Forcepoint

Customer Story

Fortune 100 Healthcare Provider Expands Security Footprint to Public Cloud

Forcepoint ONE's CASB enabled a Fortune 100 healthcare provider to safely deploy Office 365.

An on-premises focus for security delayed the deployment of Office 365 applications like OneDrive and SharePoint. The organization needed a Cloud Access Security Broker (CASB) that could provide granular access control, inline data protection, and discovery of PHI, PII and intellectual property flowing through managed and unmanaged devices. After evaluating multiple vendors, the healthcare provider chose Forcepoint ONE for its CASB and integrated Data Loss Prevention (DLP).

CUSTOMER PROFILE:
The Fortune 100 healthcare provider supports over 700 locations worldwide with the help of its 50,000 staff.

INDUSTRY:
Healthcare

HQ COUNTRY:
United States

PRODUCT:
› Forcepoint ONE

Walking To The Cloud

Protecting data is difficult. But securing it as it flows through tens of thousands of managed and unmanaged devices from public cloud apps? Regardless of how complex it might be, this Fortune 100 healthcare provider knew it wasn't impossible.

In a similar fashion to other organizations in its industry, the firm moved to Office 365 to boost its workforce's productivity. However, its security coverage stopped the project in its tracks.

"Our existing architecture for this type of protection was an on-premises mix of NGFW, SWG, and DLP," the healthcare provider's CISO said. "It wasn't purpose-built to protect data in the cloud, and we initially thought we might have trouble integrating a new solution."

While the team had deployed Outlook, it wanted to implement tighter security controls for accessing and sharing data before it rolled out OneDrive and SharePoint. Its BYOD policy meant users across the world could interact with PHI, PII, and intellectual property from their personal devices. This opened up the healthcare provider to risks like data leakage or a breach.

Initially the company looked toward native Office 365 security controls but found that it did not provide an adequate level of data protection, especially when access was coming from an unmanaged device. After looking outside of the Microsoft suite and the solutions already in place, CASB became an attractive option.

A CASB that Meets All Needs

On the heels of successfully deploying Outlook, the company wanted a comprehensive – yet easy to use – solution so it could continue with the other Office 365 applications.

"At the top of our list was usability, both for our own team and the end users," the CISO said. "We also wanted strict but seamless access control, API functionality, and the ability to discover and protect data across our managed and unmanaged devices."

Challenges

- Protect PHI, PII, and corporate intellectual property flowing out of the cloud onto managed and unmanaged devices.
- Find a solution that integrates with on-premises Next-Generation Firewall (NGFW), Secure Web Gateway (SWG), and DLP from other vendors.

The healthcare provider shifted its attention to a CASB as a means of applying the security controls it needed in public cloud apps. It trialed three vendors – including Forcepoint ONE.

In the trials, it quickly became apparent that its existing architecture would limit its choice of CASB. Most of the solutions the healthcare provider trialed were API-driven solutions, meaning the security team would only be able to detect data leakage after it had occurred.

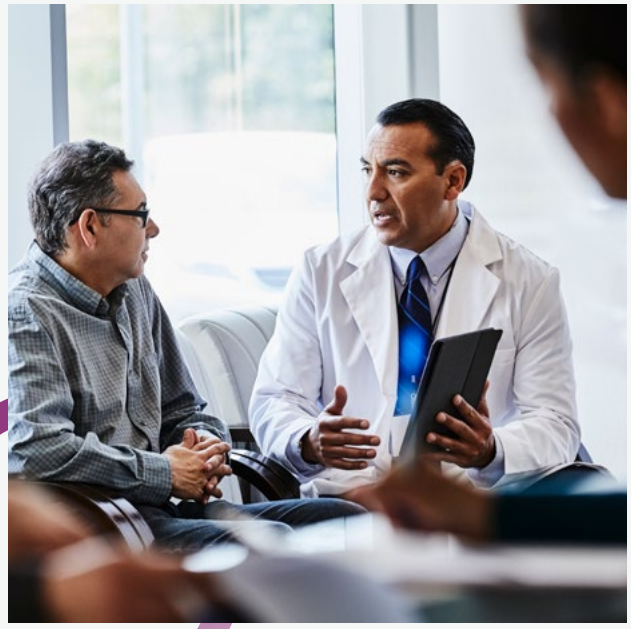
Forcepoint ONE's inline data protection found in its CASB provided real-time security, ensuring that users could not remove proprietary or personal data from OneDrive or SharePoint. Because the CASB was agentless, this functionality was also extended to users interacting with data on their personal devices.

Powering Workforce Productivity

The Fortune 100 healthcare provider ultimately chose Forcepoint ONE's CASB.

Forcepoint ONE is a unified platform that includes DLP. Having a DLP integrated with the CASB meant the organization did not have to rely solely on an external DLP via ICAP, as a CASB from another vendor would need to.

The healthcare provider was able to quickly implement the CASB and continue with its Office 365 rollout, supplying critical protection to channels where lack of coverage creates risk of a data breach.



Approach

- Deploy Forcepoint ONE's agentless CASB.
- Leverage integrated DLP.

Results

- Rapid rollout and integration of CASB with on-premises solutions to secure public cloud applications such as OneDrive and SharePoint.
- Enable real-time data protection and avoid reactive approach offered by API-only solutions.
- Extend security to unmanaged devices to support BYOD policies.