Forcepoint

Resumen de la solución

Forcepoint Data Loss Prevention for Cloud Email

Proteja y controle su correo electrónico, sacando provecho de la tecnología de protección contra la pérdida de datos (DLP) de mayor confianza de la industria

Desafío

- Cada vez más datos sensibles se fugan de las organizaciones a través de canales múltiples.
- El correo electrónico es el vector de amenazas más popular para los ataques.
- Proteger los datos sin sofocar la productividad empresarial nunca antes ha sido tan importante o complejo.

Solución

- Forcepoint amplía la solución de DLP más confiable de la industria al canal del correo electrónico.
- Monitoree con precisión y evite la pérdida de datos confidenciales a través del correo electrónico.
- Aproveche los beneficios de una solución en la nube totalmente administrada para escalar la protección del correo electrónico saliente y así satisfacer las demandas de su empresa.

Resultado

- Maximice la eficiencia reduciendo dramáticamente la cantidad de incidentes de falsos positivos por correo electrónico
- Aumente el cumplimiento de tres veces más políticas predefinidas que cualquier otro proveedor de DLP.
- Migre su DLP a Forcepoint en tan solo seis semanas valiéndose de la experiencia, las políticas listas para implementar y la transferencia de conocimiento de primer nivel de Forcepoint.

La seguridad de datos es, cada vez más, un tema central para las organizaciones de todo el mundo. Ya sea que sus empleados trabajen dentro de los límites tradicionales de una oficina o en la nueva realidad de trabajo híbrido o remoto, la complejidad de mantener los datos seguros entre múltiples canales ha aumentado. El correo electrónico es un canal crítico sobre el que las organizaciones deben ganar visibilidad y control para detener la exfiltración no deseada de datos de archivos valiosos, propiedad intelectual (IP) e información. Entre los ejemplos comunes de la pérdida de datos a través del correo electrónico se incluyen los siguientes:

→ **Envío de datos o archivos de una organización** a cuentas de correo electrónico privadas mediante el correo electrónico de la empresa.

→ **Fuga de datos confidenciales** de la organización a causa de negligencia del usuario o cuentas comprometidas.

→ **Empleado con malas intenciones que envía archivos y datos** confidenciales a competidores externos, medios de noticias y sitios web. Con frecuencia con la intención de cometer fraude, sabotear a la organización o robar datos de propiedad exclusiva.

→ **Como resultado de ataques de phishing y malware o adware y spam,** usuarios internos con buenas intenciones cooperan inconscientemente con atacantes para exfiltrar propiedad intelectual (IP) y datos críticos.

"El correo electrónico es el vector de amenazas más popular y utilizado por los atacantes para distribuir malware a una organización. Además, es una línea directa de contacto entre los usuarios y los delincuentes cibernéticos, que lleva al fraude y compromiso de correos electrónicos empresariales multimillonarios cada año".

IDC, PARTICIPAÇÕES NO MERCADO MUNDIAL DE SEGURANÇA DE MENSAGENS, 2021: TRABALHO HÍBRIDO IMPULSIONA A NECESSIDADE DE INTEGRAÇÃO DA INVESTIGAÇÃO DE AMEAÇAS, DOC N.º US49144522, JUNHO DE 2022

Es imperativo que las organizaciones cuenten con visibilidad y control robustos de los correos salientes a fin de proteger la propiedad intelectual de los ataques dirigidos y de la exposición accidental. Esto se logra mediante la protección contra la pérdida de datos (DLP). Según IDC: "En los últimos 24 meses hemos presenciado un renacimiento del mercado de tecnologías para la pérdida de datos. Las técnicas de clasificación arcanas y manuales están siendo reemplazadas por el aprendizaje automatizado y la automatización. El contexto es el factor que más contribuye a esto. La eficacia y eficiencia de las soluciones ha mejorado".[1] La seguridad del correo electrónico, combinada con todos los nuevos avances en DLP que descubre, protege y monitorea información confidencial, es esencial para controlar el importante vector del correo electrónico. Si no se cuenta con capacidades de DLP sólidas, las fugas de seguridad de correo electrónico pueden perjudicar gravemente el negocio y la reputación de su organización.

La ventaja de Forcepoint DLP for Cloud Email

Como líder en soluciones de seguridad de datos, Forcepoint DLP for Cloud Email brinda una visibilidad y un control sin precedentes del correo saliente. En combinación con las ofertas de DLP para dispositivos finales, la nube, la web y las redes, DLP for Cloud Email es una solución potente y múltiple para proteger los datos de una organización. La DLP de Forcepoint está diseñada para evitar la pérdida de datos en todos los lugares en los que trabaje su personal y donde sea que residan los datos.

Identificación de datos extrema

La DLP de Forcepoint ofrece más de 1500 clasificadores y plantillas predefinidos que permiten realizar el despliegue y la identificación de datos confidenciales rápidamente. También aprovecha tecnologías de avanzada, utilizando análisis del lenguaje natural, aprendizaje automatizado y una de las tecnologías de localización (fingerprinting) más fuertes de la industria para identificar con precisión datos en reposo, en movimiento y en uso. En términos de la seguridad de datos, la visibilidad es clave. DLP Discover de Forcepoint brinda una visibilidad sólida seguida de la identificación de datos formal de modo que todos los datos se sometan a un control adecuado. Esto es importante para distintos fines:

- → **Cumplimiento.** Forcepoint DLP cubre reglamentaciones críticas como RGPD, HIPA y muchas más en 83 países para asegurarse de que las organizaciones se rijan en todo momento por los estándares de cumplimiento.
- → **Simplicidad.** La creación e implementación de clasificadores que satisfagan las necesidades y los requisitos comerciales de las organizaciones consume una enorme cantidad de tiempo y recursos para el despliegue de una DLP. Con los clasificadores y las plantillas predefinidos de Forcepoint, las organizaciones pueden desplegar rápidamente clasificadores específicos a una gama de industrias y tipos de datos, lo que simplifica de manera drástica la DLP.
- → **Eficiencia.** Con la tecnología de identificación de datos completa de Forcepoint, Forcepoint DLP reduce radicalmente la cantidad de falsos positivos, a la vez que clasifica y prioriza los incidentes críticos para su investigación.

Control de políticas unificado

Una estrategia de DLP sólida debe abarcar todos los canales principales, como los dispositivos finales, la nube, la web y el correo electrónico. Con frecuencia, las organizaciones tratarán a cada uno de estos canales en silos con diferentes productos de DLP que se enfocan en un solo canal, como la nube o el correo electrónico. Con Forcepoint puede proteger todos estos canales con una única solución y administrarlos aplicando una sola política. Poder escribir una vez y desplegar múltiples veces brinda un control inigualable sobre los datos de su organización, y le permite visualizar todos los canales críticos en donde ocurre la pérdida de datos en un único lugar. El uso de políticas con DLP for Cloud Email también permite ver dispositivos adicionales como tabletas y teléfonos, que no suelen estar cubiertos por las soluciones de dispositivos finales comunes.

Escalabilidad sin precedentes

Forcepoint DLP for Cloud Email tiene la ventaja de ser en servicio en la nube totalmente administrado, lo que ofrece la elasticidad de recursos común en los despliegues en la nube. Si, por ejemplo, en algún momento ocurre una explosión de correo electrónico saliente, DLP for Cloud Email permite realizar una ampliación rápida y, luego, una reducción de los recursos para satisfacer eficazmente las demandas de dicha explosión. También permite que el servicio de DLP continuo satisfaga las demandas de su organización sin tener que desplegar y configurar hardware adicional para hacerlo.

Protección adaptable al riesgo

Forcepoint es el primer proveedor de la industria en brindar DLP adaptable al riesgo. Mediante el monitoreo continuo de la actividad de los usuarios, la solución le da rienda suelta a sus empleados para que hagan más y solo interviene cuando identifica actividad de alto riesgo o patrones de comportamiento riesgoso. La automatización posibilita la aplicación casi en tiempo real; en otras palabras, puede anticiparse y detener una fuga de datos antes de que ocurra.

1 IDC, Worldwide Digital Loss Technologies Market Shares, 2020: La DLP ha muerto, ¡larga vida a la DLP!, Doc. n.º US48261521, octubre de 2021

Las soluciones de Forcepoint DLP for Cloud Email

DLP for Cloud Email: Protección de datos salientes

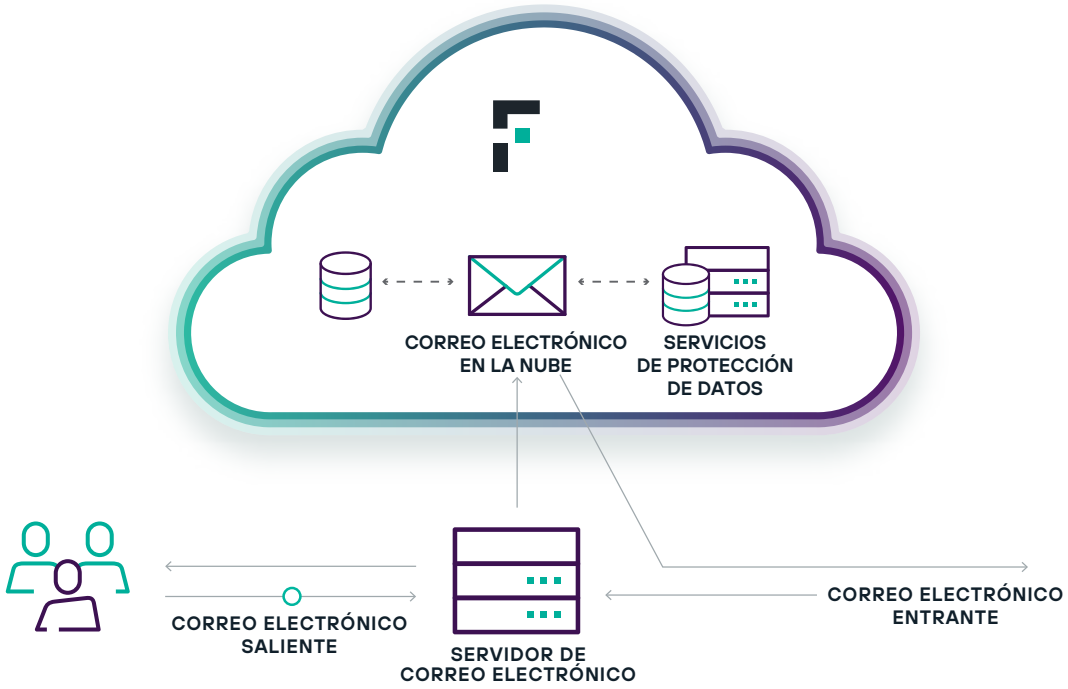
Forcepoint simplifica el despliegue de DLP for Cloud Email dado que trabaja en línea con su proveedor de seguridad de correo electrónico existente para examinar los correos salientes. Mediante el uso de los conectores universales, DLP for Cloud Email Universal Connectors, Forcepoint integra productos de terceros proveedores populares, como Google y Microsoft, para reenviar todos los correos electrónicos salientes, o los que se seleccionen, a la nube Forcepoint Cloud. Allí, Forcepoint DLP los examina según las acciones y políticas de DLP y su plan de DLP predefinido. Se puede permitir, colocar en cuarentena o cifrar (con un módulo de cifrado aparte) los correos electrónicos antes de su envío. Se envían notificaciones sobre los correos en cuarentena y se establece la configuración para retenerlos por hasta 30 días, a menos que un administrador autorizado los libere. Para mantener la reputación de una organización, también se examinan todos los correos salientes en busca de spam, virus y malware.

Características estándar:

- → **Interfaz de políticas simple** que brinda protección contra virus, malware y spam
- → **Paneles, registros e informes de presentación**
- → **Suscripción al correo electrónico personal**

Complementos:

- → **Historial de informes extendido Forcepoint Cloud Email Extended Reporting History** (opciones para 6, 12 y 18 meses)
- → **Módulo de cifrado Forcepoint Email Security Encryption Module**
- → **Módulo de análisis de imágenes Forcepoint Email Security Image Analysis Module**



forcepoint.com/contact