Forcepoint

Solution Brief

Forcepoint ONE Web Security

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
- La arquitectura distribuida elimina los puntos de congestión en la plataforma durante tiempos de mucha actividad
- Incluye el Remote Browser Isolation (RBI), para una navegación segura, así como de descargas de fuentes no categorizadas y sitios recientemente registrados

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
- Reduce los costos mediante la simplificación de las operaciones de seguridad

La web es, simultáneamente, una bendición y una maldición. La mayoría de las personas dependen de ella para obtener la información que necesitan para hacer su trabajo, pero la web también crea riesgos de exfiltración de datos, violaciones de las políticas de recursos humanos, pérdidas de productividad e infecciones de malware. La IA generativa (GenAI) solo ha aumentado el riesgo: Mientras que promete incrementos masivos de productividad, también expone a su organización a riesgos mucho mayores. Sin embargo, con las salvaguardas adecuadas, puede aprovechar los aumentos de productividad que la IA puede ofrecer, a la vez que mantiene los datos confidenciales seguros y garantiza un uso aceptable de ellos. Cuando las consecuencias de no mantener los datos y las personas seguras aumentan cada día, la protección de las interacciones en la web se convierte en un requisito estratégico para las organizaciones modernas.

Brinde a los empleados acceso rápido y seguro a la web

La mayoría de las soluciones de seguridad web modernas obligan a todo el tráfico web a desviarse a través de un sistema de datos centralizado, ya sea on-premises o en la nube, lo que agrega una latencia que puede interferir significativamente con las aplicaciones web modernas. Y, mientras que las arquitecturas de la nube están diseñadas específicamente para escalar ascendente o descendentemente bajo demanda, muchos proveedores de Secure Web Gateway (SWG) carecen de tal tipo de presencia altamente distribuida en la nube. Por el contrario, Forcepoint ONE cuenta con una arquitectura distribuida que no solo proporciona una arquitectura de nube altamente resiliente, con más de 300 puntos de presencia en todo el mundo, sino que va aún más allá, con una opción que le proporciona aún más flexibilidad a los clientes: un agente en el dispositivo que elimina los puntos de congestión y que puede ofrecer una capacidad de ejecución de hasta el doble para contenido web y apps sensibles al rendimiento que su competencia, las SWG. Esta opción refuerza las políticas de seguridad a nivel local, en el dispositivo del usuario, para pueda haber un intercambio directo del tráfico entre el usuario y el sitio web.

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

La web puede ser un espacio distractivo que no siempre se utiliza para asuntos empresariales. Los controles web de Forcepoint ONE te permiten bloquear, usar una página de confirmación, poner límites de tiempo, solicitar autenticación de múltiples factores, y permitir o incluso utilizar RBI para aislar el tráfico. Puedes gestionar el acceso en función del grupo de usuarios, la postura del dispositivo y la ubicación. Esto puede permitirle a una organización implementar fácilmente controles de bloqueo del uso de shadow IT en sitios de GenAI, por ejemplo, mediante la generación de un código con una página de bloqueo para dirigir a los agentes de tales actividades a recursos sancionados por la empresa, así como la granularidad para distinguir entre otros tipos de sitios de IA, como para permitir el acceso a sitios de IA conversacionales o de generación de multimedia, mientras también se aplican barreras de seguridad en torno a los datos que se pueden, y que no se pueden, publicar en esos sitios.

Bloquee la carga de datos confidenciales a sitios web no autorizados

Con nuestro motor de seguridad, puedes evitar el envío de datos regulados o de propiedad intelectual a bases personales almacenamiento de archivos, redes sociales, cuentas de correo electrónico personales o sitios de GenAI. Puedes escanear y bloquear cargas de archivos y publicaciones de texto para datos confidenciales con controles que son fáciles de usar. Opcionalmente, los clientes pueden heredar políticas de prevención de pérdida de datos (DLP) avanzadas de Forcepoint ONE Data Security para que aumenten con la solución líder en seguridad de datos avanzada de la industria.

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

El servicio de Forcepoint ONE Web Security proporciona múltiples formas de protección contra malware transmitido por la web, incluyendo el bloqueo de categorías de sitios web, el escaneo en línea de archivos descargados y protección avanzada contra amenazas Zero Trust, como el aislamiento remoto del navegador. Con el Forcepoint RBI, hasta sitios o archivos descargados que están contaminados pueden usarse de manera segura y eficiente.

Detecte y controle la TI paralela (shadow IT)

El servicio de seguridad web trabaja para identificar sitios web que están en uso en lugar de las apps preferidas de la empresa. Estos sitios de "shadow IT" se recopilan automáticamente y y se muestran en el panel de control de Apps de nube.

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.

Forcepoint ONE Web Security maximiza el tiempo de actividad, la productividad y el rendimiento

El servicio Web Security forma parte de Forcepoint ONE, nuestra plataforma avanzada en la nube, con 300 puntos de presencia (PoP), accesibilidad global y tiempo de actividad comprobado del 99,999 %, para proteger el acceso a la web y preservar la productividad del usuario. Forcepoint ONE integra CASB, SWG y ZTNA para facilitar un acceso seguro a SaaS corporativos, la web y apps privadas, 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 pueden gestionar el acceso y controlar las cargas y descargas de archivos con cualquier sitio en tiempo real, incluida la implementación de acceso web de Zero Trust mediante el uso del Forcepoint RBI.

Veamos cómo el servicio de seguridad web simplifica las cosas cuando Carlos, una analista de negocios que trabaja desde casa, inicia su jornada 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 integrada para la web, la nube y apps privadas

Además de la seguridad web, la plataforma de seguridad en la nube de Forcepoint ONE protege el acceso a datos empresariales en cualquier inquilino de SaaS corporativo y apps privadas:

- **Nube (SaaS e IaaS):** El CASB aplica control de acceso contextual, prevención de pérdida de datos (DLP) y protección contra malware en cualquier app web de interacción pública que admita la integración de SAML 2 con proveedores de identidad (IdP) terceros desde cualquier navegador y en cualquier dispositivo conectado a internet. Los datos en reposo en infraestructuras como servicio (IaaS) y softwares como servicio (SaaS) populares también se pueden escanear para datos sensibles y malware, y puede remediar. Se integra con Forcepoint ONE Data Security para reforzar las políticas de DLP avanzadas a través de canales del borde de servicios de seguridad (SSE).
- **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:** Amplíe el nivel esencial de RBI con CDR para un uso más allá de sitios desconocidos o recién registrados, para implementar una forma suprema de protegerse de las amenazas web, o Advanced Malware Detection and Protection para entornos de pruebas ("sandboxing") y analítica de malware de clase Enterprise.

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