Forcepoint

Resumen de la solución

Agente de seguridad de acceso a la nube

Proteja los datos en cualquier aplicación en la nube y acceda desde cualquier dispositivo

Desafío

- Cuide y controle el acceso a aplicaciones administradas desde dispositivos personales (BYOD)
- Controle la carga y descarga de datos confidenciales en cualquier aplicación de SaaS administrada
- Detenga el malware oculto en archivos de datos empresariales
- Detección de Shadow IT

Solución

- Seguridad de aplicaciones en la nube con protección contra amenazas avanzadas y DLP integrada
- Acceso granular de Zero Trust y controles de datos basados en usuario, dispositivo o ubicación
- Plataforma AWS de hiperescalamiento que maximiza el tiempo productivo y minimiza la latencia
- Aplicación de DLP en dispositivos administrados y no administrados

Resultado

- Aumento de la productividad, lo que permite que las personas utilicen la información 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
- Optimización del cumplimiento con procesos demostrables para controlar la información

Los nuevos modelos de fuerza laboral de hoy exigen que los usuarios en cualquier lugar tengan acceso rápido pero controlado a los datos empresariales en todas partes. Quiere decir que las personas necesitan acceso a datos en aplicaciones en la nube como Microsoft 365, Google Workspace, Slack, Jira y Salesforce desde cualquier tipo de dispositivo o ubicación. Con más de 250 aplicaciones SaaS para una empresa promedio, la visibilidad y el control pueden fácilmente volverse inmanejables.

Proteja el acceso a las aplicaciones empresariales desde dispositivos personales (BYOD) y no administrados

Forcepoint simplifica la seguridad en la nube. El servicio Cloud Access Security Broker (CASB) de Forcepoint ONE implementa acceso de Zero Trust que permite que las aplicaciones en la nube esenciales para la empresa puedan utilizarse de manera segura desde los dispositivos personales de empleados (BYOD) y desde dispositivos no administrados de socios y contratistas.

Controle la carga y descarga de datos confidenciales en cualquier aplicación de SaaS administrada

Ofrecemos un conjunto de políticas de seguridad para controlar los datos confidenciales, con desempeño líder en la industria, sin importar dónde y cómo los empleados y los contratistas se conecten a internet. Gestionar el acceso a estas aplicaciones desde dispositivos móviles facilita la adopción y la productividad, mientras que disponer de diferentes políticas basadas en la identidad y la ubicación proporciona controles granulares de Zero Trust. El escaneo en línea en busca de datos confidenciales y malware mantiene seguros los datos en todas las aplicaciones SaaS. Obtendrá más seguridad sobre cómo se comparten los datos confidenciales en las aplicaciones de la empresa y, con la prevención contra la pérdida de datos (DLP) integrada, no necesitará productos puntuales para detener las filtraciones de datos.

Detenga el malware oculto en archivos de datos empresariales

Forcepoint ONE CASB puede detectar y bloquear malware en datos en movimiento entre usuarios y la aplicación de SaaS mediante el uso de los motores de análisis de malware Bitdefender y Trellix. También puede detectar malware en archivos en soluciones de almacenamiento de IaaS y SaaS populares y colocar esos archivos en cuarentena.

Detección de Shadow IT

Forcepoint ONE CASB revela la Shadow IT y genera una calificación de riesgo para las aplicaciones no autorizadas mediante el análisis de múltiples atributos. Esto permite a los equipos de TI tener un conocimiento más profundo del uso de SaaS dentro de su organización y aplicar los controles de seguridad necesarios. El CASB detecta aplicaciones SaaS no gestionadas que se utilizan mediante registros de red o con telemetría de Forcepoint ONE Secure Web Gateway para permitir que se apliquen políticas de seguridad consistentes a aplicaciones SaaS sancionadas y no sancionadas, de modo que los datos empresariales permanezcan seguros en cualquier lugar donde se utilicen.

El CASB de Forcepoint ONE maximiza el tiempo productivo, la disponibilidad y la productividad

Nuestro CASB hace parte de Forcepoint ONE, nuestra plataforma en la nube basada en hyperscaler con más de 300 puntos de presencia (PoP), accesibilidad global y tiempo de actividad comprobado del 99,99 % para proteger las aplicaciones en la nube sin problemas y preservar la productividad del usuario. Otras soluciones desvían el tráfico de red hacia y desde las aplicaciones en la nube a centros de datos privados en lugar de ubicaciones más cercanas a los usuarios y las aplicaciones a las que acceden. Esto da como resultado un rendimiento deficiente, haciendo que las aplicaciones sensibles a la latencia, como Slack, fallen y que los empleados terminen buscando atajos de alto riesgo.

Simplificación de la seguridad en la nube 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 los datos para usuarios de dispositivos administrados y no administrados (como las computadoras de BYOD, empleados terceros o socios).

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

Carlos inicia sesión en su cuenta de Salesforce desde su computadora portátil de la empresa.	El CASB de Forcepoint ONE administra las conexiones a las aplicaciones empresariales, permitiendo a los usuarios iniciar sesión con fluidez y seguridad.
Carlos navega directamente a salesforce.com o a través de un portal corporativo de la aplicación.	Salesforce redirige la sesión al CASB (a través de SAML), que analiza si el dispositivo es administrado, su ubicación y su postura respecto de la seguridad. Basándose en políticas de seguridad predefinidas, el CASB confirma la identidad de Juan mediante aplicaciones de autenticación multifactor.
Se le da a Carlos acceso a aplicaciones administradas.	Las políticas de administración también controlan el acceso directo a la aplicación, el acceso controlado o la denegación del acceso. Esto ocurre en milisegundos sin afectar la productividad del empleado. Todo el tráfico desde el dispositivo de Juan y la aplicación pasa a través del CASB (utilizando un proxy inverso o directo).
Carlos decide descargar un pronóstico de ingresos de Salesforce.	El CASB analiza todo archivo descargado desde la aplicación en busca de malware y datos confidenciales. Según el resultado y la política, puede bloquear archivos de malware y bloquear, dar seguimiento o cifrar datos confidenciales. Si una política restringe la descarga de datos confidenciales solo a dispositivos no administrados, la descarga se permite dado que Juan está utilizando una computadora de la empresa.
Juan intenta transferir datos confidenciales o un archivo contaminado con malware a través de Slack.	El CASB también puede verificar los archivos que se cargan a aplicaciones en la nube. El CASB puede bloquear la subida automáticamente. Incluso puede bloquear la carga de archivos a aplicaciones no autorizadas mediante el agente unificado en el dispositivo.

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

Además de CASB, la plataforma todo en uno Forcepoint ONE protege el acceso a información empresarial en cualquier sitio web y aplicación privada:

- **Web:** El Secure Web Gateway (SWG) monitorea y controla las interacciones con cualquier sitio web basándose en el riesgo y la categoría, bloqueando la descarga de malware o las cargas de datos confidenciales a cuentas de correo electrónico e intercambio de archivos personales. Nuestro SWG en el dispositivo aplica políticas de uso aceptables en dispositivos administrados en cualquier lugar.
- **Aplicaciones privadas:** El Zero Trust Network Access (ZTNA) protege y simplifica el acceso a aplicaciones privadas sin la complicación o el riesgo asociado con las VPN.
- **Capacidades adicionales** , como el escaneo de proveedores en la nube en busca de configuraciones riesgosas Cloud Security Posture Management (CSPM) y SaaS Security Posture Management (SSPM), según sea necesario.

Para 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