Fortune 500 Asset Manager Secures its Data in Any Cloud

The Forcepoint ONE platform helped the investment firm secure its data in cloud applications like Slack, Salesforce and Office 365.

Ahead of deploying public cloud applications, this Fortune 500 asset management firm sought complete assurance its clients' data would remain private and secure. After evaluating every Cloud Access Security Broker (CASB) on the market, the company chose to adopt Forcepoint ONE. The unified platform provided a dynamic, agentless CASB that secured data on managed and unmanaged devices, enabled real-time remediation, and identified risky shadow IT.

CUSTOMER PROFILE:

The Fortune 500 investment management firm services client assets in a variety of markets. It has over 6,000 employees and operates out of nearly a dozen locations across the U.S.

INDUSTRY:

Financial Services

HQ COUNTRY:

United States

PRODUCT:

› Forcepoint ONE

Balancing Productivity with Data Security

Trust is a concept this Fortune 500 investment management firm is acutely familiar with, as it supervises over $250 billion in client assets. The high-income individuals and large organizations it counts among its clientele demands special care be taken to safeguard Personally Identifiable Information (PII) and Personally Identifiable Financial Information (PIFI).

As the business positioned itself to deploy Salesforce and Office 365, it sought the same level of confidence that the data flowing through these applications would remain secure.

> “No matter how reputable the platform was or what type of security it provided, we wanted to tighten access and control inbound and outbound data flow,” the CISO said.

The firm was set to deploy Salesforce and Microsoft’s Office 365, but also had a range of public cloud applications to protect, such as Slack. In Office 365, it needed to govern the flow of sensitive information across the entire suite, with a focus on SharePoint and Yammer. In other tools, it required real-time detection and remediation of PII and PIFI via masking, blocking, or encryption.

Sampling Every CASB on the Market

The firm’s IT team spent considerable time evaluating the leading Cloud Access Security Brokers (CASBs) on the market and comparing their performance to the built-in security functionality of the cloud applications.

The Forcepoint ONE unified security platform was one of the options the investment company reviewed. The solution’s agentless CASB provides secure access to public cloud applications like Salesforce, Office 365 and Slack. Because of its granular control over policies and threat protection, it quickly emerged as a
top candidate.

Forcepoint ONE also offers Zero-Trust Network Access (ZTNA) for private apps and a Secure Web Gateway (SWG) to extend data protection policies to a user’s browser, all without the need for an agent. Given the company’s Bring Your Own Device (BYOD) policy, having these functionalities housed under one roof made sense.

> “Keeping our future plans in mind, the single pane of glass view it gave us was a big motivational driver—normally, you’d need at least three different tools to achieve everything you can with Forcepoint ONE,” the CISO said.

Challenges

- Assure the security and privacy of client data on public cloud applications.
- Maintain visibility and control over data usage on managed and unmanaged devices.
- Detect and manage PII and PIFI usage across all cloud applications

Securing Data Wherever It Flows

Forcepoint's unique agentless CASB delivered a smooth user experience on top of strong data protection capabilities.

By integrating with third-party Single Sign-On (SSO) vendors to sit in the middle between the access management tool and the business application, the investment firm was able to extend security to BYOD users without introducing a VPN or any extra steps to their day-to-day routine.

> "Forcepoint gives us the all-important ability to secure data both upstream and downstream on unmanaged devices," the CISO said.

That protection extended to cloud applications that other security vendors may have trouble securing in real-time, such as Slack. Additionally, the company was able to find areas of risk with inbound or outbound data flowing from potentially malicious hosts and shadow IT applications.

The investment firm continues to look to adopt new cloud platforms to improve user productivity, without giving up control or visibility of the data that resides there.

Approach

- Evaluate all CASB offerings in the market.
- Implement Forcepoint ONE.

Results

- Complete governance over data flowing through public and private cloud applications via managed and unmanaged devices.
- Gained ability to detect and remediate PII and PIFI in real-time via masking, blocking, or encryption.
- Identified risky outbound data flows originating from shadow IT applications.