10 Melhores soluções de proteção de terminais para MSP/MSSPs em 2025

Data: 2025-08-24 21:00:59

Autor: Inteligência Against Invaders

Os provedores de serviços gerenciados (MSPs) e os provedores de serviços de segurança

gerenciados (MSSPs) são os guardiões da segurança cibernética para uma clientela vasta e

diversificada.

Em 2025, seu papel é mais crítico do que nunca, pois as empresas de todos os tamanhos enfrentam uma enxurrada cada vez mais sofisticada e implacável de ameaças cibernéticas.

A pedra angular de sua estratégia de defesa reside em soluções robustas de proteção de terminais, capazes de proteger os inúmeros desktops, laptops, servidores e pontos de extremidade móveis que formam a linha de frente da presença digital de uma organização.

Escolher a melhor proteção do ponto de extremidade para os MSPs é uma decisão complexa, exigindo uma solução que não apenas oferece recursos de segurança de ponta como Detecção de terminais e resposta (EDR) e detecção e resposta gerenciadas (MDR), mas também se alinham às necessidades operacionais e comerciais exclusivas dos provedores de serviços.

Isso inclui gerenciamento de multi-tenância, modelos de preços flexíveis e implantação e manutenção simplificadas.

Este artigo investiga as 10 melhores soluções de proteção de terminais para MSP/MSSPs em 2025, fornecendo uma análise aprofundada de suas capacidades, vantagens e considerações para os provedores de serviços que buscam fornecer segurança de endpoint de classe mundial a seus clientes.

Por que os MSPs/MSSPs requerem proteção de terminal especializada

As demandas feitas nas soluções de proteção de terminais para MSPs e MSSPs são distintas daquelas das implantações tradicionais da empresa:

Escalabilidade e multi-literidade: A capacidade de gerenciar e monitorar a segurança em vários ambientes de clientes de um único console unificado é fundamental.

Multi-literidade não é apenas um recurso; É um requisito fundamental para a eficiência operacional.

Facilidade de implantação e gerenciamento: Os MSPs geralmente lidam com implantações em diversas infra -estruturas com diferentes conhecimentos técnicos.

As soluções devem ser fáceis de implantar, configurar e gerenciar remotamente, minimizando a

necessidade de intervenção no local.

Preços flexíveis e econômicos: Os MSPs normalmente operam em modelos baseados em assinatura e precisam de soluções de proteção de terminais com preços flexíveis, por dispositivo ou por usuários que se alinham às suas ofertas de serviço e permitem lucratividade.

Pilha de segurança integrada: A proteção do endpoint deve se integrar perfeitamente com outros Serviços de segurança Oferecido pelo MSP/MSSP, criando uma postura de segurança coesa e abrangente para seus clientes.

Inteligência e resposta acionáveis ??de ameaças: A solução deve fornecer informações claras e acionáveis ??sobre as ameaças e facilitar a rápida resposta e remediação, geralmente remotamente, pela equipe de segurança do MSP.

As soluções destacadas abaixo foram avaliadas com base em sua capacidade de atender a essas necessidades críticas da comunidade MSP/MSSP em 2025.

Tabela de comparação: top 10 melhores soluções de proteção de terminais para MSP/MSSPs em 2025

1. Palo Alto Redes

Por que escolhemos:

O Cortex XDR se destaca por sua capacidade de correlacionar dados de várias camadas de segurança, fornecendo uma visão holística do paisagem de ameaças em toda a base de clientes de um provedor de serviços.

Essa abordagem unificada aumenta significativamente a precisão da detecção de ameaças e acelera os tempos de resposta a incidentes, cruciais para os MSPs que gerenciam vários ambientes diversos.

O portal de vários inquilinos foi projetado para gerenciamento eficiente e permite que os MSPs ofereçam serviços XDR sofisticados, agregando valor significativo às suas ofertas de segurança.

Especificações:

O Cortex XDR integra a proteção do terminal com dados de segurança de rede e nuvem para detecção e resposta estendidas.

Os principais recursos incluem análises comportamentais alimentadas por IA, análise de causa raiz automatizada, serviços de caça de ameaças gerenciados (XDR Pro) e um portal de vários inquilinos para MSPs com controle de acesso baseado em funções e gerenciamento de políticas centralizado.

Motivo para comprar:

Se você é um MSP/MSSP que procura oferecer recursos XDR avançados que fornecem uma visão unificada de ameaças entre pontos de extremidade, redes e nuvens, o Cortex XDR oferece uma plataforma poderosa e integrada.

Seus recursos de multiestação e automação foram projetados para otimizar operações e aprimorar o valor de seus serviços de segurança.

Características:

- **Detecção de camadas cruzadas:** Correlaciona dados de pontos de extremidade, redes e nuvens para uma visibilidade mais ampla de ameaças.
- **Análise de IA:** Usa o aprendizado de máquina para detectar ameaças sofisticadas e evasivas.
- **Análise de causa raiz automatizada:** Identifica rapidamente a origem e a propagação dos ataques.
- **Caçar ameaças gerenciadas (XDR Pro):** Serviço opcional, fornecendo uma caça proativa de ameaças por especialistas em redes Palo Alto.
- **Portal de vários inquilinos:** Gerenciamento simplificado de vários ambientes de clientes com controles granulares.

Prós:

- Recursos XDR abrangentes de um fornecedor de segurança líder.
- Detecção aprimorada de ameaças e resposta a incidentes mais rápida.
- Arquitetura de vários inquilinos projetada para MSPs.
- Oportunidades para oferecer serviços de segurança gerenciados de alto valor.

Contras:

- Pode ser uma solução mais complexa para implantar e gerenciar inicialmente.
- Pode exigir conhecimento especializado para aproveitar totalmente todos os recursos.

? Melhor para: MSPs/MSSPs buscando uma plataforma XDR abrangente para oferecer serviços avançados de detecção, investigação e resposta em diversos ambientes de clientes.

? Try Palo Alto Networks (Cor
tex XDR) here ? Palo Alto Networks Official Website

2. Crowdstrike Falcon

Por que escolhemos:

O design nativo da nuvem do Crowdstrike Falcon e o agente leve e único simplificam a implantação e o gerenciamento em vários pontos de extremidade, uma vantagem significativa para os MSPs.

Sua inteligência de ameaças líderes do setor, alimentada pelo gráfico de ameaça de crowdstrike, fornece visibilidade incomparável no cenário global de ameaças, permitindo a defesa proativa.

As APIs robustas da plataforma facilitam a integração perfeita com outras ferramentas e fluxos de trabalho MSP, aumentando a eficiência operacional.

Especificações:

O Crowdstrike Falcon oferece NGAV, EDR, Inteligência de Ameaças, Caça de Ameaças Gerenciadas (Falcon Overwatch) e gerenciamento de vulnerabilidades, todos entregues através de um único agente leve gerenciado por meio de um console em nuvem de vários inquilinos.

Possui ferramentas poderosas de pesquisa e investigação, bem como recursos de remediação automatizados.

Motivo para comprar:

Se o seu MSP/MSSP exigir uma plataforma de proteção de terminais nativos de alto desempenho e nuvem, com inteligência excepcional de ameaças e recursos de integração perfeita, o Crowdstrike Falcon é um dos principais candidatos.

Sua escalabilidade e conjunto de recursos robustos são adequados para proteger uma gama diversificada de ambientes de clientes.

Características:

- **Arquitetura nativa em nuvem:** Fornece escalabilidade, agilidade e facilidade de gerenciamento.
- **Agente leve e leve:** Simplifica a implantação e minimiza o impacto no ponto final.
- **Gráfico de ameaças de crowdstrike:** Rede global de inteligência de ameaças, fornecendo informações em tempo real.
- **Falcon Overwatch:** Serviço opcional de caça a ameaças gerenciadas para detecção proativa de ameaças.
- **APIs robustas:** Facilitar a integração com outras ferramentas MSP e fluxos de trabalho de automação.

Prós:

- Capacidades de detecção e resposta de ameaças líderes do setor.
- Agente leve com sobrecarga mínima de desempenho.
- Arquitetura em nuvem escalável para gerenciar vários clientes.
- Programa de parceiros forte e suporte para MSPs.

Contras:

- Pode ser uma das soluções de proteção de terminais mais caras.
- Alguns recursos avançados podem exigir conhecimentos especializados para aproveitar completamente.

? Melhor para: MSPs/MSSPs buscando uma plataforma EDR nativa de alto desempenho e nuvem, com inteligência de ameaças excepcionais e recursos robustos de integração.

? Try CrowdStrike Falcon here ? CrowdStrike Official Website

3. Sentinelone Singularity

Por que escolhemos:

A abordagem autônoma e orientada pela IA da SentineLone para a segurança reduz significativamente a dependência da detecção tradicional baseada em assinatura e permite a defesa em tempo real contra conhecidos e desconhecidos ameaças.

Sua plataforma unificada de singularidade fornece uma visão abrangente em várias superfícies de ataque, simplificando o gerenciamento para os MSPs.

Os poderosos recursos de automação e remediação da plataforma minimizam a necessidade de intervenção manual, aumentando a eficiência operacional para os provedores de serviços.

Especificações:

A SentineLone Singularity oferece proteção de carga de trabalho NGAV, EDR, XDR e nuvem de NGAV, XDR e nuvem através de um único agente e um console de gerenciamento unificado e multi-inquilino.

Os principais recursos incluem IA comportamental para prevenção de ameaças autônomas, caça às ameaças em tempo real e remediação automatizada com recursos de reversão.

Motivo para comprar:

Se o seu MSP/MSSP priorizar uma solução de segurança de terminal autônoma e autônoma que oferece proteção abrangente em várias superfícies de ataque e minimize a necessidade de intervenção manual, a SentineLone Singularity for uma escolha líder.

Seus recursos unificados de plataforma e automação são adequados para gerenciar ambientes de clientes complexos com eficiência.

Características:

- **Proteção autônoma de IA:** Prevenção em tempo real, detecção e resposta alimentada pela IA comportamental.
- **Plataforma de singularidade unificada:** Segurança abrangente em pontos de extremidade, nuvem, contêineres e IoT.
- **Agente único:** Simplifica a implantação e o gerenciamento em diversos ambientes.
- **Caça de ameaças em tempo real:** Ativa a identificação proativa de ameaças avançadas.
- **Remediação automatizada com reversão:** Contém e reverte automaticamente atividades maliciosas.

Prós:

- Prevenção e resposta de ameaças autônomas altamente eficazes.
- A plataforma unificada fornece ampla visibilidade e controle.
- Agente único simplifica a implantação e o gerenciamento.
- Forte foco na inovação e na segurança pronta para o futuro.

Contras:

- Os recursos avançados de IA podem ter uma curva de aprendizado mais acentuada.
- Os modelos de preços podem ser complexos, dependendo da escala e dos recursos necessários.

? Melhor para: MSPs/MSSPs que buscam uma plataforma de segurança de pontos de extremidade autônoma e alimentada por IA que fornece proteção abrangente e simplifica o gerenciamento em diversas superfícies de ataque.

`? Try SentinelOne Singularity here ?` SentinelOne Official Website

4. Sophos Intercept X

Por que escolhemos:

A Sophos Intercept X é a favorita entre os MSPs devido aos seus recursos abrangentes de segurança e ao console central de gerenciamento da Sophos, construído por propósitos.

Os recursos de aprendizado profundo da plataforma oferecem excelente proteção contra malware conhecido e desconhecido, enquanto sua tecnologia anti-ransomware criptograma oferece defesa robusta contra ataques de ransomware.

O recurso de segurança sincronizado, que se integra a outros produtos da Sophos, aprimora a visibilidade e a resposta de ameaças gerais.

Especificações:

A Sophos Intercept X oferece NGAV, EDR, anti-ransomware (CryptoGuard), prevenção de exploração e detecção de ameaças de aprendizagem profunda, todas gerenciadas pelo console central de vários inquilinos.

Ele fornece opções de licenciamento flexíveis e um forte programa de parceiros adaptados para MSPs.

Motivo para comprar:

Se o seu MSP/MSSP exigir uma solução abrangente e fácil de gerenciar de proteção contra pontos de extremidade, com um forte histórico e um programa de parceiro dedicado, o Sophos Intercept X é uma excelente opção.

Seu conjunto de recursos robustos e console de gerenciamento intuitivo simplificam as operações e fornecem segurança confiável para uma ampla gama de clientes.

Características:

- **Tecnologia de aprendizado profundo:** Prevenção de ameaças preditivas que identifica e

bloqueia malware conhecido e desconhecido.
- **CryptoGuard:** Anti-ransomware avançado que impede a criptografia de arquivo e relembra atividades maliciosas.
- **Explorar prevenção:** Bloqueia as técnicas usadas nos ataques de exploração.
- **Sophos Central:** Console de gerenciamento unificado e com vários inquilinos para todos os produtos da Sophos.
- **Segurança sincronizada:** Integra -se aos firewalls do Sophos para uma resposta aprimorada de ameaças.

Prós:

- Recursos de segurança abrangentes em um único agente.
- Console de gerenciamento intuitivo e robusto de vários inquilinos.
- Programa de parceiros forte com excelente suporte para MSPs.
- Eficácia comprovada contra uma ampla gama de ameaças, incluindo ransomware.

Contras:

- Pode ser mais caro do que algumas outras soluções.
- O grande número de recursos pode ser esmagador para MSPs ou clientes muito pequenos.

? Melhor para: MSPs/MSSPs que buscam uma solução abrangente e fácil de gerenciar de proteção para pontos de extremidade com um forte programa de parceiros e eficácia comprovada contra diversas ameaças.

`? Try Sophos Intercept X here ?` Sophos Official Website

5. Trellix

Por que escolhemos:

Trellix combina a extensa inteligência de ameaças e o legado de segurança de terminais de McAfee com a detecção avançada de ameaças e Resposta de incidentes Especialização de Fireeye.

Este sindicato cria uma poderosa plataforma de proteção de terminais capaz de abordar um amplo espectro de ameaças, do malware de commodities a sofisticados ameaças persistentes avançadas (APTs).

Para os MSPs, a Trellix oferece uma plataforma de gerenciamento de vários inquilinos e opções de licenciamento flexíveis para atender a diversas necessidades do cliente.

Especificações:

A Trellix Endpoint Security oferece NGAV, EDR, Endpoint Firewall e Ameak Intelligence, gerenciados por meio de um console de nuvem de vários inquilinos unificados.

As principais características incluem detecção de ameaças movidas a máquina, análise

comportamental, prevenção de exploração e feeds de inteligência de ameaças integrados.

Motivo para comprar:

Se o seu MSP/MSSP exigir uma plataforma abrangente de proteção de terminais apoiada pela experiência combinada e pela inteligência de ameaças de McAfee e FireEye, a Trellix oferece uma solução robusta.

Sua amplitude de recursos e recursos de gerenciamento de vários inquilinos são projetados para atender às diversas necessidades de segurança da sua base de clientes.

Características:

- **Experiência combinada:** Aproveita os pontos fortes de McAfee e Fireeye.
- **Segurança abrangente de endpoint:** Oferece o Firewall NGAV, EDR e Endpoint em um único agente.
- **Inteligência avançada de ameaças:** Ameaças integradas se alimentam de McAfee e Fireeye.
- **Aprendizado de máquina e análise comportamental:** Detecta ameaças conhecidas e desconhecidas.
- **Console em nuvem de vários inquilinos:** Gerenciamento centralizado para vários ambientes de clientes.

Prós:

- Ampla gama de recursos de segurança de dois fornecedores estabelecidos.
- Fortes recursos de inteligência e detecção de ameaças.
- Gerenciamento de vários inquilinos projetado para MSPs.
- Opções de licenciamento flexíveis.

Contras:

- A integração das duas plataformas herdadas está em andamento e pode ter complexidades.
- O reconhecimento da marca para Trellix ainda está se desenvolvendo.

? Melhor para: MSPs/MSSPs Procurando uma plataforma abrangente de proteção de terminais apoiada pelo legado e experiência combinados da McAfee Enterprise e Fireeye.

`? Try Trellix here ?` Trellix Official Website

6. Defender da Microsoft

Por que escolhemos:

Para MSPs e MSSPs com uma base de clientes investida fortemente no ecossistema Microsoft, o Microsoft Defender for Endpoint oferece uma solução de segurança poderosa e geralmente econômica.

Sua profunda integração com o Windows 10 e 11, juntamente com outros serviços de segurança da Microsoft, fornece uma experiência de segurança unificada e simplificada.

Embora o gerenciamento direto de multilocação tenha sido um desafio passado, a Microsoft fez avanços significativos ao permitir que os MSPs gerenciem vários inquilinos de clientes através do portal Microsoft 365 Lighthouse.

Especificações:

O Microsoft Defender for Endpoint oferece recursos de NGAV, EDR, ameaças e vulnerabilidades e recursos automatizados de investigação e resposta integrados ao sistema operacional Windows e gerenciados pelo portal do Microsoft 365 Defender (e do Microsoft 365 Lighthouse para MSPS).

Motivo para comprar:

Se o seu MSP/MSSP atender principalmente aos clientes profundamente entrincheirados no ecossistema da Microsoft, o Microsoft Defender for Endpoint oferece uma solução de segurança de endpoint poderosa, integrada e geralmente econômica.

A integração profunda simplifica a implantação e o gerenciamento nos ambientes da Microsoft.

Características:

- **Integração profunda do Windows:** Perfeitamente integrado ao sistema operacional.
- **Pilha de segurança abrangente:** Oferece NGAV, EDR e gerenciamento de vulnerabilidades.
- **Investigação e resposta automatizadas:** Investiga e remedia automaticamente ameaças.
- **Inteligência de ameaças da Microsoft:** Aproveita uma vasta rede global de inteligência de ameaças.
- **Microsoft 365 Lighthouse:** Fornece recursos de gerenciamento de vários inquilinos para MSPs.

Prós:

- Recursos de segurança poderosos e abrangentes.
- Integração profunda com o ecossistema da Microsoft.
- Frequentemente incluído nas assinaturas do Microsoft 365.
- Nenhuma instalação de agente separada necessária para o Windows 10/11.

Contras:

- Gerenciamento para pontos de extremidade não-Microsoft pode ser menos simplificado.
- O gerenciamento de multilocação através do Lighthouse, enquanto melhoria, pode não ser tão maduro quanto as plataformas dedicadas do MSP.
- O licenciamento pode ser complexo para navegar para MSPs.

? Melhor para: MSPs/MSSPs Gerenciando principalmente os clientes investidos fortemente no ecossistema da Microsoft, buscando uma solução de segurança de endpoint poderosa e integrada.

? Try Microsoft Defender here ? Microsoft Defender Official Website

7. Bitdefender GravityZone

Por que escolhemos:

O BitDefender GravityZone for MSPS se destaca por seu mecanismo de segurança altamente eficaz e de várias camadas que tem um bom desempenho em testes independentes.

Seu agente leve garante um impacto mínimo no desempenho nos pontos de extremidade dos clientes, um fator crucial para MSPs que suportam diversos ambientes de hardware.

O modelo de preços flexíveis e baseado em uso da plataforma e o console de nuvem centralizado e com vários inquilinos o tornam uma opção atraente e econômica para os provedores de serviços.

Especificações:

O BitDefender GravityZone for MSPS oferece NGAV, EDR, segurança avançada de ameaças e gerenciamento de riscos de endpoint, gerenciados por meio de um console em nuvem de vários inquilinos com licenciamento mensal flexível com base no consumo.

Motivo para comprar:

Se o seu MSP/MSSP priorizar uma solução de segurança de endpoint eficaz e de alto desempenho com uma pegada de baixo sistema e um modelo flexível de preços centrado no MSP, o BitDefender GravityZone for uma excelente opção.

Sua abordagem de segurança em camadas fornece proteção robusta sem afetar o desempenho do dispositivo do cliente.

Características:

- **Engine de segurança de alto desempenho:** Consistentemente ocupa alta em testes de segurança independentes.
- **Proteção de várias camadas:** Combina análise comportamental baseada em assinatura e avançada.
- **Agente leve:** Impacto mínimo no desempenho do terminal.
- **GravityZone Cloud Console:** Gerenciamento centralizado e multi-inquilino com controles granulares.
- **Licenciamento flexível do MSP:** Cobrança mensal baseada em uso.

Prós:

- Detecção de ameaças altamente eficaz com baixos falsos positivos.
- Impacto mínimo no desempenho do sistema.
- Modelo de precificação MSP flexível e econômico.
- Fácil de implantar e gerenciar através do console da nuvem.

Contras:

- Alguns recursos avançados podem exigir módulos ou conhecimentos adicionais.
- A interface do usuário, embora funcional, pode não ser tão moderna quanto alguns concorrentes.

? Melhor para: MSPs/MSSPs que buscam uma solução de segurança de endpoint leve e de alto desempenho com um modelo de preços flexível e amigável para MSP.

`? Try Bitdefender GravityZone here ?` `Bitdefender Official Website`

8. Proteção ESET

Por que escolhemos:

O ESET Protect é favorecido pelos MSPs por sua detecção de ameaças confiáveis, baixo impacto do sistema e recursos de gerenciamento altamente configuráveis.

A plataforma ESET Protect oferece um único painel de vidro para gerenciar a segurança em todos os pontos de extremidade do cliente, com controle granular sobre políticas e relatórios.

A reputação de longa data da Eset de Excelência em Segurança e seu programa MSP dedicado fornece uma base sólida para os prestadores de serviços.

Especificações:

O ESET Protect oferece recursos NGAV, anti-malware, anti-spyware, ransomware e EDR opcional, gerenciados através da plataforma de proteção de ESET baseada em nuvem.

Possui opções flexíveis de licenciamento, relatórios detalhados e gerenciamento robusto de políticas personalizado para MSPs.

Motivo para comprar:

Se o seu MSP/MSSP exigir uma plataforma de segurança altamente personalizável e confiável com uma pegada de baixo sistema e um gerenciamento robusto de vários inquilinos, o ESET Protect é um forte candidato.

Seu equilíbrio de eficácia e desempenho de detecção o torna adequado para uma ampla gama de ambientes de clientes.

Características:

- **Tecnologia de detecção comprovada:** Pontuações consistentemente altas em testes independentes.
- **Pedra de baixo sistema:** Impacto mínimo no desempenho do terminal.
- **Plataforma de proteção do ESET:** Console de gerenciamento centralizado e multi-inquilino.

- **Políticas altamente personalizáveis:** Controle granular sobre as configurações de segurança.
- **Programa MSP dedicado:** Suporte e recursos personalizados para provedores de serviços.

Prós:

- Detecção de ameaças confiável e eficaz.
- Agente leve com o mínimo de consumo de recursos.
- Plataforma de gerenciamento flexível e personalizável.
- Programa de parceiros e suporte ao MSP forte.

Contras:

- Às vezes, a interface do usuário pode parecer menos intuitiva do que as plataformas mais modernas.
- Os recursos avançados do EDR podem exigir configuração e experiência adicionais.

? Melhor para: MSPs/MSSPs buscando uma plataforma de segurança de terminais altamente personalizáveis ??e confiáveis ??com uma pegada de baixo sistema e um gerenciamento robusto de vários inquilinos.

? Try ESET Protect here ? ESET Official Website

9. Kaspersky

Por que escolhemos:

A Kaspersky Endpoint Security é reconhecida por seu mecanismo de detecção de ameaças poderoso e de várias camadas, protegendo efetivamente os pontos de extremidade em uma ampla gama de ameaças cibernéticas.

Seu conjunto abrangente de recursos, incluindo controle de terminais, controle da Web e avaliação de vulnerabilidades, fornece aos MSPs uma solução holística de segurança para seus clientes.

O programa de parceiros robustos da Kaspersky e o console de gerenciamento de vários inquilinos atendem especificamente às necessidades dos provedores de serviços.

Especificações:

A Kaspersky Endpoint Security oferece NGAV, EDR, endurecimento de endpoint, controle da Web e dispositivos, vulnerabilidade e gerenciamento de patches e gerenciamento de patches e Anti-Ransomware Recursos, gerenciados pelo Kaspersky Security Center Console, que suporta multi-cinemas para MSPs.

Motivo para comprar:

Se o seu MSP/MSSP exigir uma solução de segurança de terminais ricos em recursos, com uma

forte ênfase na detecção de ameaças e nos recursos abrangentes de controle do ponto de extremidade, a segurança do ponto final do Kaspersky é uma escolha sólida.

Seu conjunto de recursos robustos fornece uma abordagem holística para a proteção do terminal para diversos ambientes de clientes.

Características:

- **Forte detecção de ameaças:** Proteção de várias camadas contra uma ampla gama de ameaças.
- **Controle de terminais:** Gerencia o acesso ao dispositivo, o uso de aplicativos e a navegação na Web.
- **Vulnerabilidade e gerenciamento de patches:** Identifica e remedia vulnerabilidades de software.
- **Kaspersky Security Center:** Console de gerenciamento escalonável com suporte de multiestância.
- **Programa de parceiros robustos:** Oferece recursos e suporte dedicados ao MSPS.

Prós:

- Engine de detecção de ameaças altamente eficaz.
- Conjunto abrangente de recursos de segurança.
- Console de gerenciamento escalável para MSPs.
- Forte foco na segurança dos negócios.

Contras:

- Considerações geopolíticas podem ser uma preocupação para alguns clientes.
- O console de gerenciamento pode ser complexo para navegar inicialmente.

? Melhor para: MSPs/MSSPs que buscam uma solução de segurança de terminais ricos em recursos com forte detecção de ameaças e recursos abrangentes de controle do ponto de extremidade.

`? Try Kaspersky Endpoint Security here ?` [`Kaspersky Official Website`]

10. Trend Micro

Por que escolhemos:

Trend Micro Apex One fornece uma solução abrangente de segurança de terminais, com uma forte ênfase na prevenção e detecção de ameaças.

Sua abordagem de segurança em camadas, incorporando aprendizado de máquina, análise comportamental e proteção contra vulnerabilidades, oferece defesa robusta contra diversas ameaças.

As opções de implantação flexíveis de console multi-inquilino da plataforma atendem bem às

necessidades operacionais de MSPs gerenciando vários ambientes de clientes.

Especificações:

Trend Micro Apex One oferece NGAV, análise comportamental, prevenção de exploração, detecção e resposta de pontos de extremidade (EDR) e proteção de vulnerabilidades, gerenciados por meio de um console centralizado e multi-inquilino.

Ele fornece opções de implantação flexíveis (nuvem, local, híbrido) e um programa de parceiro robusto para MSPs.

Motivo para comprar:

Se o seu MSP/MSSP exigir uma plataforma abrangente de segurança de terminais com uma abordagem em camadas para prevenção e detecção de ameaças, juntamente com a implantação flexível e o gerenciamento de vários inquilinos, o Trend Micro Apex One é uma opção viável.

Sua amplitude de recursos e presença estabelecida no mercado de segurança tornam -a uma escolha confiável.

Características:

- **Abordagem de segurança em camadas:** Combina técnicas tradicionais de detecção de ameaças tradicionais.
- **Análise comportamental:** Detecta e bloqueia o comportamento malicioso.
- **Explorar prevenção:** Protege contra vulnerabilidades de software.
- **Detecção e Resposta do terminal (EDR):** Fornece recursos de visibilidade e resposta.
- **Gerenciamento de vários inquilinos:** Console centralizado para gerenciar vários clientes.

Prós:

- Conjunto abrangente de recursos de segurança.
- Opções de implantação flexíveis.
- Fortes capacidades de prevenção e detecção de ameaças.
- Fornecedor de segurança estabelecido e respeitável.

Contras:

- Às vezes, a interface do usuário pode parecer datada em comparação com as plataformas mais recentes.
- Os recursos de EDR podem não ser tão profundamente integrados quanto algumas soluções EDR construídas para propósitos.

? Melhor para: MSPs/MSSPs buscando uma plataforma abrangente de segurança de terminais com uma abordagem em camadas para prevenção de ameaças e opções flexíveis de implantação.

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

Conclusão

A seleção da solução ideal de proteção de terminais é uma decisão crítica para MSPs e MSSPs em 2025.

A escolha ideal não apenas fornecerá segurança robusta para seus clientes, mas também se alinhará com sua eficiência operacional, necessidades de escalabilidade e objetivos de lucratividade.

As 10 principais soluções destacadas neste artigo oferecem pontos fortes e capacidades exclusivos, desde o XDR abrangente do Cortex Palo Alto Redes até a agilidade nativa da nuvem do Falcon Crowdstrike, a IA autônoma da SentineLone e o design centrado no MSP da gravidade da gravidade e do softemcept X.

Por fim, a melhor solução de proteção de terminais para o seu MSP/MSSP dependerá de uma avaliação cuidadosa de suas necessidades específicas do cliente, experiência técnicaconsiderações orçamentárias e objetivos estratégicos.

Ao entender minuciosamente os recursos, benefícios e possíveis desvantagens de cada uma dessas plataformas líderes, os provedores de serviços podem tomar uma decisão informada que os capacitará a fornecer serviços excepcionais de segurança de endpoint e solidificar sua posição como parceiros de segurança cibernética no cenário de ameaças em evolução de 2025.