unmanaged.	Contribute
		ID.GV-4: Governance and risk management processes address cybersecurity risks	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
IDENTIFY (ID)	**Risk Assessment (ID. RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	Netskope discovers cloud apps in use in the enterprise and provides a Cloud Confidence Index (CCI) score to each app. This is a scoring system that takes into account many criteria, including recently disclosed vulnerabilities and exploits. Netskope investigates the SaaS app for vulnerabilities and exploits such as Heartbleed, POODLE SSL v3 Fallback, etc. This category in the CCI ensures that your organization is less susceptible to attacks that could lead to a data breach, damage to brand reputation, or loss of customer trust. In addition, Netskope uses User and Entity Behavior Analytics (UEBA) to determine when anomalous behavior has occured, which can help identify a possible exploited vulnerability, and point to an area for further investigation.	Inform
		ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources	Netskope Cloud Threat Exchange (CTE) integrates with threat intelligence from open source and commercial information-sharing forums to collect, analyze, and leverage intelligence on known malicious domains and IP addresses as part of the overall threat detection capability. CTE also automatically bidirectionally shares IOCs between deployed defenses, including endpoints, SIEMs, SOAR, and IR systems. Netskope threat protection, part of NG-SWG, CASB and other Netskope solutions, also includes over 40 threat intelligence feeds.	Complete
		ID.RA-3: Threats, both internal and external, are identified and documented	Netskope NG-SWG provides a User Confidence Index (UCI) and behavior-based analytics on user activities, which can help organizations identify internal threats. Netskope NG-SWG can detect data bulk uploads, downloads, and deletes, plus proximity, failed logins, shared credentials, rare events, risky countries, and data exfiltration between company and personal SaaS instances. Netskope Advanced Threat Protection can detect external malware from web and cloud delivery and analyze to block in real time. Netskope provides detailed analysis of the malware type, which can help organizations understand the type of threats and external threat actors impacting their organization.	Contribute
		ID.RA-4: Potential business impacts and likelihoods are identified	Netskope helps to supplement this category in an important way. Understanding which SaaS apps are in use within an enterprise, and more importantly, how they are being used, how much duplication of apps, plus company and personal instances are all critical factors in accurately assessing business impacts of data loss to SaaS applications. Netskope provides the ability to quantify how much potentially sensitive data resides in SaaS platforms beyond the corporate network perimeter. Netskope also provides the control set to secure this data. In addition, as part of delivering visibility on network and cloud performance, Netskope Digital Experience Management (DEM) helps customers understand 'first mile' performance from Netskope's cloud, powered by the NewEdge network) to their critical cloud and SaaS apps.	Inform
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Netskope CCI provides a risk-based score to over 55,000 cloud applications. This risk-based score can help organizations understand the overall impact using a specific SaaS application may have on an organization. In addition, Netskope UCI calculates risk scores for individual users and devices, based on alerts, events, and activity anomalies. Additional risk information is provided by Netskope Cloud Risk Exchange (CRE), which allows sharing of risk values for individual users and devices with other security solutions. Both CCI and UCI can be used within adaptive policy controls.	Contribute
		ID.RA-6: Risk responses are identified and prioritized	Netskope Security Posture Management (SPM) is available for public cloud (CSPM) and managed SaaS applications (SSPM), and includes remediation instructions for all compliance violations and labels each with a severity to help inform response. Netskope Cloud Risk Exchange (CRE) has the ability to normalize risk scores from multiple sources and invoke investigations into or actions to reduce risk from significant changes in user or device risk scoring.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	Netskope does not map to this subcategory	N/A
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Netskope CCI provides a risk-based score to over 55,000 cloud applications. Organizations can adjust the given CCI score, based on risk elements which are important to the organization, such as the selling of data to third parties, or adherence to GDPR.	Inform
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis	Netskope does not map to this subcategory	N/A
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Netskope does not map to this subcategory	N/A
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Netskope scores SaaS applications in its Cloud Confidence Index (CCI) and provides many important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	Contribute
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	Netskope does not map to this subcategory	N/A
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	Netskope does not map to this subcategory	N/A
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Netskope NG-SWG and Netskope Private Access provides auditing and verification of user identities and credentials. Netskope NG-SWG also allows organizations to manage and audit credentials for unmanaged SaaS applications, including detecting shared credentials used across multiple devices by multiple users, proximity alerts, rare events, and risky countries. CSPM and SSPM also provide security configuration, auditing, compliance, and company checks for user identities in cloud services and managed SaaS apps.	Contribute
		PR.AC-2: Physical access to assets is managed and protected	Netskope does not map to this subcategory	N/A
		PR.AC-3: Remote access is managed	Netskope is a cloud platform designed specifically to enforce controls for remote users and provides absolutely critical capabilities in this area for web, SaaS, Shadow IT, and IaaS/PaaS remote access. Netskope's reverse proxy also allows administrators to safely govern access from non-corporate devices to IT-managed apps and cloud services by granting restricted access (such as allowing login, but blocking downloads). This ensures that when remote access must be granted from a non-corporate device, it can be done in a controlled fashion to ensure a high level of end-user productivity without sacrificing security controls. Netskope also extends the access control functionality of web gateways to remote users without needing to steer traffic back to the corporate network. This means that corporate web policy is enforced for remote users alongside cloud access controls in the same platform and policy. Finally, Netskope can also provision internal applications to remote users without the need for inbound access rules and traditional VPNs. This Zero Trust Network Access (ZTNA) capability ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN).	Complete
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Netskope provides granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to least privilege. When access to a SaaS application is granted, administrators can differentiate between personal, third-party, and corporate-owned instances of the same managed app and adjust policy controls accordingly. Activity controls can be implemented for both corporate-owned devices for web, SaaS, Shadow IT, and IaaS/PaaS, as well as personal devices accessing corporate managed apps and cloud services. ZTNA capabilities ensure that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access and inbound access rules.	Complete
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Netskope Private Access provides Zero Trust secure access to private enterprise applications. This ensures that servers and applications hosted in corporate networks are securely segregated from external access through Netskope. This Zero Trust Network Access (ZTNA) capability ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN). In addition, Netskope Borderless SD-WAN offers network level segmentation via application/identity aware firewall and VLANs.	Contribute
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Netskope NG-SWG provides detailed logging of all web and cloud activity by users, including inline app and cloud service API-level actions decoded by Netskope's Cloud XD patented technology. This detailed activity level of logging and proxy transaction events will assist organizations in asserting non-repudiation for actions in their SaaS applications.	Contribute
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Netskope NG-SWG extends SSO/MFA across managed and unmanaged apps and cloud services, and detects 100+ inline actions within SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. When a risky action is detected, such as an upload of company data to a non-managed SaaS application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user. Adaptive policy controls can also leverage CCI ratings for apps and UCI risk scoring for the user to determine what is permitted.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	Netskope NG-SWG can provide real-time user coaching when performing actions in SaaS applications. Netskope can coach users on data loss risks, including the context of app risk and user risk, and when performing activities with the option to proceed or cancel, or to provide a justification for managed and unmanaged apps, and websites so business processes can continue. Netskope can also redirect users to third party solutions like KnowBe4 for just in time training, reflecting the combination of the attempted activity and the users' perceived danger level to the company.	Contribute
		PR.AT-2: Privileged users understand their roles and responsibilities	Netskope NG-SWG detects specific activities within SaaS applications, such as upload, post, delete, or download. When a risky action is detected, such as an upload to a non-managed SaaS application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user. Netskope can also require a business justification for the risky activity.	Contribute
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	Netskope NG-SWG detects specific activities within SaaS applications, such as upload, post, delete, or download. Netskope can block certain actions by third-party users with instructional coaching, providing safter alternatives, requesting a justification, or a proceed or cancel alert message in real time. Netskope can also redirect users to third party solutions like KnowBe4 for just in time training, reflecting the combination of the attempted activity and the users' perceived danger level to the company.	Contribute
		PR.AT-4: Senior executives understand their roles and responsibilities	Netskope NG-SWG detects specific activities within SaaS applications, such as upload, post, delete, or download. When a risky action is detected, such as an upload to a non-managed SaaS application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user. Netskope can also require a business justification for the risky activity.	Contribute
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	Netskope NG-SWG detects specific activities within SaaS applications, such as upload, post, delete, or download. When a risky action is detected, such as an upload to a non-managed SaaS application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user. Netskope can also require a business justification for the risky activity.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
PROTECT (PR)	**Data Security (PR. DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	Netskope provides data-at-rest scanning and protection capabilities for IT managed SaaS and IaaS applications. This includes the ability to perform data loss prevention scans which can alert on DLP violations and take corrective action. The Netskope platform can be configured to automatically revoke sharing permissions or encrypt a file, for example if a file containing sensitive information is being shared excessively.	Contribute
		PR.DS-2: Data-in-transit is protected	The Netskope cloud platform provides the ability to enforce real-time control on data-in-transit across all SaaS, IaaS, and web usage within the enterprise including widely adopted Shadow IT apps and cloud services. Netskope's cloud-hosted, enterprise-grade data loss prevention capabilities ensure that data is protected in transit anywhere in the enterprise, including remote users with the current pandemic conditions. Netskope's DLP engine is fully integrated into the entire cloud platform, ensuring that both data-at-rest and data-in-transit are protected by the same set of policies and workflows. This ensures that policy is easy to implement and the DLP program is easy to maintain in an ongoing capacity.	Complete
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Netskope does not map to this subcategory	N/A
		PR.DS-4: Adequate capacity to ensure availability is maintained	Netskope Borderless SD-WAN offers adequate capacity for remote devices accessing critical SaaS applications and critical on-premises applications via providing multiple performance tiers to fit the scenario.	Contribute
		PR.DS-5: Protections against data leaks are implemented	Netskope's cloud platform is constructed specifically to address key gaps existing in traditional security stacks. With the continuous adoption of SaaS apps and cloud services for data hosting and storage, organizations are struggling to extend traditional security controls for these apps and cloud services. Netskope is also able to enforce real-time protections on data-in-motion to unsanctioned, user-adopted Shadow IT applications. This type of granular data protection control is difficult or impossible for many enterprises to accurately address without the Netskope cloud platform in place. Netskope provides this capability for thousands of cloud-hosted SaaS applications and cloud services. Netskope leverages a global-scale, cloud-native security platform to implement security controls in the cloud for any user, device, or location. In addition, Netskope's Endpoint DLP provides monitoring and protection for endpoint data in use, including device control for USB storage devices.	Complete
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Netskope API-based IaaS Storage Scan can scan cloud storage buckets and blobs to detect unauthorized changes to cloud storage data, including detecting if legitimate software has been replaced with malware. In addition, Netskope Security Posture Management (SPM) solutions, including CSPM (cloud services) and SSPM (SaaS), can be used to verify settings and configurations in cloud services and SaaS applications.	Inform
		PR.DS-7: The development and testing environment(s) are separate from the production environment	Netskope does not map to this subcategory	N/A
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
PROTECT (PR)	**Information Protection Processes and Procedures (PR. IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	Netskope CSPM enables organizations to develop and maintain a baseline configuration of their AWS, Azure, and GCP environments. CSPM provides assessments against common security and regulatory frameworks, such as CIS, PCI, NIST, and HIPAA. Netskope CSPM can alert when cloud infrastructure deviates from the baseline, and can be configured to remediate any detected misconfigurations. Netskope SSPM provides the same functionality for managed SaaS applications. Also, Netskope NG-SWG provides inline IaaS/PaaS user traffic analysis for 250+ AWS services and 9,000+ APIs, plus similar inline functionality for GCP and Azure environments.	Contribute
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	Netskope does not map to this subcategory	N/A
		PR.IP-3: Configuration change control processes are in place	Netskope API-based IaaS Storage Scan can scan cloud storage buckets and blobs to detect unauthorized changes to cloud storage data, including detecting if legitimate software has been replaced with malware. Netskope CSPM and SSPM can be configured to detect and provide remediation configuration changes in cloud services and SaaS, which are made outside the regular change management process. Misconfigurations, such as public S3 buckets, can be immediately revoked to reduce any organizational risk or exposure.	Inform
		PR.IP-4: Backups of information are conducted, maintained, and tested	Netskope does not map to this subcategory	N/A
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Netskope does not map to this subcategory	N/A
		PR.IP-6: Data is destroyed according to policy	Netskope does not map to this subcategory	N/A
		PR.IP-7: Protection processes are improved	Netskope does not map to this subcategory	N/A
		PR.IP-8: Effectiveness of protection technologies is shared	Netskope Advanced Analytics (AA) can assist by identifying trends, give visibility into areas of concern, and allows the use of data to take action. AA can monitor the effectiveness of your security program and communicate results to stakeholders. AA helps management, compliance teams, and applications owners align on key performance indicators to keep organizations focused on the same goals.	Inform
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Netskope does not map to this subcategory	N/A
		PR.IP-10: Response and recovery plans are tested	Netskope does not map to this subcategory	N/A
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Netskope can enforce additional controls for personnel who are deemed to be high-risk users, for example those who may be leaving an organization. This could include adding a user to a more restrictive set of controls when their risk profile increases (such as when they are in the process of leaving an organization). Additionally, Netskope can help to ensure that HR platforms and services are accessed appropriately (i.e., by the appropriate personnel, activities are controlled, excessive permissions are not granted, etc.). Netskope threat research shows employees are 3x more likely to copy company data to personal app instances in the last 30 days of employment where instance-awareness policy controls can prevent this user behavior.	Contribute
		PR.IP-12: A vulnerability management plan is developed and implemented	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Netskope does not map to this subcategory	N/A
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	The Netskope platform is able to log activity of remote users and ensure that corporate policy is enforced on their managed devices. This ensures that remote activities, such as maintenance occurring in Infrastructure-as-a-Service platforms, are logged at minimum, and policy can be enforced on those activities as well. Netskope Private Access is also able to grant remote access capabilities to remote employees in a Zero Trust model, without the need for inbound access rules that can expose other parts of the network.	Complete
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Netskope operates as a next-generation inline proxy and records user activity firsthand. All user activity on SaaS, IaaS, and the web is recorded in a way that is meaningful to administrators. Rather than simply providing bytes up and bytes down to web destinations, Netskope records the actual activities taking place, such as Share, Edit, Delete, Upload, Like, View, etc. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the CLS (Cloud Log Shipper) tool, or automatically creating service tickets with the CTO (Cloud Ticket Orchestrator) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real-time.	Contribute
		PR.PT-2: Removable media is protected and its use restricted according to policy	Netskope's Endpoint DLP provides monitoring and protection for endpoint data in use, including device control for USB storage devices.	Complete
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Netskope NG-SWG can be configured to only allow certain activites on both managed and unmanaged SaaS solutions. This allows organizations to permit generic actions on unmanaged SaaS products, such as download files, but prevent or restrict actions which aren't essential, such as an upload action. Netskope Private Access also helps to restrict access to internal applications, resources, and systems at a group or user level granularity.	Complete
		PR.PT-4: Communications and control networks are protected	Netskope Private Access protects private networks through a Zero Trust model. This ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN). Netskope NG-SWG Advanced Threat Protection provides real-time malware detection and IPS capabilities for organizational web traffic, incorporating threat intelligence to detect malicious web traffic traversing an organization's network. Netskope Cloud Firewall (CFW) provides firewall policies for egress traffic across ports and protocols for users and offices.	Complete
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Netskope Borderless SD-WAN offers hot standby at remotes sites to help achieve resilience requirements at remote locations.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	Netskope Behavior Analytics identifies baselines of user behavior for web, app, and cloud services activity via real-time inline and API out of band monitoring across its Security Service Edge (SSE) solutions. A user confidence index (UCI) risk score is supported by 67 detectors, 44 machine learning models, and 9 sequential anomaly rules to detect insiders, data exfiltrationn, and compromised accounts and devices. UCI scores can be shared with 3rd party solutions via Cloud Risk Exchange (CRE) and used in adaptive access policies. UEBA time lines and event correlation are provided in dashboards, drill down reports, plus advanced analytics to uncover unknown risks. Netskope automatically identifies a baseline of normal user behavior via real-time monitoring of user activity. Anomaly alerts are generated when unusual activity occurs. Netskope also serves to identify and secure new services being onboarded by end-users (Shadow IT).	Contribute
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	Netskope supplements this control by logging user activity with a set of details in order to provide critical context to events that may be involved in an incident. This includes information such as the device the event occurred on, the user, the app or service being accessed, the activity (such as a share, upload, delete, etc.), and many other important criteria. This event stream can be fed into a customer's SIEM tool to further facilitate the investigation of incidents.	Contribute
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Netskope's open architecture and CLS (Cloud Log Shipper) tool enables third-party integration with market-leading security services, including Splunk, CrowdStrike, QRadar, Rapid7, Exabeam, AWS, Google, Microsoft, Sumologic, and LogRhythm. Customers can integrate their Netskope deployment with existing solutions within their environment to ensure that the detailed data generated by Netskope is collected and correlated. Risky user data from Microsoft, Mimecast, ProofPoint, and KnowBe4 can be correlated to Netskope User Confidence Index scores with Cloud Risk Exchange (CRE) and converted into a weighted, aggregate score for tracking, investigation, policy controls, and responding.	Contribute
		DE.AE-4: Impact of events is determined	Netskope NG-SWG monitors user activity in real time, detecting and understanding all inline JSON-based API actions in apps and cloud services. With Netskope, security teams are able to map communication, and data flows to an exceptional degree of accuracy. This can help understand the impact of an incident if it occurs within an organization's SaaS cloud app, including managed and unmanaged applications, and by instance (company vs personal). In addition, Netskope Digital Experience Management (DEM) provides visibility and actionable insights on network and cloud performance to ensure the best user and app experience.	Contribute
		DE.AE-5: Incident alert thresholds are established	Netskope NG-SWG provides customizable alert thresholds for malware detection, unauthorized actions, DLP, malicious sites, and compromised credentials. Alert thresholds can be configured for anomaly detections, such as large file uploads, downloads, and deletes.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
DETECT (DE)	**Security Continuous Monitoring (DE. CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	Without the Netskope platform, a significant amount of visibility can be lost. Netskope performs SSL decryption at a global scale, and monitors activity from users that are remote as well as within the corporate network. Monitoring and policy enforcement of corporate assets is extended beyond the corporate network perimeter, with a cloud platform able to understand user activity and data flows in web, modern SaaS apps, cloud services , and egress traffic with inline proxy, firewall and IPS network defenses.	Contribute
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Netskope does not map to this subcategory	N/A
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	The Netskope platform provides a significant amount of visibility to network administrators. Netskope not only monitors SaaS, Shadow IT, IaaS, web and egress traffic from both on-network and remote users, but app and cloud service activity is also logged to the extent that specific user actions within cloud apps is recorded (e.g. Share, Edit, Delete, Upload, Download, etc). This is due to Netskope's unique ability to decode inline unpublished API calls and JSON streams to record user activity in real time across apps and cloud services, including by instance (company vs personal).	Contribute
		DE.CM-4: Malicious code is detected	Netskope NG-SWG Advanced Threat Protection provides anti-malware detection, bare-metal and cloud sandboxing, and ML-based detection to detect and prevent malicious code being executed. Netskope ATP provides pre-execution analysis and heuristics for 3,500+ file format families, with 3,000+ static binary threat indicators for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types.	Contribute
		DE.CM-5: Unauthorized mobile code is detected	Netskope does not map to this subcategory	N/A
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Netskope can monitor activity from SaaS provider activity logs via API integration, and also monitors inline end-user activity for both managed and unmanaged services by identifying user activities e.g., Edit, Share, Delete, Upload, Reboot, etc.) via forward proxy. Reverse proxy capabilities even allow for inline enforcement on non-corporate devices that are accessing corporate SaaS applications. Netskope Private Access can monitor external service provider access to internal resources.	Contribute
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Netskope monitors SaaS, Shadow IT, IaaS, web, and egress traffic for the entire enterprise. Netskope can monitor activity on personal devices connecting to corporate SaaS apps, and can monitor activity from corporate devices going to SaaS, Shadow IT, IaaS, and web. This ensures that unauthorized connections, software, devices, and even unauthorized personnel can be monitored and controlled via real-time policy. In addition, Netskope IoT Security extends zero trust to the IoT environment through discovery, classification, and management of IoT devices in the hybrid enterprise network. The solution's HyperContext® platform discovers both managed and unmanaged devices on the corporate network and derives rich device-level contextual intelligence for deep insights into the device behavior and risk profile, while enforcing policies for granular access control and micro-segmentation.	Contribute
		DE.CM-8: Vulnerability scans are performed	Cloud misconfigurations, including public storage buckets and open security groups, can leave organizations vulnerable to attacks.The Cloud Security Posture Management (CSPM) solution scans the cloud environment for misconfigured security settings and issues with cloud service configuration. SaaS Security Posture Management (SSPM) provides similar configuration, compliance, and company checks for managed apps.	Inform

Function	Category	Subcategory	Netskope reference	Coverage
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	Netskope can support the roles and responsibilities for detection by leveraging information such as data sensitivity, region, staff business unit or teams, or other customizable information provided via the directory infrastructure.	Inform
		DE.DP-2: Detection activities comply with all applicable requirements	Netskope is able to detect and block traffic that is considered anomalous when compared to peer activity by Netskope's predefined conditions, rules, and machine-learning technology.	Contribute
		DE.DP-3: Detection processes are tested	Netskope can aggregate and alert on automated testing results from third-party systems if they are configured to send the results to Netskope.	Inform
		DE.DP-4: Event detection information is communicated	Netskope provides security and network teams with a high degree of visibility into user activity on the web, SaaS, Shadow IT, and IaaS. This activity can be distributed through a variety of means, including high-level reports, advanced analytics, detailed event logs, and even exported using CLS to third-party tools (e.g., SIEM, UBA, XDR, Zero-Trust, or SOAR applications) using Cloud Log Shipper (CLS) or near real-time transaction event streaming. In addition, Netskope Digital Experience Management (DEM) provides broader visibility on network and cloud performance, granular insights into user experience, traffic patterns, app usage and even Netskope Client adoption).	Contribute
		DE.DP-5: Detection processes are continuously improved	Netskope continuously improves detection processes by advancing its integration with security operation center processes and third party solutions. APIs are provided for sandboxing, retrospective hunting, plus the Cloud Exchange modules for threat intel sharing, log export, risk score exhange, and workflow automation with orchestration and collaboration solutions. To also improve detection process, MITRE ATT&CK analysis is provided in sandboxing reports.	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	Netskope does not map to this subcategory	N/A
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	Netskope does not map to this subcategory	N/A
		RS.CO-2: Incidents are reported consistent with established criteria	Netskope Digitial Experience Manager (DEM_ provides visibility on network and cloud performance so degradation, failover or critical health/status information is accessible in near real-time. In addition, Netskope Cloud Ticket Orchestrator (CTO) allows customers to map customer alerts, events, and log data into whatever format is required to facilitate automated workflows in ServiceNow, Jira, and Pager Duty, or notifications in Slack, Teams, Email, etc.	Contribute
		RS.CO-3: Information is shared consistent with response plans	Due to the fact that Netskope is able to provide both detailed activity logs and high-level reports, security teams can be assured that they will have the information they need to effectively communicate critical information consistent with response plans that are in place. Netskope Cloud Ticket Orchestrator (CTO) enables the automatic creation of tickets in IT Service Management (ITSM) solutions and collaboration systems from events.	Inform
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Netskope does not map to this subcategory	N/A
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	The Netskope Cloud Exchange (CE) provides customers with powerful integration tools to leverage investments across their security posture. Netskope Cloud Threat Exchange (CTE) enables bidirectional threat intelligence sharing. This can be integrated with both open and closed-source intelligence feeds, ensuring that up-to-date threat intelligence is in the Netskope platform. Cloud Risk Exchange (CRE) enables sharing of risk scores for user and devices, normalizing scores, and the ability to trigger actions with Netskope Clout Ticket Orchestrator (CTO).	Contribute

Function	Category	Subcategory	Netskope reference	Coverage
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	Netskope NG-SWG integrates with the customer's SIEM via near real-time transaction event streaming, Cloud Log Shipper (CLS), and SOAR tools with Cloud Ticket Orchestrator (CTO), which can generate alerts or tickets based on incident notifications from Netskope. Reports can be directly generated on notification from SIEM and SOAR systems and investigated via the Netskope interface.	Contribute
		RS.AN-2: The impact of the incident is understood	Netskope NG-SWG provides detailed insights and rich metadata for user traffic across five lanes including web, SaaS, Shadow IT, IaaS, and public-facing custom apps. This can significantly help inform the impact of a cyber incident, including the number of systems, users, and online services impacted by the incident.	Inform
		RS.AN-3: Forensics are performed	Netskope captures and displays key data points that are critical for forensic investigations. This includes activity-level detail for user traffic analyzed for web and cloud access. Netskope is able to show administrators user activity in services that would be unmonitored without the Netskope platform in place including Shadow IT and personal app instances. Netskope can also provide the file-content details of DLP violations so that forensics can be performed on policy violations.	Contribute
		RS.AN-4: Incidents are categorized consistent with response plans	Netskope incident severity can be set by the organization, in accordance with existing severity and incident categorization criteria. This enables organizations to have consistent categorization across tools and response plans.	Contribute
		RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
RESPOND (RS)	**Mitigation (RS. MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	Netskope inline policy controls ensure that additional restrictions can be enforced in the event of an incident. This can include, for example, a restrictive set of policies that can be immediately put in place to ensure particular applications are not accessed or activities within particular applications are not performed. For example, a non-corporate instance of a SaaS application can be immediately blocked upon discovery of its use in an incident (while still allowing the corporate instance of the same app). Netskope Remote Browser Isolation (RBI) can also be used to contain web-based attacks and incidents within a remote browser, that is completely isolated from the user's device.	Contribute
		RS.MI-2: Incidents are mitigated	Netskope NG-SWG with Advanced Threat Protection, Remote Browser Isolation (RBI), Cloud Firewall (CFW), and Client Traffic Exploit Prevention (CTEP) provides active mitigation against malware, risky websites, phishing, browser attacks, OS vulnerabilities, and firewall egress controls over ports and protocols. Further, Netskope Private Access provides Zero Trust access to organizational applications, protecting and mitigating remote access attacks (e.g., ransomware entry point) which can arise from the use of traditional VPNs and compromised RDP, SSH, and remote access.	Contribute
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Netskope Private Access can enforce conditional access policies and posture checks for access to organizational applications. In the instance where a new vulnerability is identified in an Operating System or software component, Netskope can block access to devices running this vulnerable software, mitigating the impact of the new vulnerability.	Contribute
	Improvements (RS. IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	Netskope does not map to this subcategory	N/A
		RS.IM-2: Response strategies are updated	Netskope does not map to this subcategory	N/A

Function	Category	Subcategory	Netskope reference	Coverage
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	Netskope does not map to this subcategory	N/A
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	Netskope does not map to this subcategory	N/A
		RC.IM-2: Recovery strategies are updated	Netskope does not map to this subcategory	N/A
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, internet service providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	Netskope does not map to this subcategory	N/A
		RC.CO-2: Reputation is repaired after an incident	Netskope does not map to this subcategory	N/A
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Netskope does not map to this subcategory	N/A

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

To learn more visit, https://www.netskope.com.