K7 SECURITY

K7 ENDPOINT SECURITY

EDIÇÃO DE GRAFENO

A nova norma em
Proteção Empresarial contra Ransomware

As empresas modernas estão a lutar contra um malware cada vez mais potente, especialmente o ransomware, que pode perturbar gravemente as operações e até mesmo resultar em falência, e a sobrecarga de desempenho das soluções de segurança de terminais que tornam o hardware e as redes mais lentos, criando estrangulamentos operacionais e aumentando o custo da cibersegurança devido às atualizações da infraestrutura de IT necessárias para manter o desempenho das IT. O K7 Endpoint Security - Graphene resolve estes dois problemas, fornecendo um EDR proactivo e robusto sem quebrar os orçamentos.

O K7 Endpoint Security - Graphene foi especialmente criado com uma tecnologia com patente pendente para satisfazer os requisitos das operações obrigatórias e das indústrias de infraestruturas críticas que utilizam hardware de endpoint diversificado. O grafeno é um supermaterial que é 200 vezes mais forte do que o aço e 1000 vezes mais leve do que o papel, representando perfeitamente a proteção robusta do K7 que é leve em termos de hardware e recursos de rede.

Anti-Malware de Classe Empresarial

A K7 Security desenvolve soluções anti-malware para endpoints e servidores para pequenas, médias e grandes empresas, oferecendo uma vasta gama de funcionalidades e capacidades para combater as ameaças mais destrutivas da atualidade. Disponível nas edições Standard, Advanced, Advanced+ e Graphene, o Endpoint Security da K7 pode suportar vários modos de gestão centralizada (no local ou na nuvem) para simplificar a implementação, otimizar as operações de IT e cumprir os requisitos de conformidade internos e externos.

Tecnologia de Deceção Pendente com EDR Proativo

K7 Endpoint Security – Graphene combina a tecnologia Deception com patente pendente, desenvolvida pela K7, com o EDR proativo da K7 para antecipar, identificar e bloquear a próxima geração de ransomware antes que uma carga maliciosa possa ser implantada.

Proteção Remota contra Ransomware

O ransomware remoto, que os agentes de ameaças implantam em endpoints desprotegidos para atacar arquivos em pastas compartilhadas em endpoints protegidos, não pode ser detetado por soluções convencionais de segurança de endpoints. K7 Endpoint Security – O Graphene foi especialmente desenvolvido pela K7 para identificar e parar ransomware remoto e bloquear automaticamente o endpoint infetado desprotegido para proteger a infraestrutura de TI corporativa.

Proteção do Modo de Segurança

K7 Endpoint Security – A proteção antivírus e firewall do Graphene está ativada no Modo de Segurança (Apenas Rede, Apenas Mínimo, Rede e Apenas Mínimo), garantindo que o ransomware não pode infetar um ponto final iniciado no Modo de Segurança para executar diagnósticos.

Limpeza de entrada de inicialização de malware aprimorada

A estrutura de proteção proativa no K7 Endpoint Security – Graphene impede que ransomware e outros malwares sejam inicializados por meio de Entradas de Inicialização, Tarefas Agendadas e Assinatura de Eventos da Infraestrutura de Gerenciamento do Windows (WMI).

Configuração da Política Anti-Ransomware Estendida

Os administradores podem forçar os serviços de modo de usuário do K7 a iniciar muito cedo na ordem dos serviços com gerenciamento dinâmico de concessão de recursos ao sistema operacional, garantindo que o K7 proteja outros serviços durante a inicialização do dispositivo, economize tempo de varredura reduzindo a dupla verificação e inclua/exclua processos e alvos específicos do monitoramento de ransomware.

Principais características

- Proteção de terminais de baixo custo e alto desempenho e prevenção de ameaças cibernéticas para pequenas e médias empresas
- Detete e mitigue ameaças do mundo real, como vírus, spyware, ransomware e ataques de phishing
- Firewall granular com HIDS integrado para bloquear ataques direcionados no nível do dispositivo
- Proteção de acesso ao dispositivo contra ameaças de malware propagadas por USB
- O desempenho otimizado e a pequena pegada de memória prolongam a vida útil de dispositivos mais antigos
- Gerenciamento centralizado flexível local ou baseado em nuvem
- Criar e aplicar políticas consistentes de segurança de endpoint em desktops e servidores
- A Filtragem da Web permite o controlo centralizado e a aplicação granular do acesso ao Web site com base em categorias predefinidas, incluindo jogos, conteúdo relacionado com adultos, ferramentas de pirataria informática e muito mais
- Políticas centralizadas de controle de aplicativos bloqueiam aplicativos indesejados ou prejudiciais
- Relatórios complexos sobre aplicativos, dispositivos e ameaças relevantes para suas necessidades exclusivas de negócios podem ser gerados e extraídos nos formatos Excel e PDF
- O Enterprise Asset Management rastreia todos os ativos de hardware de endpoint na rede, gera relatórios e envia notificações sobre alterações
- O K7 Endpoint Security suporta um processo de migração sem esforço. Garantir uma transição sem complicações,
  K7 irá desinstalar qualquer produto existente e instalar-se automaticamente

K7 Sentry – On-access/On-demand Scans - A tecnologia de varredura on-access e on-demand identifica e bloqueia objetos de malware conhecidos e desconhecidos antes que eles afetem os sistemas.

Tecnologia de deteção heurística de malware – Complementando a deteção tradicional baseada em assinatura, a deteção heurística usa análise comportamental para identificar e bloquear proativamente malware desconhecido, além de explorações de dia zero.

Best-in-Class Ransomware Protection – proteção contra ransomware aprimorada por IA que monitora o comportamento de processos potencialmente suspeitos, com proteção avançada contra ransomware remoto.

K7 Firewall (HIDS/HIPS) – Proativamente Bloquear Ameaças - Firewall baseado em host com um Sistema de Deteção de Intrusão de Host (HIDS) integrado e Sistema de Prevenção de Intrusão de Host
(HIPS) protege contra ataques diretos no nível do aplicativo e do sistema.

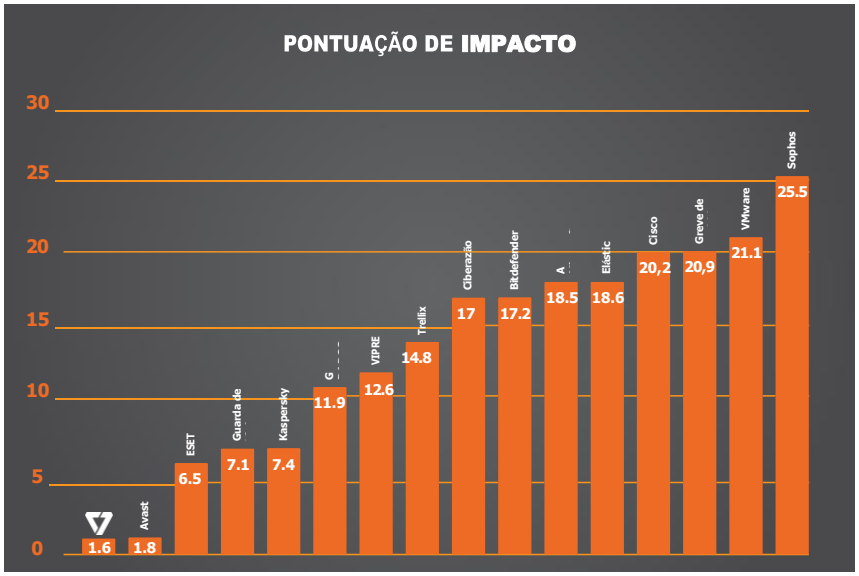
K7 SafeSurf – Navegação Online Segura - Proteja os endpoints de infeções por malware baseadas na Internet e ataques drive-by-download usando análise heurística de URL e serviços de reputação de sites baseados na nuvem para bloquear ameaças antes que cargas maliciosas possam ser implantadas.

K7 Device Control – Elimine a infeção por USB e mídia de armazenamento - Bloqueie o acesso a dispositivos de armazenamento USB desconhecidos e não autorizados que podem conter uma carga útil de malware.

K7 Application Control – Block Unauthorised Applications – Implemente uma política centralizada para controlar aplicações indesejadas instaladas em sistemas de terminais. Mensageiros instantâneos, clientes BitTorrent ou outros aplicativos com uso intensivo de largura de banda podem ser impedidos de executar, acessar a rede ou acessar a Internet.

K7 Web Filtering – Block Unauthorised Content – Definição centralizada de políticas e aplicação de restrições de acesso a conteúdos não autorizados ou impróprios. A filtragem da Web abrange milhares de sites predefinidos agrupados por categoria e bloqueados continuamente ou em horários agendados.

MENOR IMPACTO NO DESEMPENHO DO DISPOSITIVO



Comparação de recursos	Avançado	Grafeno
Detetar vírus, spyware e ataques de phishing	✓	✓
Proteção contra ransomware	✓	✓
Proteção Remota contra Ransomware	×	✓
Proteção do Modo de Segurança	×	✓
Tecnologia de Deceção	×	✓
Limpeza de entrada de inicialização de malware aprimorada	×	✓
Navegação segura (verificação de URL)	✓	✓
Proteção de e-mail	✓	✓
Firewall inteligente com HIDS/HIPS integrado	✓	✓
Gestão centralizada	✓	✓
Logs Intel de ameaças para integração de informações de segurança e gerir eventos ()	×	✓

A
n

Suporte à plataforma de segurança K7

Ponto final
Arquitetura de 32 e 64 bits*

- Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2003 (SP1 ou posterior), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022
- Suporte para Linux e Mac está disponível

Console do servidor
Arquitetura de 32 e 64 bits*

- Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022

Sobre o K7 Security

A K7 Security desenvolve soluções antimalware de terminais e servidores para pequenas, médias e empresas de classe empresarial, oferecendo uma ampla gama de recursos e capacidades para combater as ameaças digitais mais destrutivas da atualidade. O Endpoint Security do K7 pode suportar vários modos de gerenciamento centralizado para simplificar a implantação, agilizar as operações de IT e atender aos requisitos de conformidade internos e externos.

K7 SECURITY

O pioneiro global da cibersegurança

Índia | Singapura | Emirados Árabes Unidos | EUA

www.k7cybersecurity.ae

Março de