Netskope for K12

CHALLENGES FOR K12 SCHOOLS

Cloud adoption has changed the way schools work and manage data. Cloud services account for 85 percent of all web traffic flowing across internet connections. Many schools use cloud apps like GSuite to manage their education environment. A majority of web and app traffic is encrypted making it extremely difficult to inspect and take appropriate actions using legacy security. Files are improperly or publicly shared putting student and faculty data at risk. Appliances are overloaded, reports lack necessary details, and understaffed exhausted teams comb through multiple consoles to piece an incident together. Many schools implement 1-1 device programs where students are allowed to take devices home. The overhead of protecting and managing these devices puts more stress on teams that are already stretched thin. Breaches aren't slowing down, and schools continue to be both targets and victims for ransomware attacks, trojans, and data breaches. Despite these growing challenges, the budget and team size stay the same.

Thanks to Netskope there is a streamlined way to address all of these challenges in one platform.

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 and lose protection and visibility because of performance hits.

Have a 1-1 device program? Leverage the Netskope lightweight steering client for acceptable use, protection from threats like malware and phishing, data loss prevention, and granular reporting both on and off network. New policies are easily pushed from the management console to keep up with evolving needs.

Rich reporting allows admins to see DLP, threat, acceptable use, and customize reporting in one console. Streamlined incident management and granular policies allow the Netskope Security Cloud Platform to eliminate threats and remediate incidents without admin interaction, freeing staff up for more important tasks. Response actions are built into policies to prevent DLP and threat incidents.

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, botnet, phishing, and trojan attempts that have been plaguing schools.

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.

FERPA

FERPA does not prohibit the use of cloud computing solutions for the purpose of hosting education records. FERPA requires states to use reasonable methods to ensure the security of their information technology solutions. Netskope helps schools with FERPA compliance by detecting and remediating violations that exist in cloud instances today and preventing new violations from occurring. Prebuilt profiles for HIPAA, PCI, Grades, and Academic Terms detect violations with minimal false positives. Fingerprints of sensitive school forms such as IEPs can be taken to determine if copies exist in cloud instances.

CIPA

In order to receive much needed E-rate funding schools must be CIPA compliant and provide measures to block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors for computers that are accessed by minors. The Netskope Next Gen Secure Web gateway (SWG) has over 130 categories for acceptable use policies and the ability to create custom categories. These policies can be enforced on and off network protecting students with 1-1 devices.

The Netskope Security Cloud platform enables schools 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 protection. 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 cloud security, data security, threat protection — every aspect of the Netskope Cloud Platform is managed with one platform, one console, and one unified policy engine. 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