# Secure Web Gateway

## Stoppen Sie Datenverluste und Malware-Angriffe, nicht die Produktivität

## Anwendungsfälle

- Schneller und sicherer Zugang zum Internet für Mitarbeiter
- Durchsetzen von Nutzungsrichtlinien
- Sperren des Uploads sensibler Daten auf nicht zugelassene Websites
- Verhindern, dass Malware auf die Geräte der Benutzer gelangt, ohne die Benutzerfreundlichkeit zu beeinträchtigen
- Erkennen und Kontrollieren von Schatten-IT
- Verhindern, dass private Benutzerdaten im Unternehmen verwendet werden

## Lösung

- Schnelle Internetsicherheit mit integrierten DLP-Funktionen und erweitertem Schutz vor Bedrohungen
- Granulare Zero-Trust-Zugriffs- und Datenkontrollen auf der Grundlage von Benutzergruppe, Gerätetyp, Benutzerstandort, Website-Kategorie, Website-Risiko-Score usw.
- Verteilte Architektur beseitigt Engpässe auf der hochverfügbaren, hochskalierbaren AWS-Plattform
- Optionale Remote Browser Isolation (RBI) für sicheres Surfen und Herunterladen

## Ergebnis

- Steigern der Produktivität, da Mitarbeiter überall, nahtlos und sicher im Internet surfen können
- Geringeres Risiko durch Kontrolle sensibler Daten in der Cloud und Malware-Schutz
- Niedrigere Kosten durch vereinfachte Sicherheitsmaßnahmen, indem Richtlinien zentral festgelegt werden

Das Internet ist sowohl ein Segen als auch ein Fluch. Die meisten Menschen sind auf Internet-Informationen angewiesen, um ihre Arbeit zu erledigen, aber das Internet birgt auch das Risiko der Datenexfiltration, der Verletzung von Personalrichtlinien, des Produktivitätsverlusts und der Infektion mit Malware. In Zeiten, in denen die Konsequenzen von Versäumnissen bei der Sicherheit von Daten und Menschen täglich zunehmen, ist die Sicherung von Interaktionen im Internet eine strategische Anforderung für moderne Unternehmen.

**Schneller und sicherer Zugang zum Internet für Mitarbeiter**

Bei den meisten SWGs muss der gesamte Datenverkehr im Internet – sei es vor Ort oder in der Cloud – einen Umweg über ein zentrales Rechenzentrum nehmen, was zu Latenzen führt, die moderne Webanwendungen erheblich stören können. Im Gegensatz dazu verfügt das SWG in Forcepoint ONE über eine verteilte Architektur, die solche Engpässe beseitigt und einen bis zu doppelt so hohen Durchsatz für leistungsempfindliche Webinhalte und Anwendungen ermöglicht. Wir machen dies möglich, indem wir Sicherheitsrichtlinien lokal auf dem Gerät des Benutzers durchsetzen, sodass der Datenverkehr direkt zwischen dem Benutzer und der Website ausgetauscht werden kann.

**Durchsetzen von Kontrollen der Nutzungsrichtlinien für riskante Websites**

Die Verlockung kann groß sein, das Internet nicht immer nur für Unternehmensgeschäfte zu nutzen, sondern auch zur Zerstreuung. Mit dem SWG in Forcepoint ONE können Sie unproduktive oder unangemessene Websites für Benutzer mit voller Pfadkontrolle sperren oder zulassen. Sie können beispielsweise bestimmte Reddit-Subreddits sperren und andere zulassen. Sie können den Zugriff auf der Grundlage von Benutzergruppe, Gerätezustand, Standort, URL-Kategorie (vordefiniert oder benutzerdefiniert), Reputationswert und Risikowert für Unternehmensanwendungen verwalten. Benutzerdefinierte URL-Kategorien können vollständige URL-Verzeichnispfadeinträge enthalten, sodass Administratoren unterschiedliche Richtlinien für verschiedene Verzeichnisse einsetzen können.

**Sperren des Uploads sensibler Daten auf nicht zugelassene Websites**

Mit unserem SWG können Sie verhindern, dass regulierte Daten oder geistiges Eigentum an persönliche Dateispeicher, soziale Medien oder persönliche E-Mail-Konten gesendet werden. Sie können Datei-Uploads und HTTPS-Post-Methoden nach sensiblen Daten scannen und blockieren. Dabei verwenden Sie dieselben vordefinierten und benutzerdefinierten DLP-Muster, die von den CASB- und ZTNA-Diensten in Forcepoint ONE verwendet werden.

**Verhindern, dass Malware auf die Geräte der Benutzer gelangt, ohne die Benutzerfreundlichkeit zu beeinträchtigen**

Unser SWG bietet mehrere Arten des Schutzes vor Malware aus dem Internet. Dazu gehören das Blockieren von Website-Kategorien, Inline-Scans heruntergeladener Dateien und auf Zero Trust basierter erweiterter Bedrohungsschutz wie Remote Browser Isolation (RBI). Mit unserer RBI können sogar kontaminierte Websites oder heruntergeladene Dateien sicher und effizient verwendet werden.our RBI, even sites or downloaded files that are contaminated can be used safely and efficiently.

### Erkennen und Kontrollieren von Schatten-IT

Der SWG-Dienst arbeitet mit unserem CASB zusammen, um Websites zu ermitteln, die anstelle der bevorzugten Unternehmensanwendungen verwendet werden. Diese „Schatten-IT"-Websites werden automatisch erfasst und in der Konsole angezeigt.

### Verhindern, dass private Benutzerdaten im Unternehmen verwendet werden

Zum Schutz der Privatsphäre der Mitarbeiter können Unternehmen die Entschlüsselung und Überprüfung des Datenverkehrs von und zu bestimmten Kategorien von Websites verhindern, die in der Regel mit personenbezogenen Daten (PII) genutzt werden, z. B. Bank-, Gesundheitsund Versicherungsdaten.

### SWG in Forcepoint ONE maximiert Betriebszeit, Produktivität und Leistung

SWG ist Teil von Forcepoint ONE, unserer Hyperscaler-basierten Cloud-Plattform mit 300 Points-of-Presence (PoPs), globaler Erreichbarkeit und nachweislich 99,99 % Betriebszeit, um den Internetzugang zu sichern und die Produktivität der Benutzer zu erhalten. Forcepoint ONE vereint CASB, SWG und ZTNA, um den Zugriff auf unternehmenseigene SaaS-, Web- und private Anwendungen zu schützen – Sicherheit leicht gemacht.

### Vereinfachen der Internetsicherheit in der realen Welt

Mit der Forcepoint ONE Cloud-Plattform ist die Implementierung von Cloud-Sicherheit denkbar einfach.

Von einer einzigen Konsole aus können Administratoren den Zugriff verwalten und Datei-Downloads und -Uploads zwischen einem verwalteten Gerät und einer beliebigen Website kontrollieren.


**Sehen wir uns am Beispiel von Kris an, wie das SWG die Internetsicherheit vereinfacht. Kris ist Unternehmensanalyst, arbeitet von zu Hause aus und beginnt gerade seinen Arbeitstag.**

| | |
|---|---|
| Kris durchsucht „reddit.com" für unternehmensbezogene Recherchen. | Dabei besucht Kris „reddit.com/r/technology", um aktuelle Beiträge über Malware zu recherchieren. Die SWG-Inhaltsrichtlinien erlauben eine Granularität bis zur Verzeichnisebene. Dieses Subreddit gilt als arbeitsbezogen, sodass Kris darauf zugreifen kann. |
| Im Subreddit „r/technology" klickt Kris versehentlich auf einen Link zu einer unangemessenen Seite. | Der Forcepoint ONE-Administrator von Kris hat SWG-Inhaltsrichtlinien erstellt, die den Zugang zu Verzeichnissen wie „r/technology" erlauben, aber den Zugang zu unangemessenen Subreddits und Seiten blockieren. Das SWG verhindert den Fehler von Kris und blockiert die neue Seite. |
| Kris beginnt auf dem Firmenlaptop mit einer vertraulichen Tabelle, die personenbezogene Daten von Kunden enthält, und möchte auf dann auf dem privaten Laptop weiterarbeiten. Kris versucht, die Datei in den persönlichen Cloud-Speicher hochzuladen und auf dem persönlichen Laptop herunterzuladen. | Um den Verlust von Geschäftsdaten zu verhindern, hat der Forcepoint ONE-Administrator des Unternehmens eine SWG-Inhaltsrichtlinie erstellt, die das Hochladen sensibler Kundeninformationen (PII) auf alle persönlichen Filesharing-Websites blockiert. Wenn Kris versucht, die Daten hochzuladen, wird dies blockiert und es wird in einer Meldung erklärt, warum. |

## Teil einer einheitlichen Sicherheitslösung für Web-, Cloud- und private Anwendungen

Zusätzlich zum SWG sichert die All-in-One-Plattform von Forcepoint ONE den Zugang zu Geschäftsinformationen auf allen SaaS-Mandanten-Anwendungen des Unternehmens und auf privaten Anwendungen:

- **Cloud (SaaS and IaaS):** CASB wendet kontextbezogene Zugriffskontrolle, Data Loss Prevention (DLP), Verhinderung von Datenverlust) und Malware-Schutz auf jede öffentlich zugängliche Webanwendung an, die SAML 2-Integration mit Identitätsanbietern (IdPs) von Drittanbietern unterstützt, und zwar von jedem modernen Browser auf jedem mit dem Internet verbundenen Gerät aus. Ruhende Daten in gängigen IaaS- und SaaS-Systemen können ebenfalls auf sensible Daten und Malware gescannt und bereinigt werden. Es werden dieselben DLP-Abgleichmuster verwendet, die SWG und ZTNA für private Webanwendungen zur Verfügung stehen.
- **Private Anwendungen:** ZTNA schützt und vereinfacht den Zugriff auf private Anwendungen ohne die mit VPNs verbundenen Komplikationen und Risiken. Wie andere Forcepoint ONE-Lösungen wendet ZTNA kontextbezogene Zugriffskontrolle, DLP und Malware-Schutz auf alle privaten Webanwendungen an.
- **Zusätzliche Funktionen:** Zum Beispiel RBI für den ultimativen Schutz vor Web-Bedrohungen oder Cloud Security Posture Management (CSPM) zum Scannen von Cloud-Anbietern auf riskante Konfigurationen.
- **Cloud Firewall:** Add-on zu SWG, um den gesamten Internetverkehr zu schützen und vor Angriffen auf anfällige Zweigstellen zu verteidigen.

## Weitere Informationen erhalten Sie im Lösungsüberblick von Forcepoint ONE.

**Möchten Sie Daten in Cloud-Apps von jedem Gerät aus schützen?**

**Lassen Sie uns mit einer Demo beginnen.**

**forcepoint.com/contact**