Forcepoint ONE

Una plataforma Data-first SASE única

Forcepoint

Whitepaper

forcepoint.com/es

Índice

La disrupción crea oportunidades para acelerar la transformación

Durante años, la "transformación digital" ha sido la moda principal. Antes de 2020, las aplicaciones estaban saliendo lentamente de los centros de datos corporativos y yendo hacia la nube. Un pequeño porcentaje de personas trabajaba de manera remota ocasionalmente, y con frecuencia utilizaban dispositivos móviles, como teléfonos y tabletas, para complementar las computadoras portátiles corporativas. Luego, irrumpió la pandemia y todo cambió.

De la noche a la mañana, la mayoría de los empleados comenzaron a trabajar desde casa. Con la productividad en juego, muchas organizaciones se adaptaron al acelerar su migración a aplicaciones basadas en la nube, a las cuales los usuarios podían acceder mucho más fácilmente que luchando con las VPN para conectarse con las aplicaciones tradicionales de los centros de datos. Si bien esto facilitó el acceso, también redujo la visibilidad y el control que las organizaciones de TI tenían sobre los datos confidenciales.

Lamentablemente, los ladrones de datos también se adaptaron rápidamente, atacando las aplicaciones en la nube de todo el mundo. Mientras la gente hacía malabares para equilibrar su vida personal y profesional en los mundos físico y digital, los "chicos malos" aprovecharon la enorme cantidad de personas que no estaban acostumbradas a trabajar en un mundo digital hostil. Acciones simples, como utilizar un teléfono inteligente para acceder a datos de trabajo o navegar por sitios web desde una computadora portátil de trabajo para hacer compras, crearon oportunidades para el phishing, descargas involuntarias de malware y otras formas de riesgo.

Trabajar desde cualquier lugar lo está cambiando todo. Otra vez.

Con el fin de la pandemia, la gente empezó a regresar a las oficinas, pero no como lo hacían en 2019. Incluso ahora, pocas organizaciones han regresado a los viejos patrones de trabajo. Si bien muchas empresas y agencias gubernamentales están tratando de alentar a las personas para que pasen tiempo en la oficina, ya no es el lugar predeterminado donde se realiza el trabajo. Muchas personas ahora ven a la oficina como un lugar que visitan, así como solían considerar los viajes a sitios remotos, a ver socios o clientes.

Además, muchos empleados han empezado a depender de teléfonos y tabletas (dispositivos que aportan ellos mismos) para mantenerse conectados cuando no están sentados en un escritorio. Lo que solía ser una comodidad para unos pocos selectos es ahora la manera estándar en que las personas mantienen la productividad en un mundo cada vez más competitivo.

Los empleados ahora esperan (y es lo que se espera de ellos) poder trabajar **en cualquier lugar** con datos empresariales que se encuentran **en todas partes.**

Desafío:
Adaptarse para proteger su empresa

Cambiar el lugar y el modo de trabajar de la gente ya es bastante difícil en los mejores momentos. Pero las incertidumbres recientes impulsaron a muchas empresas a enfocarse primero en asegurarse de estar preparadas para capear cualquier tormenta económica. Permitir que las personas utilicen los recursos de maneras innovadoras, por ejemplo, mediante el uso seguro de IA generativa como ChatGPT y el consumo de datos desde dispositivos propios sin poner en riesgo esos datos, es fundamental para impulsar los resultados financieros de una organización. Además, con presupuestos que siguen siendo limitados, encontrar nuevas eficiencias en los gastos de capital y operativos es clave para proteger los resultados finales. Por supuesto, todo esto debe hacerse de manera segura, para que los datos confidenciales puedan utilizarse donde sea necesario sin crear más riesgo o introducir problemas con los auditores.

Ahí es donde entra Forcepoint. Creemos que el enfoque correcto y la tecnología correcta pueden convertir estos rápidos cambios en el modo de trabajar de las personas y cómo se administra la información en una oportunidad en lugar de una carga. Es por eso que creamos Forcepoint ONE, nuestra plataforma para simplificar la manera en que usted conecta y protege a su gente y sus datos en un mundo moderno donde la nube tiene prioridad. Se trata de ayudar a que tengan más productividad y a que su empresa sea más eficiente, de manera segura.

Aumente La Productividad

Reduzca Costos

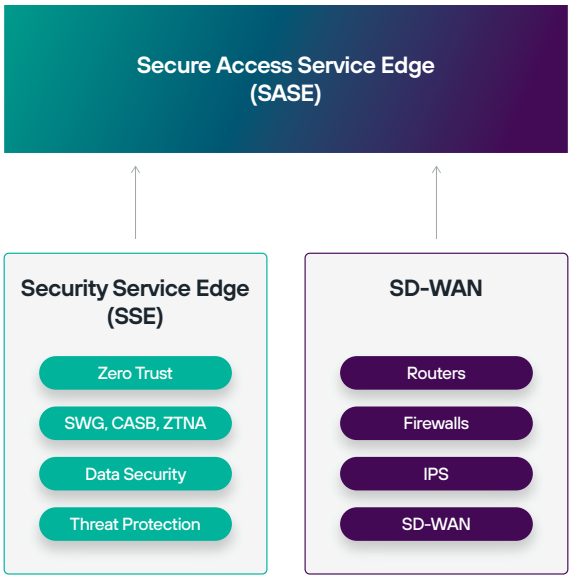
Reduzca El Riesgo

Optimice El Cumplimiento

Solución:
Secure Access Service Edge (SASE)

En 2019, Gartner propuso una nueva arquitectura de TI, Secure Access Service Edge, SASE, que une la seguridad y las redes, las administra y, a menudo, las suministra como un servicio desde la nube.

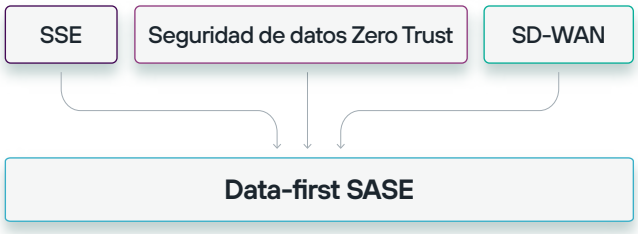
Los productos de conectividad, como los firewalls, los enrutadores, los sistemas de prevención de intrusiones y las redes centradas en las aplicaciones, ya han comenzado a converger en una nueva generación de soluciones SD-WAN unificadas. De manera similar, las arquitecturas de SASE facilitan que las puertas de enlace de seguridad apliquen políticas para la protección contra amenazas basada en los principios de confianza cero (Zero Trust) y la seguridad de datos de manera consistente en el acceso a aplicaciones en la web (SWG), en la nube (CASB) y privadas (ZTNA). Posteriormente, Gartner comenzó a referirse a este enfoque unificado con respecto a la seguridad como borde de servicios de seguridad (Security Service Edge, SSE).



Forcepoint ONE: Una plataforma Data-first SASE

Forcepoint fue uno de los primeros partidarios de la arquitectura SASE. Representa muchos de los principios y las tecnologías que ayudamos a que fueran pioneros en conectar y proteger a las empresas y las agencias gubernamentales distribuidas. Cuando la pandemia obligó a todas las organizaciones a tener una alta distribución, SASE se convirtió en el camino correcto en el momento adecuado para ofrecer la productividad y la eficiencia que nuestros clientes estaban solicitando.

Sin embargo, creemos que SASE es el punto de partida para una arquitectura moderna basada en la nube, no el punto final. Forcepoint va más allá de simplemente asegurar el acceso a los recursos empresariales: protegemos el uso continuo de los datos confidenciales en todas partes, desde el dispositivo final hasta la nube. A este enfoque lo llamamos Data-first SASE.



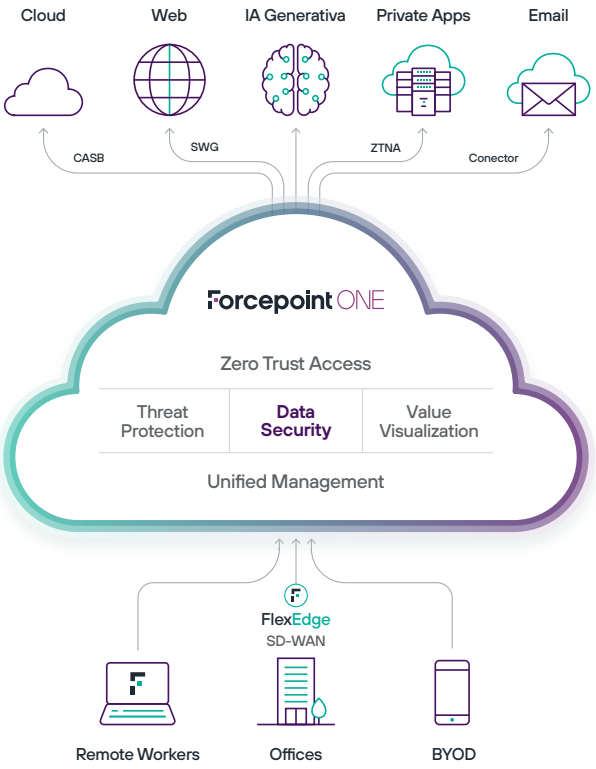
Nuestra plataforma Data-first SASE, Forcepoint ONE, une una amplia gama de tecnologías en la nube para simplificar la seguridad para las empresas y las agencias gubernamentales distribuidas. Ofrece a los empleados, contratistas y otros usuarios un acceso seguro y controlado a la información empresarial en la nube, la web y aplicaciones privadas, mientras mantiene a los atacantes afuera y los datos confidenciales adentro. En consecuencia, los usuarios pueden ser más productivos, ya sea en el hogar o en la oficina, mientras que las empresas son más eficientes.

Usos populares de Forcepoint ONE

Con Forcepoint ONE, las organizaciones pueden abordar los desafíos actuales de manera fácil y gradual. Esto permite que los equipos de TI resuelvan los problemas inmediatos rápidamente y que agreguen capacidades, según sea necesario en el futuro. Brevemente, es "Seguridad Simplificada".

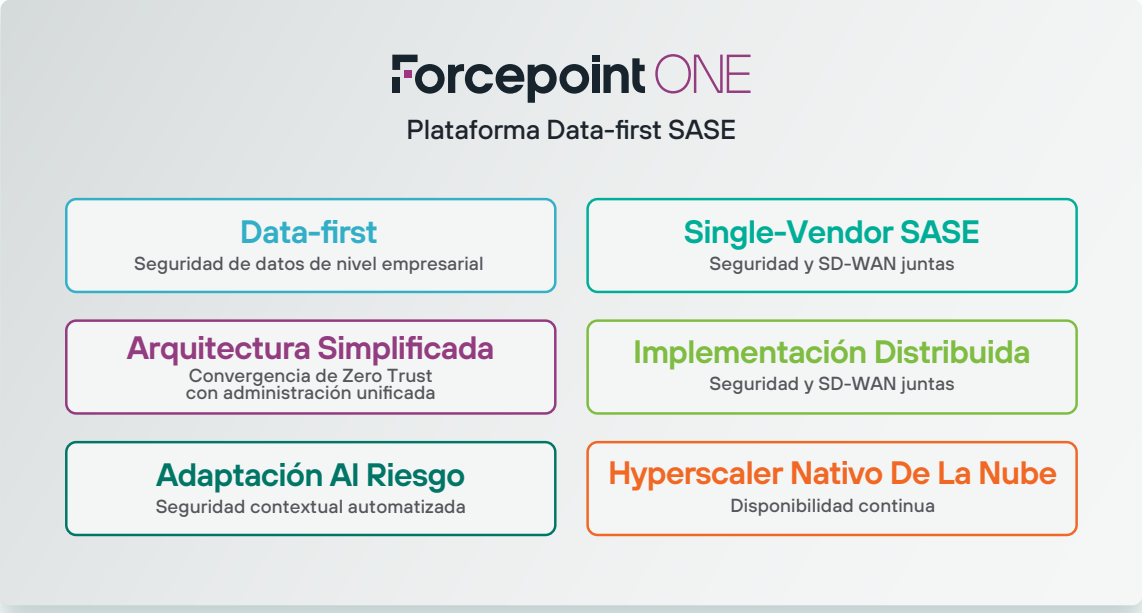
Forcepoint ONE se está utilizando en todo el mundo para:

- → **Prevenir la pérdida de datos de las aplicaciones en la nube** (especialmente en Microsoft 365 y Google Workspace) y en la web
- → **Resguardar el acceso sin agentes a las aplicaciones en la nube y privadas por el uso de dispositivos propios de los empleados (BYOD)**
- → **Implementar el acceso Zero Trust** a la nube, la web y las aplicaciones privadas de manera segura desde los usuarios remotos y en las oficinas
- → **Controlar Shadow IT, incluido ChatGPT** y otras IA generativas, habilitando el uso sin el riesgo de que se filtren datos confidenciales
- → **Simplificar las fusiones y las adquisiciones**
- → **Reemplazar las VPN** para acceder a las aplicaciones internas
- → **Acelerar el desempeño de las aplicaciones en la nube** en las sucursales
- → **Permitir que cualquier sitio web o documento descargado** se utilice de manera segura, incluso si está contaminado
- → **Detectar configuraciones erróneas** y violaciones de los marcos de cumplimiento



Seis maneras en que Forcepoint ONE SASE es diferente

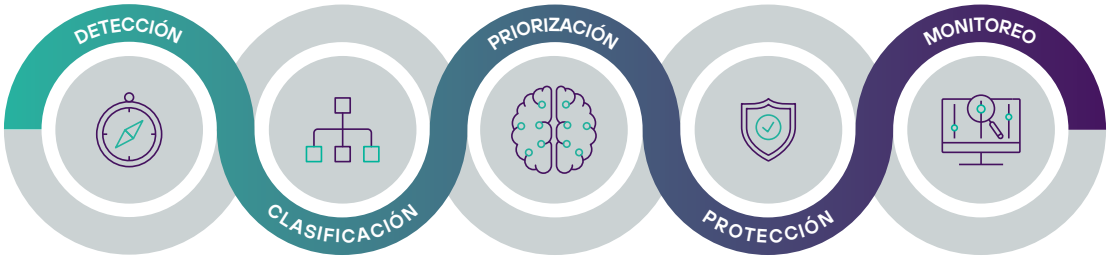
Forcepoint ONE reúne seis elementos clave para ofrecer la seguridad y las redes que las organizaciones necesitan para tener éxito en el mundo actual, que cambia rápidamente:



Data-first: seguridad de datos empresariales en todas partes

Forcepoint tiene un punto de vista diferente al de la mayoría de los proveedores. Creemos que la ciberseguridad moderna se trata fundamentalmente de permitir que los datos confidenciales en todas partes se utilicen de manera segura en cualquier lugar. Es por eso que construimos algunas de las tecnologías de seguridad de datos más sólidas de la industria en el núcleo de nuestra plataforma Forcepoint ONE y nuestras puertas de enlace de SSE: CASB (basado en API, proxy de reenvío, proxy inverso), SWG (basado en nube y en dispositivo final) y ZTNA (basado en agentes y sin agentes).

Miles de organizaciones de todo el mundo confían en la tecnología de prevención de pérdida de datos (Data Loss Prevention, DLP) de Forcepoint, que ha sido denominada "líder" por importantes analistas de la industria. Es parte de un marco basado en Zero Trust llamado ciclo de vida de la seguridad de datos, que implementa las mejores prácticas para proteger los datos de manera eficiente y efectiva contra el acceso no autorizado, el robo o la pérdida accidental.



Ciclo de vida de la seguridad de datos

Automatizamos cada paso en este ciclo de vida. Con nuestras soluciones, los clientes pueden identificar rápidamente dónde residen los datos confidenciales, clasificar los datos estructurados y no estructurados (en la nube y en las instalaciones), determinar dónde enfocar sus esfuerzos, detener la pérdida de datos en todos los canales clave de filtración (aplicaciones de dispositivo final, correo electrónico, web, red y nube) y monitorear continuamente lo que los usuarios están haciendo con los datos confidenciales.

Este enfoque va mucho más allá de la coincidencia de patrones básicos que a menudo se aplica para la seguridad de datos en otras soluciones SASE. Al clasificar los datos y organizarlos en diferentes grupos, se pueden escribir y aplicar políticas de seguridad de datos que manejen automáticamente nuevas instancias y tipos de datos confidenciales. Para simplificar la definición de políticas, especialmente para cumplir con los mandatos específicos de una región o una industria, incorporamos una de las bibliotecas de plantillas de políticas más completas de la industria. Además, nuestros gateways de Forcepoint ONE SSE para controlar el acceso a las aplicaciones en la web (SWG), en la nube (CASB) y privadas (ZTNA) permiten que las políticas de DLP se especifiquen en un solo lugar y se apliquen de manera consistente en diferentes canales.

Esta simplicidad no se limita a un conjunto de aplicaciones predefinidas. Forcepoint ONE puede aplicar controles de seguridad de datos granulares a cualquier aplicación basada en la web que utilice el mismo mecanismo de scripting de la lógica SASE programable en el campo (Field Programmable SASE Logic, FPSL), que Forcepoint mismo utiliza en sus propias políticas. Los administradores pueden desarrollar fácilmente reglas que activen atributos en una solicitud HTTP (dominio, método, URI, cadena de consulta o cookie) para detectar interacciones de usuarios, registrar las páginas que se están utilizando y, opcionalmente, bloquearlos. Por ejemplo, Forcepoint ONE puede fácilmente:

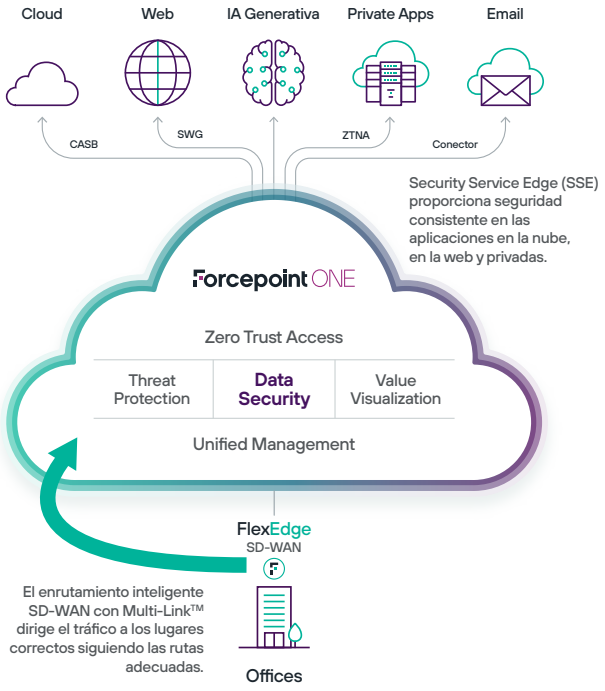
- → Bloquear los inicios de sesión en aplicaciones SaaS corporativas con una dirección de correo electrónico personal
- → Registrar cada archivo cargado en cuentas personales de Google Drive para usuarios en un grupo de usuarios de riesgo
- → Bloquear los "Me gusta" en Facebook
- → Solo permitir a los miembros del grupo de marketing publicar en LinkedIn.
- → Bloquear contenido confidencial en una publicación de Twitter

Y, como las personas en la fuerza laboral actual a menudo dependen de teléfonos, tabletas y endpoints, como estaciones de trabajo Linux o Chromebooks, **Forcepoint ONE posibilita la utilización segura de las aplicaciones web privadas internas y en la nube desde dispositivos propios de los empleados y otros dispositivos sin agente para que la gente mantenga su productividad sin poner en riesgo los datos.**

Single-vendor: seguridad y SD-WAN juntos

Forcepoint es pionero en la integración de tecnologías de seguridad y redes en un solo producto, administrado desde una sola consola. Las soluciones Forcepoint Secure SD-WAN estuvieron entre las primeras en combinar el enrutamiento SD-WAN con tecnologías de firewall de alta seguridad y prevención de intrusiones.

Nuestra combinación patentada de múltiples enlaces y múltiples ISP se utiliza en todo el mundo para transformar redes de área amplia heredadas construidas sobre circuitos privados como MPLS en SD-WAN modernas basadas en banda ancha. Forcepoint Secure SD-WAN, diseñado específicamente para una escalabilidad masiva, permite que se administren políticas para hasta 6000 sitios desde una sola consola.



Con Secure SD-WAN, las organizaciones distribuidas conectan sus sucursales y sitios remotos directamente a Internet para proporcionar el máximo desempeño para acceder a aplicaciones modernas en la nube. **Las capacidades avanzadas como dirección de aplicaciones, monitoreo de estado de aplicaciones y actualización sin intervención permiten que las organizaciones de TI suministren de manera proactiva un desempeño y un tiempo de actividad consistentes para mantener la productividad del personal y los costos de infraestructura bajos.**

En consecuencia, nuestra SD-WAN proporciona una base para implementar una arquitectura SASE convergente. Las organizaciones pueden enrutar automáticamente el tráfico para varias aplicaciones a nuestras puertas de acceso de Forcepoint ONE Security Service Edge (SSE) que se ejecutan en la nube. Esto no solo facilita la protección de datos de los empleados y las empresas, sino que también permite que se definan y apliquen políticas de seguridad para dispositivos no administrados, como computadoras portátiles de visitantes en Wi-Fi, teléfonos y tabletas BYOD, incluso impresoras y dispositivos de Internet de las cosas (IoT).

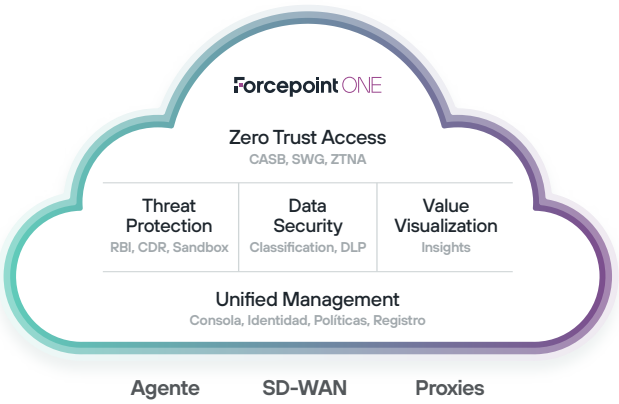
Arquitectura simplificada: administración convergente y unificada

La misión de Forcepoint es "la Seguridad Simplificada". Los días en que las personas se enorgullecían de la complejidad de la infraestructura de seguridad han terminado. Con entornos en constante cambio, los equipos de TI a menudo se ven obligados a hacer más con menos. **Reducir la complejidad ya no es solo una buena idea: es la única manera de mantener la productividad de las empresas, reducir costos e impedir que el riesgo aumente sin control.**

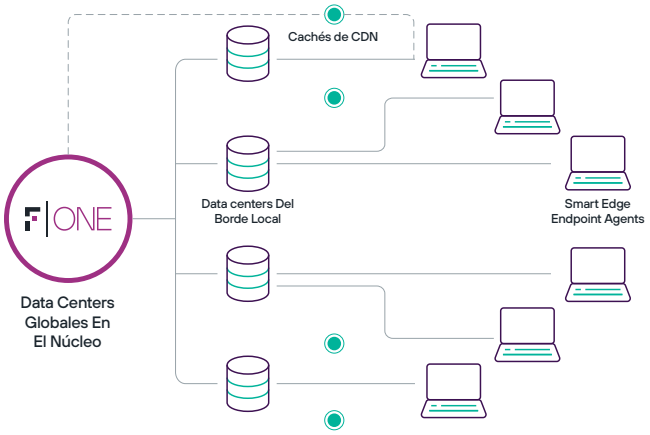
Para ayudar a los clientes a simplificar su propia arquitectura empresarial, Forcepoint ONE en sí mismo está diseñado para evitar brechas y redundancias en tecnologías que solían estar fragmentadas. Gateways para asegurar el acceso a aplicaciones en la nube, la web y aplicaciones privadas internas comparten código y utilizan un conjunto común de microservicios de seguridad subyacentes para mantener las amenazas afuera y los datos confidenciales adentro, y ayudar a los líderes empresariales a comprender mejor el valor de la conectividad y la seguridad que están brindando a la organización

Los elementos clave de la plataforma Forcepoint ONE incluyen:

- → Gateways basados en Zero Trust que controlan cómo los empleados y otros usuarios utilizan las aplicaciones en la nube (CASB), en la web (SWG) y privadas (ZTNA)
- → Servicios de protección contra amenazas avanzadas, como el aislamiento de navegadores remotos (remote browser isolation), sanitización de documentos automatizada (lo que se conoce como desarmado y reconstrucción), antivirus y entorno seguro (sandboxing) para malware.
- → Servicios de seguridad de datos de vanguardia que impiden el robo de datos confidenciales de manera consistente en cada canal (DLP).
- → Asegure el acceso sin agentes desde dispositivos BYOD y no administrados a las aplicaciones en la nube (CASB) y en la web privada (ZTNA).



- → Paneles de control interactivos que presentan visualmente los indicadores de desempeño clave y el valor económico de los servicios que Forcepoint ONE está brindando.
- → Una sola consola para establecer políticas para controlar cómo se accede a los recursos empresariales y se los utiliza.
- → PIntegración patentada de proveedores de identidad SAML para trabajar con, o complementar, los sistemas IdP existentes.



Forcepoint ONE utiliza una arquitectura de niveles múltiples. Los data centers globales realizan las funciones principales de la plataforma, como inspeccionar datos en reposo en SaaS e IaaS, verificar SaaS e IaaS para detectar configuraciones erróneas de seguridad y analizar datos de dispositivos finales.

Los data centers locales ofrecen políticas y actúan como cachés de la red de suministro de contenido (Content Delivery Network, CDN) para información solicitada con frecuencia, como la categorización de la inteligencia sobre amenazas. Estos data centers se escalan automáticamente para manejar cargas transitorias, por ejemplo cuando convergen personas en una conferencia.

Las capacidades adicionales que complementan los servicios de acceso que se proporcionan desde la nube son suministradas por un software de dispositivos finales llamado SmartEdge, que se ejecuta en computadoras portátiles administradas y otros dispositivos. SmartEdge conecta automáticamente a los trabajadores remotos con los servicios de seguridad adecuados y garantiza que se apliquen las políticas correctas. Forcepoint actualmente está integrando esta tecnología con la telemetría de nuestros otros controles de dispositivos finales y de red, para permitir que las organizaciones de TI implementen y administren una sola aplicación de dispositivos finales que proporcione todas las funciones de conectividad y seguridad de Forcepoint ONE.

Basado en los principios de Zero Trust

Las políticas para los servicios de acceso de Forcepoint ONE se basan en un enfoque de Zero Trust que especifica la identidad, la aplicación, los dispositivos y la ubicación para los que se debe aplicar cada acción dada:

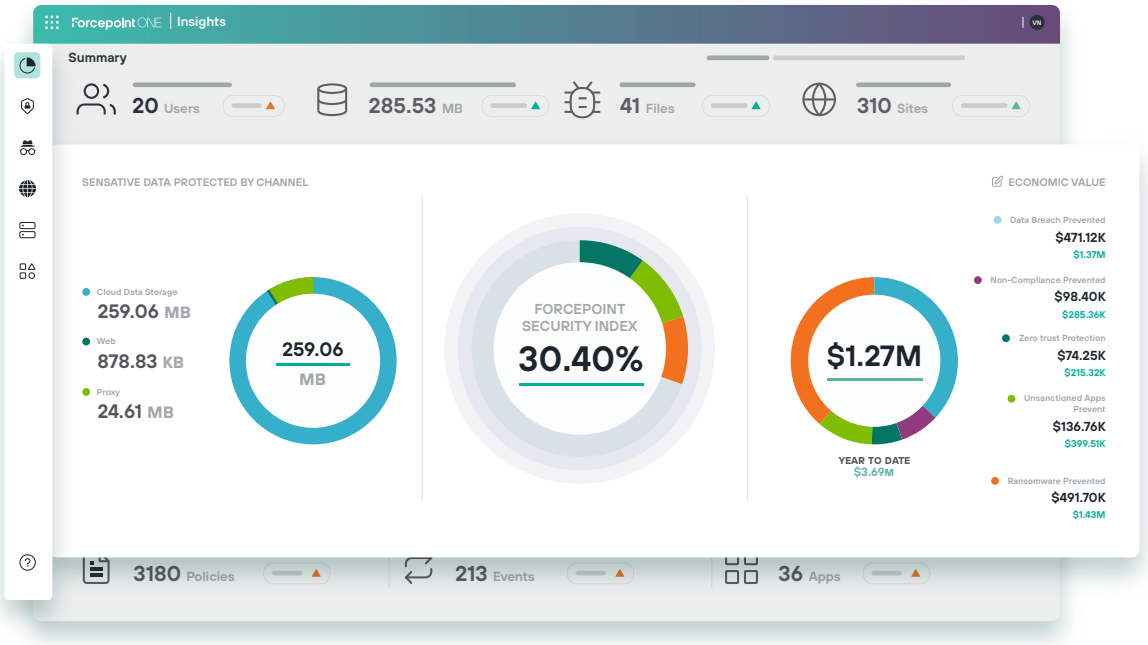
Proxy

ID	Groups	Access Method	Device	Location	Action
7073	Admins	Any	Any	Anonymizers IaaS Provider IPs	Deny
69739	Any	SSO Auth	Managed Win - AV On	Corp Network and VPN	Direct App Access
28475	Any	SSO Auth	Any	Any	Secure App Access DLP Download DLP Upload
188394	Any	Any	Any	NRD-HQ	Secure App Access DLP Download DLP Upload

Las políticas de seguridad de datos y prevención de amenazas se pueden especificar para todas las cargas y descargas, y luego, se pueden combinar con la notificación y el asesoramiento de los usuarios para garantizar que los usuarios y los datos estén protegidos.

Conectar los puntos en el valor económico de SASE

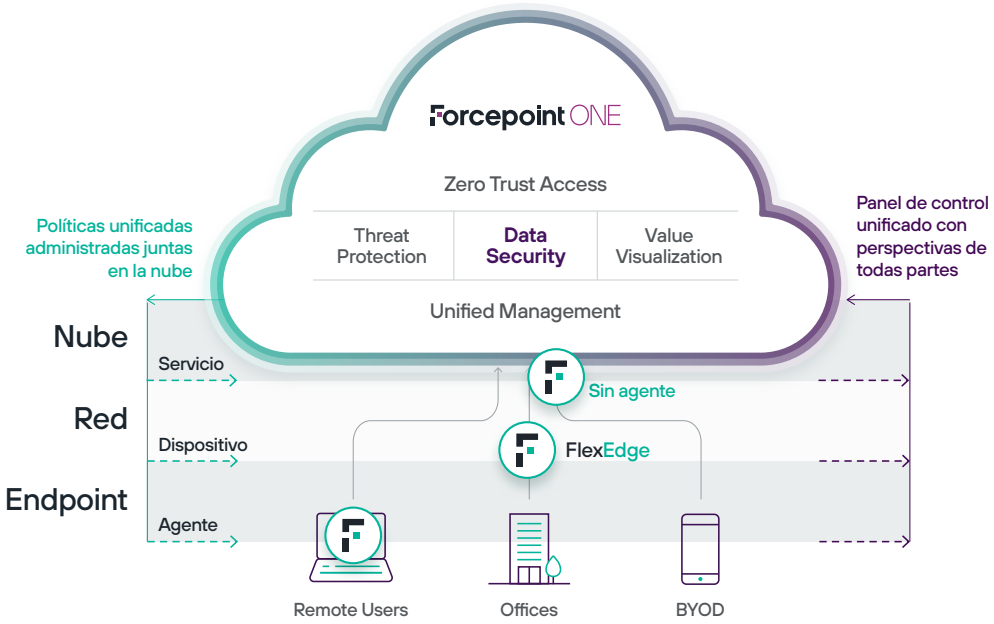
Forcepoint ONE ofrece a los administradores visibilidad completa e informes unificados en todos sus dispositivos administrados y no administrados. Nuestros paneles de control de Conocimientos proporcionan una visión consolidada de lo que está sucediendo en diferentes servicios de seguridad, que destaca el valor empresarial que Forcepoint está brindando.



Implementación distribuida de múltiples niveles en la nube, en el borde de la red y en el endpoint

La nube ha revolucionado la manera en que se administra y se proporciona la seguridad, mientras que Internet ha suplantado a la red corporativa como la columna vertebral de las operaciones de TI. Juntos, permiten que se pueda acceder fácilmente a un plano de control consolidado desde cualquier lugar. Pero la nube es el comienzo, no el final, de un enfoque moderno con respecto a la seguridad.

Si bien todas las soluciones de SASE proporcionan la aplicación de políticas basadas en la nube, vamos más allá. **Forcepoint ONE implementa las políticas de redes y seguridad donde sea necesario: cerca del usuario en el dispositivo final, cerca de la infraestructura en la red, así como cerca de las aplicaciones en la nube.**



Este enfoque distribuido optimiza el desempeño de las aplicaciones, reduce el uso del ancho de banda de la red y elimina los problemas que pueden surgir cuando el tráfico se redirecciona a través de cuellos de botella, ya sea en centros de datos privados, antiguos, o en servicios en la nube para múltiples clientes. Forcepoint ONE garantiza que se apliquen las mismas políticas en todas partes, y que se puedan utilizar los mismos paneles de control para monitorear el funcionamiento de esas políticas.

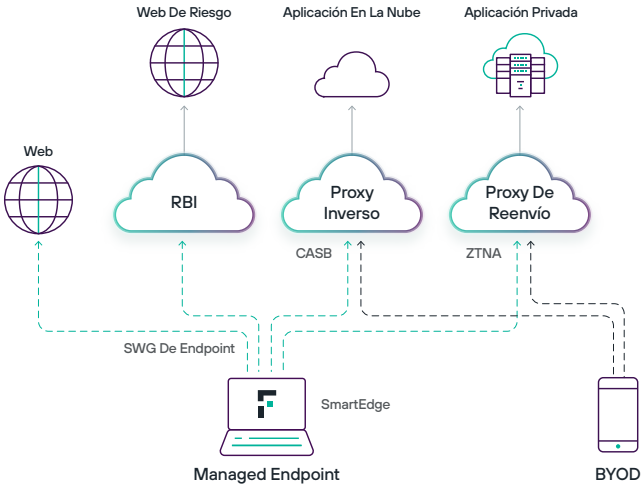
Vía de acceso a la nube basada en endpoints optimiza el desempeño de las aplicaciones y la experiencia del usuario

Por ejemplo, las arquitecturas de SWG tradicionales, que fuerzan todo el tráfico web a través de un proxy en la nube, aunque son sencillas de implementar, a menudo presentan dificultades en el mundo real:

- **Latencia :** Es el procesamiento y los saltos de red adicionales que se introducen, reduciendo las velocidades de navegación hasta a la mitad. Algunas aplicaciones en la nube (incluidas algunos de los paquetes de colaboración de oficina más populares) son sensibles a estos retrasos y pueden no funcionar correctamente.
- **Utilización del ancho de banda:** Las organizaciones que equipan sitios con múltiples enlaces de Internet podrían no estar en condiciones de aprovecharlos al máximo para optimizar el costo y el desempeño de las aplicaciones en la nube (por ejemplo, al enviar videoconferencias de alta prioridad a través de enlaces más rápidos mientras que el tráfico de prioridad baja va a través de los menos costosos).
- **Conocimiento de la ubicación:** Las aplicaciones en la nube que utilizan la dirección de Internet del endpoint para seleccionar contenido o funciones específicas (como en qué idioma presentar una página) podrían no funcionar correctamente, lo que generaría confusión en los usuarios y cargas para el servicio de soporte.
- **Cumplimiento:** En algunas situaciones, el envío de datos confidenciales desde un dispositivo final controlado hacia Internet puede activar procedimientos de filtrado (incluso si va directamente al proxy).

Microsoft recomienda específicamente que los usuarios de Microsoft 365 eviten el uso de proxies, lo que obliga a las organizaciones a elegir entre la productividad y la seguridad. Forcepoint ONE aborda estos problemas permitiendo que se apliquen políticas de seguridad web (incluidas las que son para la prevención contra la pérdida de datos) en dispositivos finales que ejecutan nuestro software SmartEdge.

SmartEdge proporciona una "vía de acceso a la nube" que enruta automáticamente el tráfico al servicio o a la aplicación adecuados en función de aquello a lo cual se está accediendo. Complementa los proxies en la nube que ofrece Forcepoint ONE para proteger dispositivos sin agentes como BYOD e IoT.



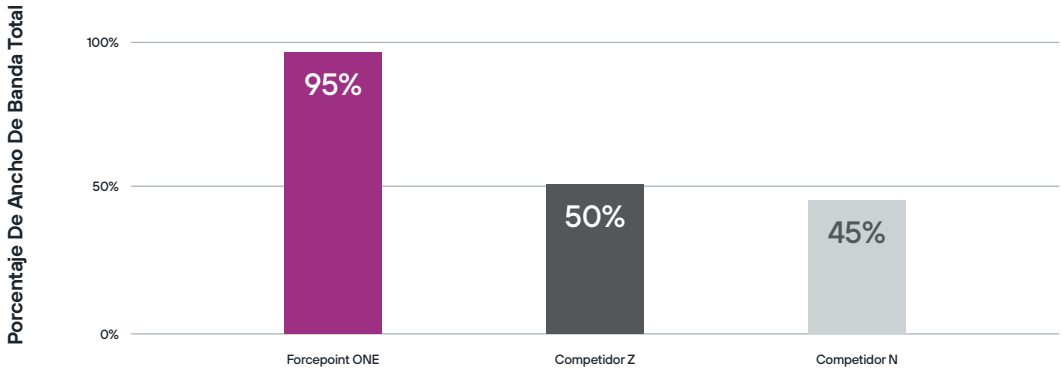
El software de endpoints SmartEdge dirige el tráfico a los lugares correctos

SmartEdge es particularmente valioso para los usuarios remotos, ya que proporciona la experiencia de usuario más natural, productiva y segura. Funciona con nuestra plataforma en la nube para garantizar que las políticas se apliquen correctamente en todas las situaciones, lo que incluye:

- → **Acceso a nueva URL:** Cuando un usuario intenta acceder a una URL por primera vez, SmartEdge SWG consulta a la caché de CDN de Forcepoint ONE más cercana para recuperar la política de navegación web adecuada para esa combinación de grupo de usuarios, tipo de dispositivo, categoría de URL, ubicación y reputación de la URL. Si el resultado de la consulta no está en el nodo de caché, la solicitud se reenvía al data center de borda local de Forcepoint ONE más cercano. Suponiendo que el sitio web no está bloqueado, todo el tráfico web se intercambia directamente entre el dispositivo y el sitio web, evitando así que hagan un giro (hairpinning).
- → **Aislamiento y protección de sitios web de riesgo de SWG:** Los sitios web de riesgo se pueden especificar en Forcepoint ONE sobre la base de su Categorización de sitio URL o sus Puntuaciones de reputación de URL. Cuando un usuario intenta acceder a un sitio web de riesgo, SWG aísla el acceso y lo redirecciona a través del aislamiento de navegador remoto (Remote Browser Isolation, RBI) de Forcepoint. RBI reduce la superficie de ataque del endpoint ocultando la dirección IP y renderizando el sitio web de manera remota en un contenedor temporal que es específico para la sesión del usuario.
- → **Movimiento de archivos desde/hacia una aplicación web segura, no sancionada:** Cuando un usuario intente subir un archivo o descargar un archivo desde una aplicación web no sancionada con una política de navegación web que aplica el acceso seguro, Forcepoint ONE bloqueará los intentos de subir o descargar archivos sobre la base de las reglas de la política para DLP o protección contra malware en la política de navegación web.

El enfoque de aplicación distribuida en Forcepoint ONE ofrece hasta el doble de desempeño de navegación que los sistemas solo en la nube con protección completa contra las amenazas transmitidas por la web o la carga inapropiada de datos confidenciales.

Rendimiento De SWG Como Porcentaje Del Ancho De Banda Total



Risk-adaptive protection para la seguridad contextual

Ahora que las personas están trabajando desde cualquier lugar con datos que residen en todas partes, definir políticas individuales para cada combinación relevante de usuarios, dispositivos, ubicaciones, aplicaciones y otros atributos es un enfoque propenso a errores y no escalable. Peor aún, un enfoque tan estático no coincide con la manera en que las organizaciones operan en el mundo real: Ellas brindan a las personas que muestran tener buen criterio la capacidad de utilizar datos y recursos confidenciales con una interferencia mínima, pero aplican controles más estrictos si se cometen errores o se toman malas decisiones.

Forcepoint es pionero en esa protección "que se adapta al riesgo", que elige dinámicamente qué políticas aplicar en función de las acciones de los usuarios, si sus dispositivos están actualizados con las pautas corporativas, la confidencialidad de los datos que están tratando de utilizar y otros factores.

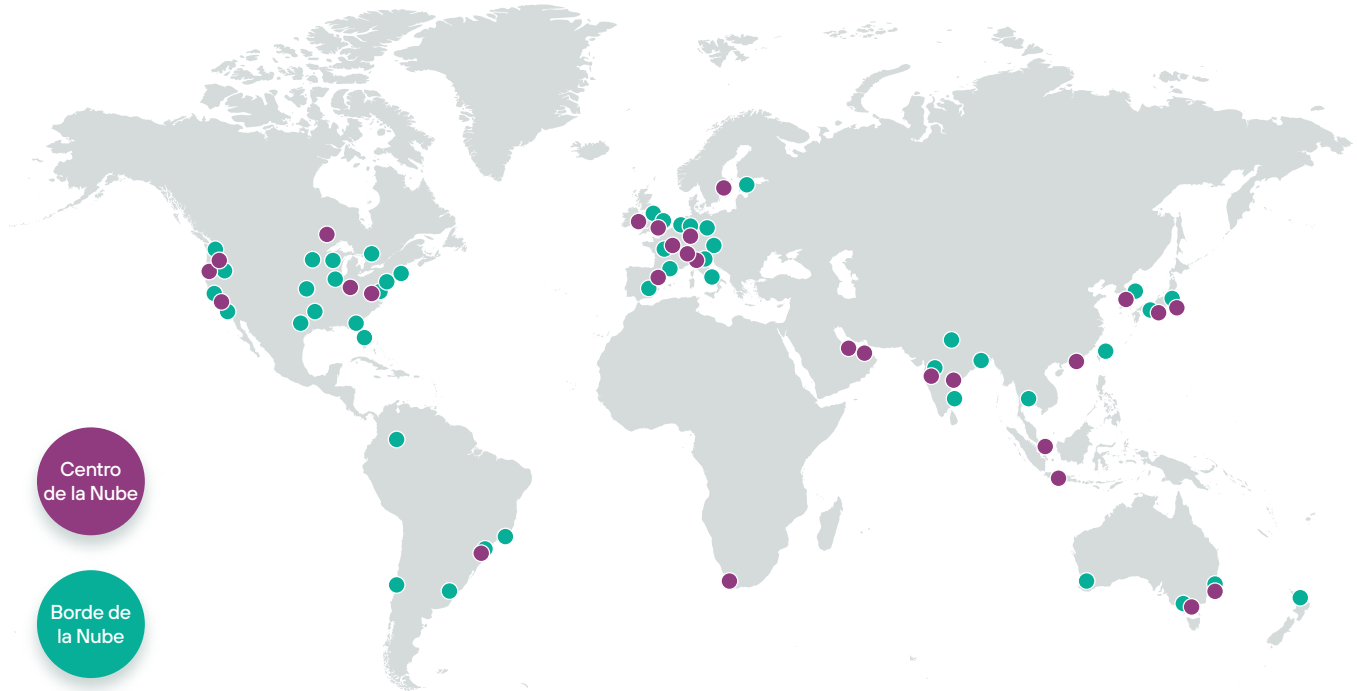
Este enfoque automatiza y personaliza la seguridad, brindando a las personas la libertad de utilizar datos confidenciales de maneras innovadoras, y enfocándose a la vez en la aplicación en las situaciones en las cuales más se la necesita. Forcepoint incorpora esta tecnología en nuestras soluciones DLP enterprise, que se pueden utilizar para proteger datos en una amplia gama de canales, como en dispositivos finales, en redes y en el correo electrónico, así como en aplicaciones en la nube y en la web que están protegidas con los servicios SSE de Forcepoint ONE.
El resultado es una mejor productividad de los usuarios, costos operativos más bajos (simplificación de la definición de políticas y reducción de las llamadas urgentes al servicio de soporte por parte de usuarios que están siendo bloqueados) y menos riesgo.

Hyperscaler nativo en la nube, disponibilidad continua

Los servicios en la nube normalmente se implementan de varias maneras:

- → **Data centers de propiedad exclusiva:** En las primeras épocas de la web, los proveedores que querían ofrecer software como servicio tenían que desarrollar y mantener sus propios data centers. Si bien esto proporciona el mayor nivel de control, e inicialmente a menudo era la única opción, ahora el costo que requiere lo hace muy poco común.
- → **Centros de colocation:** Actualmente, cuando los proveedores hablan de "sus" centros de datos, suelen referirse a centros de colocation que son propiedad de otros y operados por otros. Esto conlleva menos esfuerzo que armar un data center de propiedad exclusiva, pero de todos modos requiere un nivel significativo de complejidad y costo de operación.
- → **Nubes públicas de hyperscaler:** Cuando las organizaciones van a poner aplicaciones en la nube, incrementalmente, la manera más rápida es usar entornos de nube pública, como Amazon (AWS), Microsoft (Azure), Google (GCP), Oracle (OCI) y otros. Estos sistemas, conocidos como "hyperscalerss", porque se enfocan en proporcionar entornos de escalamiento, también ofrecen una variedad de servicios que pueden usar los proveedores de aplicaciones para simplificar su propio desarrollo. Además, los hyperscalers a menudo ya están disponibles en la mayoría de las regiones donde los proveedores desean brindar servicios y están diseñados con algunos de los niveles más altos de seguridad física.

Forcepoint ONE fue diseñado desde el inicio para ejecutarse en hyperscalers. Basado en AWS, tiene presencia regional en todos los continentes excepto en la Antártida:



Su escalabilidad elástica permite que los servicios se escalen o se reduzcan de manera dinámica. Por ejemplo, si una gran cantidad de usuarios se reúnen en una sola ubicación, Forcepoint ONE puede generar capacidad adicional sin requerir la implementación de hardware físico. Además, con tantas aplicaciones que ahora están alojadas en hyperscalers (50 % de los diez mil sitios web principales, 40 % de los cien mil sitios web principales, 23 % del millón de sitios web principales están en AWS, tener a Forcepoint ONE con base allí también mantiene la seguridad cerca de las aplicaciones y sus datos.

La plataforma Forcepoint ONE está diseñada para proporcionar disponibilidad continua sin necesidad de tiempo de inactividad para mantenimiento planificado. **Utiliza una estrategia de implementación "azul y verde" que permite que las actualizaciones y las nuevas capacidades se publiquen en vivo sin que el servicio esté fuera de línea.**

El resultado: mejor productividad y menos llamadas frenéticas a los servicios de ayuda.

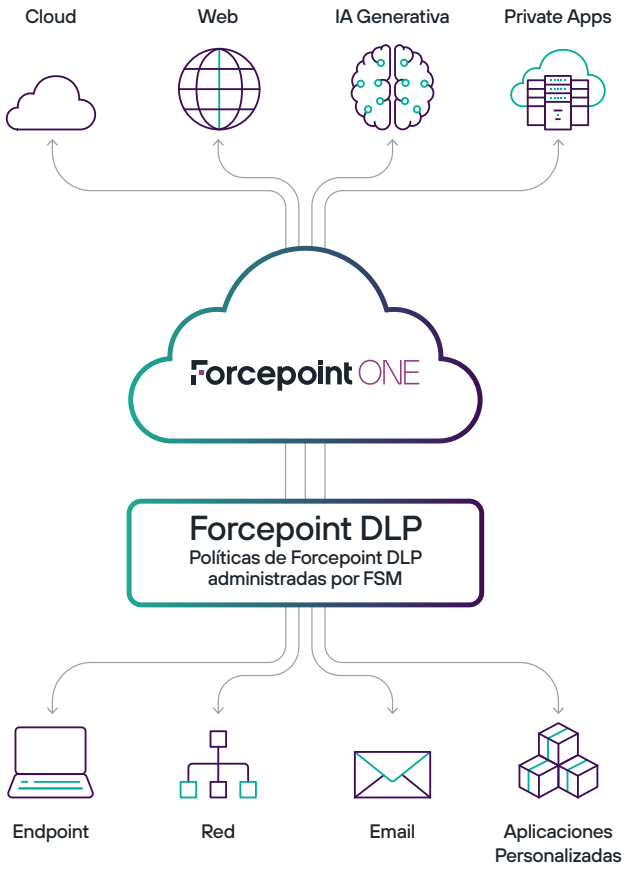
Ofrecemos seguridad de datos en todas partes, incluso para las IA generativas

Las soluciones de Forcepoint trabajan juntas para permitir que las mismas políticas de seguridad de datos se apliquen sin problemas desde el dispositivo final hasta la nube, y en todas partes. Esto permite que las organizaciones administren la seguridad de datos desde una sola consola, con visibilidad y control consistentes. Va más allá de la coincidencia de patrones básicos de la mayoría de las puertas de enlace de SSE, proporcionando seguridad completa de nivel empresarial, complementada con un producto pionero de Forcepoint, risk-adaptive protection, y el monitoreo continúo basado en Zero Trust.

Con el rápido surgimiento de innovaciones como ChatGPT y otras, una seguridad de datos sólida es más importante que nunca en este momento. Las IA generativas son la forma más reciente de "Shadow IT": Ofrecen enormes ganancias en productividad, pero potencialmente pueden poner en gran riesgo los datos confidenciales.

Forcepoint le permite aprovechar las IA generativas manteniendo al mismo tiempo el control de quién puede usarlas y cómo:

- → Limite el acceso a personas o grupos específicos que estén autorizados para probar o usar IA.
- → Controle las cargas de archivos, así como el cortado y pegado.
- → Inspeccione y proteja los datos confidenciales contra las filtraciones.



Forcepoint ONE: Data-first SASE para el mundo moderno

SASE ha pasado rápidamente de ser una arquitectura académica a ser la manera más común en que las organizaciones planean conectarse y proteger a sus fuerzas laborales modernas. Forcepoint ONE reúne más de una década de experiencia en cada uno de los servicios de seguridad enfocados en datos, servicios de nube y redes directos a Internet, proporcionando una plataforma integral para brindar a los usuarios de manera segura acceso rápido y eficiente a recursos empresariales en cada etapa del camino de una organización hacia la nube.

Forcepoint

forcepoint.com/es/contact

Acerca de Forcepoint

Forcepoint simplifica la seguridad para empresas y gobiernos de todo el mundo. La plataforma todo en uno y realmente nativa en la nube, de Forcepoint, facilita la adopción de un enfoque de Zero Trust y evita el robo o la pérdida de datos confidenciales y propiedad intelectual sin importar desde donde trabajen las personas. Forcepoint, con sede en Austin, Texas, crea entornos seguros y confiables para los clientes y sus empleados en más de 150 países. Interactúe con Forcepoint en www.forcepoint.com/es, Twitter y LinkedIn.