Forcepoint

Datasheet

Forcepoint Data Detection and Response

Detección y respuesta continuas para proteger su información más confidencial

Características y beneficios clave:

- **Detección de amenazas y respuesta continuas:** Forcepoint DDR monitorea continuamente la actividad de datos para detectar amenazas de seguridad y responder a ellas de manera dinámica, lo que ayuda a contener y mitigar las amenazas antes de que provoquen daños significativos.
- **Análisis de datos avanzado y clasificación con IA:** Aprovechando el análisis de datos avanzado y AI Mesh de Forcepoint DSPM, Forcepoint DDR identifica vulnerabilidades de datos y actividades sospechosas, lo que permite gestionar las amenazas de manera proactiva.
- **Visibilidad de datos integral:** Forcepoint DDR proporciona una amplia visibilidad en entornos de nube y endpoint, lo que evita las fugas de datos al garantizar que se aborden las posibles vulnerabilidades.
- **Investigación de incidentes mejorada:** Al ofrecer detalles de nivel forense mediante el seguimiento del ciclo de vida de un archivo, Forcepoint DDR mejora la investigación de incidentes de seguridad, lo que conduce a decisiones de corrección más precisas y reduce los falsos positivos.

Las organizaciones están lidiando con un aumento alarmante de fugas de datos, impulsadas por la rápida adopción de tecnologías de IA y cloud computing. Estas fugas de datos están afectando a empresas de todo el mundo, lo que provoca pérdidas financieras significativas y daños a la reputación. El desafío radica en la capacidad de detectar y responder a estas fugas antes de que ocurran para poder garantizar la protección de los datos confidenciales.

Forcepoint Data Detection and Response (DDR)

Forcepoint DDR powered by GetVisibility es una solución clave para abordar estos desafíos. Proporciona una detección de amenazas continua y visibilidad mejorada de los riesgos de los datos, lo que garantiza que las organizaciones puedan ver los cambios en los datos que probablemente estén llevando a fugas de forma eficaz. Al aprovechar respuestas impulsadas por IA, Forcepoint DDR ofrece neutralización de amenazas, lo que ayuda a las organizaciones a mantener medidas de seguridad sólidas. Su amplia visibilidad en la nube y los endpoints, combinada con el seguimiento del linaje de datos, la convierte en una herramienta esencial para proteger información confidencial, reducir las pérdidas financieras y mantener la confianza del cliente.

Detección de amenazas continua y respuestas impulsadas por IA

Forcepoint DDR proporciona una detección continua de amenazas y visibilidad mejorada de los riesgos de los datos, lo que garantiza que las organizaciones puedan identificar amenazas, monitorearlas y responder a ellas. Aprovechando las respuestas potenciadas por AI Mesh de Forcepoint, Forcepoint DDR neutraliza las amenazas, ofreciendo una defensa sólida contra las fugas de datos.

Amplia visibilidad en la nube y los endpoints

Forcepoint DDR ofrece amplia visibilidad en entornos de nube y endpoints. Esta vista integral ayuda a las organizaciones a evitar la exfiltración de datos y garantiza que se monitoreen y aborden las posibles vulnerabilidades. La inclusión del seguimiento del linaje de datos mejora aún más la capacidad de contrarrestar fugas potenciales con precisión.

Productividad mejorada y reducción de costos

Con una detección continua de amenazas y respuestas dinámicas, Forcepoint DDR permite a los equipos de seguridad concentrarse, ayudando a priorizar los cambios de datos y permisos que apuntan a fugas de datos potenciales en acción. Esto mejora la productividad y respalda los objetivos de la organización de reducir los costos y los riesgos, y mantener la confianza del cliente.

Adición clave a Forcepoint DSPM

En un contexto en el que las empresas buscan proteger su postura de datos, reduciendo los datos riesgosos on-prem y en la nube, Forcepoint DDR aporta una visibilidad continua de los riesgos a Forcepoint DSPM. En lugar de tener que ejecutar un análisis de detección completo de las ubicaciones de los datos primero, Forcepoint DDR permite realizar un monitoreo continuo de la postura de seguridad de datos inmediatamente después de su implementación. Incluso sin análisis de detección previos, Forcepoint DDR detecta nuevos riesgos de datos a medida que ocurren y permite corregirlos. Esto evita continuamente nuevos riesgos para la postura general de seguridad de datos.

Al integrar estas funciones avanzadas, Forcepoint DDR no solo protege los datos, sino que también asegura el futuro de las organizaciones en la era de IA generativa y cloud computing.

FUNCIONALIDAD	BENEFICIO
Monitoreo continuo	Ofrece una visibilidad continua de las actividades de datos riesgosos que permite a las organizaciones detectar amenazas potenciales y responder a ellas.
Alertas automatizadas	Reduce el tiempo de respuesta a las fugas de datos potenciales mediante la priorización y el envío de alertas basadas en las amenazas de riesgos de datos detectadas.
Detección de movimiento de datos	Garantiza que los datos permanezcan dentro de los límites autorizados, protegiendo la propiedad intelectual y la información confidencial.
Implementación de medidas ante violaciones de las políticas	Protege el cumplimiento con las regulaciones de protección de datos mediante la detección de violaciones de las políticas y el envío de alertas al respecto.
Herramientas de cumplimiento	Simplifica el cumplimiento de los requisitos reglamentarios con un monitoreo continuo e historiales de datos detallados para simplificar las auditorías y los informes de cumplimiento.
Gestión de riesgos proactiva	Define lo que constituye riesgos dentro de la organización y permite aplicar medidas para su control mediante políticas de gobernanza personalizables.
Seguimiento de archivos que se comparten más de lo necesario	Aumenta la visibilidad de la exfiltración de datos, revelando las cadenas de eventos maliciosos o las fugas accidentales.
Integración de herramientas de seguridad de terceros	Mejora la respuesta a incidentes y la administración de amenazas a través de la integración con soluciones SIEM y SOAR.
Cobertura de la nube y los endpoints	Permite a las organizaciones comprender y proteger sus datos por completo al proporcionar amplia visibilidad en todo el ecosistema de datos.
Tipos de datos detallados y clasificación de confidencialidad	Proporciona visibilidad del contexto de los datos, lo que permite a los equipos de seguridad evaluar los riesgos y responder de manera eficaz.
AI Classification (AI Mesh)	Proporciona una clasificación de datos de mayor precisión que es eficiente y altamente entrenable.
Capacidades de análisis forense	Mayor precisión en la corrección y reducción de falsos positivos a través de la investigación exhaustiva de los incidentes de seguridad.
Investigación de incidentes dinámica	Acelera los tiempos de respuesta a incidentes, reduce el impacto de los incidentes de seguridad y mejora continuamente la postura de seguridad general de la organización.
Visibilidad del linaje de datos	Permite a las organizaciones comprender por completo el ciclo de vida de sus datos a través del seguimiento histórico detallado de archivos no estructurados.

Forcepoint

forcepoint.com/contact