Forcepoint

Customer Story

Healthcare Giant Achieves Compliance with Unified Security Platform

The Forcepoint ONE platform unifies security to help this healthcare giant protect its complex network and maintain compliance with HIPAA, PCI-DSS and other regulations.

A complex network of physicians and hospitals make it difficult to protect access to data from managed and unmanaged devices across multiple locations. After trying different solutions, the healthcare provider chose Forcepoint ONE—a unified security platform. The agentless CASB with SAML SSO, SWG, and DLP all combined to deliver true Zero Trust and ensure the organization complied with regulations such as HIPAA and PCI-DSS.

CUSTOMER PROFILE:
The healthcare provider boasts one of the largest networks in North America. The organization operates over 800 locations with the support of its more than 150,000 employees.

INDUSTRY:
Healthcare

HQ COUNTRY:
United States

PRODUCT:
› Forcepoint ONE

Network Complexity Risks Non-Compliance

No organization knows complexity better than this healthcare giant, whose 150,000 team members work in harmony to deliver best-in-class care across more than 800 locations.

Over time, data protection became increasingly difficult due to a complicated network architecture. Surging cloud adoption and an influx of unmanaged devices from its physicians threatened its ability to maintain compliance and protect sensitive information.

"We needed greater visibility and control of PHI and PII, wherever it was being accessed—especially on devices we didn't manage," the organization's CISO said.

The business needed to comply with federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standards (PCI-DSS) and various state regulations concerning its Personally Identifiable Information (PII). However, it had to manage all these needs without impacting the productivity of its large network of physicians and hospitals.

Simplifying Security with Forcepoint ONE

Initially, the organization considered adopting a third-party Single Sign-On (SSO) solution to pair with Microsoft's native security for Office 365.

Because the organization is composed of sister institutions with different domains and Active Directory (AD) trees, the IT team couldn't deploy third-party SSO at scale. Additionally, Microsoft's built-in security lacked real-time threat protection and granular control over data.

"We were trying to protect our network—which was pretty complex in its own right—with siloed point products, which created challenges in itself," the CISO said.

The organization needed to strike a balance: future-proof its security posture, so it could continue to expand its use of cloud services like Office 365 and ServiceNow, while avoiding the risk of introducing resource-intensive solutions that didn't communicate with each other.

Ultimately, the healthcare provider decided on Forcepoint ONE for a unified approach to managing web, cloud, and private application access through an assortment of integrated security tools.

Challenges

- Provide secure access for 150,000 physicians across multiple domains and Active Directory trees.
- Comply with federal regulations such as HIPAA and PCI-DSS, as well as state regulations for Personally Identifiable Information (PII).
- Extend security footprint to managed and unmanaged devices throughout 800+ locations.

Maintaining Compliance Without Losing Flexibility

Forcepoint ONE delivered the capabilities the healthcare giant needed to maintain compliance with HIPAA and PCI-DSS. At the same time, the unified platform simplified security within the complex network through the help of:

- → An agentless Cloud Access Security Broker (CASB) with SAML SSO to govern cloud application access for managed and unmanaged devices from one portal.
- → Secure Web Gateway (SWG) to extend policies to web applications.
- → Data Loss Prevention (DLP) to prevent unauthorized access to or exfiltration of PHI and PII, wherever the data resides.

The platform delivers true Zero Trust capability, empowering employees to remain productive by limiting access to sensitive data. The healthcare provider now ensures physicians and staff only have access to the applications they need through an agentless CASB.

Despite the complex architecture of the network, the project was easy to deploy. Adoption was quick considering employees didn't need to install any agents. The healthcare provider now leverages Forcepoint ONE as a central platform to evolve its security strategy as new threats emerge.

Approach

- Deploy Forcepoint ONE.

Results

- Unified security solution delivered visibility, compliance, and access control on the cloud at scale.
- Maintained compliance in Office 365, ServiceNow, and other places data resides.
- Provided simple and secure access for managed and unmanaged devices via an agentless CASB with an integrated SAML SSO.