How a Hospital IT Team Gets "More Sleep and More Smiles" Thanks to Advanced Inline CASB

An internationally-recognized hospital partnered with Netskope to enhance data security, dramatically overhaul its DLP effectiveness to reach zero false positives, better equip its remote workforce, and achieve the all-too-rare balance of making things easy and secure.

Now, says its IT leadership, "We get more sleep and we get more smiles."

THE CHALLENGE

A well-known hospital, renowned for its groundbreaking research and other specialties, had two significant challenges related to its IT environment and use of cloud applications.

The first was to prevent any authorized exfiltration of patient data and do so without causing unnecessary friction, false positives, or security alerts that would slow down its fast-moving staff's ability to collaborate.

No team wants to enable the sending of private data where it shouldn't go, either unintentionally or maliciously. At the same time, user experience and security can't be a trade-off. And in a remote-heavy environment—here is a hospital that shifted from 200 to 20,00 remote employees in a very short span during the COVID-19 pandemic—that trade-off isn't just inconvenient, it's unacceptable.

"Sure, I can tell the entire staff you can't use this app and it's blocked and that's the way it is, and I can sleep peacefully knowing it is secure," said the hospital's head of IT security. "But I can't make anyone happy. I can't make anyone more productive doing it that way, telling them they can't use the tools they need to get things done."

The second challenge was to prevent malware from entering the hospital network via what the hospital discovered was a constellation of SaaS apps, both managed and unmanaged, both authorized and unauthorized (or "shadow").

PROFILE

INDUSTRY
Health

REGION
United States of America

CHALLENGES

- Prevent any authorized exfiltration of patient data and do so without causing unnecessary friction
- Prevent malware from entering the hospital network on both managed and unmanaged SaaS apps

BENEFITS

- Provided visibility and control for thousands of managed and unmanaged apps
- Improved data protection

SOLUTIONS

- Adv. DLP (Exact Data Match)
- Real-Time Protection for SaaS
- CASB Inline

Making its Office 365 implementation secure was a big job already, further compounded by how many hospital team members were linking it to various other applications, including file transfer services such as Dropbox. The hospital didn't have a reliable view of which connections to Dropbox and other apps were benign or potentially exposing data. But it couldn't just shut down those apps, shaky security or not—a too-aggressive lockdown against non-sensitive collaboration would have brought staff productivity to a crawl.

Enter Netskope.

THE SOLUTION AND IMPLEMENTATION

The hospital's IT team experienced daily escalations over concerns of unauthorized data moving around using insecure apps. Its then-current DLP solution was cross-checking against HIPAA dictionaries—that is, using the healthcare compliance law's definitions as the basis of keywords and other rules—but at best only achieving 70% accuracy, meaning false positives and unnecessary escalation nearly 30% of the time.

In-line CASB quickly became a primary need for improving data protection and reducing false positives—specifically a level of visibility and control for thousands of apps (managed and unmanaged), including users, file names, and activity.

Implementing Netskope brought an immediate impact.

"We experienced a lot of back-and-forth with staff that an organization like ours can never really get ahead of," said the head of IT. "We needed an exact data match. We needed to get an index of existing patients and be able to match it to enforce all the rules. Netskope did this for us—with literally zero false positives."

THE RESULTS

CASB Inline helped the hospital and its now-heavily-distributed staff of caregivers, researchers, and other stakeholders confidently manage and prevent the unintentional or unapproved movement of sensitive data between cloud app instances, with full context of app risk, user risk, and access risk.

Beyond dramatically improved accuracy and zero false positives, the hospital was also able to increase the visibility of all of its SaaS apps in use throughout the network, and supplement its existing firewall and other security tools without disruption.

The hospital successfully reclaimed countless hours previously spent on manual escalation, chasing down false positives, and forensics. The team is also confident in its ability to prevent sensitive data exfiltration on a scale that might have been "too big to fit neatly on a slide," said the head of IT.

He continued: "Before, we could never be 100%. We couldn't say that to our auditors or say with confidence that all patient data was prevented from flowing into Dropbox. We also couldn't give users the flexibility of using apps for non-sensitive transfers. Rarely do we have a security solution like this that can make things so easy and secure."

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.