

# Forcepoint ONE Web Security

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.
- › Eine verteilte Architektur beseitigt Engpässe auf Plattformen mit hoher Verfügbarkeit
- › Remote Browser Isolation (RBI) für sicheres Surfen und das Herunterladen von unkategorisierten und neuen Websites

## 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
- › Kosten senken durch vereinfachte Sicherheitsabläufe

Das Netz ist sowohl ein Segen als auch ein Fluch. Die meisten Menschen sind von den darin enthaltenen Informationen abhängig, um ihre Arbeit zu erledigen, aber das Web birgt auch Risiken in Bezug auf Datenexfiltration, Verstöße gegen HR-Richtlinien, Produktivitätsverlust und Malware. GenAI hat den Druck weiter erhöht: Obwohl es massive Produktivitätsteigerungen verspricht, wird Ihr Unternehmen einem viel höheren Risiko ausgesetzt. Mit den richtigen Vorgaben können Sie jedoch die Produktivitätssteigerungen von KI nutzen und gleichzeitig sensible Daten schützen und eine akzeptable Nutzung gewährleisten. Da die negativen Auswirkungen, die daraus resultieren, dass die Daten und die Menschen nicht geschützt werden, täglich zunehmen, ist die Sicherung von Webinteraktionen eine strategische Notwendigkeit für moderne Unternehmen.

### Schneller und sicherer Zugang zum Internet für Mitarbeiter

Bei den meisten modernen Websicherheitslösungen wird der gesamte Web-Traffic über ein zentrales Rechenzentrum umgeleitet – ob lokal oder in der Cloud –, wodurch zusätzliche Latenzzeiten entstehen, die moderne Web-Anwendungen erheblich beeinträchtigen. Und obwohl Cloud-Architekturen für eine individuelle Skalierung entwickelt wurden, fehlt bei vielen SWG-Anbietern solch eine hochgradig verteilte Cloud-Präsenz. Im Gegensatz dazu bietet Forcepoint ONE eine verteilte Architektur, die nicht nur über eine sehr stabile Cloud-Architektur mit über 300 Präsenzpunkten auf der ganzen Welt verfügt, sondern auch eine alternative Option bietet, die den Kunden noch mehr Flexibilität bietet: einen On-Device-Agenten, der Engpässe beseitigt und einen bis zu doppelten so hohen Durchsatz für leistungsempfindliche Webinhalte und Apps liefert wie konkurrierende Secure Web Gateways. Diese Option setzt die Sicherheitsrichtlinien lokal auf dem Gerät des Benutzers um, sodass der Datenverkehr direkt zwischen dem Benutzer und der Website ausgetauscht werden kann.

### Durchsetzen von Kontrollen der Nutzungsrichtlinien für riskante Websites

Man kann sich im Web sehr schnell von Dingen ablenken lassen, die nicht unbedingt mit der Arbeit zu tun haben. Mit den Web-Kontrollen in Forcepoint ONE können Sie Datenverkehr blockieren, eine Bestätigungsseite verwenden, Kontingenzzeit verwenden, eine Multi-Faktor-Authentifizierung anfordern oder zulassen und sogar RBI verwenden, um den Datenverkehr zu isolieren. Sie können den Zugriff basierend auf Benutzergruppe, Geräteposition und Standort verwalten. Dadurch können Unternehmen ganz einfach Kontrollen durchsetzen, um die Nutzung von GenAI-Websites durch Schatten-IT-Systeme zu blockieren, beispielsweise zum Generieren von Code mit einer Blockierseite, um sie auf konzerneigene Ressourcen zu leiten, und die Granularität, um zwischen anderen Arten von KI-Websites zu unterscheiden, z. B. um den Zugriff auf KI-Webistes zu erlauben, die Konversationen und Multimedia generieren, und gleichzeitig Vorgaben zu machen, welche Daten auf diesen Websites veröffentlicht werden können.

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

Mithilfe unserer Sicherheitsengine können Sie verhindern, dass regulierte Daten oder geistiges Eigentum an persönliche Dateispeicher, soziale Medien, persönliche E-Mail-Konten oder GenAI-Websites gesendet werden. Mit benutzerfreundlichen Kontrollen können Sie Datei-Uploads und Posts von vertraulichen Daten finden und blockieren. Optional können Kunden erweiterte DLP-Richtlinien von Forcepoint ONE Data Security übernehmen, um die führende Datensicherheitslösung der Branche zu vervollständigen.

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

Der Forcepoint ONE Websicherheitsdienst bietet mehrere Arten von Schutz vor webbasierter Malware, einschließlich der Blockierung von kategorisierten Websites, Inline-Scans von heruntergeladenen Dateien und Zero-Trust-basiertem, erweitertem Bedrohungsschutz wie Remote Browser Isolation. Mit Forcepoint RBI können auch Websites oder heruntergeladene Dateien, die kontaminiert sind, sicher und effizient verwendet werden.

### Erkennen und Kontrollieren von Schatten-IT

Der Websicherheitsdienst identifiziert Websites, die anstelle von bevorzugten Unternehmens-Apps verwendet werden. Diese „Schatten-IT“-Seiten werden automatisch erfasst und im Dashboard der Cloud-Apps 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-, Gesundheits- und Versicherungsdaten.

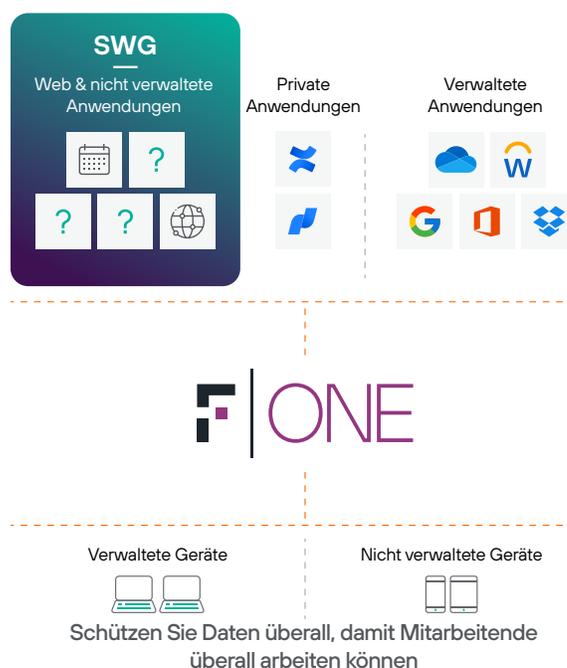
### Forcepoint ONE Web Security maximiert die Verfügbarkeit, e Produktivität und die Leistung

Der Websicherheitsdienst ist Teil von Forcepoint ONE, unserer fortschrittlichen Cloud-Plattform mit 300 Präsenzpunkten (PoPs), globaler Zugänglichkeit und einer bewährten Verfügbarkeit von 99,999 %, um den Webzugriff zu sichern und die Produktivität der Benutzer aufrechtzuerhalten. Forcepoint ONE kann in CASB, SWG und ZTNA integriert werden, um den Zugriff auf unternehmenseigene SaaS-, Web- und private Apps zu sichern, was die Sicherheit vereinfacht.

### Vereinfachen der Internetsicherheit in der realen Welt

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

Administratoren können den Zugriff über eine einzige Konsole verwalten und die Datei-Downloads und -Uploads von jeder Website in Echtzeit kontrollieren, einschließlich der Durchsetzung von Zero Trust Web Access mit Forcepoint RBI.





**Schauen wir uns einmal an, welche Vorteile der Websicherheitsdienst für Kris, einen Business Analysten, der von zu Hause aus arbeitet, bietet.**

<p>Kris durchsucht „reddit.com“ für unternehmensbezogene Recherchen.</p>	<p>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.</p>
<p>Im Subreddit „r/technology“ klickt Kris versehentlich auf einen Link zu einer unangemessenen Seite.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>

## Teil einer integrierten Sicherheitslösung für Web-, Cloud- und private Apps

Zusätzlich zur Websicherheit sichert die Forcepoint ONE Cloud-Sicherheitsplattform den Zugriff auf Geschäftsinformationen auf allen unternehmenseigenen SaaS-Mandanten und privaten Apps:

- **Cloud (SaaS und IaaS):** CASB wendet kontextbezogene Zugriffskontrollen, Datenverlustprävention (DLP) und Malware-Schutz auf jede öffentlich zugängliche Web-App an, die eine SAML 2-Integration mit Identitätsanbietern (IdPs) von Dritten unterstützt, und zwar von jedem modernen Browser auf jedem mit dem Internet verbundenen Gerät. Daten im Ruhezustand in beliebigen IaaS und SaaS können auf sensible Daten und Malware gescannt und geschützt werden. Kann mit Forcepoint ONE Data Security integriert werden, um erweiterte DLP-Richtlinien über SSE-Kanäle umzusetzen.
- **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:** Erweitern Sie die wesentliche RBI-Ebene mit CDR, um auch unbekannte oder neu registrierte Websites vor Bedrohungen aus dem Internet zu schützen, oder fügen Sie erweiterte Advanced Malware Detection and Protection für Malware-Sandboxing und -Analysen auf Unternehmensniveau hinzu.

## 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](https://forcepoint.com/contact)