Forcepoint

Solution Brief

Secure Web Gateway

Stop data loss and malware attacks, not productivity

Use Cases

- Give employees fast, safe access to the web
- Enforce acceptable use policy
- Block uploading of sensitive data to unsanctioned websites
- Stop malware from getting onto user devices without compromising usability
- Detect and control shadow IT
- Prevent corporate exposure to users' private data

Solution

- Fast web security with integrated DLP and advanced threat protection
- Granular Zero Trust access and data controls based on user group, device type, user location, website category, website risk score and more
- Distributed architecture eliminates chokepoints on high-uptime, hyper-scaling AWS platform
- Optional Remote Browser Isolation (RBI) for safe browsing and downloads

Outcomes

- Increase productivity, enabling people to browse the web 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

The web is both a blessing and a curse. Most people depend upon it for information to do their jobs, but the web also creates risks of data exfiltration, HR policy violations, productivity loss, and malware infection. When the consequences of failing to keep data and people safe are growing every day, securing web interactions is a strategic requirement for modern organizations.

Give employees fast, safe access to the web

Most SWGs force all web traffic to detour through a centralized data center—whether on-premises or in the cloud—adding latency that can significantly interfere with modern web applications. And, while hyper-scaler cloud architectures are specifically designed to scale up and out on demand, many SWG vendors lack such a highly distributed cloud presence and instead manage outdated infrastructure that contain internal network bottlenecks. In contrast, the SWG in Forcepoint ONE has a distributed architecture that not only provides a hyper-scalable cloud architecture with over 300 Points of Presence around the world but goes even further with an alternative option to give customers even more flexibility—an on-device agent that eliminates chokepoints and can deliver up to twice the throughput for performancesensitive web content and apps as competing SWGs. This option enforces security policies locally on the user's device so that traffic can be exchanged directly between the user and the website.

Enforce acceptable use policy (AUP) controls on risky websites

The web can be a distracting place that is not always used for company business. The SWG in Forcepoint ONE lets you block or allow visitors to nonproductive or inappropriate websites with full path control; for example, you can block certain Reddit subreddits while allowing others. You can manage access based on user group, device posture, location, URL category (predefined or custom), reputation score, and enterprise app risk score. Custom URL categories can include full URL directory path entries, letting administrators apply different policies for different directories.

Block uploading of sensitive data to unsanctioned websites

With our SWG, you can prevent regulated data or intellectual property from being sent to personal file storage, social media, or personal email accounts. You can scan and block file uploads and HTTPS Post methods for sensitive data with the same predefined and custom DLP patterns used by the CASB and ZTNA services in Forcepoint ONE.

Stop malware from getting onto user devices without compromising usability

Our SWG provides multiple forms of protection against web-borne malware, including blocking categories of websites, inline scanning of downloaded files, and Zero Trustbased advanced threat protection such as Remote Browser Isolation. With our RBI, even sites or downloaded files that are contaminated can be used safely and efficiently.

Detect and control shadow IT

The SWG service works in concert with our CASB to identify websites that are being used in place of preferred company apps. These "shadow IT" sites are automatically collected and displayed in the console.

Prevent corporate exposure to users' private data

To protect employee privacy, organizations can prevent decryption and inspection of traffic going to and from specific categories of websites that are typically used with personally identifiable information (PII), such as banking, healthcare, and insurance data.

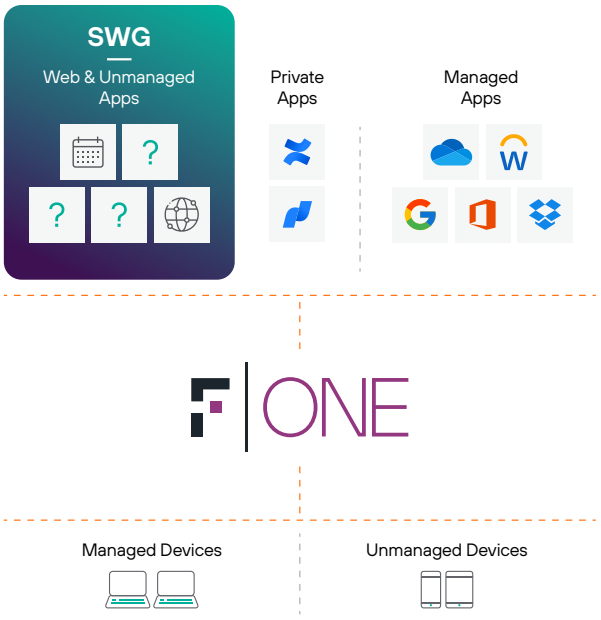
SWG in Forcepoint ONE maximizes uptime, productivity, and performance

SWG 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 web access and preserve user productivity. Forcepoint ONE unifies CASB, SWG, and ZTNA to secure access to corporate SaaS, web, and private apps, making security simple.

Making web 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 between ny website and any site or managed device—including enforcing Zero Trust Web Access using Forcepoint RBI.



Secure data everywhere, for people working anywhere

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

Kris browses reddit.com for company related research.	Kris visits reddit.com/r/technology to research recent posts on malware. The SWG content policies allow granularity to the directory level; this subreddit is considered work-related so Kris can access it.
Within the r/technology subreddit, Kris accidentally clicks a link to an inappropriate page.	Kris' Forcepoint ONE administrator has created SWG content policies that allow access to directories such as r/technology, but block access to inappropriate subreddits and pages. The SWG prevents Kris' error and blocks the new page.
Kris starts a confidential spreadsheet on their company laptop that includes customer PII and wants to continue working on their personal laptop. They try to upload the file to personal cloud storage and download it to their personal laptop.	To prevent business data loss, the company's Forcepoint ONE administrator created a SWG content policy that blocks upload of sensitive customer information (PII) to any personal file sharing website. When Kris attempts the upload, it is blocked, and a message pops up to explain why the upload was blocked.

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

In addition to SWG, the Forcepoint ONE all-in-one platform secures access to business information on any corporate SaaS tenant and private apps:

- → **Cloud (SaaS and IaaS):** SCASB applies contextual access control, data loss prevention (DLP), and malware protection to any public facing web app supporting SAML 2 integration with third party identity providers (IdPs), from any modern browser on any internet connected device. Data at rest in popular IaaS and SaaS can also be scanned for sensitive data and malware and remediated. Uses the same DLP match patterns available to SWG and ZTNA for private web apps.
- → **Private apps:** ZTNA secures and simplifies access to private applications without the complication or risk associated with VPNs. Like other Forcepoint ONE solutions, ZTNA also applies contextual access control, DLP, and malware protection to any private web app.
- → **Additional capabilities:** Such as RBI for the ultimate form of protection from web threats, or Cloud Security Posture Management (CSPM) to scan cloud providers for risky configurations.
- → **Cloud Firewall:** Add-on to SWG to secure all internet traffic and safeguard against attacks designed to exploit vulnerable branch sites.

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