Forcepoint

Datasheet

Forcepoint ONE

Cloud Access Security Broker

Multimode CASB with agentless reverse proxy, forward proxy, and API modes.

Key Benefits:

- 99.99% verified uptime since 2015
- Auto-scaling and over 300 points of presence on AWS minimizes latency and maximizes throughput
- Unified administration console reduces repetitive and redundant configuration management
- Unified managed device agent for CASB, SWG, and ZTNA simplifies deployment
- Active Directory sync agent accelerates user onboarding
- Data-in-motion scanning blocks malware and data exfiltration between users on any device and any managed SaaS application.
- Field Programmable SASE Logic can block specific HTTP/S request methods resulting in granular control of any element in a managed SaaS web page
- Data-at-rest scanning of selected SaaS and IaaS identifies malware and sensitive data independent of data-in-motion scanning
- File level encryption of managed SaaS applications ensures data privacy and data sovereignty without completely blocking access to data
- Shadow IT reporting helps identify unsanctioned application risk
- Digital Rights Management (DRM) provides more flexibility with new ways to secure sensitive data.

The Forcepoint ONE Cloud Access Security Broker (CASB) is one of the three foundational gateways of the Forcepoint ONE cloud platform. It controls access to managed SaaS applications and shadow IT applications while providing Data Loss Prevention (DLP) and malware protection.

Agentless Reverse Proxy Mode

Agentless reverse proxy mode enforces granular access with Forcepoint ONE integrated DLP and malware scanning from any device using a modern browser. It is ideal for monitoring and controlling access from BYOD and contractor devices. It leverages Forcepoint ONE's patented integration with any SAML 2.0 compliant IdP to redirect users to a Forcepoint ONE reverse proxy, where a complementary session with the SaaS application is established.

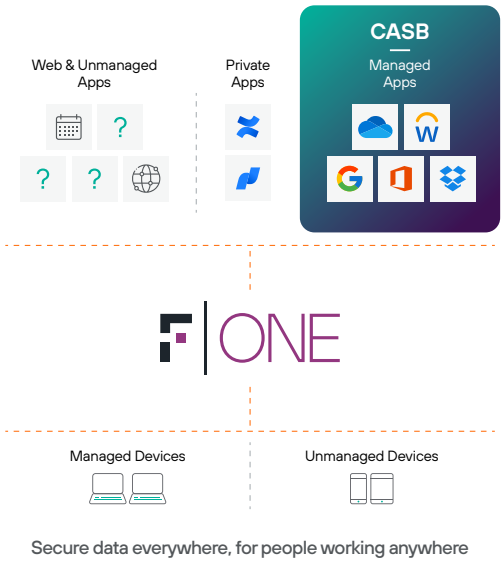

Figure 1: Forcepoint ONE CASB agentless reverse proxy with AJAX/VM.

Combined with Forcepoint ONE's unique AJAX/VM technology, executing within the user's browser, the Forcepoint ONE agentless reverse proxy mode ensures proper URL and cookie rewriting resulting in compatibility with any SaaS application. Key features that let you control and monitor app usage in reverse proxy mode are proxy policies, field-level encryption, shadow IT reports, and reverse proxy reports.

Proxy Policies

Access control options and associated DLP and malware scanning options for data in motion to and from managed SaaS applications are set in proxy policies. These let administrators set access to managed SaaS app as direct app access, deny, or secure app access (all traffic passes through the reverse proxy with the option of enforcing DLP and malware scanning). Criteria for policy enforcement include user group, access method (browser, non-browser client app, or any), device OS, device profile, and location.

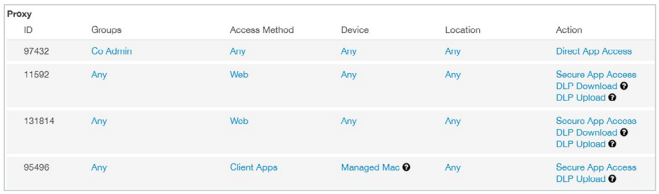

Figure 2: List of proxy policies for a managed SaaS app

A single app can have a list of multiple proxy policies that are evaluated sequentially until a policy is found where all of the match criteria in the policy match the connection request. Then the appropriate enforcement action is applied.

When secure app access is specified, a single proxy policy may include a list of DLP and malware scanning polices for upload to the SaaS app, and another list for download from the SaaS app. In addition, if a managed SaaS app has field level encryption enabled, the proxy policy lets you specify whether a field is displayed unencrypted based on the field security level or whether the user location matches the data creation location. This supports data privacy and data sovereignty

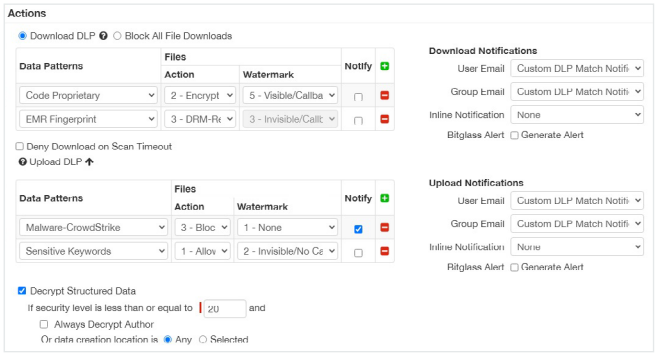

Figure 3: Proxy Policy details for a secure app access connection.

Within a single proxy policy, the download DLP policies let you control download of both sensitive data and malware, while the upload DLP policies let you control upload of sensitive data and malware. Simply use dropdown menus to specify a data pattern to match, a file action, and watermark/tracking control, and click the checkbox if you want people to be notified about the match.

Forcepoint ONE includes over 190 predefined data patterns that help you enforce regional and industry standards regarding PII, PHI, and personal financial data. There are also two reserved data patterns for invoking malware scanning powered by CrowdStrike or Bitdefender. You can also create custom data patterns that use simple regular expression up through complex Boolean expressions, and special data patterns for identifying records. The special match patterns include database matching (using exact match), similarity to a standard form (using file fingerprinting), and any HTTP/S request method (using Field Programmable SASE Logic – FPSL).

For download proxy policies, file actions are encrypt, block (replace contents with block message), deny (do not transfer), apply DRM, and watermark and track.

For upload proxy policies, file actions are encrypt (for Office 365, Google Workspace, and Salesforce), block (replace contents with block message), deny (do not transfer), mask data (Salesforce Chatter, O365 Teams, and Slack), and watermark and track.

Field-Level Encryption

Agentless reverse proxy mode lets you encrypt structured data in many popular SaaS apps with support for full AES 256-bit encryption or tokenization, a built-in keystore or your own Key Management Interoperability Protocol (KMIP) keystore, and vaultless encryption and tokenization. You can also specify security levels for each field to control when the field is decrypted for the user.

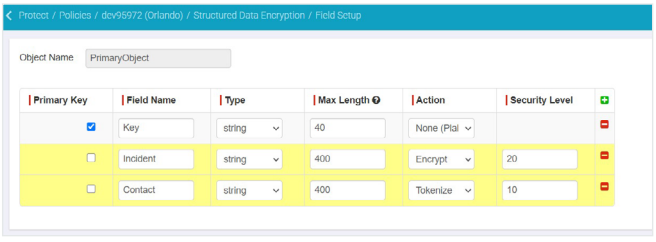

Figure 4: Field-level encryption settings.

Shadow IT Reports

The agentless reverse proxy mode supports shadow IT reporting. Shadow IT usage is collected from the log data from corporate firewalls and proxy servers, either by manual import or through a Forcepoint ONE syslog collector. Reports show application distribution by trust rating, as calculated by Forcepoint ONE, and top accessed applications with drill down to individual applications and individual source IP addresses, helping you understand your organizations, risk posture relative to web traffic. The Forcepoint ONE CASB can also let you control shadow IT traffic in forward proxy mode (see below).

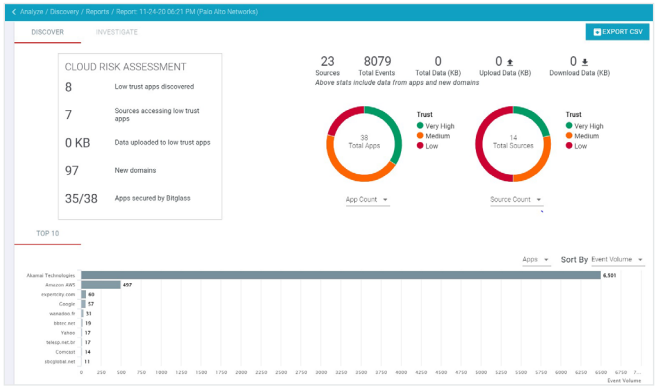

Figure 5: Shadow IT Discovery report.

The reverse proxy mode offers reports to give you extensive insight into managed SaaS traffic passing through the reverse proxy: the 'Data in Motion' sections of both the Data Security and Threat dashboards, and the proxy logs report. The Data Security dashboard displays details on sensitive data identified by the Forcepoint ONE platform, including movement of sensitive data into and out of applications secured by the Forcepoint ONE platform as well as showing sensitive uploads to unsanctioned apps, sensitive downloads to unmanaged devices, top groups and users moving sensitive data, and more.

The Threat dashboard includes the same types of metrics as the Data Security dashboard, but specifically for malware and cyber threats.

The Threat dashboard includes the same types of metrics as the Data Security dashboard, but specifically for malware and cyber threats.

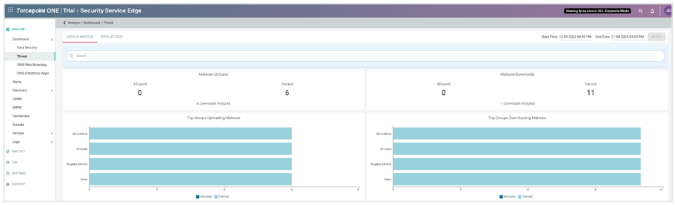

Figure 6: Proxy Dashboard

The proxy logs report plots application activity and watermark, DLP and DRM activity over time, and lists recent events grouped by summary, audit, and data leakage categories.

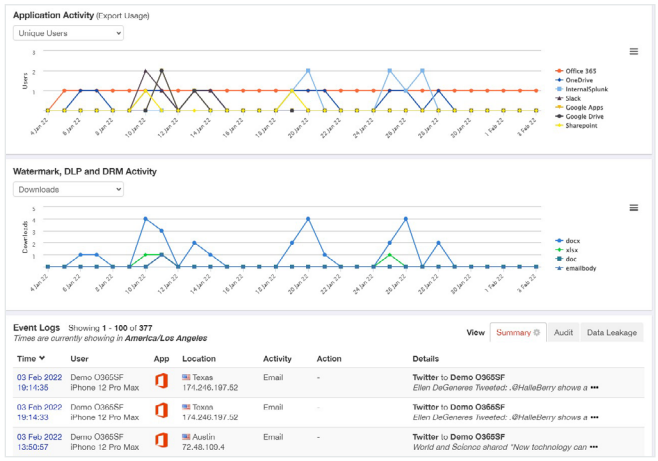

Figure 7: Proxy Logs Report

Forward Proxy Mode

Forward proxy mode uses the Forcepoint ONE unified agent for Windows or MacOS. All managed SaaS traffic still passes through the Forcepoint ONE reverse proxy but without the need for URL rewriting to connect with the user device. Forward proxy mode supports all of the features of the agentless reverse proxy mode, including enforcing DLP and malware scanning through proxy policies, but it also supports use of non-browser clients, such as the Microsoft Outlook client and the Slack client. In addition, forward proxy mode supports shadow IT control.

Shadow IT Control

Shadow IT control lets you control access to any shadow IT app using proxy policies which are evaluated in sequence like managed SaaS proxy policies. However, proxy policies for shadow IT apps do not enforce DLP and malware scanning for upload and download. Instead, they are limited to the following connection control options: render the app in read-only mode, coach (display a recommendation for a company sanctioned alternative app and either allow or deny access to the original shadow IT app), or deny access without a coaching message.

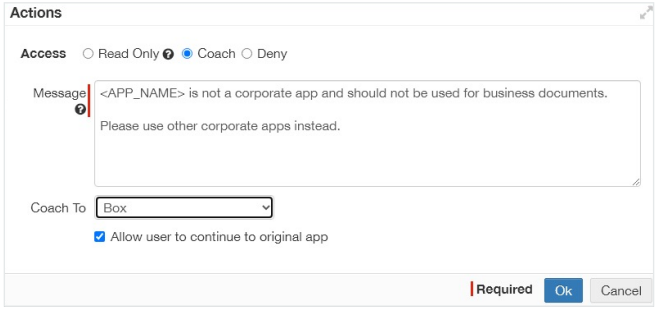

Figure 8: Shadow IT proxy policy details showing the coach options.

If you need to support DLP and malware scanning policies to shadow IT apps, use SWG content policies instead.

API Mode

In API mode, the CASB uses API calls to your SaaS or IaaS tenant to scan data at rest for sensitive data or malware and perform automatic remediation actions such as restrict sharing, quarantine, copy, add classification metadata, or notify the file owner. It supports historical file scanning and can apply OCR to image files and image only PDF files before scanning for sensitive data. API mode is supported out-of-box for many popular SaaS and IaaS including Google Workspace, Office 365, Salesforce, ServiceNow, Box, Dropbox, Atlassian Confluence, Github, Webex Teams, Slack, AWS, GCP, and Azure. API mode ensures that even if new files or updates to old files bypass the reverse proxy, they can be scanned for sensitive data.

API Policies

API policies control scanning data rest in IaaS and SaaS. Like proxy policies, several API policies can be applied to a single SaaS app and are evaluated sequentially.

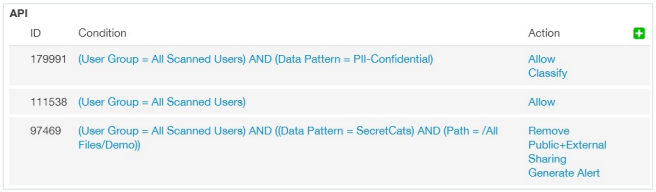

Figure 9: List of API policies.

Within a policy, you can specify match criteria based on user group, DLP data pattern, file path, file name, sharing status (external, internal, public, or any), file size, owner, shared with username, create date, and modified date. The data match patterns used in an API policy can be any of the custom or predefined match patterns shared across the proxy policies and SWG content policies, letting you have unified control of sensitive data and malware.

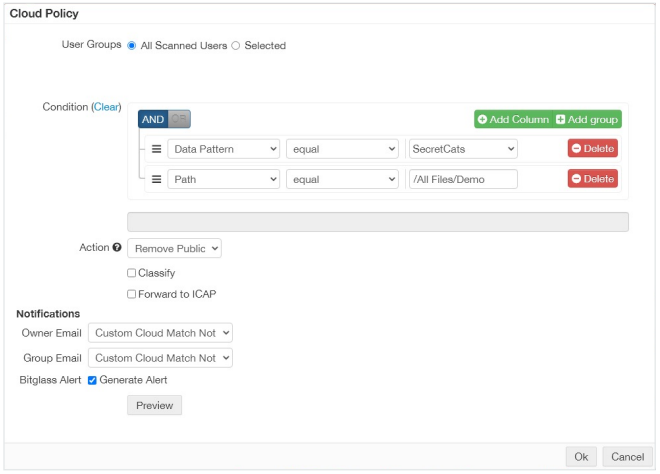

Figure 10: API policy details

When a match of conditions for a scanned file occurs, possible API policy actions include modify sharing (remove public, remove public and external, remove all), allow, quarantine, create copy, and encrypt.

CASB Third-Party Integrations

The Forcepoint ONE CASB additionally can be configured to integrate with various other data security systems as outlined below.

- **Security Information and Event Management (SIEM).** Forcepoint ONE integrates with any system that supports syslog. This allows third party apps to upload logs from Forcepoint ONE for visualization and analysis.
- **On-premises DLP Systems.** Forcepoint ONE integrates with any on-premises DLP system that supports theInternet Content Adaptation Protocol (ICAP). This provides customers the ability to send files at rest in managed SaaS or IaaS cloud storage, that are flagged by Forcepoint ONE as having sensitive data, to the onpremises DLP system using TLS encryption. The files are enriched with data such as source and destination IP and the email address of the file owner.
- **Security Orchestration and Response (SOAR).** Forcepoint ONE supports two-way integration between Forcepoint ONE and the selected SOAR platforms. In these cases, the SOAR platform is used to automate activities within Forcepoint ONE and another tool.
- **Data Classification.** Forcepoint ONE can use classification metadata from any data classifier in a DLP match pattern.
- **Endpoint Management.** As part of the SAML login process, Forcepoint ONE can validate a client certificate stored on a Windows, Mac, Android, or IOS device to confirm it is managed by an endpoint management system. This knowledge lets the administrator apply different access policies for users logging in via managed vs. unmanaged devices.

Forcepoint ONE Platform Features

The Forcepoint ONE CASB additionally supports these features built into to the Forcepoint ONE platform:

- **Platform-level contextual access control.** Users cannot be granted access to any of the three foundational gateways unless they are authenticated according Forcepoint ONE login policies that factor in user location, device type, device posture, user behavior, and user group. When user login through a new device is detected, or "impossible travel" travel based on client IP address is detected, the user can be presented a mutifunction authentication (MFA) challenge to prevent use of stolen credentials.
- **Unified management console** for configuration, monitoring, and reporting for SWG, CASB, and ZTNA. Lets administrators reuse DLP match patterns across SWG, CASB, and ZTNA for private web applications, and see a consolidated view of all traffic and anomalies.
- **Unified on-device agent** for Windows or macOS with unique auto-generated and auto-rotated certificates.
- **Active Directory Sync Agent** synchronizes your current AD users and groups with Forcepoint ONE users and groups.
- **Auto-scaling, distributed architecture on AWS** with over 300 points of presence resulting in 99.99% verified service uptime since 2014.

Forcepoint ONE CASB Features and Benefits

FEATURE	BENEFIT
Auto-scaling, distributed architecture on AWS with over 300 POPs worldwide.	→ 99.99% uptime. → Minimal latency: often even faster than direct application access. → Allows in-line proxying of Slack traffic without timeouts.
Integration with any SAML compatible IdP in SAML relay or ACS proxy mode. Optional built-in IdP using Microsoft ADFS.	→ Flexible deployment. → Denial of service protection when using SAML relay mode.
Active Directory Sync Agent. Synchronizes your current AD users and groups with Forcepoint ONE users and groups.	→ Leverages your existing Microsoft AD instance to quickly onboard users and maintain the groups they are assigned to.
Contextual access control based on user group, device type, location, or time of day, with escalation to Multi-Factor Authentication based on "impossible travel," unauthorized location, or unknown device. Additional layer of access control for individual websites or applications based on user group, device type, or location.	→ Detects and blocks suspicious login attempts. → Reduces risks associated with stolen passwords. → Segments users based on risk and need to access.
Single unified agent for on-device SWG, CASB forward proxy, and ZTNA for non-web applications. Includes support for deployment through MDM systems and uses self-generated auto-rotated certificates.	→ Simplifies agent deployment. → Enhances security. → Reduces IT overhead.
Single administrator console for managing all system capabilities across all applications, users, and devices.	→ Reduces complexity and time to value. → Increases visibility and control.
DLP and malware scanning for data in motion. Scans file attachments downloaded from or uploaded to any web-based app or website for malware or sensitive data and logs and blocks the transfer as appropriate.	→ Stops data leakage and spread of malware in transit between users and any corporate SaaS application.
Field Programmable SASE Logic. Monitors, logs, and optionally blocks any HTTP/S request method based on any portion of the request method.	→ More fine-grained control of app usage. → Ability to block upload of sensitive data as message posts.
DLP and malware scanning for data at rest in selected IaaS and SaaS storage. Supports historical scanning and OCR of images files and image-only PDF files.	→ Stops data leakage and spread of malware in selected SaaS and IaaS. → Ensures that even if new files or updates to old files bypass the reverse proxy, they can be scanned for sensitive data.
File level encryption of managed SaaS.	→ Ensure data privacy and data sovereignty without completely blocking access to data.
Agentless shadow IT reporting using logs from corporate firewalls and proxies.	→ Detect unauthorized app usage from on-prem devices without an agent.
Shadow IT control using the unified agent in forward proxy mode.	→ Stop users from accessing certain unmanaged apps while recommending use of corporate sanctioned alternatives.
Detailed reporting of managed SaaS traffic.	→ Complete visibility of access to managed SaaS apps including those accessed from unmanaged devices.