Forcepoint

Customer Story

Fortune 100 Healthcare Provider Protects Microsoft 365 Data Using Forcepoint CASB

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

An on-premises focus for security delayed the deployment of Microsoft 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 Data Security**, including **Forcepoint CASB (inline + API)**, and F**orcepoint Web Security**, combined with **integrated Forcepoint Data Loss Prevention (DLP).**

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 Microsoft 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."

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(s):

- **Forcepoint CASB**
- **Forcepoint DLP**
- **Forcepoint Web Security**

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 Microsoft 365 security controls but found that they 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, robust CASB with inline and API-based capabilities became the clear requirement.

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 Microsoft 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."

The team evaluated three vendors and found that most solutions relied heavily on **API-only controls**, meaning threats and data leakage were often detected only after they occurred.

Forcepoint, on the other hand, delivers comprehensive cloud security with **equally strong API-based and inline CASB capabilities**. This includes inline CASB enforcement, CASB API discovery, and endpoint web controls, providing true **real-time protection** across SaaS and private applications.

Forcepoint's **inline data protection** ensures sensitive data is monitored and controlled in real time within services like OneDrive and SharePoint. Its **agentless design** extends protection to unmanaged and personal devices without requiring installation or configuration, enabling secure access everywhere users work.

Powering Workforce Productivity

By choosing Forcepoint's Data Security Cloud platform, the organization gained:

- → **Unified data protection** with a single DLP policy across inline CASB, CASB API, web and endpoint
- → **Faster deployment** of OneDrive, SharePoint and other Microsoft 365 applications
- → **Consistent, real-time enforcement** eliminating previous gaps that increased breach risk

Extended BYOD protection through agentless controls Forcepoint's integrated approach allowed the provider to modernize its cloud security architecture quickly and confidently, ensuring sensitive data remained protected, no matter where users worked or what device they used.

Challenge:

- Protect PHI, PII and corporate intellectual property flowing out of the cloud onto managed and unmanaged devices

Approach:

- Deploy Forcepoint's **inline CASB** and agentless CASB API controls
- Extend secure access through Forcepoint Web Security
- Utilize **integrated Forcepoint DLP**, with unified policy control across cloud, web and endpoint

Results:

- Rapid integration of cloud security controls to protect OneDrive, SharePoint and other SaaS applications
- Real-time, inline data protection – avoiding the delayed detection model of API-only CASB solutions
- Expanded protection to unmanaged devices to safely support global BYOD
- Consistent cloud, web and endpoint enforcement through Forcepoint's unified data protection