10 Melhores empresas de detecção e resposta de terminais (EDR) em 2025

Data: 2025-08-24 19:59:28

Autor: Inteligência Against Invaders

Em 2025, o ponto final continua sendo o principal campo de batalha para os cibernéticos, tornando a

implementação da EDR Solutions uma necessidade crítica para as defesas robustas de segurança

cibernética.

Laptops, desktops, servidores, dispositivos móveis e cargas de trabalho em nuvem são pontos críticos de entrada e repositórios de dados, tornando -os principais alvos para ameaças cibernéticas sofisticadas.

Embora o software antivírus tradicional (AV) ofereça uma defesa de linha de base contra malware conhecido, é muitas vezes insuficiente combater o cenário em constante evolução de ataques sem arquivo, explorações de dias zero, ransomware e ameaças persistentes avançadas (APTs). Para abordar essas ameaças sofisticadas, as organizações estão cada vez mais se voltando para soluções de EDR.

É aqui que as soluções de detecção e resposta para terminais (EDR) se tornam indispensáveis.

EDR vai muito além da prevenção básica. Ele monitora continuamente a atividade do ponto de extremidade, coletando grandes quantidades de dados (telemetria) em processos, conexões de rede, modificações de arquivos e comportamento do usuário.

Esses dados são analisados ??usando análises avançadas, aprendizado de máquinae inteligência de ameaças para detectar atividades suspeitas que o antivírus tradicional pode perder.

Crucialmente, a EDR fornece às equipes de segurança as ferramentas para investigar, conter e remediar ameaças rapidamente, minimizando o tempo de permanência e os possíveis danos.

Para um mergulho mais profundo nas distinções entre AV tradicional e EDR, explore como EDR vs. antivírus: a melhor segurança do ponto final em 2025 destaca a evolução da proteção do endpoint.

Este artigo analisa meticulosamente as 10 melhores empresas de EDR para 2025, escolhidas por suas capacidades inovadoras, eficácia comprovada de detecção de ameaças, recursos de resposta robusta e valor geral na garantia da empresa moderna.

A evolução da proteção do endpoint: por que o EDR é crucial em 2025

O perímetro digital se dissolveu e o terminal agora é a linha de frente. Uma solução robusta de EDR não é mais um luxo, mas uma necessidade por vários motivos importantes:

Além da detecção baseada em assinatura: As ameaças modernas geralmente não dependem de assinaturas facilmente identificáveis.

O EDR usa análise comportamental e aprendizado de máquina para identificar anomalias e padrões suspeitos que indicam um ataque, mesmo que o malware específico nunca tenha sido visto antes.

Visibilidade e contexto profunda: Os agentes da EDR coletam continuamente a telemetria rica de pontos de extremidade, fornecendo às equipes de segurança uma linha do tempo abrangente dos eventos.

Essa visibilidade é crucial para entender a causa raiz, o escopo e o impacto de um ataque.

Caça proativa de ameaças: Embora o EDR automatize muitas detecções, também capacita analistas humanos a procurar proativamente indicadores sutis de compromisso (COI) e táticas, técnicas e procedimentos (TTPs) que possam significar um ataque furtivo e contínuo.

Resposta rápida de incidentes: As ferramentas EDR fornecem recursos para contenção imediata (por exemplo, isolando um dispositivo infectado, matando processos maliciosos) e remediação guiada ou automatizada, reduzindo significativamente o tempo que os atacantes precisam mover dados lateralmente ou exfiltrar.

Análise forense: Pós-incidente, os dados granulares coletados pela EDR permitem que as equipes de segurança realizem investigações forenses completas, aprendam com violações e fortalecem as defesas futuras.

Integração com XDR e SIEM: Muitas soluções líderes de EDR servem como a camada fundamental para plataformas estendidas de detecção e resposta (XDR), que se correlacionam dados em todo Várias camadas de segurança (endpoint, rede, nuvem, identidade, email) para uma visualização holística.

Eles também alimentam dados críticos de endpoint em Informações de segurança e gerenciamento de eventos (SIEM) Sistemas para registro e análise centralizados.

Compreender a interação entre essas tecnologias é fundamental para uma estratégia de segurança abrangente; Nosso artigo sobre MDR vs. EDR vs. XDR: Comparações e diferenças investem nesses conceitos.

Em 2025, as principais soluções EDR são caracterizadas por agentes leves, arquiteturas nativas da nuvem para escalabilidade, IA/ml avançada para detecção autônoma, fortes recursos de integração e ênfase na redução de falsos positivos para combater a fadiga de alerta.

Nossa metodologia de seleção para as principais empresas EDR (2025 Focus)

Nosso rigoroso processo de avaliação para os principais fornecedores de EDR em 2025 focou nos seguintes critérios críticos:

Eficácia de detecção: Capacidade comprovada de detectar uma ampla gama de ameaças, incluindo zero dias, ransomware, ataques sem arquivo e ameaças de nível de estado-nação,

demonstradas consistentemente em testes independentes (por exemplo, Avaliações de Mitre ATT e CK).

Recursos de resposta: A amplitude e a eficácia das ações de resposta, incluindo contenção automatizada, remediação remota e recursos de reversão.

Visibilidade e telemetria: A profundidade e amplitude de dados coletados de terminaisfornecendo um contexto rico para investigações.

Integração de AI/Aprendizado de Machine: A sofisticação e eficácia dos modelos de IA/ML para detecção e prevenção de ameaças autônomas e reduzir os falsos positivos.

Desempenho e agente leve: Impacto mínimo no desempenho do terminal e na experiência do usuário.

Arquitetura nativa em nuvem: Escalabilidade, facilidade de implantação e atualizações contínuas oferecidas por plataformas baseadas em nuvem.

Usabilidade e gerenciamento: Console de gerenciamento intuitivo, facilidade de implantação e relatórios claros.

Ecossistema de integração: Capacidade de se integrar a outras ferramentas de segurança (Siem, DISPARARsoluções de identidade) e forneça dados para plataformas XDR.

Inteligência de ameaças: A qualidade e a pontualidade dos feeds de inteligência de ameaças integrados.

Suporte e reputação do cliente: Reconhecimento do setor e feedback positivo do cliente.

Tabela de comparação: 10 melhores empresas de detecção e resposta para pontos de extremidade (EDR) 2025

1. Crowdstrike Falcon Insight

Por que escolhemos:

Crowdstrike Falcon Insight XDR é um líder de mercado devido à sua arquitetura nativa em nuvem, agente leve e capacidade incomparável de detectar e prevenir sofisticado ameaças usando a IA e análise comportamental.

Seu módulo Falcon Insight, especificamente, fornece profunda visibilidade da atividade do terminal, capacitando as equipes de segurança com dados abrangentes para caça e investigação, solidificando sua posição como uma solução EDR de primeira linha.

Especificações:

O CrowdStrike Falcon Insight XDR é construído na plataforma Falcon nativa em nuvem, oferecendo visibilidade e proteção em tempo real em pontos de extremidade, cargas de trabalho em nuvem, identidade e dados.

Isso o torna um exemplo líder de soluções modernas de EDR. Possui um agente único leve que coleta e analisa extensa telemetria.

As principais especificações incluem análises comportamentais movidas a IA, indicador de detecções de ataque (IOA), remediação automatizada, caça proativa de ameaças pela equipe do Falcon Overwatch (se o Falcon completo estiver empacotado) e a extensa integração de inteligência de ameaças.

Ele tem um bom desempenho nas avaliações de Mitre ATT e CK.

Motivo para comprar:

O CrowdStrike Falcon Insight XDR é ideal para organizações que buscam uma solução EDR de ponta de alto desempenho, com prevenção robusta, detecção e recursos de resposta.

Se você priorizar o impacto mínimo do sistema, a visibilidade abrangente e um forte histórico contra ameaças sofisticadas, o CrowdStrike é um excelente investimento para fortalecer sua postura de segurança de endpoint.

Características:

- Arquitetura nativa em nuvem com um único agente leve.
- Análise comportamental movida a IA para detecção avançada de ameaças.
- Visibilidade em tempo real em todas as atividades do terminal.
- Ações automatizadas de resposta a incidentes e remediação.
- Capacidades proativas de caça de ameaças (especialmente com o Falcon Overwatch).
- Inteligência integrada de ameaças do gráfico de ameaças de Crowdstrike.
- Mitre ATT & CK Framework Mapping para entender o ataque.
- Suporte de plataforma cruzada (Windows, MacOS, Linux, Contêineres).

Prós:

- Capacidades de detecção e prevenção líder do setor.
- Impacto mínimo no desempenho do terminal.
- Visibilidade excepcional e dados forenses.
- Escalável para organizações de todos os tamanhos.
- Forte integração com outros módulos de segurança (higiene de TI, gerenciamento de vulnerabilidades).

Contras:

- Pode ser uma solução de preço premium.
- Os benefícios completos são realizados ao alavancar a plataforma Falcon mais ampla.
- A interface pode ser complexa para novos usuários devido à sua profundidade.

? Melhor para: empresas e organizações maduras de segurança que exigem o melhor EDR orientado a IA, com visibilidade profunda, pegada mínima e proteção de ameaças comprovadas em diversos sistemas operacionais.

? Try CrowdStrike Falcon Insight here ? CrowdStrike Official Website

2. SentineLone

Por que escolhemos:

A SentineLone Singularity Platform se destaca por sua mistura única de prevenção, detecção e resposta autônomas de IA, todos no dispositivo.

Isso o torna uma das soluções EDR mais eficazes disponíveis. Isso permite a neutralização de ameaças rápidas de raios, mesmo quando os terminais estão offline, reduzindo a dependência da conectividade em nuvem.

A capacidade da plataforma de automatizar a remediação complexa e fornecer uma “história” de ataques simplifica as operações de segurança para equipes ainda menores.

Especificações:

A plataforma SentineLone Singularity fornece proteção, detecção e resposta de pontos de extremidade autônomos entre pontos de extremidade, cargas de trabalho em nuvem, dispositivos IoT e sistemas de identidade.

Possui uma história patenteada Motor AI Isso correlaciona os eventos em uma narrativa abrangente de ataque.

As principais especificações incluem IA comportamental em tempo real, remediação automatizada (incluindo recursos de reversão), caça proativa de ameaças por meio de resposta de vigilância (uma opção de serviço gerenciado) e um único agente que opera offline.

Motivo para comprar:

A plataforma SentineLone Singularity é ideal para organizações que buscam uma solução EDR que priorize proteção e resposta autônoma em tempo real, mesmo sem conectividade em nuvem constante.

Se você deseja reduzir significativamente a carga de trabalho de segurança manual, simplificar investigações complexas de incidentes e ter recursos robustos de recuperação de ransomware, a SentineLone oferece uma solução poderosa e eficiente.

Características:

- IA autônoma para prevenção e remediação de ameaças no dispositivo.
- História automatizada IA ??para visualização abrangente de ataques.
- Rollback com um clique para restaurar pontos de extremidade de ataques de ransomware.
- Cobertura de plataforma cruzada (Windows, MacOS, Linux, Kubernetes, Recipientes).
- A caça a ameaças proativas e validação de incidentes.
- Console unificado para segurança de extremidade, nuvem e identidade.

- Orientado pela API para extensos recursos de integração.

Prós:

- Detecção e resposta autônomas excepcionais, mesmo offline.
- Forte recursos anti-ransomware com reversão.
- Investigação de incidentes simplificados com a história da história.
- Baixo custo total de propriedade por meio da automação.
- Tem um desempenho consistente em testes independentes.

Contras:

- Pode exigir alguma ajuste inicial para otimizar para ambientes específicos.
- Os benefícios completos são realizados com um compromisso com a plataforma de singularidade.
- Alguns recursos avançados podem exigir treinamento adicional.

? Melhor para: organizações que procuram uma solução EDR com fortes recursos autônomos de IA, resposta rápida no dispositivo, proteção abrangente de ransomware e investigações de incidentes simplificadas.

`? Try SentinelOne here ?` `SentinelOne Official Website`

3. Microsoft Defender

Por que escolhemos:

O Microsoft Defender for Endpoint evoluiu para uma solução EDR formidável, profundamente integrada no suíte Microsoft 365 mais amplo.

Sua integração nativa com sistemas operacionais Windows, Azure AD e Cloud Services fornece visibilidade incomparável e proteção perfeita para ambientes centrados na Microsoft.

Essa integração rígida simplifica a implantação e o gerenciamento de organizações já investidas no ecossistema da Microsoft.

Especificações:

O Microsoft Defender for Endpoint fornece dispositivos unificados de segurança de extremidades entre os dispositivos Windows, MacOS, Linux, Android e iOS.

Ele aproveita a vasta inteligência de ameaças da Microsoft, aprendizado de máquina e monitoramento comportamental.

As principais especificações incluem investigação e remediação automatizadas, recursos avançados de caça de ameaças, gerenciamento de vulnerabilidades e integração com Microsoft 365 Defensor para recursos XDR em aplicativos de email, identidade e nuvem.

Motivo para comprar:

O Microsoft Defender for Endpoint é uma excelente opção para organizações profundamente investidas na Microsoft 365 e no Azure, pois oferece recursos poderosos e integrados de soluções EDR que são gerenciadas perfeitamente ao lado de outros serviços de segurança da Microsoft.

Se você priorizar a integração nativa, a implantação simplificada e o gerenciamento de segurança consolidado dentro do seu ecossistema da Microsoft, o Defender for Endpoint é uma solução atraente.

Características:

- Integração nativa com sistemas operacionais do Windows.
- Investigação automatizada e remediação de ameaças.
- Avançando a caça de ameaças com a Kusto Query Language (KQL).
- Gerenciamento de vulnerabilidades interno e gerenciamento de postura de segurança.
- Gerenciamento centralizado através do Microsoft 365 Defender Portal.
- Suporte de plataforma cruzada além do Windows.
- Inteligência de ameaças integradas da Microsoft.

Prós:

- Integração perfeita com o ecossistema da Microsoft.
- Visibilidade abrangente em ambientes da Microsoft.
- Investigação e remediação automatizadas robustas.
- Incluído com certas licenças do Microsoft 365, oferecendo um bom valor.
- Forte desempenho nas avaliações de Mitre ATT e CK.

Contras:

- A funcionalidade completa é melhor realizada em um ambiente predominantemente da Microsoft.
- Alguns recursos avançados podem exigir um conhecimento profundo das ferramentas de segurança do Microsoft.
- Pode ser complexo para navegar para ambientes pesados ??não-Microsoft.

? Melhor para: organizações investiram fortemente em ecossistemas da Microsoft (Microsoft 365, Azure), buscando recursos integrados e abrangentes de EDR com gerenciamento simplificado e integração nativa do sistema operacional.

`? Try Microsoft here ?` [Microsoft Official Website]

4. Cortex Palo Alto Networks

Por que escolhemos:

A Palo Alto Networks Cortex XDR é líder no espaço da EDR Solutions principalmente porque foi

pioneira no conceito de detecção e resposta (XDR), unificando dados de pontos de extremidade, redes, nuvem e fontes de identidade.

Enquanto suas raízes estão em segurança de endpoint, sua capacidade de correlacionar alertas em vários domínios fornece uma visão holística dos ataques, tornando -o incrivelmente eficaz para paisagens complexas de ameaças e permitindo uma sofisticada caça às ameaças.

Especificações:

A Palo Alto Networks Cortex XDR é uma plataforma XDR acionada por IA que integra a Endpoint Security (EDR) com dados de firewalls, cargas de trabalho em nuvem e fontes de identidade.

Usa aprendizado de máquina para Analisar dados brutosdetecte ameaças e automatize a resposta.

As principais especificações incluem análise de causa raiz automatizada, caça a ameaças gerenciadas (opcional), análise de comportamento do usuário e um Data Lake centralizado para retenção e investigação de dados de longo prazo.

Motivo para comprar:

O Palo Alto Networks Cortex XDR é ideal para organizações que desejam evoluir além do EDR tradicional para uma abordagem XDR mais holística, correlacionando dados de segurança em toda a sua infraestrutura.

Se você precisar de uma poderosa detecção de ameaças orientada pela IA, análise de causa raiz automatizada e a capacidade de procurar ameaças em vários domínios de segurança, o Cortex XDR é uma escolha de primeira linha.

Características:

- Detecção e resposta unificadas no ponto final, rede, nuvem e identidade.
- A IA e a detecção de ameaças orientadas por aprendizado de máquina.
- Análise de causa raiz automatizada e visualização de ataque.
- Serviço de caça de ameaças gerenciadas (Cortex XDR Pro).
- Proteção do terminal, incluindo prevenção de exploração e detecção de malware.
- Visibilidade abrangente sobre a atividade do usuário e da rede.
- Integração com ferramentas de segurança de terceiros via APIs abertas.

Prós:

- Fortes capacidades XDR para uma visão holística das ameaças.
- Excelente detecção de ameaças e análise de causa raiz.
- Automatiza investigações complexas, reduzindo a carga de trabalho do analista.
- Aproveita a forte inteligência de ameaças da Palo Alto Networks.
- Altamente eficaz para ataques complexos e de vários estágios.

Contras:

- Pode ser uma solução mais complexa para implementar e gerenciar em comparação com os

EDRs puros.
- Os benefícios completos requerem adoção além dos dados apenas do terminal.
- Os preços podem ser mais altos, especialmente para a oferta completa do XDR.

? Melhor para: empresas e grandes organizações que buscam uma solução avançada de EDR que escala perfeitamente uma plataforma XDR completa para detecção e resposta de ameaças unificadas em ambientes complexos.

`? Try Palo Alto Networks here ?` Palo Alto Networks Official Website

5. Sophos Intercept

Por que escolhemos:

Sophos Intercept X com EDR se destaca por seu forte foco nos recursos anti-ransomware (CryptoGuard) e na AI de aprendizado profundo, tornando-o altamente eficaz contra ameaças conhecidas e desconhecidas.

Sua interface amigável e abordagem de segurança sincronizada, onde a segurança do endpoint se comunica com outros produtos do Sophos, como firewalls, simplifica o gerenciamento de segurança e aprimora a proteção geral, tornando-o acessível para uma ampla gama de organizações.

Especificações:

Sophos Intercept X com EDR combina antivírus de próxima geração, anti-ransomware (criptograma), prevenção de exploração e aprendizado profundo AI para detecção de ameaças.

Ele fornece visibilidade em tempo real da atividade do terminal, permitindo investigação e resposta remotas.

As principais especificações incluem resposta guiada a incidentes, avaliações de postura de segurança e integração com o Sophos Central Management Console, que também gerencia outros produtos de segurança da Sophos.

Motivo para comprar:

O Sophos Intercept X com o EDR é uma excelente opção para as organizações que priorizam a proteção anti-ransomware robusta, a facilidade de gerenciamento e uma abordagem de segurança unificada por meio de segurança sincronizada.

Esses recursos o tornam uma das principais soluções EDR disponíveis. Se você deseja um EDR poderoso e orientado pela IA que seja simples de implantar e gerenciar, especialmente se você já usar outros produtos Sophos, o Intercept X é uma solução altamente eficaz.

Características:

- Aprendizagem profunda da IA ??para detecção avançada de ameaças.

- Tecnologia anti-ransomware do CryptoGuard.
- Explorar prevenção e mitigação de adversário ativo.
- Resposta de incidentes guiados e consultas de caça de ameaças.
- Análise de causa raiz para ameaças detectadas.
- Avaliação e recomendações da postura de segurança.
- Segurança sincronizada com outros produtos Sophos.

Prós:

- Excelente prevenção anti-ransomware e exploração.
- Interface amigável e fácil implantação.
- Forte IA de aprendizado profundo para altas taxas de detecção.
- A segurança sincronizada aprimora a postura geral de segurança.
- Adequado para pequenas e médias empresas e organizações maiores.

Contras:

- Os benefícios completos são realizados no ecossistema Sophos.
- Alguns recursos avançados de caça de ameaças podem ser menos intuitivos do que as plataformas XDR dedicadas.
- O desempenho em pontos de extremidade mais antigos às vezes pode ser uma preocupação (embora geralmente boa).

? Melhor para: organizações de mercado intermediário e aqueles que buscam uma solução EDR altamente eficaz e fácil de gerenciar, com um forte foco na proteção de ransomware e gerenciamento de segurança integrado.

`? Try Sophos Intercept here ?` Sophos Official Website

6. Trend Micro Apex One

Por que escolhemos:

Trend Micro Apex One (com XDR) fornece proteção robusta e abrangente que integra Recursos de EDR com foco no gerenciamento de riscos da superfície de ataque.

Sua capacidade de estender a visibilidade além do endpoint para e -mail, rede e nuvem através de sua plataforma Vision One oferece uma experiência de segurança unificada, tornando -o um forte candidato a organizações que buscam ampla detecção de ameaças e operações de segurança simplificadas.

Especificações:

Trend Micro Apex One é uma forte escolha entre as soluções EDR devido à sua detecção e resposta automatizadas de ameaças com AV de próxima geração, análise comportamental e prevenção de explorar.

Seus recursos XDR, acessados ??através da plataforma Trend Micro Vision One, estendem a visibilidade para cargas de trabalho em e -mail, rede, nuvem e servidor.

As principais especificações incluem detecção e resposta automatizadas, análise de segurança, um agente leve e integração com a inteligência global de ameaças.

Motivo para comprar:

O Trend Micro Apex One (com XDR) é uma excelente opção para organizações que desejam proteção abrangente para pontos de extremidade combinada com recursos XDR mais amplos em toda a propriedade digital.

Se você está procurando um EDR confiável e rico em recursos de um fornecedor de segurança de longa data e valoriza uma visão unificada em pontos de extremidade, email e nuvem, a Trend Micro oferece uma solução atraente.

Características:

- Recursos abrangentes de proteção e EDR.
- Integração XDR através da tendência Micro Vision One.
- Detecção e resposta automatizadas para ameaças conhecidas e desconhecidas.
- Análise comportamental, aprendizado de máquina e análise de caixa de areia.
- Controle de aplicativos e proteção contra vulnerabilidade.
- Console de gerenciamento centralizado.
- Atacar insights de gerenciamento de riscos de superfície.

Prós:

- Fortes recursos de detecção de ameaças, com foco em ameaças desconhecidas.
- Proteção abrangente em vários vetores de ataque.
- Os recursos XDR fornecem visibilidade mais ampla.
- Escalável para vários tamanhos de negócios.
- Fornecedor respeitável com ampla inteligência de ameaças.

Contras:

- A experiência XDR completa requer a adoção da plataforma Vision One.
- Alguns usuários podem achar o console menos intuitivo que as interfaces mais recentes.
- A integração com micro ferramentas não tendências para XDR pode exigir um esforço adicional.

? Melhor para: organizações que buscam uma solução EDR abrangente e bem estabelecida que possa escalar para fornecer visibilidade XDR mais ampla entre pontos de extremidade, email e ambientes em nuvem.

? Try Trend Micro Apex One here ? Trend Micro Official Website

7. Cybereason

Por que escolhemos:

A Prevenção e a Resposta dos Pontos de Endulações de Cyberason é uma das principais soluções EDR devido ao seu mecanismo exclusivo de detecção de “Malop” (Operação maliciosa).

Este motor correlaciona eventos de extremidade díspares em uma única história de ataque abrangente.

Essa abordagem contextual permite que as equipes de segurança entendam rapidamente o escopo completo de um ataque, incluindo sua causa e propagação raiz, permitindo uma resposta mais rápida e eficaz contra ameaças sofisticadas e em vários estágios, como ransomware avançado.

Especificações:

A prevenção e a resposta dos endpoint cyberason aproveita uma plataforma orientada a IA para detectar e impedir ameaças entre pontos de extremidade, redes e identidades.

Ele se concentra na identificação de “operações maliciosas” (MALOPS), correlacionando eventos maliciosos individuais em uma narrativa completa de ataque.

As principais especificações incluem prevenção autônoma, opções de resposta guiadas e automatizadas, proativo caça às ameaçase a capacidade de operar efetivamente contra ameaças sem arquivo e desconhecidas.

Motivo para comprar:

A prevenção e a resposta dos endpoint cybereason é ideal para organizações que enfrentam ataques cibernéticos avançados e com vários estágios, particularmente ransomware, e requerem uma profunda compreensão contextual das operações maliciosas.

Se você precisar de um EDR que se destaque em conectar os pontos em todo o ambiente para fornecer uma história de ataque completa e permite uma resposta rápida e precisa, a cyberason é uma escolha poderosa.

Características:

- Motor de detecção MALOP acionado por IA para visibilidade abrangente de ataques.
- Remediação automatizada e guiada de ameaças.
- A caça a ameaças proativas e validação de incidentes.
- Ransomware Prevenção e Recuperação de Recuperação.
- Visibilidade em tempo real em atividades de endpoint.
- Alertas contextualizados para reduzir falsos positivos.
- MITRE ATT & CK Framework mapeamento.

Prós:

- Excepcional na detecção e correlação de ataques de vários estágios.

- Poderoso contra ransomware e ameaças sem arquivo.
- Reduz a fadiga de alerta, concentrando -se em histórias de ataque completo.
- Fornece informações forenses profundas para investigações.
- Fortes capacidades de prevenção autônoma.

Contras:

- O desempenho ideal é alcançado ao usar a plataforma abrangente da Cybereason.
- O conceito “Malop” pode exigir uma leve curva de aprendizado para novos usuários.
- Os preços podem estar no nível mais alto de algumas organizações preocupadas com o orçamento.

? Melhor para: organizações que combatem ataques cibernéticos sofisticados e multi-estágios (como ransomware avançado) que precisam de uma profunda compreensão contextual de “operações maliciosas” e recursos rápidos e precisos de resposta.

`? Try Cybereason here ?` `Cybereason Official Website`

8. VMware Carbon Black

Por que escolhemos:

O VMware Carbon Black EDR é uma solução altamente considerada para centros de operações de segurança (SOCs) e Resposta de incidentes (IR) equipes, oferecendo coleta de dados brutos e recursos de resposta ao vivo.

Sua força reside em fornecer aos analistas de segurança ferramentas de investigação profundas e informações forenses sobre a atividade do terminal, capacitando -os a realizar uma análise completa de caça e incidentes de ameaças, tornando -o um favorito entre as equipes de segurança mais maduras.

Especificações:

O VMware Carbon Black EDR é uma das principais soluções de EDR devido ao seu registro contínuo e armazenamento de dados de terminais, que fornecem visibilidade em tempo real da atividade do terminal.

É construído para operações de segurança e equipes de resposta a incidentes, oferecendo consultas avançadas de caça de ameaças, listas de observação automatizadas e recursos de resposta ao vivo.

As principais especificações incluem implantação flexível (nuvem ou no local), integração com ferramentas SIEM/Soar e a capacidade de capturar informações forenses detalhadas.

Motivo para comprar:

O VMware Carbon Black EDR é mais adequado para organizações com centros de operações de

segurança maduros e equipes dedicadas de resposta a incidentes que exigem dados granulares para investigações profundas e caça proativa de ameaças.

Se sua equipe tiver a experiência e precisar de poderosas capacidades forenses e controle flexível sobre o seu EDR, o EDR preto carbono é uma opção de primeira linha.

Características:

- Registro de dados de pontos de extremidade contínua e abrangente.
- A caça avançada de ameaças usando consultas personalizadas.
- Listas de observação automatizadas para atividades suspeitas.
- Capacidades de resposta ao vivo para investigação e remediação imediatas.
- Dados forenses detalhados para análise pós-incidente.
- Abra a API para integração com outras ferramentas de segurança.
- Suporta vários sistemas operacionais.

Prós:

- Profundidade excepcional de visibilidade e dados de terminais brutos.
- Caça poderosa de ameaças e capacidades forenses.
- Altamente personalizável para equipes de segurança experientes.
- Opções de implantação flexíveis.
- Forte para resposta a incidentes e análise de causa raiz.

Contras:

- Pode ter uma curva de aprendizado mais acentuada para analistas menos experientes.
- Requer pessoal de segurança qualificado para maximizar seu valor.
- Pode gerar um alto volume de dados, exigindo armazenamento robusto.

? Melhor para: Centros de Operações de Segurança (SoCs) e equipes de resposta a incidentes (IR) que precisam de dados forenses profundos, poderosas ferramentas de caça de ameaças e controle extensivo sobre investigações de segurança de endpoint.

`? Try VMware Carbon Black EDR here ?` [VMware Carbon Black Official Website]

9. Fortiedr

Por que escolhemos:

A Fortiedr é uma das principais soluções EDR devido aos seus fortes recursos de proteção pré e pós-infecção, oferecendo proteção, detecção e resposta automatizada em tempo real.

Como parte do tecido mais amplo de segurança da Fortinet, ele se integra perfeitamente a outros produtos da Fortinet, como o FortiGate Firewalls, fornecendo uma defesa unificada e automatizada em toda a rede e endpoint, tornando -o particularmente atraente para os clientes da Fortinet existentes.

Especificações:

A Fortiedr fornece proteção automatizada em tempo real para pontos de extremidade antes, durante e após um ataque.

Emprega aprendizado de máquina, análise comportamental e inteligência de ameaças para detectar e bloquear ameaças.

As principais especificações incluem proteção de pré-execução e pós-execução, manuais de resposta automatizada de incidentes, ferramentas de investigação remota e integração perfeita com o tecido de segurança Fortinet.

Ele suporta Windows, MacOS e Linux pontos de extremidade.

Motivo para comprar:

O Fortiedr é uma escolha ideal para organizações já investidas no Fortet Security Fabric, procurando estender sua defesa unificada ao ponto de extremidade com recursos robustos de EDR.

Se você deseja uma integração perfeita entre sua rede e segurança de endpoint, juntamente com uma forte resposta automatizada, a Fortiedr oferece uma solução abrangente.

Características:

- Proteção de prejuízo (preventiva) e pós-infecção (detecção e resposta).
- Resposta automatizada de incidentes em tempo real com manuais personalizáveis.
- Aprendizado de máquina e análise comportamental para detecção.
- Ferramentas de coleta e investigação de dados forenses.
- Integração com o Fortet Security Fabric para defesa unificada.
- Recursos de reversão para restaurar arquivos afetados.
- Opção de serviço gerenciado disponível.

Prós:

- Excelente integração com o ecossistema Fortinet.
- Fortes recursos de resposta automatizados com manuais.
- Proteção eficaz de pré e pós-infecção.
- Bom para consolidar os fornecedores de segurança para usuários da Fortinet.
- Escalável para vários tamanhos corporativos.

Contras:

- Os benefícios maximizados são para organizações que já usam produtos Fortinet.
- A interface pode parecer menos moderna em comparação com alguns EDRs nativos da nuvem.
- A inteligência de ameaças pode estar mais concentrada no ecossistema Fortinet.

? Melhor para: organizações que fazem parte do ecossistema Fortinet e desejam integração perfeita entre sua rede e segurança de endpoint, com foco na resposta automatizada de ameaças em tempo

real.

? Try FortiEDR here ? Fortinet Official Website

10. Cisco Secure Endpoint

Por que escolhemos:

Cisco Secure Endpoint, anteriormente conhecido como AMP por pontos de extremidade, aproveita a vasta rede de inteligência de ameaças globais da Cisco e seu profundo entendimento de segurança de rede para fornecer recursos abrangentes de EDR.

Sua capacidade de monitorar e analisar continuamente a atividade do terminal, combinada com os recursos avançados de proteção de malware e de resposta a incidentes, o torna um forte candidato a organizações que buscam uma solução de segurança integrada em um ambiente mais amplo da Cisco.

Especificações:

O Cisco Secure Endpoint fornece proteção avançada de proteção de malware, soluções EDR e recursos de resposta a incidentes em uma ampla gama de pontos de extremidade (Windows, MacOS, Linux, Android, iOS).

Ele utiliza a inteligência de ameaças de talos da Cisco, aprendizado de máquina e análise comportamental. As principais especificações incluem monitoramento contínuo, segurança retrospectiva, controle automatizado de surtos e integração com outros produtos seguros da Cisco para uma postura de segurança unificada.

Motivo para comprar:

O Cisco Secure Endpoint é uma excelente opção para organizações que já utilizam a infraestrutura de rede e segurança da Cisco, procurando uma solução de EDR que se integra perfeitamente e se beneficie da extensa inteligência de ameaças da Cisco.

Se você priorizar uma abordagem de segurança integrada de um fornecedor global confiável, o Cisco Secure Endpoint oferece recursos robustos de EDR.

Características:

- Monitoramento e gravação de pontos de extremidade contínuos.
- Recursos avançados de proteção de malware (AMP).
- Segurança retrospectiva para detectar ameaças que foram perdidas inicialmente.
- Controle e contenção automatizados de surto.
- Integrado à inteligência de ameaças da Cisco Talos.
- Análise de causa raiz e cronogramas detalhados de eventos.
- Console único para gerenciamento simplificado.

Prós:

- Aproveita a extensa inteligência global de ameaças da Cisco.
- Fortes recursos de análise retrospectiva.
- Bom para organizações que já usam produtos de segurança da Cisco.
- Visibilidade abrangente para ameaças entre pontos de extremidade.
- Escalável para grandes empresas.

Contras:

- O melhor valor é realizado quando integrado a outras soluções da Cisco.
- A interface do usuário pode ser menos intuitiva para aqueles que não estão familiarizados com as plataformas de segurança da Cisco.
- A implantação e a configuração podem ser complexas para equipes menores.

? Melhor para: empresas e grandes organizações investiram fortemente na infraestrutura de rede e segurança da Cisco, buscando uma solução EDR integrada que se beneficie da inteligência global de ameaças.

`? Try Cisco Secure Endpoint here ?` Cisco Official Website

Conclusão

O terminal continua sendo o ativo mais exposto e freqüentemente direcionado no cenário digital de qualquer organização.

Em 2025, confiar apenas no antivírus tradicional é semelhante a levar uma faca a um tiroteio.

As soluções de detecção e resposta de terminais (EDR) são o arsenal moderno, fornecendo as capacidades de visibilidade, detecção e resposta necessárias para se defender contra ameaças cibernéticas sofisticadas e evasivas.

As 10 principais empresas EDR descritas neste artigo representam a vanguarda da inovação em segurança do Endpoint.

Cada um oferece uma mistura única de detecção acionada por IA/ML, caça proativa de ameaças e recursos rápidos de resposta projetados para proteger seus ativos críticos.

Ao escolher estrategicamente o parceiro EDR certo que se alinha às necessidades, orçamento e ecossistema de segurança existentes da sua organização, você pode fortalecer significativamente sua fronteira digital, minimizar o impacto das violações e capacitar suas equipes de segurança a ficar à frente da curva na paisagem de ameaças cibernéticas em constante evolução.

Investir em uma solução robusta de EDR não é apenas sobre tecnologia; Trata -se de investir na resiliência e continuidade do seu negócio.