Forcepoint

Resumen de la solución

Agente de seguridad de acceso a la nube

Proteja de manera simple 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 TI paralela (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

El acceso a aplicaciones en la nube y datos desde dispositivos móviles es algo común para la fuerza laboral híbrida de la actualidad. La empresa promedio emplea más de 280 aplicaciones de SaaS, lo que incluye herramientas de colaboración como Microsoft 365, Google Workplace, Slack o Jira que son indispensables para los contratistas y empleados remotos. Utilizar estos servicios sin un método para administrar el acceso desde dispositivos móviles o de establecer la confianza en los dispositivos (postura respecto de los dispositivos) suma complejidad y riesgo.

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. Administrar el acceso a estas aplicaciones desde dispositivos móviles facilita la adopción y la productividad, mientras que contar con distintas políticas basadas en la postura respecto de los dispositivos y la ubicación brinda un control granular de Zero Trust que mantiene los datos seguros. Usted obtiene una mayor certeza sobre cómo se comparten los datos confidenciales en las aplicaciones de la empresa en cualquier dispositivo, incluso los personales. La prevención contra la pérdida de datos (DLP) está integrada, de modo que no necesita productos específicos para detener las fugas de datos.

Detenga el malware oculto en archivos de datos empresariales

Nuestro 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 CrowdStrike. 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 TI paralela (shadow IT)

El CASB no solo visibiliza la TI paralela (shadow IT), sino que además brinda control y asesoramiento sobre el uso seguro y mejores alternativas. El CASB detecta y enumera aplicaciones de SaaS en uso no administradas, lo que permite a los administradores desarrollar políticas para los dispositivos de la empresa que pueden bloquear el acceso o mostrar un mensaje al usuario dirigiéndolo a aplicaciones de SaaS aprobadas.

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

Nuestro CASB forma parte de Forcepoint ONE, nuestra plataforma basada en la nube de hiperescalamiento con 300 puntos de presencia (PoP), accesibilidad global y con un tiempo productivo probado del 99,99 % para proteger las aplicaciones en la nube con fluidez y preservar la productividad de los usuarios. Otras soluciones desvían el tráfico de la red desde y hacia aplicaciones en la nube a centrales de datos privadas en lugar de ubicaciones cercanas a los usuarios. 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.

Proporcionar **seguridad en la nube integral** para cada interacción

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 única consola, los administradores pueden administrar el acceso y controlar las cargas y descargas de archivos para los usuarios de dispositivos administrados y no administrados (como los dispositivos personales o BYOD y las computadoras de los socios o contratistas).

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 Carlos 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 del dispositivo de Carlos y las aplicaciones pasa por el CASB (mediante un proxy inverso).
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 administrados, la descarga se permite dado que Carlos está utilizando una computadora de la empresa.
Carlos intenta transferir datos confidenciales o un archivo contaminado con malware a través de Slack o cargar los datos a su almacenamiento personal de Dropbox.	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.
- **Existen capacidades adicionales,** como el Remote Browser Isolation (RBI) o el análisis de proveedores en la nube en busca de configuraciones riesgosas (CSPM), 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.