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
- Detecte y controle la shadow IT

Solución

- Seguridad de aplicaciones SaaS con DLP integrado y protección contra amenazas avanzadas
- 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 la actualidad exigen que los usuarios en cualquier lugar tengan un acceso rápido pero controlado a los datos empresariales en todas partes. Esto significa que las personas necesitan acceso a los datos en aplicaciones de SaaS, como Microsoft 365, Google Workspace, Slack, Jira y Salesforce desde cualquier tipo de dispositivo o ubicación. Con más que 250 aplicaciones de SaaS para la empresa promedio, la visibilidad y el control pueden volverse fácilmente inmanejables.

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

Forcepoint simplifica la seguridad en la nube. El servicio de CASB de Forcepoint ONE implementa el acceso Zero Trust, el cual permite que las aplicaciones de SaaS críticas para el negocio se utilicen de manera segura desde los dispositivos personales de los 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 los usuarios y la aplicación SaaS mediante el uso de motores de malware de múltiples proveedores antimalware de terceros. También puede detectar malware en archivos en soluciones de almacenamiento de IaaS y SaaS populares y colocar esos archivos en cuarentena.

Detecte y controle la shadow IT

Forcepoint ONE CASB revela la TI en la sombra, o "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 de SaaS no administradas en uso mediante registros de firewall y proxies corporativos para permitir que se apliquen políticas de seguridad consistentes a aplicaciones de SaaS sancionadas y no sancionadas, de modo que los datos comerciales se mantengan seguros en cualquier lugar donde se utilicen.

Solución de seguridad SaaS que maximiza el tiempo de actividad, la disponibilidad y la productividad

Nuestro CASB está construido sobre una arquitectura nativa en la nube, basada en hyperscaler, con más de 300 puntos de presencia (PoP), accesibilidad global y un tiempo de actividad comprobado del 99.99 % para proteger las aplicaciones de SaaS sin problemas y preservar la productividad del usuario. Otras soluciones desvían el tráfico de la red hacia y desde aplicaciones de SaaS a centros de datos privados en lugar de desviarlos a ubicaciones más cercanas a los usuarios y las aplicaciones a las que acceden. Esto da como resultado un rendimiento deficiente que causa 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

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 de SaaS. El CASB puede bloquear automáticamente la carga. Incluso puede bloquear la carga de archivos a aplicaciones no autorizadas mediante el agente unificado en el dispositivo.

Parte del enfoque de Forcepoint Data Security Everywhere

La misión de Forcepoint Data Security Everywhere permite a las organizaciones proteger datos en SaaS, web, correo electrónico, red y endpoints, para que las personas puedan trabajar de manera segura en cualquier lugar con datos en todas partes.

Extensión de las capacidades de DLP líderes en la industria a las aplicaciones SaaS

Con Forcepoint, las organizaciones pueden utilizar sus políticas de Forcepoint DLP existentes para proteger datos en aplicaciones SaaS, extendiendo la misma seguridad de datos líder en la industria a la nube con solo unos simples clics. Las políticas de DLP unificadas aplicadas desde una única consola ayudan a ofrecer una seguridad de datos consistente de clase empresarial a las aplicaciones SaaS, lo que simplifica la gestión de la seguridad de datos, minimiza las fugas y optimiza el cumplimiento. Los clientes pueden derivar los siguientes beneficios a través de esta integración:

- → Seguridad de datos en la nube simplificada con políticas y consola unificadas.
- → Más de 1700 clasificadores y plantillas de políticas listos para implementar para una cobertura integral y soporte de cumplimiento para más de 150 regiones.
- → Configuración y tiempo al valor en minutos, mejorando la productividad de los equipos de TI y de seguridad.
- → Eliminación productos de seguridad redundantes y fragmentados para lograr ahorros de costos significativos.

Lea el folleto de Forcepoint DLP para obtener más información.

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

Comencemos con una demo.

forcepoint.com/contact