Forcepoint

Datasheet

Forcepoint Data Detection and Response

Detecção e resposta contínuas para proteger suas informações mais confidenciais

Principais recursos e benefícios:

- **Detecção e resposta contínuas a ameaças:** o Forcepoint DDR monitora continuamente a atividade de dados para detectar e responder a ameaças de segurança dinamicamente, ajudando a conter e mitigar ameaças antes que elas causem danos significativos.
- **Análise avançada de dados e AI Classification:** aproveitando análises de dados avançadas e o Forcepoint DSPM AI Mesh, o Forcepoint DDR identifica vulnerabilidades de dados e atividades suspeitas, permitindo o gerenciamento proativo de ameaças.
- **Visibilidade de dados abrangente:** o Forcepoint DDR fornece visibilidade abrangente em ambientes de nuvem e de endpoint, evitando violações de dados ao garantir que possíveis vulnerabilidades sejam eliminadas.
- **Investigação de incidentes aprimorada:** oferecendo detalhes em nível forense rastreando o ciclo de vida de um arquivo, o Forcepoint DDR aprimora a investigação de incidentes de segurança, levando a decisões de correção mais precisas e reduzindo falsos positivos.

As organizações estão enfrentando um aumento alarmante de violações de dados, impulsionado pela rápida adoção de tecnologias de computação em nuvem e IA. Essas violações de dados estão impactando as empresas globalmente, resultando em grandes perdas financeiras e danos à reputação. O desafio está na capacidade de detectar e responder a essas violações antes que elas ocorram, garantindo a proteção de dados confidenciais.

Forcepoint Data Detection and Response (DDR)

O Forcepoint DDR powered by GetVisibility é uma solução essencial para abordar esses desafios. Fornece detecção contínua de ameaças e visibilidade aprimorada de riscos de dados, garantindo que as organizações possam ver com eficácia as alterações nos dados que provavelmente estão levando a violações de dados. Ao aproveitar respostas orientadas por IA, o Forcepoint DDR oferece neutralização de ameaças, ajudando as organizações a manter medidas de segurança robustas. Sua ampla visibilidade na nuvem e nos endpoints, combinada com o rastreamento de linhagem de dados, torna-o uma ferramenta essencial para proteger informações confidenciais, reduzir perdas financeiras e manter a confiança dos clientes.

Detecção contínua de ameaças e respostas orientadas por IA

O Forcepoint DDR fornece detecção contínua de ameaças e visibilidade aprimorada de riscos de dados, garantindo que as organizações possam identificar, monitorar e responder a ameaças. Aproveitando as respostas habilitadas pelo AI Mesh da Forcepoint, o Forcepoint DDR age para neutralizar ameaças, oferecendo uma defesa robusta contra violações de dados.

Visibilidade extensa na nuvem e nos endpoints

O Forcepoint DDR oferece visibilidade abrangente em ambientes de nuvem e de endpoint. Essa visão abrangente ajuda as organizações a evitar a exfiltração de dados e garante que possíveis vulnerabilidades sejam monitoradas e minimizadas. A inclusão do rastreamento de linhagem de dados aumenta ainda mais a capacidade de combater possíveis violações com precisão.

Produtividade aprimorada e redução de custos

Com detecção contínua de ameaças e respostas dinâmicas, o Forcepoint DDR permite que as equipes de segurança se concentrem, ajudando a priorizar alterações de dados e permissões apontando para possíveis violações de dados em ação. Isso aumenta a produtividade e apoia as metas organizacionais de reduzir custos, reduzir riscos e manter a confiança do cliente.

Adição de chaves ao Forcepoint DSPM

À medida que as empresas buscam proteger sua postura de dados, reduzindo os dados arriscados em locais de nuvem e on-prem, o Forcepoint DDR traz visibilidade contínua de riscos para o Forcepoint DSPM. Em vez de precisar executar uma varredura de descoberta completa dos locais de dados primeiro, o Forcepoint DDR permite o monitoramento contínuo da postura de segurança de dados imediatamente após a implantação. Mesmo sem varreduras de descoberta prévias, o Forcepoint DDR detecta e permite a correção de novos riscos de dados à medida que estão acontecendo. Isso evita continuamente novos riscos para a postura geral de segurança de dados.

Ao integrar esses recursos avançados, o Forcepoint DDR não apenas protege os dados, mas também protege o futuro das organizações na era da GenAI e da computação em nuvem.

FUNCIONALIDADE	BENEFÍCIO
Monitoramento contínuo	Obtenha visibilidade contínua sobre atividades de dados arriscadas, permitindo que as organizações detectem e respondam a possíveis ameaças.
Alertas automáticos	Reduz o tempo de resposta a possíveis violações de dados priorizando e enviando alertas com base em ameaças de risco de dados detectadas.
Detecção de movimentação de dados	Garante que os dados permaneçam dentro de limites autorizados, protegendo a propriedade intelectual e as informações confidenciais.
Aplicação de violações de políticas	Protege a conformidade com os regulamentos de proteção de dados detectando e alertando sobre violações de políticas.
Ferramentas de conformidade	Simplifica a adesão aos requisitos regulatórios com monitoramento contínuo e históricos de dados detalhados para simplificar auditorias e relatórios de conformidade.
Gerenciamento proativo de riscos	Define e permite a aplicação do que constitui risco dentro da organização usando políticas de governança personalizáveis.
Rastreamento de arquivos compartilhados com excesso	Aumenta a visibilidade sobre a exfiltração de dados, revelando uma cadeia maliciosa de eventos ou uma violação acidental.
Integração de ferramentas de segurança de terceiros	Aprimora a resposta a incidentes e o gerenciamento de ameaças por meio da integração com as soluções SIEM e SOAR.
Cobertura de nuvem e endpoints	Permite que as organizações entendam e protejam totalmente seus dados, fornecendo ampla visibilidade em todo o ecossistema de dados.
Classificação detalhada de tipo de dados e sensibilidade	Fornece visibilidade do contexto dos dados, permitindo que as equipes de segurança avaliem riscos e respondam de forma eficaz.
AI Classification (AI Mesh)	Fornece precisão superior na Data Classification, que é eficiente e altamente treinável.
Recursos forenses	Maior precisão de correção e redução de falsos positivos por meio de investigação completa de incidentes de segurança.
Investigação dinâmica de incidentes	Acelera os tempos de resposta a incidentes, reduzindo o impacto de incidentes de segurança e melhorando continuamente a postura de segurança geral da organização.
Visibilidade de linhagem de dados	Capacita as organizações a entender totalmente o ciclo de vida de seus dados por meio de rastreamento histórico detalhado de arquivos não estruturados.

Forcepoint

forcepoint.com/contact