Forcepoint

Solution Brief

Cloud Access Security Broker

Secure data simply 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 and control 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

Accessing cloud apps and data from mobile devices is commonplace for today's hybrid workforce. The average enterprise deploys more than 280 SaaS apps, including collaboration tools like Microsoft 365, Google Workplace, Slack, or Jira that are indispensable to remote employees and contractors. Using these services without a way to manage access from mobile devices or establish trust in the devices (device posture) adds complexity and risk.

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 device posture and location provides granular Zero Trust control that keeps data safe. You gain more certainty over how confidential data is shared in company apps on any device, even personal ones. Data loss prevention (DLP) is built-in, so you don't need point products to stop data breaches.

Stop malware hidden in business data files

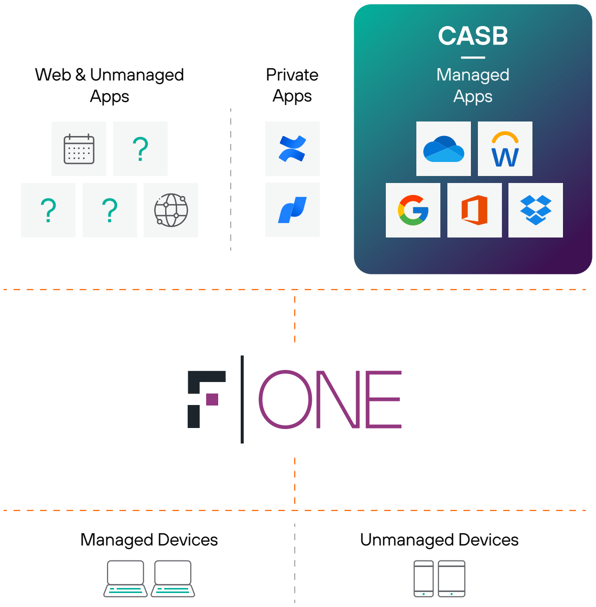
Our CASB can detect and block malware in data in motion between users and the SaaS app using malware engines from Bitdefender and CrowdStrike. It can also detect malware in files in popular SaaS and IaaS storage and quarantine those files.

Detect and control shadow IT

The CASB not only brings shadow IT into the light but also provides control and coaching on safe usage and better alternatives. The CASB detects and lists unmanaged SaaS apps in use, allowing administrators to build policies for company devices that can block access or display a message to the user directing them to approved SaaS apps.

CASB in Forcepoint ONE maximizes uptime, availability, and productivity

Our CASB is part of Forcepoint ONE, our hyperscaler-based cloud platform with 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 close to users. This leads to poor performance, causing latency-sensitive apps like Slack to fail and employees to seek high-risk workarounds.



Provide **total cloud security** for every interaction

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 file downloads and uploads 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 apps.
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 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 managed 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 or upload the data to their personal Dropbox storage.	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 RBI or scanning cloud providers for risky configurations (CSPM) 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.