Leading insurer transitions to Netskope for more efficient control over cloud access, web browsing

Case Study

Offering a variety of individual and group life and health insurance plans, this insurance company operates across 100+ branches to actively enhance and protect the lives of more than 1.5 million people. The company also offers extensive digital touchpoints to enhance the customer experience.

How to provide web and cloud security in response to a massive transition to remote work?

When the licenses on its legacy web and cloud security appliances came up for renewal, the IT & Security teams at this insurance company wanted to evaluate alternatives. In part, the team was motivated by uncertainties associated with the legacy vendor's recent merger with another company.

Another major driver, however, was the need for a security solution that would better accommodate what had become a largely remote workforce. The insurance company's legacy solution did not provide enough visibility into the cloud services and apps that its remote workers were using, nor did it provide insight into the workers' browsing activity on the internet.

Specifically, the IT team was concerned about shadow IT, including personal and rogue instances of managed apps. As many as 97% of shadow IT apps are freely adopted by business units and users. The team wanted more granular access controls, as well as threat controls that extended beyond websites, since 68% of malware today is cloud-delivered, mainly from personal and rogue instances of cloud storage apps, as well as malicious Office documents.

"We evaluated the Netskope technology for 10 days and found the performance while accessing applications was better, with detailed visibility for the applications being accessed including activities performed, which met our requirements."

– CISO & Data Protection Officer, at Insurance Company

Profile

Industry	Region	Employees	Revenue
Financial Services	Global	2500+	$900M+

Challenges

- Need to secure cloud/web use of largely remote workforce.
- Lack of visibility into cloud app and web browsing activity.
- Concerns about merger affecting legacy vendor's business.

Solutions

- Netskope Security Cloud with Netskope client on endpoints.

Results

- Discovery of unmanaged app use.
- Effective application of controls for better data governance.
- No more appliance maintenance or patching, saving staff time.

Robust cloud access and web security controls place minimal burden on remote users

The insurance company's IT team implemented the Netskope solution in Inline mode: The Netskope clients on the managed endpoints provide real-time visibility and control through the Netskope Security Cloud. The lightweight client uses minimal CPU resources on the client system, and all proxy and security functionality is performed in the cloud.

This has significant performance implications for users, as their CISO says, "We evaluated the Netskope technology for 10 days and found the performance while accessing applications was better, with detailed visibility for the applications being accessed including activities performed, which met our requirements."

Beyond the typical ability to allow, deny, or parse URLs, the Netskope Security Cloud provides a wide range of policy control variables including app, app risk, action, and data sensitivity, with adaptive policies to invoke step-up authentication and real-time coaching to users.

> "Netskope as a security services edge is automatically updated, we no longer need to maintain and patch appliances"
>
> –CISO & Data Protection Officer at Insurance Company

Granular visibility enables effective management of cloud/web risk, as unified platform reduces TCO

Using the Netskope solution, the IT team discovered that its remote users were accessing multiple unsanctioned apps. In response, they applied controls for data movement, developed app risk profiles, and are now coaching users to select safer app alternatives. The team has also leveraged Netskope to block malicious web requests, including cloud-delivered malware and cloud-enabled threats.

The insurance company's CISO appreciates the seamless deployment of the Netskope solution and the fact that it provides one security cloud platform, one console, one policy engine, and one client for remote users. "Netskope as a security services edge is automatically updated, we no longer need to maintain and patch appliances," he says.

Migrating to Netskope has also reduced the company's total cost of ownership (TCO) for its web and cloud security tools. "We didn't need to invest in multiple hardware and software products or in additional licenses for conditional access," their CISO explains.

He also notes that Netskope's unified cloud platform will make it easy for the IT team to build more controls in the future, such as Granular SaaS / IaaS control & Data Protection (CASB) Zero Trust Network Architecture (ZTNA), cloud security posture management (CSPM), SaaS Security Posture Management (SSPM), firewall-as-a-service (FWaaS) functions, and controls specified in the regional Cyber Security Framework.

"Implementation was quick and was fully supported by our Netskope partner," the CISO says. "The transformation project was operational before the timeline, and fine-tuning was part of the timely delivery process."