Forcepoint

Solution Brief

Cloud Access Security Broker

Secure data in any cloud 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 shadow IT

Solution

- Cloud 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 cloud apps like Microsoft 365, Google Workspace, Slack, Jira, and Salesforce from any kind of device or location. With more that 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 cloud 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

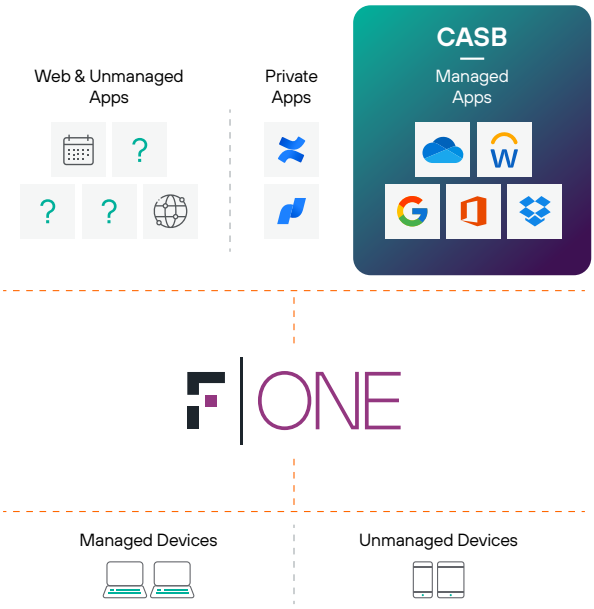
Forcepoint ONE CASB can detect and block malware in data in motion between users and the SaaS app using malware engines from Bitdefender and Trellix. It can also detect malware in files in popular SaaS and IaaS storage and quarantine those files.

Detect 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 or with telemetry from Forcepoint ONE Secure Web Gateway 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.

CASB in Forcepoint ONE maximizes uptime, availability, and productivity

Our CASB is part of Forcepoint ONE, our hyperscaler-based cloud platform with over 300 points of presence (PoPs), global accessibility, and proven 99.99% uptime to secure cloud apps seamlessly and preserve user productivity. Other solutions detour network traffic to and from cloud 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.



Secure data everywhere, for people working anywhere

Making Cloud Security Simple in the Real World

The Forcepoint ONE cloud platform provides an "easy button" for implementing cloud security.

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.

Kris logs into their Salesforce account from their corporate-issued laptop.	The CASB in Forcepoint ONE manages connections to business apps, allowing users to log on seamlessly and safely.
Kris browses directly to salesforce.com or through a corporate application portal.	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.
Kris is granted managed app access.	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).
Kris decides to download a revenue forecast from Salesforce.	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.
Kris attempts to transfer sensitive data or a file contaminated with malware via Slack.	The CASB also can check files being uploaded into cloud apps. The CASB can automatically block the upload. It can even block uploading of files into unsanctioned apps using the on-device unified agent.

Part of a unified security solution for web, cloud, and private apps

In addition to CASB, the Forcepoint ONE all-in-one platform secures access to business information on any website and private app:

- → **Web:** SWG monitors and controls interactions with any website based on risk and category, blocking download of malware or uploads of sensitive data to personal file sharing and email accounts. Our on-device SWG enforces acceptable use policies on managed devices anywhere.
- → **Private apps:** ZTNA secures and simplifies access to private applications without the complication or risk associated with VPNs.
- → **Additional capabilities** such as scanning cloud providers for risky configurations Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) as needed.

Read the Forcepoint ONE Solution Brief for more details.

Ready to secure data in cloud apps from any device?

Let's start with a demo.

forcepoint.com/contact