

Cloud Access Security Broker

Secure data in any SaaS app, accessed from any device

Challenge

- › Safeguard and control access to managed apps from BYOD
- › Control sensitive data uploading and downloading in any managed SaaS app
- › Stop malware hidden in business data files
- › Detect and control shadow IT

Solution

- › SaaS app security with integrated DLP and advanced threat protection
- › Granular Zero Trust access and data controls based on user, device, or location
- › Hyper-scaling AWS platform maximizes uptime and minimizes latency
- › DLP enforcement across managed and unmanaged devices

Outcome

- › Increase productivity, enabling people to use information anywhere seamlessly and safely
- › Reduce risk through control of sensitive data in the cloud and stopping malware
- › Reduce costs by simplifying security operations with a single place to set policies
- › Streamline compliance with demonstrable processes for controlling information

Today's new workforce models demand that users anywhere have fast, yet controlled access to business data everywhere. This means people need access to data in SaaS apps like Microsoft 365, Google Workspace, Slack, Jira, and Salesforce from any kind of device or location. With more than 250 SaaS apps for the average enterprise, visibility and control can easily become unmanageable.

Safeguard access to business apps from BYOD and unmanaged devices

Forcepoint simplifies cloud security. The CASB security service of Forcepoint ONE implements Zero Trust access that enables business-critical SaaS apps to be safely used from the personal devices of employees (BYOD) and unmanaged devices of partners and contractors.

Control sensitive data uploading and downloading in any managed SaaS app

We give you one set of security policies to control sensitive data, with industry-leading performance regardless of where and how employees and contractors connect to the internet. Managing access to these apps from mobile devices facilitates adoption and productivity, while having different policies based on identity and location provides granular Zero Trust controls. Inline scanning for sensitive data and malware keeps data across all SaaS apps safe. You gain more certainty over how confidential data is shared in company apps and with data loss prevention (DLP) built in, you don't need point products to stop data breaches.

Stop malware hidden in business data files

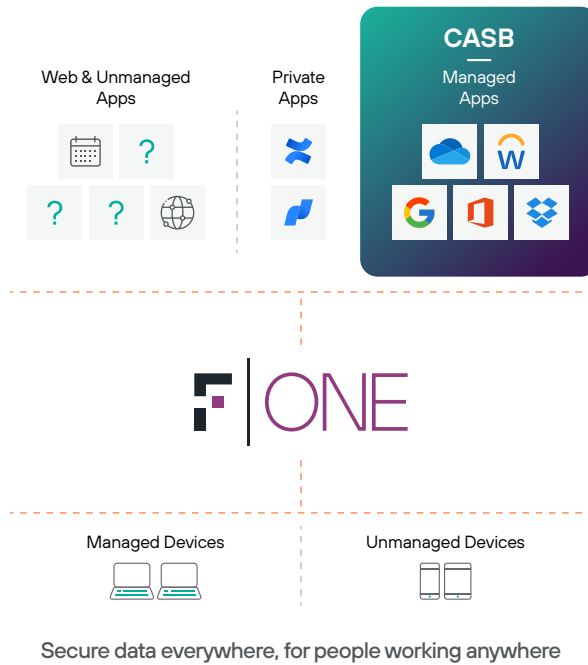
Forcepoint ONE CASB can detect and block malware in data in motion between users and the SaaS app using malware engines from multiple third-party anti-malware engines. It can also detect malware in files in popular SaaS and IaaS storage and quarantine those files.

Detect and control shadow IT

Forcepoint ONE CASB brings shadow IT into the light and generates a risk score for unsanctioned apps by analyzing multiple attributes. This allows IT teams to have a deeper understanding of SaaS usage within their organisation and enforce necessary security controls. The CASB detects unmanaged SaaS apps in use using networking logs from corporate firewalls and proxies to enable consistent security policies to be applied to sanctioned and non-sanctioned SaaS apps so that business data stays safe anywhere it is used.

SaaS security solution that maximizes uptime, availability, and productivity

Our CASB is built over a cloud-native, hyperscaler-based architecture with over 300 points of presence (PoPs), global accessibility, and proven 99.99% uptime to secure SaaS applications seamlessly and preserve user productivity. Other solutions detour network traffic to and from SaaS applications into private data centers instead of locations closer to users and the applications they are accessing. This leads to poor performance, causing latency-sensitive apps like Slack to fail and employees to seek high-risk workarounds.



Making Cloud Security Simple in the Real World

From one console, administrators can manage access and control data for users of both managed and unmanaged devices (such as BYOD and contractors' or partners' computers).

Let's see how CASB simplifies cloud security when Kris, a business analyst working from home, starts their workday.

<p>Kris logs into their Salesforce account from their corporate-issued laptop.</p>	<p>The CASB in Forcepoint ONE manages connections to business apps, allowing users to log on seamlessly and safely.</p>
<p>Kris browses directly to salesforce.com or through a corporate application portal.</p>	<p>Salesforce redirects the session to the CASB (through SAML), which analyzes whether the device is managed, its location, and its security posture. Based on pre-defined security policies, the CASB confirms Kris' identity through multifactor authentication.</p>
<p>Kris is granted managed app access.</p>	<p>The admin policies also control direct access to the app, controlled access, or no access at all. This happens in milliseconds without impacting employee productivity. All traffic from Kris' device and the app passes through the CASB (using a reverse or forward proxy).</p>
<p>Kris decides to download a revenue forecast from Salesforce.</p>	<p>The CASB scans any file downloaded from the app for malware and sensitive data. Depending upon the result and policy, it can block malware files and block, track, or encrypt sensitive data. If a policy restricts download of sensitive data to unmanaged devices, the download is allowed since Kris is using a company laptop.</p>
<p>Kris attempts to transfer sensitive data or a file contaminated with malware via Slack.</p>	<p>The CASB also can check files being uploaded into SaaS apps. The CASB can automatically block the upload. It can even block uploading of files into unsanctioned apps using the on-device unified agent.</p>

Part of Forcepoint's Data Security Everywhere approach

Forcepoint's Data Security Everywhere mission enables organizations to protect data across SaaS, web, email, network and endpoints, so that people can safely work anywhere with data everywhere.

Extending industry-leading DLP capabilities to SaaS applications

With Forcepoint, organizations can utilize their existing Forcepoint DLP policies for securing data in SaaS applications, extending the same industry-leading data security to the cloud with just a few simple clicks. Unified DLP policies enforced from a single console helps deliver consistent, enterprise-class data security to SaaS applications, simplifying data security management, minimizing breaches, while streamlining compliance. Customers can derive the following benefits through this integration:

- Simplified cloud data security with unified policies and console.
- Out-of-the-box 1,700 classifiers and policy templates for comprehensive coverage and compliance support for 150+ regions.
- Configuration setup and time-to-value in minutes, improving the productivity of IT/security teams.
- Eliminating redundant and fragmented security products to achieve significant cost savings.

Read the Forcepoint DLP brochure for more details.



Ready to secure data in cloud apps from any device?

Let's start with a demo.

forcepoint.com/contact