



Indian Insurance Leader Keeps Partner Cloud Collaborations Safe with Forcepoint

This leading Indian insurance company relies on Forcepoint to help boost employee and partner collaboration and productivity using cloud applications—without sacrificing data security for their life insurance and retirement plan customers.

One of India's biggest life insurance providers does more than provide customers and their families with peace of mind should an accident or illness occur. It also provides comprehensive savings and retirement solutions as part of its protection services and must safeguard customer financial data as securely as a bank. To better compete in its crowded market, the company leverages cloud applications to boost employee productivity and business partner collaboration, relying on Forcepoint to help provide end-to-end protection for all of its data in the cloud.

CUSTOMER PROFILE:

Leading life insurer, long-term savings plan and retirement solution provider.

INDUSTRY:

Financial Services

HQ COUNTRY:

India

PRODUCT:

Forcepoint Cloud Access Security Broker (CASB)

As one of India's biggest life insurance and retirement plan providers, this company is entrusted by its customers with their most personal and valuable information. Because it works closely with third-party business partners and agents to conduct business, the company relies on a number of cloud apps and services for data storage, file sharing, voice and video collaboration, and other productivity and workflow applications.

Keeping customer data safe while conducting so much business over the cloud means the company has to take cloud security very seriously. And like about half of all global companies, it has increased its cloud security budget in recent years.

A more robust security solution for Office 365

The company recently completed the migration of its entire, 10,000-strong workforce to Microsoft Office 365. The insurer's core IT services are now conducted over the cloud, including:

- Outlook for email
- OneDrive for data storage
- SharePoint for file sharing
- Skype for voice and video collaboration

While Microsoft provides a baseline level of security for all of those operations, like many enterprise Office 365 users, the company requires a more robust cloud security solution to reduce the risk of a costly, reputation-damaging data breach.

Additionally, it relies on a number of non-Microsoft cloud apps for activities like CRM, which also need to be protected with the best available cloud security. In all instances, securing employee access to cloud applications is the first concern for the IT team,

but not the only one. How the cloud is used by the company's partners—mainly, agency and multi-channel distributors of its products—must also be factored into decisions about how to best control access to applications and protect data.

An end-to-end cloud protection plan

The company needed an end-to-end solution to secure all of the cloud data it was generating and sharing with partners. The insurer maintains an enormous amount of critical data on its Office 365 cloud application, challenging the IT team to better monitor who is accessing what data on Office 365 and stop bad actors from accessing that data.

Given the parameters of the situation, it wanted a Cloud Access Security Broker (CASB) solution that could understand what sensitive data was being processed and stored in the cloud, provide visibility into cloud app account usage, and control data and application access in Office 365 and other cloud apps by employees and business partners—and do all of this with both managed and unmanaged devices.

To add to the challenge, the company also wanted its CASB solution to help address other key security requirements such as data loss prevention, cloud encryption, mobile data protection, and identity management, as well as augmenting malware detection on the Office 365 platform.

"While embracing the cloud to leverage greater efficiency and productivity, we are also committed to securely enabling our Office 365 application to protect all our customers' data and ensure compliance with regulatory requirements," said the Assistant Vice President for IT.



Challenges

Securing customer data shared and stored in the cloud for collaboration with outside partners.

Additional protection for Office 365.



Approach

Deploy Forcepoint CASB to provide visibility, protect data, and control application access in the cloud.

Leverage additional CASB cybersecurity features.

After careful evaluation of competitive products, the company selected Forcepoint CASB.

Seamless integration, quick installation

Forcepoint CASB met all of the requirements for cloud security and proved to be the best solution for a host of reasons, including:

- Seamless integration with the company's existing VMware AirWatch mobile device management solution
- Support for all major mobile operating systems
- Quick installation—Forcepoint and the system integrator were able to deploy and bring CASB online in just one day

Since its deployment, Forcepoint CASB has helped the company gain complete visibility and control over all its Office 365 application usage, according to the AVP.

"The solution enables real-time activity monitoring and analytics with the help of a dashboard that provides a comprehensive and consolidated view of activity and transaction logging," he said.

"This helps identify potential exposure by user, group, location, device, application action, and more. The system correlates user activity and proactively responds to any suspicious and anomalous activity that could indicate a threat."

The company now has what it values most—the ability to securely work with its trusted partners using collaborative cloud tools that deliver cost efficiencies that can be passed along to its customers.



Results

- > **Installation** in just one day.
- > **Visibility and control** over all Office 365 usage.
- > **Access control** for other cloud applications and data protection.
- > **Seamless integration** with the existing mobile device management.

