Netskope for Higher Ed

CHALLENGES FOR HIGHER ED

Cloud adoption has changed the way schools work and manage data. Higher education institutions have been quick to move to the cloud because of benefits such as availability, scalability, and cost reduction. A majority of web and app traffic is encrypted making it extremely difficult to inspect and take appropriate actions using legacy tools. Appliances are overloaded, reports lack necessary details, and understaffed exhausted teams comb through multiple consoles to piece an incident together. Many institutions are rampant with student BYOD and IoT devices that can't have a client or certificate installed. The overhead of protecting and managing these devices puts more stress on teams that are already stretched thin. Breaches aren't slowing down, and higher ed continues to be targets 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.

Take control of sensitive data that already lives in cloud instances via APIs and prevent future violations with inline protections. When sensitive data lives in IaaS providers like GCP, Azure, or AWS Netskope's Continuous Security Assessment checks instances against industry benchmarks like CIS or custom profiles and rules to ensure instances remain secure. When student BYOD devices need access to a managed app use the Netskope reverse proxy to get detailed logging and policies on unmanaged devices.

Rich reporting allows admins to see data loss prevention (DLP), advanced threat protection (ATP), 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 DLP violations without admin interaction, freeing staff up for more important tasks. Response actions are built into policies to prevent data loss and threat incidents.

Rapid growth of cloud apps has led to their increased use across the threat kill chain, presenting a challenge to security teams trying to disrupt the use of apps to propagate ransomware. Netskope threat protection stops malware, botnet, and phishing without disrupting benign activities and internet access that supports a learning environment.

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 requires institutions 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.

HIPAA HITECH

Many higher ed intuitions manage research and medical information. 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.

GLBA

While the Gramm-Leach-Bliley Act primarily regulates financial institutions many higher education institutions are also required to adhere to components of the GLBA because student loan activity flows through these institutions. Netskope provides the visibility and control institutions need to address GLBA compliance needs.

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, instance, content category, activity and data — to automatically protect your data by blocking risky 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

netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership. **To learn more, visit netskope.com**