Forcepoint ONE Web Edition

Descripción de la solución

Octubre 2022

Forcepoint

Table of Contents

Descripción general de la solución

Forcepoint ONE Secure Web Gateway (SWG) es una de las tres opciones de licenciamiento fundamentales de la plataforma de nube todo en uno Forcepoint ONE.

Forcepoint ONE SWG monitoriza y controla cualquier interacción con cualquier sitio web, lo que incluye bloquear el acceso a sitios web según la categoría y la puntuación de riesgo, bloquear la descarga de malware, bloquear la carga de datos confidenciales a cuentas personales para compartir archivos, detectar Shadow TI y, opcionalmente, proporcionar aislamiento remoto del navegador (RBI – Remote Browser Isolation) con desarme del contenido y reconstrucción segura (CDR – Content Disarm and Reconstruction).

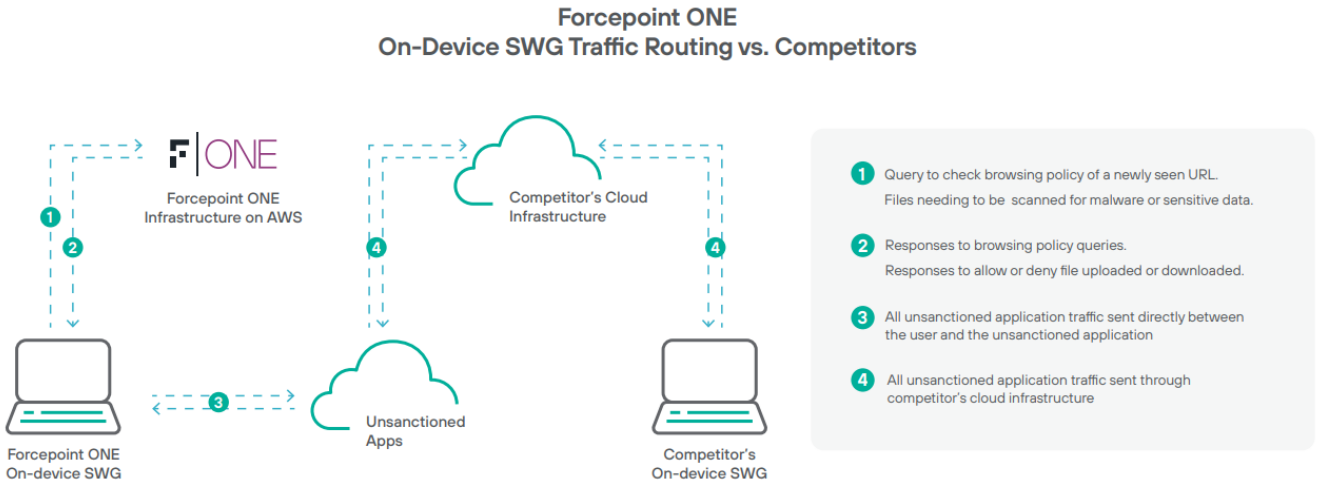
Ventajas clave de Forcepoint ONE

- Tiempo de actividad verificado del 99,99 % desde 2015.
- El escalado automático, más de 300 puntos de presencia y la arquitectura SWG distribuida minimizan la latencia y maximizan el rendimiento.
- La consola de administrador unificada reduce la gestión de configuración repetitiva y redundante.
- Gestión centralizada de agentes de dispositivo unificado para CASB, SWG y ZTNA, simplificando la implementación y administración posterior.
- El aprovisionamiento de SCIM acelera la incorporación de usuarios.
- El escaneo de datos en movimiento bloquea el malware y la exfiltración de datos entre los usuarios y cualquier aplicación web, sin importar dónde se encuentren.
- La lógica SASE programable en campo puede bloquear métodos de solicitud HTTP/S específicos, lo que da como resultado un control granular de cualquier elemento en una página web.
- RBI con CDR permite el uso seguro de sitios web desconocidos y el uso seguro de archivos descargados de esos sitios web.
- Controla el acceso al sitio web hasta nivel de directorio URL
- La función SWG no puede ser anulada, “bypasseada” o deshabilitada por el usuario.

Arquitectura Forcepoint ONE SWG

Forcepoint ONE SWG requiere la instalación del agente unificado de Forcepoint ONE para Windows o MacOS. Debido a que Forcepoint ONE SWG está basado en agentes, protege los datos del usuario y de la empresa, sin importar dónde se encuentre el usuario: en casa, en el movimiento o en la oficina. Por diseño, el agente unificado que alimenta el SWG no puede ser detenido o desinstalado por el usuario sin la aprobación de un administrador del tenant de Forcepoint ONE, lo que garantiza que el usuario no pueda hacer bypass fácilmente. Y debido a que el agente de Forcepoint ONE también es compatible con el forward proxy CASB y ZTNA para clientes sin navegador, estas capacidades se pueden habilitar con la licencia adecuada y no requieren descargas de software adicionales ni ninguna otra acción por parte del usuario final.

Un problema clave asociado con el SWG en el dispositivo de otros proveedores es el rendimiento. Forcepoint ONE aborda este problema con una combinación de tecnologías. Primero, Forcepoint ONE tiene una arquitectura distribuida en AWS con más de 300 puntos de presencia en los principales centros de población, y cada punto de presencia admite el escalado automático. Esto significa que la latencia se reduce cuando el agente en el dispositivo necesita comunicarse con el backplane de Forcepoint ONE en AWS. En segundo lugar, Forcepoint ONE SWG tiene una arquitectura distribuida en la que el agente en el dispositivo ejecuta la aplicación de políticas. Esto significa que es necesario que pase poco tráfico a través del backplane de Forcepoint ONE en AWS, como se muestra a continuación en la imagen.



Como se muestra en la imagen, el agente SWG en el dispositivo de Forcepoint ONE, a la izquierda, solo necesita comunicarse con el backplane de Forcepoint ONE en AWS en dos situaciones: cuando intenta acceder por primera vez a un sitio web que no se visitó recientemente para determinar las restricciones de acceso y cuando intentar cargar o descargar archivos u otros datos que deben analizarse en busca de malware o datos confidenciales.

En comparación, el agente SWG en el dispositivo del otro proveedor, a la derecha, debe enviar todo el tráfico web a través del backplane cloud del proveedor para la inspección y el reenvío del tráfico. Este enrutamiento de todo el tráfico web a través de la infraestructura en la nube del otro proveedor puede causar una pérdida de hasta el 50 % en el rendimiento efectivo, lo que genera problemas de productividad para los usuarios en ubicaciones con poco ancho de banda. Debido a que las cargas y descargas de archivos son una pequeña

fracción del tráfico total de Internet para la mayoría de los usuarios, Forcepoint ONE SWG generalmente puede admitir un rendimiento de aproximadamente el 95 % del ancho de banda total disponible de Internet, mientras reduce la latencia, lo que respalda una mayor adopción por parte de los usuarios.

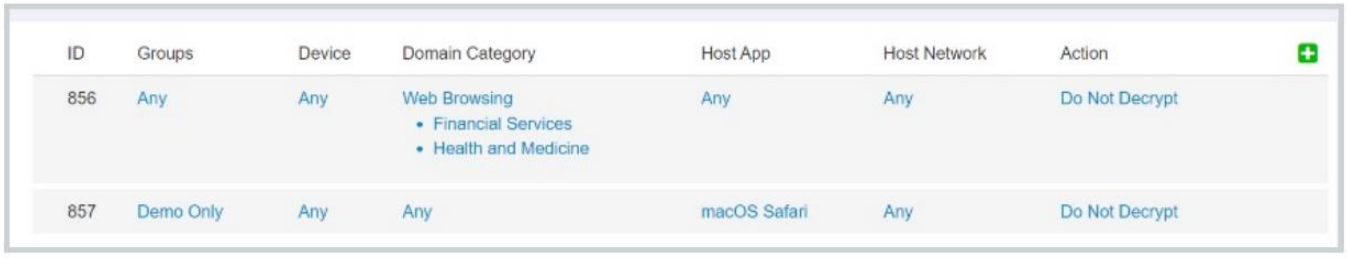
Características de Forcepoint ONE SWG

Las siguientes características forman parte de las capacidades core de la solución Forcepoint ONE SWG.

SWG Connection Policies

Permita que los administradores restrinjan el acceso a una variedad de sitios web o permitan que la conexión pase por alto el forward proxy SWG y no se descifre, y opcionalmente registre cada intento de conexión.

Los criterios para la aplicación de políticas incluyen grupo de usuarios, estado del dispositivo, categoría del dominio (categorías web predefinidas de Webroot BrightCloud, categorías de aplicaciones empresariales predefinidas de Forcepoint ONE o categorías personalizadas), aplicación host (navegadores web o aplicaciones que no son de navegador) y red del host (dirección IP del servidor DNS o sufijo DNS del usuario). Admite la privacidad del usuario al permitir que las conexiones a sitios financieros o de atención médica personal pasen sin cifrar.

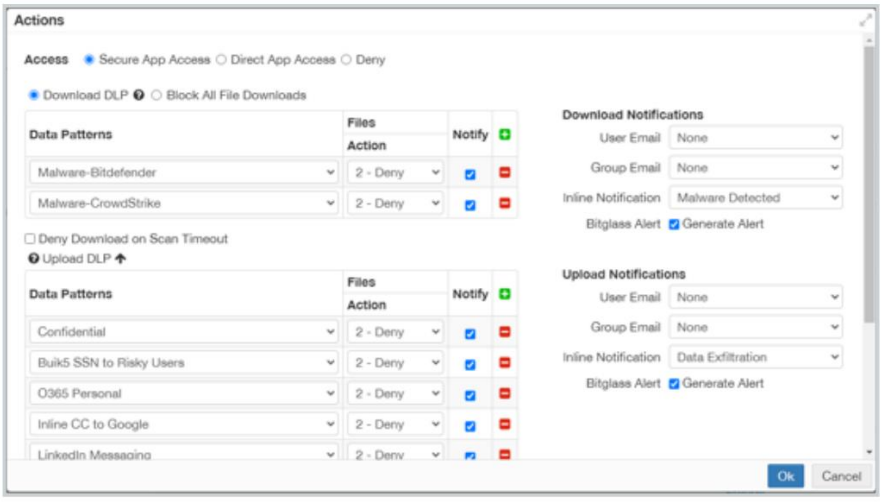


ID	Groups	Device	Domain Category	Host App	Host Network	Action
856	Any	Any	Web Browsing • Financial Services • Health and Medicine	Any	Any	Do Not Decrypt
857	Demo Only	Any	Any	macOS Safari	Any	Do Not Decrypt

SWG Content Policies

Permita que los administradores especifiquen reglas para denegar una conexión, permitir una conexión directa, establecer una conexión de acceso seguro a la aplicación (para hacer cumplir DLP y protección contra malware) o con licencias adicionales, establecer una conexión de acceso aislado mediante RBI con CDR. Los criterios para la aplicación de políticas incluyen el grupo de usuarios, la postura del dispositivo, la ubicación, la categoría de URL (predefinida o personalizada), la puntuación de reputación del sitio web y la puntuación de riesgo de la aplicación empresarial de Forcepoint ONE. Las categorías de URL personalizadas pueden incluir entradas de ruta de directorio de URL completa que permiten a los administradores aplicar diferentes políticas para diferentes directorios. Esto se puede usar para bloquear ciertos subreddits de Reddit, por ejemplo.

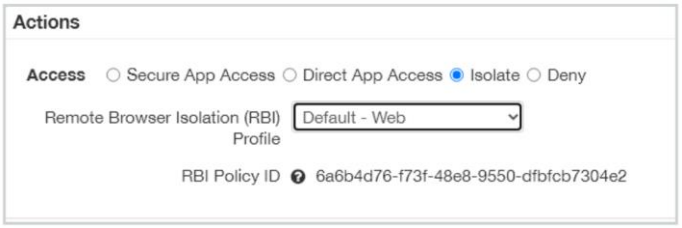
Cuando se especifica el acceso seguro a la aplicación en una política de contenido de SWG, el administrador puede especificar varias políticas de carga y descarga de DLP para bloquear la descarga o carga de datos confidenciales o malware (mediante el DLP integrado de Forcepoint ONE).

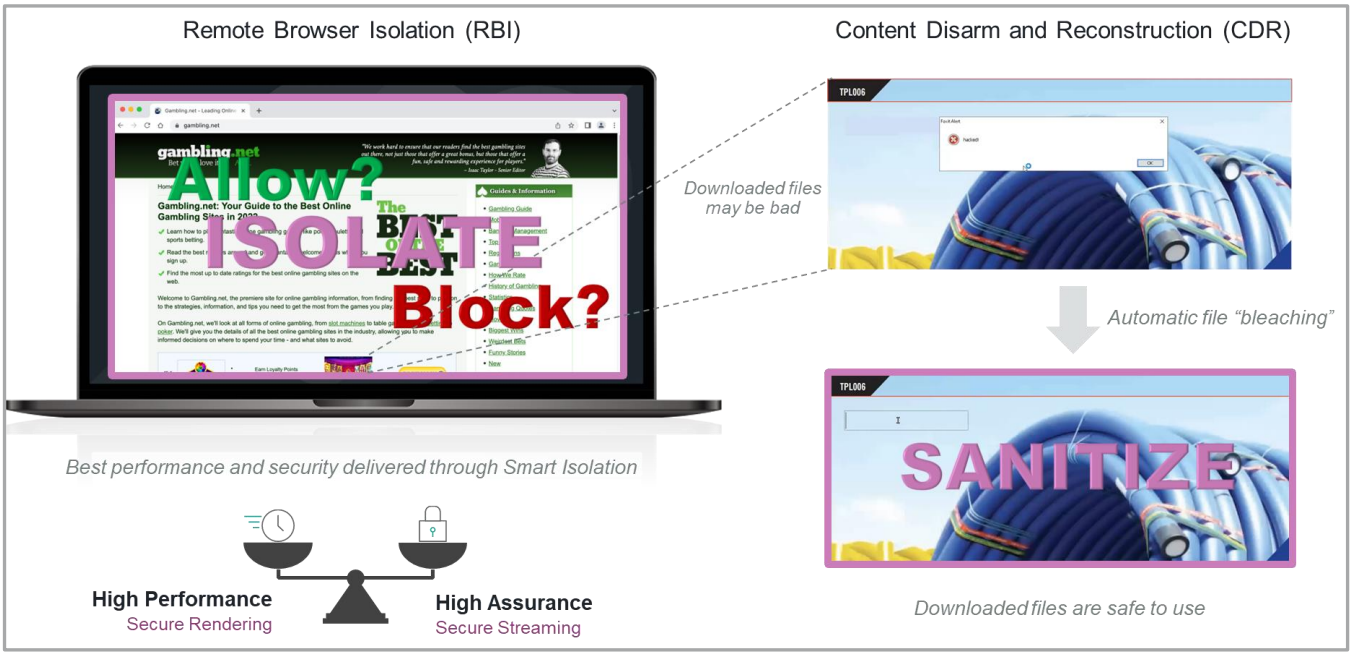


Perfiles RBI

Permita que los administradores especifiquen parámetros para una sesión de RBI que determinen qué tan restrictiva es la sesión.

Cuando una política de contenido SWG especifica una conexión de acceso aislado, el administrador también debe seleccionar un perfil RBI en el menú desplegable.





La siguiente tabla resume los valores y funciones permitidos de los parámetros del perfil RBI.

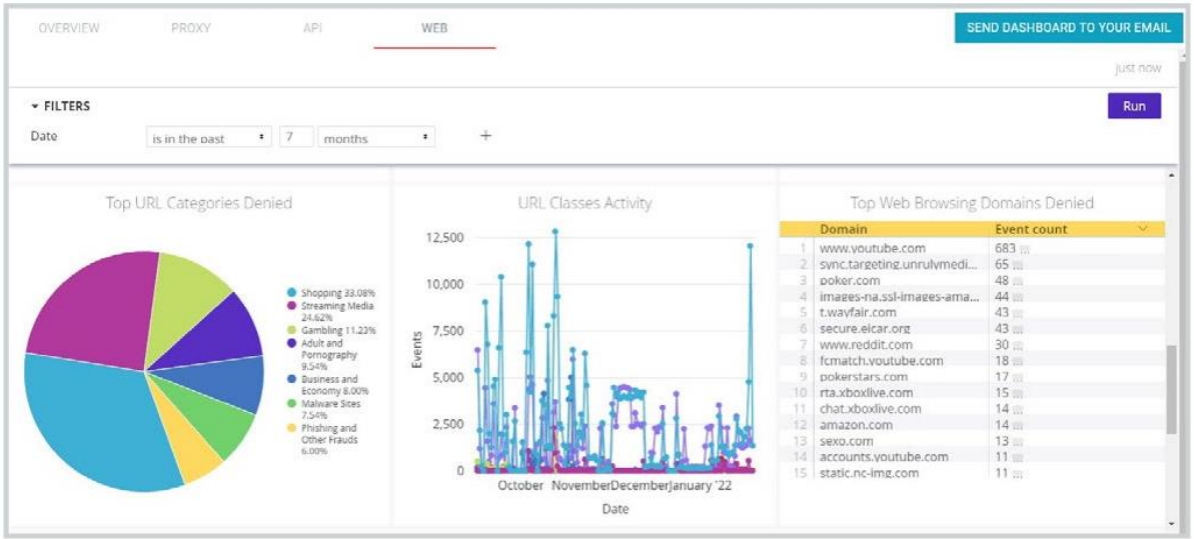
NAME	VALUES	DEFAULT	USAGE
Threat Level	Off (0), Moderate (60), High (80)	High	→ Renders site in read only mode if site threat level is higher than the specified value
TLS Error Policy	Fail, Warn, Ignore	Warn	→ Action the browser will take when navigating to bad TLS/Cert sites
Allow Downloads	Checkbox	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 → AV Scan: download after successful AV scan → 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. → 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 → uploads is 400,000 KB (400MB)

SWG Discovery Dashboard

Muestra representaciones gráficas del tráfico web y de aplicaciones empresariales agrupadas por reputación web o puntuación de confianza de la aplicación empresarial Forcepoint ONE, con vistas adicionales para datos cargados o descargados por sitio web y datos confidenciales cargados en sitios web agrupados por dominio y patrón de coincidencia.

Web Dashboard

Muestra representaciones gráficas de los patrones de tráfico web agrupados por categorías web, lo que brinda al administrador una descripción general de los tipos de sitios web que los usuarios visitan o intentan visitar y son bloqueados. Incluye datos adicionales sobre intentos de descarga de malware e intentos de carga de datos confidenciales.



Claves de la Plataforma Forcepoint ONE

Forcepoint ONE SWG también es compatible con estas funciones integradas en la plataforma Forcepoint ONE:

- **Control de acceso contextual**. Los usuarios no pueden navegar por Internet a menos que Forcepoint ONE los autentique y les permita iniciar sesión según las políticas de inicio de sesión que consideran la ubicación del usuario, el tipo de dispositivo, la postura del dispositivo, el comportamiento del usuario y el grupo de usuarios.
- **Prevención de pérdida de datos (DLP).** Los archivos y el texto se escanean al cargarlos o descargarlos en busca de datos confidenciales, se informan y bloquean según corresponda.
- **Field Programmable SASE Logic (FPSL).** Cualquier método de solicitud HTTP/S se puede registrar y, opcionalmente, bloquear en función del contenido de cualquier parte del método de solicitud.
- **Malware Scanning**. Los archivos se analizan durante la carga o la descarga en busca de malware mediante motores de análisis de CrowdStrike o Bitdefender, y se bloquean cuando se detectan.
- **Consola de administración unificada** para configuración, monitoreo y generación de informes para SWG, CASB y ZTNA. Permite a los administradores reutilizar patrones de coincidencia de DLP en SWG, CASB y ZTNA para aplicaciones web privadas.
- **Agente unificado** en el dispositivo para Windows o macOS con certificados únicos generados y rotados automáticamente.
- **99,99 % de tiempo de actividad del servicio**

Características y beneficios de Forcepoint ONE SWG

FEATURE	BENEFIT
Auto-scaling, distributed architecture on AWS with over 300 POPs worldwide.	→ 99.99% uptime. → 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. → 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. → Reduces risks associated with stolen passwords. → 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. → Enhances security. → Reduces IT overhead.
Single administrator console for managing all system capabilities across all applications, users, and devices.	→ Reduces complexity and time to value. → Increases visibility and control.

FEATURE	BENEFIT
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. → 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. → Monitors and controls shadow IT. → Blocks upload of sensitive data to unsanctioned websites. → 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.

Introducción a Forcepoint RBI

Proporcione a los usuarios un acceso seguro a sitios no categorizados y sitios maliciosos conocidos cuando sea necesario mediante Forcepoint Web Security con Remote Browser Isolation.

Si bien el acceso web y el correo electrónico son fundamentales para la mayoría de las organizaciones, sabemos que estas herramientas también son responsables de las amenazas de seguridad más peligrosas. El riesgo se ve amplificado por el crecimiento explosivo de usuarios que acceden a datos desde diferentes dispositivos desde cualquier parte del mundo. Forcepoint facilita la adopción de una postura proactiva contra estas amenazas con una solución que combina una protección contra amenazas web de clase mundial con capacidades que evitan que el malware basado en la web de día cero llegue a sus endpoints o a su red.

Mejore la seguridad con el aislamiento remoto del navegador

La tecnología de seguridad web de Forcepoint proporciona una protección contra amenazas inigualable. El motor de clasificación avanzada (ACE) identifica las amenazas mediante un análisis integral que incluye líneas de base de comportamiento e inteligencia de amenazas global en tiempo real. Y la plataforma de seguridad dinámica funciona con inteligencia de comportamiento centrada en el ser humano para comprender las actividades de riesgo. Forcepoint Remote Browser Isolation ofrece una protección mejorada para entornos seguros mediante el aislamiento del navegador.

El aislamiento del navegador evita que los sitios web entreguen malware, exploits de día cero y amenazas de phishing a los endpoints, lo que mejora la seguridad y la productividad al permitir un amplio acceso a la web para los usuarios. Los sitios web sospechosos o con riesgo como, sitios sin categorizar o nuevos dominios, y las URL de phishing, se procesan en contenedores virtuales remotos, lo que aísla los dispositivos de las amenazas, mientras que los usuarios disfrutan de una experiencia de navegación segura y totalmente interactiva.

Forcepoint Web Security con aislamiento de navegador remoto

La solución integrada ofrece una experiencia de navegación web nativa y sin problemas al tiempo que permite un acceso seguro y sin complicaciones a los sitios web que los usuarios necesitan para realizar su trabajo con éxito.

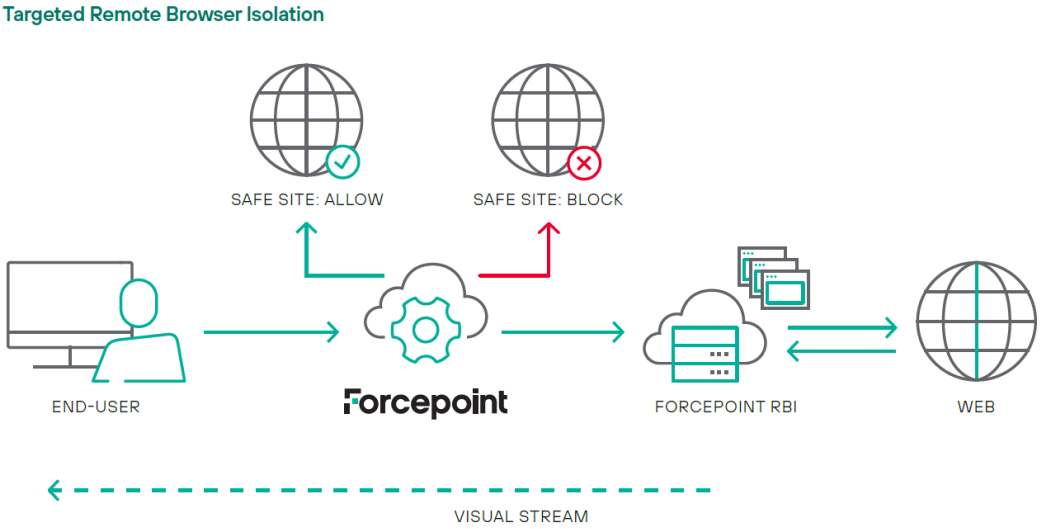
Los enlaces, las cookies, los marcadores, los portapapeles, etc. están completamente disponibles a través de todos los navegadores estándar, en cualquier dispositivo, bajo cualquier sistema operativo. Forcepoint Web Security está integrado con Forcepoint Remote Browser Isolation para proporcionar visibilidad e inteligencia de amenazas web con funciones completas para modificar el acceso web en función de políticas y análisis forense de comportamiento.

Casos de uso clave para el aislamiento de navegador remoto de Forcepoint:

- Ampliar acceso web sin riesgo adicional. Expanda de forma segura el acceso web a sitios no categorizados y con riesgoso.
- Proteja a los usuarios VIP y otros usuarios de alto riesgo. Proteja a los usuarios con privilegios elevados separando sus terminales de las amenazas web.
- Bloquear ataques de phishing. Evite que el phishing comprometa los endpoints, entregue ransomware

o robe credenciales.

- Prevenir la pérdida de datos. Mantenga los datos confidenciales de aplicaciones web fuera de los cachés del navegador; limitar las actividades de intercambio de datos de los usuarios en los sitios web.



Forcepoint Web Security ecosystem and remote browser integration protecting browser environments from malware threats.

Forcepoint Zero Trust Content Disarm and Reconstruction for Web Gateways

Las empresas se ven comprometidas por amenazas de día cero que penetran en la organización antes de que las defensas basadas en la detección puedan ponerse al día o por amenazas completamente desconocidas que tienen éxito sin haber sido identificadas correctamente.

Las descargas web pueden contener amenazas que provocan el mal funcionamiento de las aplicaciones y otorgan a los atacantes control sobre los sistemas empresariales.

Las cargas web pueden contener más información de la que una organización desea divulgar, lo que daña el negocio al revelar la propiedad intelectual.

La exclusiva tecnología Zero Trust CDR de Forcepoint asume que todos los datos son inseguros u hostiles; no trata de distinguir lo bueno de lo malo. Haciéndola la verdadera solución Zero Trust.

Zero Trust CDR puede integrarse con su defensa web existente en cuestión de momentos.

Las organizaciones dependen de la Web para compartir información, informar procesos comerciales clave y realizar transacciones. Las defensas web perimetrales existentes (pasarelas proxy web y firewalls) no pueden hacer frente a la avalancha de amenazas conocidas, desconocidas y de día cero ocultas en documentos e imágenes comerciales. Si no se controla, este vector de ataque es una amenaza existencial para las empresas. Los documentos e imágenes que descargan los usuarios contienen amenazas que pueden hacer que las aplicaciones no funcionen correctamente y dar a los atacantes control sobre los sistemas comerciales. Los documentos e imágenes que cargan pueden contener más información de la que la organización desea divulgar, lo que perjudica el negocio al revelar propiedad intelectual. Hasta la fecha, nadie ha encontrado una manera de detener el flujo de amenazas.

Derrota a la amenaza desconocida

Las defensas web perimetrales, los proxies y los cortafuegos existentes proporcionan una primera línea de defensa, detectando amenazas conocidas buscando las firmas de exploits encontrados anteriormente o comportamientos inseguros. Pero una y otra vez las empresas se ven comprometidas por amenazas de día cero que penetran en la organización antes de que las defensas basadas en la detección puedan ponerse al día o por amenazas completamente desconocidas que tienen éxito sin haber sido identificadas correctamente. Zero Trust Content Disarm and Reconstruction (CDR) para Web Gateways es la única forma de derrotar no solo las amenazas conocidas sino también las amenazas de día cero y desconocidas en el contenido a medida que cruzan el límite de la web porque no depende de la detección o la detonación de sandbox. En su lugar, utiliza un proceso único de transformación para garantizar una protección total.

Transforme su seguridad web

Zero Trust CDR para Web Gateways funciona extrayendo la información comercial de los documentos e imágenes en el flujo de navegación web. Los datos que llevan la información se descartan junto con cualquier amenaza. A continuación, se crean y entregan al usuario nuevos documentos e imágenes. Nada viaja de un extremo a otro, excepto el contenido seguro. Los atacantes no pueden entrar y la empresa obtiene lo que necesita.

Este proceso se llama transformación. No puede ser vencido; el equipo de seguridad está satisfecho porque se elimina la amenaza, mientras que los usuarios comerciales están satisfechos porque obtienen la información que necesitan.

Zero Trust CDR es la única forma de garantizar que las amenazas se eliminen del contenido. Prescindiendo de los paradigmas fallidos de detección y aislamiento de amenazas, la exclusiva tecnología Zero Trust CDR de Forcepoint asume que todos los datos son inseguros u hostiles; no trata de distinguir lo bueno de lo malo.

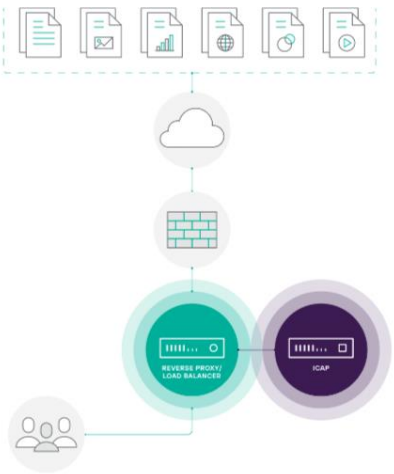
Enriquece la experiencia de navegación

Mientras los equipos de seguridad luchan para lidiar con los atacantes cibernéticos que parecen estar constantemente un paso por delante, es el usuario empresarial el que sufre. El tiempo dedicado a lidiar con alertas de seguridad de falsos positivos o esperar a que los documentos sean revisados y liberados inhibe los procesos comerciales y limita la productividad. Y cuando las cosas van mal, la reparación es costosa y requiere mucho tiempo.

Zero Trust CDR para Web Gateways enriquece la experiencia del usuario en la web y las redes sociales porque obtienen acceso oportuno a la información comercial que necesitan leer, compartir y realizar transacciones, sin ningún riesgo de compromiso por el contenido que consumen.

Garantice contenido digitalmente puro

A medida que el uso de la web y las redes sociales continúa informando todos los aspectos de los negocios, nunca ha sido más importante garantizar que el contenido que transmite sea seguro, puro y libre de amenazas. Cualquier empresa que sea capaz de establecer un historial para garantizar a sus usuarios, socios comerciales y clientes el acceso a contenido comercial limpio y puro se diferenciará en lo que se está convirtiendo rápidamente en un panorama cibernético sin ley.



Zero Trust CDR para Web Gateways hace exactamente eso, asegurando que las empresas puedan aprovechar los beneficios del uso de la Web y las redes sociales con la confianza de que el contenido comercial que manejan está libre de amenazas.

Perfecta integración con las defensas existentes

Adicionalmente, Forcepoint Zero Trust CDR se puede adquirir como solución independiente a otras soluciones del portfolio Forcepoint, por ejemplo, para integración con plataformas existentes proxy de otros fabricantes que no sean Forcepoint.

Zero Trust CDR para web se integra a la perfección con las defensas web perimetrales, como proxies web y los firewalls de aplicaciones existentes mediante el protocolo ICAP estándar de la industria.

Implementada como un "sidecar", la solución está configurada para que la pasarela proxy web o el firewall pase documentos e imágenes a un servidor Forcepoint Gateway eXtension (GX) a través de ICAP, donde se transforman para eliminar cualquier amenaza oculta y luego se devuelven al proxy para su entrega en adelante al usuario.

La integración con la defensa web perimetral existente toma unos minutos y los archivos de integración preconstruidos están disponibles para una serie de firewalls y proxies populares para facilitar aún más el proceso.

La solución Forcepoint Zero Trust CDR también es aplicable a otros casos de uso como la protección del correo electrónico o para la transferencia segura de documentos entre aplicaciones.

Detenga la infiltración de malware en el contenido

Los documentos de Office, los archivos de documentos portátiles de Adobe (PDF) y las imágenes son ahora los portadores más comunes de malware.

La complejidad de estos formatos de archivo y las aplicaciones que los manipulan los convierte en un objetivo natural para los atacantes. Cualquiera que sea el malware, desde ransomware y troyanos bancarios hasta kits de acceso remoto y registradores de teclas, los ciberdelincuentes saben que el mejor lugar para ocultar su última amenaza de día cero es dentro de un documento comercial cotidiano. Técnicas como el uso de malware sin archivos y el polimorfismo de archivos hacen que sea aún más difícil lidiar con la amenaza utilizando la seguridad cibernética basada en la detección convencional y la Web es el vector perfecto para la infiltración.

Zero Trust CDR para Web Gateways garantiza que los usuarios comerciales puedan cargar y descargar documentos e imágenes comerciales a través de la web con total tranquilidad debido a la forma única en que se transforman. Cada documento e imagen está sujeto a transformación y cada uno está libre de amenazas.

Detenga la pérdida de datos oculta en la esteganografía de imágenes

La esteganografía es la ocultación encubierta de datos dentro de archivos aparentemente inocuos. Es una forma de codificar un mensaje secreto dentro de otro mensaje, llamado portador, y solo el destinatario deseado puede leerlo. Ahora Stegware, la militarización de la esteganografía por parte de los atacantes cibernéticos está en aumento. Se ofrece de forma predeterminada en kits de malware como servicio en la Dark Web. Se ha utilizado en campañas de publicidad maliciosa para extorsionar a miles de usuarios y poner de rodillas a sitios de noticias de buena reputación. Se ha utilizado junto con sitios web de redes sociales para robar activos financieros de alto valor ocultos en imágenes aparentemente inocuas. Todo esto son malas noticias para los profesionales de TI que utilizan herramientas que identifican datos no seguros, ya que la esteganografía es imposible de detectar.

Zero Trust CDR para Web Gateways garantiza que todas las imágenes vistas por un usuario que navegue por la Web o se comunique a través de las redes sociales estén completamente libres de cualquier contenido oculto con Stegware. El proceso de transformación destruye cualquier contenido oculto haciendo que la imagen sea inútil para el atacante. Zero Trust CDR para Web Gateways aumenta la iniciativa de gobernanza y prevención de pérdida de datos existente, como el Reglamento general de protección de datos (GDPR), porque detiene por completo la pérdida de datos encubierta a través de la esteganografía de imágenes.

Interrupción de canales de comando y control (CnC)

Los ataques cibernéticos más sofisticados y perniciosos suelen implicar el establecimiento de un canal de comando y control (CnC) entre el atacante remoto y una estación de trabajo dentro de la red empresarial. A menudo, estos canales se establecen cuando una estación de trabajo previamente comprometida se pone en contacto con un servidor remoto, por ejemplo, a través de una imagen en un sitio de redes sociales, o cuando un malware previamente desconocido se disfraza como un documento comercial válido.

Zero Trust CDR para Web Gateways garantiza que se interrumpan los intentos de establecer un CnC. El proceso de transformación elimina cualquier amenaza que pueda estar oculta en los documentos, la Web y las imágenes de las redes sociales. Un tablero forense hace posible ver copias de documentos e imágenes "antes y después", lo que ayuda a identificar comportamientos sospechosos y ayuda a que los usuarios rindan cuentas.

Beneficios

- Siempre ofrece contenido seguro y libre de amenazas a través de los límites de la web
- Derrota a la amenaza desconocida
- Transforme su seguridad web
- Enriquece la experiencia de navegación
- Integración perfecta
- Detener el software malicioso
- Esteganografía de combate
- Disfruta de una protección sin igual

Mejoras con la migración a Forcepoint ONE para Web Security

Forcepoint ONE le brinda seguridad Zero Trust moderna para controlar el acceso, las actividades y el uso de datos en aplicaciones web, en la nube y privadas. Construido sobre una verdadera plataforma en la nube SASE/SSE, su Secure Web Gateway (SWG) tiene prevención de pérdida de datos (DLP) sólida y fácil de usar, capacidades de seguridad en la nube CASB e incluso Zero Trust Network Access (ZTNA).

Forcepoint ONE permite que las políticas corporativas se administren de forma centralizada y se apliquen en el endpoint o en la nube. Esto ofrece la mejor combinación de velocidad, seguridad y facilidad de administración, en casa, en la oficina o en cualquier lugar intermedio.

Pasarse a Forcepoint ONE puede ayudarlo a abordar iniciativas comerciales apremiantes como:

- Convertir su fuerza de trabajo remota en una fuerza de trabajo híbrida, de manera eficiente y segura.
- Asegurar el acceso de invitados a la web desde sus oficinas de acuerdo con sus propias políticas.
- Identificar y controlar aplicaciones de "Shadow TI" no autorizadas que podrían poner en riesgo sus datos.
- Transición de su infraestructura a una arquitectura SASE moderna basada en Zero Trust.

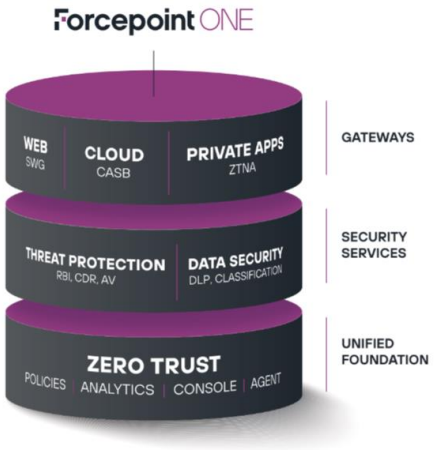
Simplificando su cambio a Forcepoint ONE

Junto con nuestra red global de partners de soluciones, estamos aquí para hacer que la migración de su solución de seguridad web existente a Forcepoint ONE sea un rápido éxito.

Con nuestro innovador enfoque de seguridad Zero Trust Web Access, puede modernizar y simplificar con confianza sus operaciones de seguridad mientras hace que su fuerza de trabajo remota e híbrida sea más segura y productiva.

¿Qué edición de Forcepoint ONE es adecuada para usted?

Forcepoint ONE ofrece una variedad de servicios de seguridad. Puede comenzar solo con las capacidades que necesita ahora (como la seguridad web) y expandirse más tarde a nuestra plataforma todo en uno. De cualquier manera, obtiene protección unificada contra amenazas y seguridad de datos desde UNA consola, con UN conjunto de políticas para administrar, de UN proveedor en el que puede confiar.



	FORCEPOINT WEB SECURITY	FORCEPOINT ONE WEB EDITION	FORCEPOINT ONE ALL-IN-ONE CLOUD EDITION
Architecture			
Deployment options	on-prem, hybrid, datacenter cloud	hyperscaler cloud	hyperscaler cloud
Elastic scalability	—	●	●
FedRAMP	—	●	●
Unified console for SWG, CASB, ZTNA	—	●	●
Secure Web Gateway (SWG)			
Direct-to-web fast connectivity for remote users	●	●	●
Agentless (BYOD, IoT, guests) site connectivity	●	●[1]	●[1]
Policies for guest networks	●	●[1]	●[1]
Localized access to web	●	●	●
Zero Trust browsing (RBI)	add-on	add-on	add-on
Zero Trust download file cleansing (CDR)	add-on	add-on	add-on
Cloud Access Security Broker (CASB)			
Shadow IT reporting & blocking	●	●	●
Inline inspection & control	add-on	●	●
API inspection	—	—	●
Zero Trust Network Access (ZTNA)			
Remote access to private apps without user VPNs	—	● 1 app	● Unlimited
Data Security			
Built-in DLP enforcement	add-on for SWG	SWG, CASB, ZTNA	SWG, CASB, ZTNA
Extensive library of PII, PHI, PCI policies	●	●	●
Classification tags for policy automation	●	●	●
Data security dashboard	—	●[1]	●[1]
Advanced Threat Protection			
Malware scanning	●	●	●
Advanced malware scanning	add-on	add-on	add-on
Threat dashboard	●	●[1]	●[1]
Support			
Essential support[2] included	—	●	●

Opciones de licenciamiento Forcepoint ONE

A continuación, se puede ver las opciones de contratación Forcepoint ONE y el alcance de las características incluidas en las diferentes versiones:

	Features	Web Edition	ZTNA Edition	CASB Edition	Cloud Edition
	Unified policies & Cloud console mgt	✓	✓	✓	✓
	Shadow IT reporting	✓	N/A	✓	✓
	Endpoint based Web security	✓	N/A	N/A	✓
	Professional DLP channels protection	Web, Unlimited Inline Cloud Apps, 0 API apps	Unlimited HTTP/S Inline Private Apps	Inline and API	Included Web, ZTNA, and CASB
	Zero Trust cloud / private apps security	1 Private App	Unlimited	N/A	Unlimited
	ZTNA for on-prem DLP FSM or SMC	✓	✓	✓	✓
	Incl. Essential Support (upgradeable)	✓	✓	✓	✓
A La Carte Add-Ons	RBI (Selective)	Add-On (SWG only)	N/A	N/A	Add-On (SWG only)
	CDR	Included in RBI, Roadmap	Roadmap	Included in RBI, Roadmap	Included in RBI, Roadmap
	Crowdstrike Malware Protection	Add-On	Add-On	Add-On	Add-On
	API scanning	N/A, Upgrade to CASB or Cloud Edition	N/A	3 Apps included, add-on via 3 App Packs	3 Apps included, add-on via 3 App Packs
	Dedicated API Nodes for improved perf.	N/A	N/A	Add-On	Add-On
	SSPM and/or CSPM modules	Priced by account/subscription count	N/A	Priced by account/subscription count	Priced by account/subscription count
	IaaS Scanning	N/A	N/A	Priced by data volume scanned	Priced by data volume scanned

forcepoint.com/contact

About Forcepoint

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint human point system delivers risk-adaptive protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.