



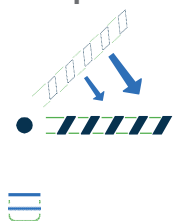
Impedindo o desconhecido e apanhando o conhecido.

Descubra o conjunto de segurança da próxima geração: Thor Premium Enterprise.

Apresentando EDR de próxima geração e detecção proativa autónoma, juntamente com uma base de código impecável, este poderoso pacote contém as camadas de segurança críticas para proteger sua organização neste cenário de ameaça.

Prevenção – Mitigação – Resiliência

A premiada suíte de segurança de várias camadas com recursos de próxima geração:



O Darklayer GUARD™ incluído, é tudo o que precisa para detecção e resposta (EDR) neste cenário, trazendo um bloqueio único de malware baseado em tráfego para evitar a infecção e eliminar o risco de perda de dados.



Com o módulo X-Ploit Resilience, sua organização pode ir além do Scm/Wsus com a ferramenta de implantação de políticas mais poderosa, flexível e intuitiva.

Você poderá obter uma visão geral incomparável e controlar seu inventário de software e, ao mesmo tempo, obter uma gestão preventiva de vulnerabilidades.

Com correção automática de vulnerabilidades, e instalação de updates de terceiros e da Microsoft, além de relatórios de inteligência essenciais,

O X-Ploit Resilience traz tudo em um só lugar, com controlos granulares para que você possa agir com precisão.

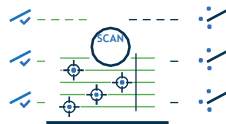


Com o módulo Infinity Management, os administradores de qualquer organização obtêm a capacidade exclusiva de implantar software e patches que não estão disponíveis no catálogo X-Ploit Resilience.

Thor Premium Enterprise oferece as camadas de segurança vitais para a sua organização, misturando técnicas de defesa de ameaças “next-gen” com um poderoso recurso de gestão de software que se integrará facilmente com as suas soluções existentes.



O VectorN Detection™, com a sua análise comportamental de tráfego ganha as ferramentas necessárias para antecipar ataques e mapear os pontos críticos de segurança da sua empresa.



Thor Vigilance, o módulo de detecção e correção de baixo custo e próxima geração da Heimdal Security usa técnicas conhecidas tanto pelos mecanismos antivírus tradicionais como os de próxima geração, para lhe fornecer a camada de segurança essencial.

O que torna este Antivírus verdadeiramente único é o nível incomparável de inteligência que ele usa para a avaliação de ameaças.

Trabalhando em conjunto, o Darklayer GUARD™ e o VectorN Detection™ fornecem indicadores de ataque, melhorando recursos locais e de análise de ameaças na nuvem..

Várias ferramentas de implantação criam confusão, abrandam o seu tempo de reação e abrem a sua empresa para malware e ataques ransomware.

99% VULNERABILIDADES EXPLORADAS

99% de vulnerabilidades exploradas serão conhecidos pela segurança e profissionais de TI por pelo menos um ano.

- Gartner

Software ultrapassado é o mais comum vetor de ataque. Deixa a sua organização exposta e podem resultar em infecções ransomware ou perda de dados críticos.

\$5 MILHÕES EM CUSTOS POR DANOS

\$5 Milhões – O custo médio de um único ataque de ransomware

- Ponemon Institute

3,785 PERDAS DE DADOS CORPORATIVAS

Em 2017, conforme registado no (IC3). Em média, acontecem 10 violações de dados diariamente.

- FBI

A gestão de vulnerabilidades não deve ser um jogo de “malucos”, nem o maior atraso nos seus fluxos de trabalho por ter soluções antiquadas e opacas.

Descubra o que significa ter controle sobre o seu ambiente e implantar o mais alto nível de resiliência cibernética

Principais produtos e inteligência

Avaliado pelo FBI, trabalhando com Europol e a USDOJ e endossado por NC3



Solução anti malware do ano



Em 2017, as empresas gastaram uma média de 2,4 milhões e 2 milhões para lidar com malware e ataques baseados na Web, respectivamente.

Estes são custos para detectar, recuperar, investigar e gerir a resposta a incidentes. Também são cobertos os custos que resultam de atividades pós-fato e esforços para reduzir a interrupção dos negócios e a perdas de clientes. Estes custos não incluem despesas e investimentos feitos para sustentar a postura de segurança de uma organização ou a conformidade com padrões, políticas e regulamentos.

-The Cost of Cyber Crime Study 2017, Ponemon Institute

Qual o seu gasto em comparação com estes números?

A natureza modular do Thor Premium Enterprise foi designado "Solução Anti Malware do Ano". Você pode implementar o pacote inteiro para segurança essencial de várias camadas, ou pode escolher os recursos que atualmente estão em falta na sua empresa.

Adicione a resiliência cibernética de última geração e a prevenção de ameaças ao seu ambiente, independentemente da sua configuração atual.

| Features | THOR FORESIGHT PROACTIVE | THOR VIGILANCE REACTIVE | THOR PREMIUM PROACTIVE REACTIVE | REGULAR ANTIVIRUS REACTIVE | REGULAR FIREWALL REACTIVE |
|--|-----------------------------|----------------------------|------------------------------------|-------------------------------|------------------------------|
| Unique Threat Prevention of the Most Advanced Ransomware Viruses, Spyware and APTs | ✓ | | ✓ | | |
| Traffic-based Malware Blocking (HIPS) | ✓ | | ✓ | | |
| Exploit & Dropper Blocking (HIPS) | ✓ | | ✓ | | |
| Attack Forensics & Source Identifier (IOAs, IOCs) | ✓ | | ✓ | | |
| Threat Hunting (EDR) | ✓ | | ✓ | | |
| Multi-layered, AI-Powered Protection | ✓ | | ✓ | | |
| Software/Asset/Patch Management | ✓ | | ✓ | | |
| Data Leakage Blocking | ✓ | | ✓ | | ✓ |
| Traffic-based Malware Detection (HIDS, IOAs, IOCs) | ✓ | | ✓ | | ✓ |
| Browser-based Protection | ✓ | | ✓ | | ✓ |
| Phishing Protection | ✓ | | ✓ | ✓ | ✓ |
| Firewall | | ✓ | ✓ | ✓ | ✓ |
| Next-Gen Antivirus | | ✓ | ✓ | ✓ | ✓ |
| * Local Signature / File-based Scanning | | ✓ | ✓ | ✓ | ✓ |
| * Real-time Cloud Scanning | | ✓ | ✓ | ✓* | |
| * Sandbox and Backdoor Inspection | | ✓ | ✓ | ✓* | |
| * Process / Behavior-based Scanning | ✓ | ✓ | ✓ | ✓* | |
| Lightweight Installation and Smooth Performance | ✓ | ✓ | ✓ | | |
| Very Easy to Use | ✓ | ✓ | ✓ | | |

Modules:

- ✓ EDR, proteção por código autônomo e inteligência crítica para evitar, não apenas mitigar ameaças. Darklayer GUARD™, a filtragem de ameaça única, e VectorN Detection™, o avanço chave alimentado por "machine learning" para proteção adaptativa contra malware de 2ª geração, são componentes-chave da Thor Foresight, trabalhando juntos para fornecer proteção por código autônomo contra malware e detecção ao longo de múltiplos vetores de ataque.

Detecção impecável, baseada em código e mitigação poderosa.

O Thor Vigilance, o antivírus da próxima geração, apresenta assinatura local e verificação baseada em arquivo para análise a pedido, análise em tempo real com detecção de "machine learning", análise em nuvem e inspeção em área restrita para detectar e bloquear ameaças em desenvolvimento, juntamente com análises heurísticas e baseadas em comportamento para detectar alterações de código e acionar alertas para atividades potencialmente mal-intencionadas.

- ✓ Gestão de vulnerabilidades, implantação de políticas personalizada. X-Ploit resiliência permite que a sua organização veja e gira o seu inventário de software e, ao mesmo tempo, uma gestão preventiva de vulnerabilidades. Esta escalável, flexível e intuitiva pode lidar com o software da Microsoft e de terceiros "on-the-fly", em qualquer lugar.
- ✓ Controle incomparável sobre o seu catálogo de software, com segurança na vanguarda. O módulo Infinity Management fornece aos administradores de qualquer organização a capacidade exclusiva de implantar software interno e patches que não estão disponíveis no catálogo X-Ploit Resilience.

Sua organização precisa de verdadeira resiliência cibernética contra ameaças conhecidas e desconhecidas.

Entre em contacto hoje para conhecer o nosso produto premiado e que módulo do Thor Premium Enterprise é mais ajustado para si?



Contact us at

+45 7199 9177

or

corpsupport@heimdalsecurity.com