Soluciones de Proofpoint y Amazon Web Services

Proofpoint ofrece a los clientes de AWS cumplimiento y seguridad centrados en las personas

Productos

- Controles de acceso adaptables
- Proofpoint Cloud App Security Broker
- Administración del estado de seguridad cloud (CSPM)
- Proofpoint Email Fraud Defense
- Proofpoint Emerging Threats Intelligence
- Proofpoint Enterprise Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Threat Response Auto-Pull
- Acceso a red zero-trust

Ventajas principales

- Simplifique la seguridad y el cumplimiento normativo de AWS en varias regiones con una administración centralizada.
- Identifique y clasifique los datos sensibles en repositorios de almacenamiento cloud.
- Bloquee inicios de sesión sospechosos e impida la usurpación de cuentas con los recursos de AWS.
- Consiga visibilidad de la actividad de usuarios y datos en todas las instancias de EC2 y Amazon WorkSpaces en AWS.
- Facilite un acceso remoto seguro a su equipo.
- Ponga automáticamente en cuarentena los mensajes de correo electrónico maliciosos que consiguen sortear las soluciones del perímetro.

Las plataformas cloud como Amazon Web Services (AWS) han transformado nuestra forma de trabajar. Actualmente, los empleados las utilizan para teletrabajar en la nube, mientras que las organizaciones recurren a ellas para reducir costes, ganar agilidad e innovar con más rapidez. Con esta transformación, los ciberdelincuentes han desviado su atención del antiguo perímetro de la red a las personas, así como a los datos, los sistemas y los recursos a los que estas acceden. En este panorama cambiante, es preciso proteger el acceso a los recursos de AWS, prevenir la pérdida de datos y cumplir las normativas. Proofpoint ofrece una serie de productos que pueden ayudarle a lograrlo.

Nuestras soluciones le ayudan con:

- Las aplicaciones y servicios no aprobados (Shadow IT)
- Cuentas comprometidas
- Infracciones de cumplimiento
- Suplantación de identidad en el correo electrónico
- Acceso no autorizado
- Pérdida y filtración de datos
- Amenazas internas
- Actividad sospechosa en la red

Descubrimiento de recursos y cuentas en AWS

Proofpoint Cloud App Security Broker (CASB) combina controles centrados en las personas con detección de cuentas cloud comprometidas, DLP y administración de aplicaciones cloud y de terceros. Le ayuda a proteger plataformas cloud como AWS. Nuestro agente CASB multimodal es compatible con modelos de despliegue basados en API y proxy.

Proofpoint CASB simplifica la seguridad y el cumplimiento normativo de AWS en varias regiones con una administración centralizada. Le ofrece visibilidad de todas sus aplicaciones de software como servicio (SaaS) y de todos sus recursos de infraestructura como servicio (IaaS) en AWS.

La solución le ayuda a:

- Ver las tendencias de creación de recursos. Localizar anomalías, como un exceso de recursos creados o eliminados.
- Analizar en detalle recursos descubiertos. Asegurarse de que las cuentas se aprovisionan de acuerdo a las normativas y las mejores prácticas.
- Auditar los registros de tráfico de red. Descubrir aplicaciones cloud y cuentas de AWS que acceden a su red.

Prevención de amenazas cloud

Los controles de acceso adaptables de Proofpoint CASB permiten aplicar en tiempo real medidas de seguridad basadas en el riesgo, el contexto y la función. Bloquean automáticamente el acceso de ciberdelincuentes, o redes y ubicaciones peligrosas conocidos. Y aplican controles basados en riesgos a usuarios de alto riesgo y nivel de privilegios alto. Los controles basados en el riesgo pueden incluir una autenticación más estricta, reglas para dispositivos gestionados y la implementación de VPN.

Los controles de acceso adaptables bloquean los inicios de sesión sospechosos. Impiden la usurpación de cuentas con los recursos de AWS.

La solución le ayuda a:

- Bloquear el acceso a cuentas de usuarios atacados frecuentemente para evitar inicios de sesión sospechosos.
- Crear una lista de bloqueo de países en los que su organización no tiene presencia.

Identificación de servicios mal configurados

Como parte de Proofpoint CASB, se ofrece administración del estado de seguridad cloud (CSPM). CSPM le ayuda a gestionar su estado de seguridad en su entorno cloud y le permite organizar, configurar y mantener sus recursos cloud. Todo ello contribuye a mejorar el cumplimiento de las normativas.

La solución le ayuda a:

- Descubrir configuraciones y ajustes que se apartan de las bases de referencia publicadas.
- Recomendar las mejores prácticas para solucionar errores de configuración que presenten un riesgo de seguridad.
- Simplificar la seguridad cloud y el cumplimiento de normativas con una administración centralizada de recursos cloud en las distintas cuentas y regiones.

Protección de datos sensibles

Proofpoint Enterprise Data Loss Prevention (DLP) reúne nuestras soluciones para correo electrónico, cloud y DLP para endpoints. Combina telemetría de contenido, comportamiento y amenazas procedente de estos canales. Esto le permite abordar el espectro completo de casos de pérdida de datos centrada en las personas.

Proofpoint Enterprise DLP le ayuda a identificar y clasificar datos sensibles en repositorios de almacenamiento cloud.

La solución le ayuda a:

- Supervisar las actividades de archivos para detectar violaciones de DLP.
- Controlar los cubos S3 para identificar excesos de información compartida.
- Crear directivas de seguridad de los datos. El producto utiliza 240 clasificadores de DLP integrados, incluidos identificadores inteligentes incorporados, diccionarios, reglas y plantillas que se comparten con otros productos de DLP de Proofpoint.

Protección de cuentas de AWS

Amazon GuardDuty utiliza la información de Proofpoint Emerging Threats (ET) Intelligence para proteger instancias de AWS.

Proofpoint ET Intelligence es la fuente de inteligencia sobre amenazas más puntual y precisa del sector. Combina una base de datos de amenazas observadas en todo el mundo y análisis de malware con información actualizada al minuto sobre reputación de direcciones IP y dominios. Ofrece a sus equipos de seguridad la inteligencia y el contexto necesarios para detener e investigar los ataques maliciosos.

Proporcionamos productos y soluciones de seguridad, cumplimiento, riesgo digital y respuesta de próxima generación. La información sobre reputación de direcciones IP y dominios de nuestra solución ET se basa en una de las redes más extensas de tecnologías de protección. Cubre entornos de correo electrónico, dispositivos móviles, redes sociales, SaaS y de red.

Gestión de las amenazas internas

Proofpoint ITM forma parte de la plataforma Proofpoint Information and Cloud Security. Le protege frente a la pérdida de datos, los actos maliciosos y los daños a la marca por la acción del personal interno. Proofpoint ITM le defiende contra los usuarios autorizados que pueden actuar de forma malintencionada o negligente. Y correlaciona la actividad de los usuarios y el movimiento de los datos para protegerle de fugas provocadas por usuarios internos.

Proofpoint ITM le ofrece visibilidad de la actividad de usuarios y datos en todas las instancias de EC2 y Amazon WorkSpaces en AWS.

La solución le ayuda a:

- Obtener una vista completa de la actividad relacionada con los endpoints. Conocer el contexto completo de los incidentes causados por los usuarios.
- Ver el contexto de las amenazas para grupos concretos de usuarios. Todo ello le ayuda a gestionar mejor el riesgo asociado a ellos.

Acceso remoto seguro a las aplicaciones cloud

Proofpoint ZTNA es una alternativa zero-trust y centrada en las personas al uso de VPN. Facilita un acceso remoto seguro a cualquier aplicación empresarial, sin importar donde se encuentre la aplicación. Proofpoint ZTNA proporciona a sus usuarios un acceso microsegmentado y seguro a cientos de instancias cloud, automatiza la conectividad de cloud a cloud y permite la conexión de redes cloud híbridas entre servidores locales y clouds públicas.

Proofpoint ZTNA facilita un acceso remoto seguro a las aplicaciones alojadas en AWS para empleados, contratistas, colaboradores y clientes.

La solución le ayuda a:

- Administrar las políticas de acceso remoto a todos los recursos de la empresa en su data center o en AWS desde una sola consola.
- Adoptar un modelo de confianza cero (zero-trust) que ofrece acceso segmentado, verificado y auditado para todo tipo de usuarios.

Mejora de la confianza en su correo electrónico

Proofpoint Email Fraud Defense (EFD) protege a su organización frente a los fraudes por correo electrónico. Le proporciona visibilidad completa de los dominios parecidos y los mensajes enviados utilizando su dominio. También reduce los riesgos que puedan presentar sus proveedores. Identifica los proveedores y los dominios parecidos registrados por terceros.

Proofpoint EFD protege los mensajes de correo electrónico procedentes de Amazon SES. Le ofrece la visibilidad, las herramientas y los servicios necesarios para autorizar el correo electrónico legítimo.

La solución le ayuda a:

- Abordar los problemas que presentan los sistemas de envío de correo electrónico mal configurados y las dificultades de entrega relacionadas con los controles interrumpidos de validación de la autenticación del correo electrónico.
- Identificar y denunciar suplantaciones de identidad en el correo electrónico.
- Poner de manifiesto los problemas de firmas con DKIM y SPF que encuentran los destinatarios de correo electrónico.

Cuarentena automática del correo electrónico malicioso

El dispositivo Proofpoint Threat Response Auto Pull (TRAP) puede alojarse en AWS. Permite a sus equipos de seguridad analizar el correo electrónico y eliminar automáticamente los mensajes maliciosos. También retira los mensajes no deseados del buzón de correo de los usuarios y los pone en cuarentena una vez entregados.

Proofpoint TRAP ayuda a optimizar el proceso de respuesta a incidentes del correo electrónico. Es una potente solución que reduce el tiempo que necesitan sus equipos de seguridad para limpiar el correo electrónico.

La solución le ayuda a:

- Monitorizar automáticamente los buzones de correo para detectar amenazas.
- Reducir exponencialmente el tiempo que necesitan los equipos de seguridad y mensajería cuando revisan la organización y la respuesta de seguridad del correo.
- Poner en cuarentena los mensajes reenviados a personas o listas de distribución.

Para obtener más información sobre la colaboración de Proofpoint con AWS, visite **proofpoint.com/us/partners/aws**.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.