Netskope for Government

Government organizations across levels — federal, state, and local — are adopting cloud and web services because of the flexibility, scalability, and cost savings that these services provide. But with with so many cyber incidents and breaches happening, it's critical to protect cloud and web usage and secure sensitive data for compliance and privacy.

QUICK GLANCE

- Comply with government security requirements from FISMA, FITARA, OMB, NIST, DoD, and more
- Address privacy and security concerns over sensitive data
- Monitor cloud and web risks and control costs
- Enforce security and access controls over cloud and web services
- Protect against cloud threats and malware

GOVERNMENT AND CLOUD USAGE

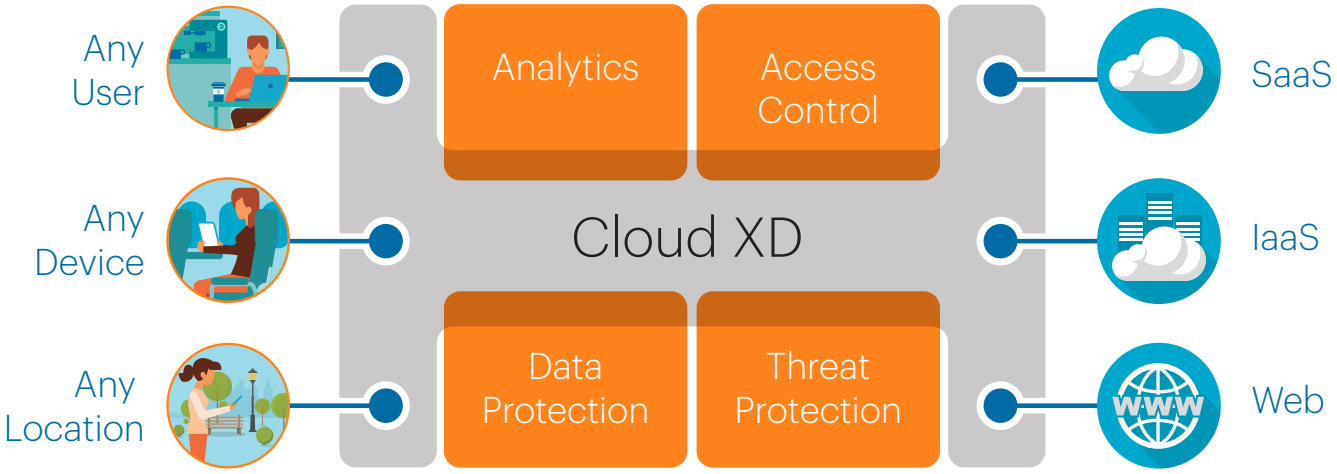
Government organizations are increasingly under attack from state-sponsored groups and hackers and face scrutiny over their budgets and use of resources. This leads to a variety of regulations and protections like the Federal Information Security Modernization Act (FISMA), Federal Information Technology Acquisition Reform Act (FITARA), and more.

Netskope helps U.S. public sector and government agencies and departments comply with federal regulations, protect sensitive data, and defend against threats across SaaS, IaaS, and web. Following NIST recommendations for cyber security, data protection, incident response and threat management, Netskope addresses the cloud and web aspect across all stages noted: identify, protect, detect, respond, and recover.

Security Requirements Across NIST Stages

STAGE	REQUIREMENTS
Identify	• Identify all services in use across SaaS, IaaS, and web • Assess cloud and web risk with contextual information on devices, user identity, location, and more • Evaluate enterprise-readiness of cloud services in use based on objective criteria like availability, business continuity, certifications, privacy, data security, vulnerabilities, and more
Protect	• Enforce security policies to restrict risky activities • Place access controls to ensure proper usage of cloud and web services • Secure sensitive data with strong encryption
Detect	• Detect and remediate cloud threats like malware with automated workflows • Identify and place controls over data exfiltration activities and other insider threats or privileged account abuses
Respond	• Use comprehensive cloud incident management for full resolution of incidents from start to finish • Take advantage of automated workflows like quarantining of suspected DLP violations and real-time user coaching
Recover	• Run reporting with ad hoc queries and dynamic reports across all cloud usage for auditing and compliance purposes • Use cloud risk dashboard to continuously inform organizational continuity and recovery plans

Netskope Security Cloud



FEATURES

Deep visibility and risk assessment of cloud and web usage

Find and assess all cloud services in use, sanctioned or unsanctioned, as well as web use. Evaluate cloud and web usage in the organization with full contextual detail including users, sessions, performance, devices, browsers, time periods, locations, content (including type), and even user activity (e.g., "share" or "upload") and size of traffic per cloud service. The Netskope Cloud Confidence Index (CCI) also allows government organizations to assess the enterprise-readiness of cloud services based on a set of objective criteria across security, auditability, data privacy, and more. Use ad hoc queries and dynamic reports in real time for a dashboard of usage and risk. Answer questions like "Who is sharing sensitive content outside of the agency?" or "Which cloud services in use are high risk to the agency?"

Granular security policies and access controls over cloud and web services

Netskope provides granular, contextual control over sanctioned and unsanctioned cloud services and websites in real time and in data at rest in sanctioned services. Rather than take a coarse-grained approach of blocking services, set security policies at a contextual level based on service or website, user, activity, device, and more. Choose policy enforcement actions such as block, alert, bypass, encrypt, quarantine, and coach. For sanctioned services and suites like Microsoft Office 365, G Suite, Box, and more, Netskope provides governance across identity, services, activities, devices, and data. Enforce policies such as "Encrypt all PII content uploaded to cloud services" or "Alert on the download of PII from any cloud service to a mobile device," and more. For unsanctioned and ecosystem services, Netskope provides visibility and control at the service and category level or globally with set-it-once policies like "No download of PII to a mobile device" or "Allow people to receive content from their partners' cloud storage services, but block them from uploading to or sharing from any except our agency's sanctioned one." Enforce these policies across all users, even if they are remote, mobile, or using a native app or sync client.

Comprehensive DLP

Netskope DLP prevents sensitive data leakage in the cloud and web with accuracy and precision across sanctioned and unsanctioned services in real time and for data at rest. Reduce false positives with Netskope DLP, which detects sensitive content accurately across 1000+ file types and across structured and unstructured data, using 3,000+ pre-defined data identifiers, metadata extraction, proximity analysis, fingerprinting, exact match, and more. Existing on-premises DLP solutions can also be integrated out of the box with secure ICAP. Netskope also offers incident management capabilities with closed-loop administration and remediation workflows to facilitate the end-to-end incident management process. Included in this are privacy features such as role-based access controls (RBAC). Protect data in the cloud with AES 256-bit encryption for data-at-rest and FIPS 140-2 Level III certified fault tolerant, in-the-cloud key management solution with integrated hardware security module (with an optional on-premises key manager or via integration with an existing one).

Cloud threat and malware protection

With a comprehensive vantage point over cloud and web service usage, Netskope combines threat intelligence, static and dynamic analysis, and machine-learning based anomaly detection to enable real-time detection, prioritized analysis, and remediation of threats that may originate from — or be further propagated by — the cloud and web. Using threat intelligence, static and dynamic analysis, and anomaly detection, Netskope detects and remediates the latest viruses, advanced persistent threats (APTs), spyware, adware, worms, ransomware, and other malware. Netskope also guards against cloud threats such as compromised credentials (that are re-used or shared), privileged user and access abuse such as data exfiltration from a sanctioned service to an unsanctioned one, and access to malicious sites.

USE CASE	DESCRIPTION
FITARA compliance	FITARA compliance requirements include consolidation of services to reduce cost and management and enhance security. In relation to the cloud, Netskope can be deployed to help identify all cloud services being used (including unsanctioned, shadow IT cloud services) and determine which are redundant. The cloud services can be evaluated across contextual usage criteria to identify location (including from countries that may be high risk), device, user identity, and more. The Netskope Cloud Confidence Index can be used to evaluate various cloud services for vendor assurance and due diligence before standardization. Additionally, inline controls allow for automated coaching of government employees to sanctioned cloud services. Netskope offers comprehensive deployment options to facilitate unique use cases, including remote workers, BYOD, and shared networks.
FISMA and NIST federal requirements	In order to strengthen information security systems, FISMA outlines multiple guidelines that can be applied to cloud usage, including the summarized ones below: • **Overall visibility and continuous monitoring.** Netskope can continuously inventory all cloud and web services in use with contextual data on users, devices, locations, cloud activity, data being shared, and more. Ad hoc reports and dynamic queries can be run in real time to fulfill auditing requirements. • **Risk and vulnerability assessments in services used.** The Netskope Cloud Confidence Index evaluates over 20,000 cloud services across objective criteria. Services with vulnerabilities or other attributes that may impact organizational continuity or security can be evaluated and rated according to risk based on usage. • **Security controls and data protection.** Security policies based on contextual information like use of an unmanaged device or risky activity like sharing can be restricted with granular security controls from Netskope. Sensitive data can be secured with AES 256-bit encryption. Access controls are included in these controls, as well as cloud threat and malware protection. Administrators can follow up with suspected violations with full cloud incident management capabilities. • **Determination of effectiveness of security controls and programs.** To determine if security controls are effective over time and align with risk tolerance (especially with respect to the cloud), Netskope provides risk dashboards that are customizable based on what information is important to the administrator. • **Authorization and accreditation enforcement.** Agencies and CISOs designate Authority to Operate (ATO) designations for cloud systems and the subsequent flow downs on conditions for an ATO can be continuously monitored for compliance and overall risk by service, users, sessions, or domains. This can also be correlated with overall user behavior scores for all consumed cloud services.
Cloud privacy and risk assessment	This encompasses multiple regulations across public and private sectors, like HIPAA or PCI-DSS. With a cloud access security broker (CASB) like Netskope, it's possible to identify all sensitive data being used in cloud services and either secure it with encryption or place security controls to restrict risky activities like sharing with unauthorized individuals or to unauthorized cloud services. Protections can be placed on systems of record to ensure sensitive data like personally identifiable information is secure. Netskope inline- and API introspection-based capabilities can be configured to find and secure PII, identify cloud activities in scope for privacy impact assessments, privacy threshold assessments, System of Records Notices (SORNs), and others.