

Forcepoint ONE: la plataforma en la nube simplifica la seguridad para la fuerza laboral híbrida

Casos de uso

- › Obtenga visibilidad y control de las interacciones de los trabajadores híbridos con los datos en aplicaciones web, en la nube y privadas.
- › Evite el uso indebido de datos confidenciales a los que se accede desde dispositivos administrados y no administrados.
- › Controla el acceso a contenido web de alto riesgo y diferentes tipos de sitios de GenAI.
- › Proporcione acceso remoto, rápido y seguro a recursos empresariales y aplicaciones privadas sin la complejidad de las VPN.

Solución

- › Una sola plataforma unificada permite administrar políticas de seguridad consistentes en todas las aplicaciones empresariales.
- › Un servicio todo en uno proporcionado en la nube que protege el acceso y los datos al combinar Secure Web Gateway (SWG) Cloud Access Broker (CASB) y Zero Trust Network Access (ZTNA).
- › Protección contra amenazas avanzadas integradas y seguridad de datos para mantener a los atacantes fuera y los datos confidenciales dentro.
- › Capacidades adicionales, como RBI con CDR para acceso web Zero Trust y CSPM para escanear inquilinos de la nube pública en busca de configuraciones riesgosas.
- › Forcepoint Classification para etiquetado de datos.

Resultado

- › Simplificada: reúne la seguridad para la web, la nube y las aplicaciones privadas en una plataforma unificada (con soporte sin agente).
- › Moderno: combina los principios de Zero Trust con una arquitectura SASE y seguridad avanzada, como Remote Browser Isolation y la desinfección de archivos descargados.
- › En todas partes: está disponible a nivel mundial, con más de 300 puntos de presencia (PoP).
- › Confiable: ofrece un tiempo de actividad verificado del 99,99 % desde 2015.
- › Rápido: utiliza la implementación distribuida y el escalado automático para eliminar los puntos de congestión.

Seguridad Data-first

La seguridad está cada vez más compleja, pero hay una mejor manera. Los usuarios ahora están trabajando desde cualquier lugar con datos que se propagan en todas partes: en sitios web, aplicaciones en la nube y aplicaciones privadas.

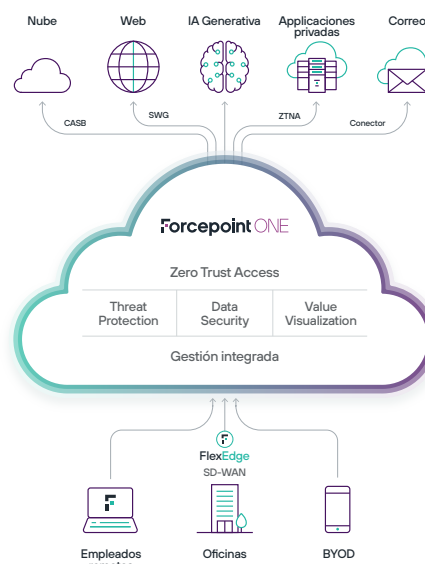
Para respaldar las iniciativas de retorno a la oficina (RTO) y las fuerzas laborales híbridas, los equipos de seguridad necesitan una plataforma de seguridad convergente que ponga a los datos en el centro de la imagen. Los controles de seguridad deben poder extenderse a través del acceso a la web, la nube y las aplicaciones privadas con visibilidad y control consistentes, para que las organizaciones puedan moverse a la izquierda de la pérdida para detener la pérdida de datos antes de que ocurra.

Con una solución data-first, los datos empresariales pueden protegerse en todas partes para personas que trabajan en cualquier lugar.

Forcepoint ONE simplifica la seguridad

Forcepoint ONE es una plataforma en la nube integrada que hace que la seguridad sea simple. Puedes adoptar rápidamente Zero Trust y Security Service Edge (SSE, el componente de seguridad de SASE) porque hemos reunido servicios de seguridad cruciales, incluidos SWG, CASB y ZTNA.

Habilita la productividad al adoptar de manera segura nuevas tecnologías como GenAI, controlando el acceso a diferentes tipos de sitios de GenAI y haciendo respetar barreras para proteger datos confidenciales y prevenir la exposición al malware.





Las capacidades de Zero Trust nativas en la nube de Forcepoint ONE incluyen:

- **Seguridad de DLP sin agente para aplicaciones en la nube y privadas.** Utilice de forma segura aplicaciones web empresariales privadas desde dispositivos personales, manteniendo a salvo los datos confidenciales.
- **Seguridad para datos y protección contra amenazas avanzadas e integradas.** Evita la pérdida o la exfiltración de datos e impide que los hackers entren con controles consistentes en todas partes.
- **Gateways unificados para acceso a la nube, la web y las aplicaciones privadas.** Control de acceso basado en identidades a aplicaciones empresariales administradas en un solo lugar para SWG, CASB y ZTNA.
- **Escalabilidad dinámica con acceso global.** 300 PoPs construidos en AWS proporcionan una conectividad rápida y de baja latencia y un tiempo de actividad del 99,99% independientemente de dónde trabaje la gente.

Seguridad unificada para aplicaciones web, en la nube y privadas

- **Nube:** CASB aplica el acceso granular a aplicaciones corporativas SaaS y datos desde cualquier dispositivo. CASB bloquea la descarga de datos confidenciales y bloquea la carga de malware en tiempo real. Escanea los datos en reposo en SaaS e IaaS populares en busca de malware y datos confidenciales y remedios según sea necesario. CASB detecta aplicaciones de Shadow IT y controla el acceso desde cualquier dispositivo administrado.
- **Web:** SWG supervisa y controla las interacciones con cualquier sitio web sobre la base del riesgo y la categoría, bloqueando la descarga de malware o la carga de datos confidenciales a cuentas de correo electrónico y de datos compartidos personales. Nuestra seguridad web en el dispositivo hace cumplir políticas de uso aceptable en dispositivos administrados ubicados en cualquier lugar.
- **Aplicaciones privadas:** ZTNA protege y simplifica el acceso a aplicaciones privadas sin la complicación o el riesgo asociados a las VPN.

Seguridad de datos y protección contra amenazas generalizadas

- **Data Loss Prevention (DLP):** los archivos y textos se analizan al cargarse y descargarse en busca de datos confidenciales y se bloquean, rastrean, encriptan o redactan según proceda. Más de 190 reglas de DLP predefinidas ayudan a optimizar el cumplimiento de normativas y proporcionar un tiempo de valoración rápido. La fácil integración con Forcepoint Enterprise DLP permite la seguridad de datos en todas partes: en el endpoint, en la red, en la web y en los servicios en la nube.
- **Escaneo de malware:** los archivos se analizan al cargarlos y descargarlos en busca de malware y se bloquean cuando se detectan.

Visibilidad y control integrados

- **Paquete de gestión integrado** para configuración, monitoreo e informes en canales SSE.
- **Políticas de inicio de sesión** para controlar el acceso a la web, la nube o las aplicaciones privadas sobre la base de la ubicación del usuario, el tipo de dispositivo, la postura del dispositivo, el comportamiento del usuario y el grupo de usuarios. Estos parámetros ayudan a evitar la apropiación de cuentas.
- **Políticas de DLP fáciles de usar** para controlar las descargas y cargas de datos confidenciales y malware para las aplicaciones SaaS administradas, aplicaciones privadas y sitios web, así como para los datos almacenados en SaaS e IaaS administrados.
- **Agente en el dispositivo** para Windows y MacOS para compatibilidad con SWG, CASB o ZTNA para aplicaciones cliente sin navegador y control de TI en la sombra.
- **Análisis unificado y visualización de valor** para una perspectiva rápida sobre los riesgos de seguridad, la utilización global y el impacto de la plataforma de seguridad en la nube todo en uno.

Capacidades adicionales disponibles según sea necesario

- **Cloud Security Posture Management (CSPM):** analiza la configuración de inquilinos de AWS, Azure y GCP en busca de configuraciones riesgosas y proporciona soluciones manuales y automatizadas.
- **SaaS Security Posture Management (SSPM):** analiza la configuración de inquilinos de Salesforce, ServiceNow y Office 365 en busca de configuraciones riesgosas y proporciona soluciones manuales y automatizadas.
- **Remote Browser Isolation (RBI):** protege a un usuario contra malware transmitido por la web en su dispositivo local al ejecutar un navegador en una máquina virtual alojada en la nube. Utiliza CDR para desinfectar archivos descargados durante una sesión de RBI de cualquier malware o elemento extraño.
- **Forcepoint Classification:** etiquetado de Data Classification con sugerencias impulsadas por IA para mejorar la precisión del etiquetado.
- **AMDP:** Analiza el comportamiento de los archivos en un área de prueba de malware para identificar contenido oculto y malicioso.

Suscripciones que desbloquean la simplicidad

Las suscripciones anuales por usuario están disponibles:

- **Edición todo en uno** para la seguridad de aplicaciones web, en la nube y privadas.
- **La edición para seguridad web** incluye el gateway de la web más CASB en línea para aplicaciones en la nube ilimitadas y elementos esenciales de RBI para sitios no categorizados o recientemente registrados para sumar soporte de API para aplicaciones en la nube y para aplicaciones privadas más adelante.
- **La edición ZTNA** protege un número ilimitado de aplicaciones privadas.
- **La edición CASB** protege un número ilimitado de aplicaciones en la nube en línea, e incluye API para 3 aplicaciones con la capacidad de agregar paquetes de aplicaciones adicionales o nodos de sondeo de API dedicados.
- **Todas las suscripciones** incluyen administración de nube centralizada, políticas con prevención de pérdida de datos, acceso automatizado a través de un agente de endpoint e informes completos.

forcepoint.com/contact