Netskope for State and Local Government

CHALLENGES FOR K12 SCHOOLS

The adoption of cloud solutions has completely changed the way organizations operate and manage data. Cloud services account for 85 percent of all web traffic flowing across internet connections. There is an average of over 2400 cloud services in use per organization and this number increases every year. A majority of this traffic is encrypted making it extremely difficult to inspect and take appropriate actions using legacy security tools. Appliances are overloaded, reports lack necessary details, and understaffed teams comb through multiple consoles to piece an incident together. Breaches aren't slowing down, and Public Sector entities continue to be a target. As these gaps in visibility and protections increase so do the regulations State and Local government entities need to answer to. There is a better way.

NETSKOPE SECURITY CLOUD PLATFORM

Netskope runs one of the world's largest and fastest security networks. Performing SSL/TLS inspection at scale allows Netskope to provide rich data and granular controls to IT admins without adding latency and friction to the user experience. Never again worry about sizing up an appliance or having to whitelist a large chunk of traffic because of performance hits.

Netskope takes a data-centric approach to cloud security, protecting data and users everywhere. Applications are protected from data loss prevention and theft. Take control of sensitive data that already lives in cloud instances via APIs and prevent future violations with inline protections. Have sensitive data in IaaS providers like GCP, Azure, or AWS? The Netskope Continuous Security Assessment checks instances against industry benchmarks like CIS or custom profiles and rules to ensure cloud services remain secure.

Leverage our intimate understanding of the cloud to safely enable the cloud and web. The Netskope platform speaks the language of apps so that admins can implement specific controls based on actions of a user or device posture. Preventing downloads from unmanaged or BYOD devices, redirecting users to managed cloud apps, and blocking the use of personal cloud storage are just a few of the actions that can be taken.

Rapid growth of cloud apps has led to their increased use across the ransomware kill chain, presenting a challenge to security teams trying to disrupt the use of apps to propagate ransomware. Netskope's threat detection helps stop ransomware and detects unauthorized encryption of files stored or synced in the cloud. Threat protection also stops malware, trojan, phishing, and botnet attempts.

COMPLIANCE

To maintain compliance in the cloud, organizations need advanced data controls that are context-aware, able to differentiate between managed and unmanaged services — and between managed and personal instances of the same services. The Netskope Security Cloud provides granular and customizable DLP policies for all of these services.

PCI DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is an international, comprehensive standard outlining the minimum security requirements for cardholder data. The standard is not a law, but any service provider that processes or handles payment card data must adhere to the regulation's requirements. Netskope's PCI profile detects and prevents PCI data from being shared publicly or outside managed applications.

HIPAA HITECH

HIPAA has specific compliance requirements tied to privacy and security. Addressing HIPAA compliance requirements is a challenge in today's cloud- and mobile-first world given the lack of visibility and control, and this is a gap Netskope fills perfectly. Use reverse proxy to prevent unauthorized access of data that is in managed apps and inline protections to prevent data misuse on managed devices.

FTI

Federal Tax Information (FTI) Data means federal or state tax returns, return information, and such other tax-related information as may be protected by State and federal law. Policies and form fingerprinting ensure FTI information remains in secure drives or managed cloud apps to prevent data mishandling or loss.

The Netskope Security Cloud platform enables organizations to extend their information protection policies and threat protection from on-premises infrastructure and applications to cloud services. Policies can detect malicious or sensitive content at rest in managed cloud services or enroute to or from any cloud service with advanced, cloud DLP and threat engines. Further, you can define granular policies — based on identity, service, content category, activity and data — to automatically protect your data by blocking activities, restricting access, encrypting data, and more.

The best part is web security, data security, threat protection — every aspect of the Netskope Cloud Platform is managed in one platform, one console, and one policy. No more console fatigue or learning multiple platforms to manage cloud security.

CLOUD RISK ASSESSMENT

Want to know if Netskope is right for your institution? Reach out to schedule a demo or Cloud Risk Assessment that will:

- Identify and build awareness around cloud usage
- Assess risk based on apps, users and data movement
- Understand potential data exposure
- Uncover malicious apps and files
- Lay out a step by step mitigation roadmap using the Netskope platform