Forcepoint

Solution Brief

Secure Web Gateway

Detenga el robo de datos y los ataques de malware, no la productividad

Casos de uso

- Brinde a los empleados acceso rápido y seguro a la web
- Aplique una política de uso aceptable
- Bloquee la carga de datos confidenciales a sitios web no autorizados
- Evite que el malware ingrese en los dispositivos de los usuarios sin comprometer su capacidad de uso
- Detecte y controle la TI paralela (shadow IT)
- Impida la exposición corporativa a los datos privados de los usuarios

Solución

- Seguridad web rápida con protección contra amenazas avanzadas y DLP integrada
- Acceso de Zero Trust granular y controles de datos basados en grupo de usuarios, tipo de dispositivo, ubicación de usuarios, categoría e sitio web, calificación de riesgo el sitio web y más
- Arquitectura distribuida que elimina los puntos de congestión en una plataforma de AWS de hiperescalamiento y alta disponibilidad
- Remote Browser Isolation (RBI) opcional para navegación y descargas seguras

Resultados

- Aumento de la productividad, lo que permite que las personas naveguen por la web en cualquier lugar con fluidez y seguridad
- Reducción del riesgo mediante el control de datos confidenciales en la nube y la detención del malware
- Reducción de costos gracias a la simplificación de las operaciones de seguridad con un único lugar desde donde establecer políticas

La web es a la vez una bendición y una maldición. La mayoría de las personas dependen de ella a fin de obtener información para su trabajo, pero la web también genera riesgos de exfiltración de datos, infracciones de políticas de RR. HH., pérdida de la productividad e infección de malware. Las consecuencias cada vez más frecuentes de no poder mantener a las personas y los datos seguros hacen que proteger las interacciones en la web sea un requisito estratégico para las organizaciones modernas.

Brinde a los empleados acceso rápido y seguro a la web

La mayoría de los Secure Web Gateway (SWG) desvían todo el tráfico de la web a través de una central de datos unificada (en las instalaciones o en la nube), lo que añade latencia que puede interferir significativamente con las aplicaciones web modernas. Y, si bien las arquitecturas en la nube hiperescaladoras están diseñadas específicamente para escalarse según la demanda, muchos proveedores de SWG carecen de una presencia en la nube tan distribuida y, en cambio, administran infraestructura desactualizada que conlleva cuellos de botella de red internos. En contraste, el SWG de Forcepoint ONE cuenta con una arquitectura distribuida que no solo brinda una arquitectura en la nube hiperescalable con más de 300 puntos de presencia en todo el mundo, sino que va más allá con una opción alternativa para dar a los clientes incluso más flexibilidad: un agente en el dispositivo que elimina los puntos de congestión y ofrece hasta el doble de capacidad para las aplicaciones y el contenido web sensibles al desempeño que los SWG de la competencia. Esta opción aplica políticas de seguridad a nivel local en el dispositivo del usuario de modo que el tráfico pueda intercambiarse directamente entre el usuario y el sitio web.

Implemente controles de política de uso aceptable (AUP) en sitios web riesgosos

La web puede generar distracciones y no siempre usarse para asuntos de la empresa. El SWG de Forcepoint ONE le permite bloquear y permitir visitantes a sitios web no productivos o inapropiados con control de la ruta completa. Por ejemplo, puede bloquear ciertos subreddits de Reddit y permitir el acceso a otros. Puede manejar el acceso según grupo de usuarios, postura del dispositivo, ubicación, categoría de URL (predefinida o personalizada), calificación de reputación y puntaje de riesgo de la aplicación de la empresa. Las categorías de URL personalizadas pueden incluir entradas de ruta de directorio de URL completas, permitiendo que los administradores apliquen distintas políticas a diferentes directorios.

Bloquee la carga de datos confidenciales a sitios web no autorizados

Con nuestro SWG, puede evitar que se envíen datos regulados o propiedad intelectual a almacenamiento de archivos personal, redes sociales o cuentas de correo electrónico personales. Puede examinar y bloquear cargas y métodos de HTTPS Post para datos sensibles con los mismos patrones de DLP predefinidos y personalizados utilizados por los servicios de CASB y ZTNA de Forcepoint ONE.

Evite que el malware ingrese en los dispositivos de los usuarios sin comprometer su capacidad de uso

Nuestro SWG brinda múltiples formas de protección contra malware transmitido por la web, lo que incluye el bloqueo de categorías de sitios web, el análisis en línea de archivos descargados, y la protección contra amenazas avanzadas basada en Zero Trust, como el Remote Browser Isolation (RBI). Con nuestro RBI, incluso los sitios o archivos descargados que están contaminados pueden utilizarse de manera segura y eficiente.

Detecte y controle la TI paralela (shadow IT)

El servicio de SWG trabaja en conjunto con nuestro CASB para identificar sitios web que se utilizan en reemplazo de aplicaciones preferidas por la empresa. Estos sitios de "TI paralela" se recopilan y muestran automáticamente en la consola.

Impida la exposición corporativa a los datos privados de los usuarios

Con el objeto de proteger la privacidad de los empleados, las organizaciones pueden impedir el descifrado y la inspección de tráfico hacia y desde categorías específicas de sitios web que normalmente se utilizan con información de identificación personal (PII), como datos de banca, salud y seguros.

El SWG de Forcepoint ONE maximiza la disponibilidad, la productividad y el desempeño

SWG forma parte de Forcepoint ONE, nuestra plataforma basada en la nube de hiperescalamiento con 300 puntos de presencia (PoP), accesibilidad global y con un tiempo productivo probado del 99,99 % para proteger el acceso web y preservar la productividad de los usuarios. Forcepoint ONE unifica CASB, SWG y ZTNA para proteger el acceso a aplicaciones privadas, web y de SaaS corporativas, simplificando así la seguridad.

Simplifica la seguridad web en el mundo real

La plataforma en la nube Forcepoint ONE ofrece un "botón fácil" para implementar la seguridad en la nube.

Desde una consola, los administradores puede gestionar el acceso y controlar las cargas y descargas de archivos entre cualquier sitio web y cualquier sitio o dispositivo administrado, incluso aplicando acceso web de Zero Trust mediante el RBI de Forcepoint.

Veamos cómo el SWG simplifica la seguridad en la web cuando Carlos, un analista comercial que trabaja desde casa, comienza su día laboral.

Carlos navega por reddit.com para hacer una investigación relacionada con la empresa.	Carlos visita reddit.com/r/technology para investigar publicaciones recientes sobre malware. Las políticas de contenido del SWG permiten granularidad a nivel de directorios; este subreddit se considera relacionado con el trabajo, de modo que Carlos puede acceder a él.
Dentro del subreddit r/technology, Carlos accidentalmente hace clic en un enlace a una página inapropiada.	El administrador de Forcepoint ONE de Carlos creó políticas de contenido para el SWG que permiten el acceso a directorios como r/technology, pero bloquean el acceso a subreddits y páginas inapropiados. El SWG evita el error de Carlos y bloquea la página nueva.
Carlos comienza una hoja de cálculo confidencial en la computadora portátil de la empresa que incluye PII de clientes y quiere seguir trabajando en su computadora portátil personal. Intenta cargar el archivo a un almacenamiento personal en la nube y descargarlo a su computadora personal.	Para impedir la pérdida de datos comerciales, el administrador de Forcepoint ONE de la empresa creó una política de contenido para el SWG que bloquea la carga de información confifencial de los clientes (PII) a cualquier sitio web de intercambio de archivos. Cuando Carlos intenta realizar la carga, esta se bloquea y aparece un mensaje que explica por qué se bloqueó la carga.

Parte de una solución de seguridad unificada para aplicaciones privadas, web y en la nube

Además de SWG, la plataforma todo en uno Forcepoint ONE protege el acceso a información empresarial en cualquier cliente de SaaS corporativo y aplicación privada:

- **Nube (SaaS e IaaS):** El CASB aplica control de acceso contextual, prevención contra la pérdida de datos (DLP) y protección contra malware a cualquier aplicación web orientada al público que admita integración SAML 2 con proveedores de identidades externos (IdP), desde cualquier navegador moderno en cualquier dispositivo conectado a internet. Los datos en reposo en IaaS y SaaS populares también pueden examinarse en busca de datos confidenciales y malware y remediarse. Utiliza los mismos patrones de coincidencia de DLP disponibles para SWG y ZTNA para las aplicaciones web privadas.
- **Aplicaciones privadas:** El acceso a la red de Zero Trust (ZTNA) protege y simplifica el acceso a aplicaciones privadas sin la complicación o el riesgo asociado con las VPN. Al igual que otras soluciones de Forcepoint ONE, el ZTNA también aplica control de acceso contextual, DLP y protección contra malware a cualquier aplicación web privada.
- **Capacidades adicionales:** como RBI para obtener la mejor forma de protección contra amenazas web o Cloud Security Posture Management (CSPM) para analizar proveedores de servicios en la nube en busca de configuraciones riesgosas.
- **Cloud Firewall:** complemento a SWG para proteger todo el tráfico de Internet y proteger contra ataques diseñados para explotar sitios de sucursales vulnerables.

Para obtener más información, lea el resumen de la solución Forcepoint ONE.

¿Está listo para proteger los datos en las aplicaciones en la nube desde cualquier dispositivo?

Comencemos con una demo.

forcepoint.com/contact