Forcepoint

Solution Brief

Forcepoint ONE Web Security

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 platform
- Include Remote Browser Isolation (RBI) for safe browsing and downloads from uncategorized and newly registered sites

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

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. GenAI has only increased the stakes - while it promises massive productivity increases it also exposes your organization to much more risk. However, with the proper guardrails you can take advantage of the productivity increases that AI can offer while keeping sensitive data safe and ensuring acceptable use. 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 modern web security solutions 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 cloud architectures are specifically designed to scale up and out on demand, many SWG vendors lack such a highly distributed cloud presence. In contrast, Forcepoint ONE has a distributed architecture that not only provides a highly resilient 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 performance sensitive web content and apps as competing Secure Web Gateways. 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 web controls in Forcepoint ONE lets you block , use a confirmation page, use quota time, prompt for multi-factor authentication, allow, or even use RBI to isolate the traffic.You can manage access based on user group, device posture, location. This can allow an organization to easily enforce controls to block shadow IT use of GenAI sites, for example, for generating code with a block page to direct them to corporate sanctioned resources, and the granularity to distinguish between other types of AI sites, say to allow access to conversational or multimedia generating AI sites while also enforcing guardrails around what data can be posted into those sites.

Block uploading of sensitive data to unsanctioned websites

With our security engine, you can prevent regulated data or intellectual property from being sent to personal file storage, social media, personal email accounts, or GenAI sites. You can scan and block file uploads and text posts for sensitive data with easy to use controls. Optionally, customers can inherit advanced DLP policies from Forcepoint ONE Data Security to augment with the industry's leading advanced data security solution.

Stop malware from getting onto user devices without compromising usability

The Forcepoint ONE Web Security service provides multiple forms of protection against web-borne malware, including blocking categories of websites, inline scanning of downloaded files, and Zero Trust based advanced threat protection such as Remote Browser Isolation. With Forcepoint RBI, even sites or downloaded files that are contaminated can be used safely and efficiently.

Detect and control shadow IT

The web security service works to identify websites that are being used in place of preferred company apps. These "shadow IT" sites are automatically collected and displayed in the Cloud Apps dashboard.

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.

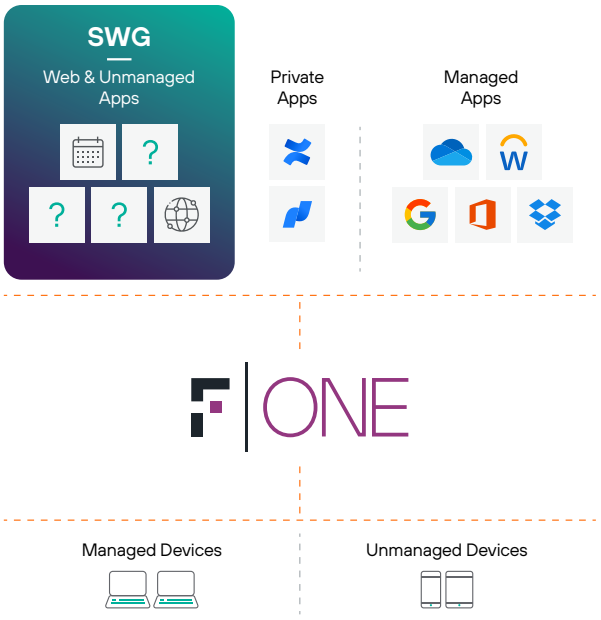
Forcepoint ONE Web Security maximizes uptime, productivity, and performance

The Web Security service is part of Forcepoint ONE, our advanced cloud platform with 300 points of presence (PoPs), global accessibility, and proven 99.999% uptime to secure web access and preserve user productivity. Forcepoint ONE integrates 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 with any site in real time including enforcing Zero Trust Web Access using Forcepoint RBI.



Secure data everywhere, for people working anywhere

Let's see how the web security service simplifies things 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 an integrated security solution for web, cloud, and private apps

In addition to web security, the Forcepoint ONE cloud security platform secures access to business information on any corporate SaaS tenant and private apps:

- **Cloud (SaaS and IaaS):** CASB 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. Integrates with Forcepoint ONE Data Security to enforce advanced DLP policies over SSE channels.
- **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:** Expand on the essential level of RBI with CDR to use beyond unknown or newly registered sites for the ultimate form of protection from web threats, or add Advanced Malware Detection and Protection for enterprise-class malware sandboxing and analytics.

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