## Forcepoint ONE

# Secure Web Gateway

The Forcepoint ONE Secure Web Gateway (SWG) is one of the three foundational gateways of the Forcepoint ONE all-in-one cloud platform. Forcepoint ONE SWG monitors and controls any interaction with any website, including blocking access to websites based on category and risk score, blocking download of malware, blocking upload of sensitive data to personal file sharing accounts, detecting shadow IT, and optionally providing Remote Browser Isolation (RBI) with Content Disarm and Reconstruction (CDR).

### Key Benefits

- 99.99% verified uptime since 2015
- Auto-scaling, over 300 points of presence, and distributed SWG architecture minimizes latency and maximizes throughput
- Unified administrator console reduces repetitive and redundant configuration management
- Unified managed device agent for CASB, SWG, and ZTNA simplifies deployment
- SCIM provisioning accelerates user on-boarding
- Data-in-motion scanning blocks malware and data exfiltration between users and any web application, no matter where they are located.
- Field Programmable SASE Logic can block specific HTTP/S request methods resulting in granular control of any element in a web page
- RBI with CDR enables safe use of unknown websites and safe use of files downloaded from those websites
- Controls website access down to the URL directory level
- SWG function cannot be bypassed or disabled by the user

### Forcepoint ONE SWG Architecture

The Forcepoint ONE SWG requires the installation of the Forcepoint ONE unified agent for Windows or macOS. Because the Forcepoint ONE SWG is agent-based, it protects the user, and company data, no matter where the user is located: at home, in the field, or in the office. By design, the unified agent powering the SWG cannot be stopped by the user or uninstalled by the user without approval from a Forcepoint ONE tenant administrator, thus ensuring its function is not easily bypassed by the user. And because the Forcepoint ONE agent also supports forward proxy CASB and ZTNA for non-browser clients, these capabilities can be enabled with the proper licensing and do not require additional software downloads or any other actions by the end user.

A key issue associated with other vendors' on-device SWG is performance. Forcepoint ONE addresses this issue with a combination of technologies. First, Forcepoint ONE has a distributed architecture on AWS with over 300 points of presence in major population centers, with each point of presence supporting auto-scaling. This means latency is reduced when the on-device agent needs to communicate with the Forcepoint ONE backplane on AWS. Second, the Forcepoint ONE SWG has a distributed architecture in which policy enforcement is performed by the on-device agent. This means that little traffic needs to pass through the Forcepoint ONE backplane on AWS, as shown in figure 1.

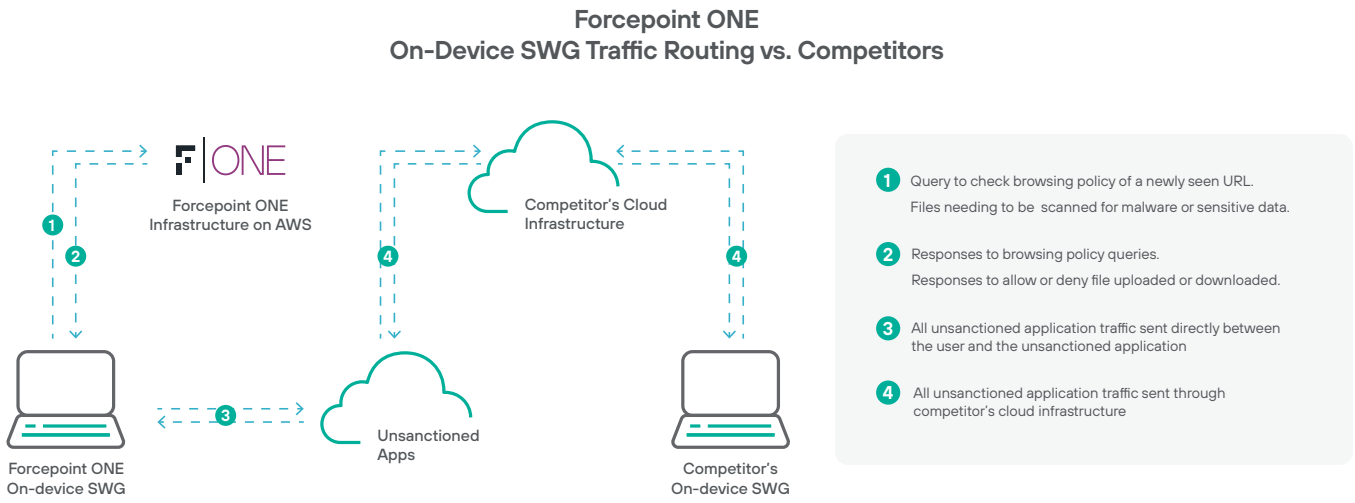


**Figure 1:** Forcepoint ONE SWG Traffic Routing vs Competitors

---

As shown in the figure, the Forcepoint ONE on-device SWG, on the left, only needs to communicate with the Forcepoint ONE backplane on AWS in two situations: when first attempting to access a website not recently visited to determine access restrictions, and when attempting to upload or download files or other data that needs to be scanned for malware or sensitive data.

By comparison, the other vendor's on-device SWG, on the right, must send all web traffic through the vendor's cloud backplane for traffic inspection and forwarding. This routing of all web traffic through the other vendor's cloud infrastructure can cause up to a 50% loss in effective throughput, thus causing productivity issues for users in low bandwidth locations. Because file uploads and downloads are a small fraction of overall internet traffic for most users, the Forcepoint ONE SWG can typically support throughput of about 95% of total available internet bandwidth, while reducing latency, thus supporting greater user adoption.

## Forcepoint ONE SWG Features

The following are the Forcepoint ONE SWG core features.

### SWG Connection Policies

Let administrators restrict access to a range of websites or allow the connection to bypass the SWG forward proxy and not be decrypted, and optionally log each connection attempt. Criteria for policy enforcement include user group, device posture, domain category (predefined web categories from Webroot BrightCloud, Forcepoint ONE predefined enterprise app categories, or custom categories), host app (web browsers or non-browser applications), and host network (user's DNS server IP address or DNS suffix). Supports user privacy by allowing connections to personal healthcare or financial sites to pass unencrypted.

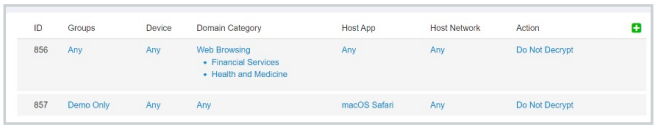


**Figure 2:** SWG Connection Policies.

### SWG Content Policies

Let administrators specify rules for denying a connection, permitting a direct connection establishing a secure app access connection (for enforcing DLP and malware protection) or with additional licensing establishing an isolated access connection using RBI with CDR. Criteria for policy enforcement include user group, device posture, location, URL category (predefined or custom), website reputation score, and Forcepoint ONE enterprise app risk score. Custom URL categories may include full URL directory path entries letting administrators apply different policies for different directories. This can be used to block certain Reddit subreddits, as an example.


**Figure 3:** SWG Content Policies.

When secure app access is specified in a SWG content policy, the administrator can specify multiple DLP upload and download policies for blocking download or upload of sensitive data or malware (using Forcepoint ONE's integrated DLP).

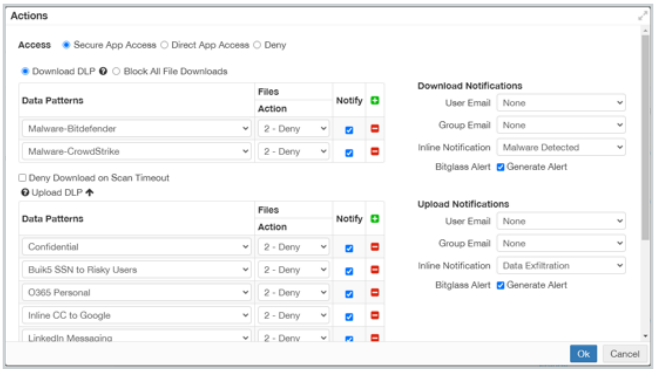


**Figure 4:** Secure app access SWG content policy

When an isolated access connection is specified by a SWG content policy, the administrator must also select an RBI profile from the dropdown menu.

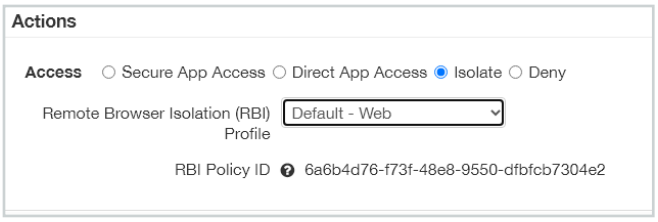


**Figure 5:** Isolated access SWG content policy

## RBI Profiles

Let administrators specify parameters for an RBI session that determine how restrictive the session is.

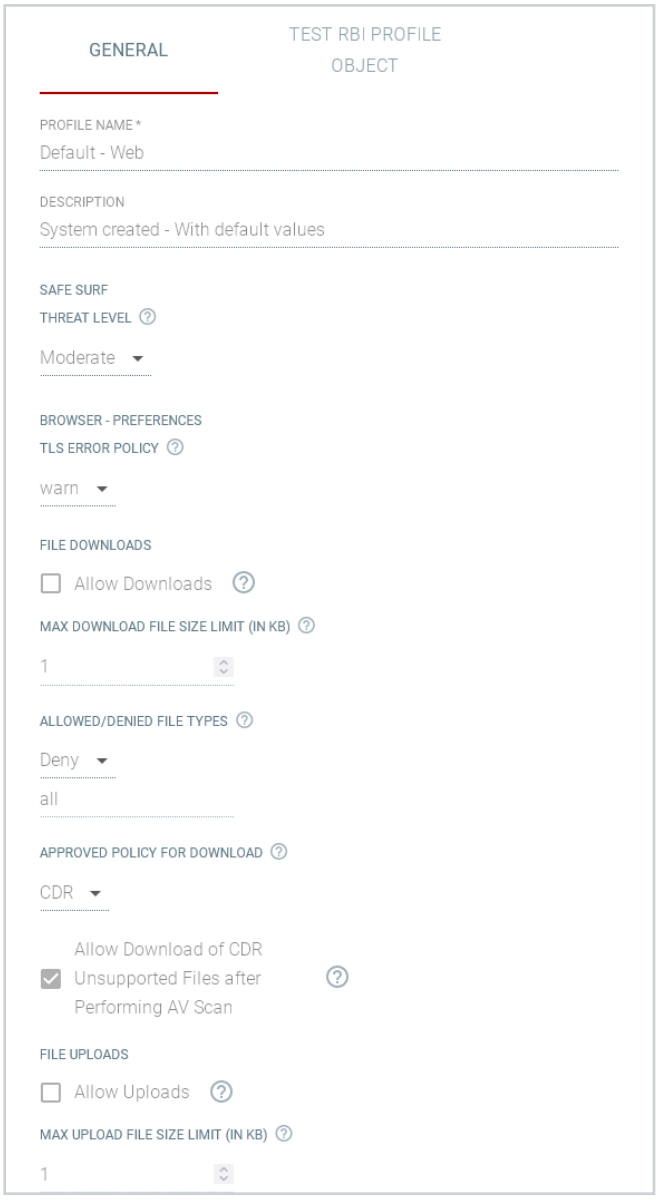


**Figure 6:** RBI Profile.

**The following table summarizes the allowed values and functions of the RBI profile parameters.**

| NAME | VALUES | DEFAULT | USAGE |
|---|---|---|---|
| Threat Level | Off (0), Moderate (60), High (80) | High | → Renders site in read only mode if site threat level is higher than the specified value |
| TLS Error Policy | Fail, Warn, Ignore | Warn | → Action the browser will take when navigating to bad TLS/Cert sites |
| Allow Downloads | Checkbox | Yes | → Allow users to download files from websites |
| Max Download File Size limit (in KB) | Integer | 100 | → Maximum file size for individual downloads is 500,000 KB (500 MB) |
| Allowed/Denied File Types (dropdpwn) | Allow or Deny | Allow | → Allow or deny uploads based on file type |
| Allowed/Denied File Types (text list) | Comma-separated list of file extensions | All | → Specify all or a subset of file types to allow or deny |
| Approved Policy for Download | CDR, AV Scan, No Scan | CDR | → CDR: apply CDR<br>→ AV Scan: download after successful AV scan<br>→ No Scan: download without scan or CDR |
| Allow Download of CDR Unsupported Files after Performing AV Scan | Checkbox | Yes | → If unchecked, and CDR cannot be performed due to file size > 250 MB or unsupported file type, block download.<br>→ If checked, and CDR cannot be performed, perform AV scan on file and download if scan passes |
| Allow Uploads | Checkbox | No | → Allow users to upload files from websites |
| Max Upload File Size limit (in KB) | Integer | 100 | → Maximum file size for individual<br>→ uploads is 400,000 KB (400MB) |

The Test RBI Object tab lets the administrator test the functionality of RBI and CDR for a specific website.


**Figure 7:** RBI Profile Test Profile Object tab.

### SWG Discovery Dashboard

Displays graphical representations of web and enterprise app traffic grouped by web reputation or Forcepoint ONE enterprise app trust score, with additional displays for data uploaded or downloaded per website, and sensitive data uploaded to websites grouped by domain and match pattern.

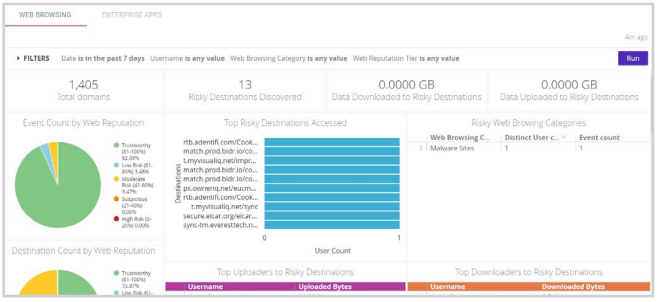


**Figure 8:** SWG Discovery Dashboard.

### Web Dashboard

Displays graphical representations of web traffic patterns grouped by web categories, giving the administrator an overview of what types of websites users are visiting, or attempting to visit and getting blocked. Includes additional data on malware download attempts and sensitive data upload attempts.

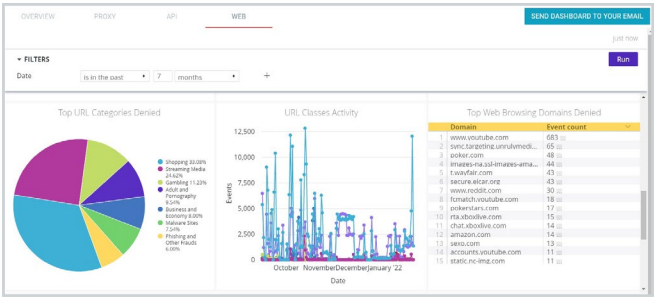


**Figure 9:** Web Dashboard.

### Shadow IT discovery

The Forcepoint ONE CASB supports shadow IT discovery for devices behind corporate firewalls. For managed devices used remotely, the on-device SWG enhances this capability by including data on all web traffic originating from managed devices with the SWG capability enabled.

### SWG bypass prevention

Users cannot kill the SWG processes on their Windows or MacOS device, and users cannot uninstall the on-device agent powering the SWG without assistance from the Forcepoint ONE tenant administrator.

## Forcepoint ONE Platform Features

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

- → **Contextual access control.** Users cannot browse the internet unless they are authenticated by Forcepoint ONE and permitted to login based on login policies which consider user location, device type, device posture, user behavior, and user group.
- → **Data loss prevention (DLP).** Files and text are scanned upon upload or download for sensitive data, reported, and blocked as appropriate.
- → **Field Programmable SASE Logic (FPSL).** Any HTTP/S request method can be logged and optionally blocked based on the content in any part of the request method.
- → **Malware scanning.** Files are scanned during upload or download for malware, using scanning engines from CrowdStrike or Bitdefender, and blocked when detected.
- → **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.
- → **Unified on-device agent** for Windows or macOS with unique auto-generated and auto-rotated certificates.
- → **99.99% service uptime**

## Forcepoint ONE SWG Features and Benefits

| FEATURE | BENEFIT |
|---|---|
| Auto-scaling, distributed architecture on AWS with over 300 POPs worldwide. | → 99.99% uptime.<br>→ Minimal latency: often even faster than direct application access. |
| Integration with any SAML-compatible IdP. SAML relay or ACS proxy mode. Optional built-in IdP using Microsoft ADFS. | → Flexible deployment.<br>→ Denial of service protection when using SAML relay mode. |
| SCIM Provisioning and AD Sync Agent. Synchronizes your Forcepoint ONE users and groups with Azure AD or Microsoft AD, respectively | → Leverages your existing Azure AD tenant or Microsoft AD instance to quickly onboard users and manage the groups they are in. |
| 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.<br>→ Reduces risks associated with stolen passwords.<br>→ 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.<br>→ Enhances security.<br>→ Reduces IT overhead. |
| Single administrator console for managing all system capabilities across all applications, users, and devices. | → Reduces complexity and time to value.<br>→ 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 web application or website. |
| 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.<br>→ Ability to block upload of sensitive data as message posts. |
| Monitors, logs, and controls access to any website from corporate Windows and Mac endpoints located anywhere with DLP and malware scanning. | → Enforces acceptable use policy.<br>→ Monitors and controls shadow IT.<br>→ Blocks upload of sensitive data to unsanctioned websites.<br>→ Blocks download of malware from any website. |
| Distributed SWG architecture. | → Reduces traffic through the Forcepoint ONE backplane, which results in near wire-speed throughput. |
| Web domain classification and reputation scoring supplemented with Forcepoint ONE enterprise app classification and risk scoring. | → Constantly updated classification and risk-scoring databases simplify access and content policy creation. |
| Custom URL categories allowing URL entries that include full directory path. | → Allows blocking of only certain directories within a website such as specific subreddits within reddit.com. |
| Optional RBI with CDR | → RBI applies a Zero Trust approach of treating all web pages as compromised and rendering them in a remote, disposable environment, enabling people to use the web without being attacked or having data stolen and applies content disarm and reconstruction of files before downloading them including the removal of malware embedded in an image file using steganography |
| SWG Discovery and Web dashboard. | → Allows administrators to see access attempts, malware download attempts, and sensitive data upload attempts at a glance. |

**forcepoint.com/contact**

Forcepoint


[FP-Forcepoint ONE SWG-Datasheet-US-EN] 29Apr2022