kaspersky 25 years

Kaspersky Optimum Security

Esteja adiante da curva em ameaças evasivas – com EDR[1]/ MDR[2] completo que não irá gastar seus recursos.

Kaspersky Optimum Security

30% dos ciberataques bem-sucedidos envolveram ferramentas de sistemas legítimas

Relatório de Análise de Respostas a Incidentes Kaspersky 2020

Desafio

Ransomware, malware e spyware financeiro todos se tornaram melhores em evadir a detecção e são fáceis e baratos de comprar na darkweb - criando uma perfeita tempestade para muitas organizações atualmente.

Os ataques avançados estão aumentando

As ameaças evasivas de hoje são projetadas para bypassar eficazmente a proteção tradicional de endpoint, trazendo novos riscos significativos para todas as empresas. Se uma ameaça não detectada criar raízes em sua infraestrutura, você poderá enfrentar perdas significativas que afetarão o desempenho da empresa:

- Interrupção de processos críticos da empresa e perda de dados
- danos significativos à reputação e perda de clientes
- multas, penalidades e lucros cessantes.

A proteção de endpoints deve ser fortalecida

Estes ataques mais recentes **evitam a detecção** ao se ocultar dentro de ferramentas de sistema legítimas e outros métodos e tecnologias prontamente disponíveis, os usando para **obter acesso, persistir e efetuar ações maliciosas dentro de sua infraestrutura de forma rápida e não detectada**

Então há o trabalho remoto, puttingendpoints – tradicionalmente a forma de entrada mais atrativa em sua infraestrutura – mais ainda em destaque.

E os recursos já são muito escassos como estão

Para fornecer a funcionalidade extra de que você agora precisa, sua organização precisa desenvolver capacidades adequadas de resposta aos incidentes.

Mas um projeto come este pode ter uma alto custo:

- os custos de software e hardware podem aumentar
- ferramentas e processos de segurança em silos e fragmentadas significam a erosão da eficiência da segurança
- muito tempo pode ser gasto em tarefas de rotina.

45% dos ataques foram detectados devido a arquivos suspeitos ou atividades suspeitas de endpoint - tornando sua detecção uma prioridade.

Como acima

A solução

O Kaspersky Optimum Security oferece uma solução eficaz de detecção e resposta à ameaças com o apoio de monitoramento de segurança ininterrupto, respostas automatizadas e busca de ameaças, junto com suporte e orientação de especialistas da Kaspersky.

Proteção ótima

Métodos de prevenção automáticos são a base de qualquer proteção de endpoints, mas eles deverão ser complementados por ferramentas avançadas se você quiser lidar com ameaças evasivas mais perigosas.

O Kaspersky Optimum Security oferece recursos de detecção avançada e resposta com base m **Aprendizado de Máquina** – todos fornecidos da nuvem. Sua equipe pode agora lidar até mesmo com ameaças que costumavam mantê-los acordados à noite, com velocidade e precisão.

Investimento ótimo

Você não precisa contratar mais pessoas, retreinar funcionários ou ficar sobrecarregado com implementações complicadas – o Kaspersky Optimum Security simplifica e ajuda a automatizar processos de resposta a incidentes cruciais – de acordo com seus requisitos específicos.

As opções no local e na nuvem e um conjunto de ferramentas prontas de segurança dimensionável se adaptam às suas necessidades, ajudando a manter baixa a complexidade de sistemas de TI, aumentar a produtividade do usuário e a implementação com custos transparentes.

Equilíbrio ótimo

Atinja o equilíbrio ideal entre simplificação e eficácia, inteligência humana e automação, eficiência e funcionalidade – sem arriscar a sua proteção!

O Kaspersky Optimum Security ajuda você a reduzir os riscos de perder dinheiro, clientes e a sua reputação e fortalece suas defesas contra ameças novas, desconhecidas e evasivas. Assim, você estará pronto para enfrentar o cenário de ameaças em rápida evolução dos dias de hoje.

Principais benefícios

- **Defenda a sua empresa contra o risco real de danos e interrupções** representado pela última onda de ameaças evasivas letais.
- **Desenvolva a sua própria capacidade de resposta a incidentes** com um conjunto de ferramentas de EDR (Detecção e Resposta em Endpoints) simples de usar.
- **Leve sua detecção ao próximo nível com facilidade -** através de um MDR (Detecção e Resposta Gerenciada) poderosa e livre de problemas).
- Diminua os riscos de infecção significativamente ao **treinar seus funcionários e conscientizá-los em segurança**
- Preserve recursos preciosos por meio da **automação de operações e proteção gerenciada.**
- Economize tempo e esforços com uma solução cujos diversos recursos são tosos gerenciados **em um único console na nuvem ou no local.**

55% dos ataques demoraram semanas ou mais sr detectados

Como acima

Principais recursos

O Kaspersky Optimum Security oferece uma ampla gama de recursos essenciais para proteção contra ameaças evasivas – no núcleo onde a detecção, análise e resposta residem.

Detecção avançada

- **Algoritmos de análise de comportamento com base em aprendizado de máquina** para expor de forma rápida e precisa comportamentos suspeitos
- **Buscas de ameaças automatizadas** com base em Indicadores de Ataque proprietários (IoAS) para encontrar ameaças complexas ocultas, tudo apoiado por especialistas da Kaspersky
- Controle de anomalias adaptativo **para ajustar automaticamente a configuração das ferramentas de redução da superfície de ataque** com base nos perfis de usuários
- Detecção na nuvem, incluindo uma **sandbox na nuvem incorporada**.

Análise direta

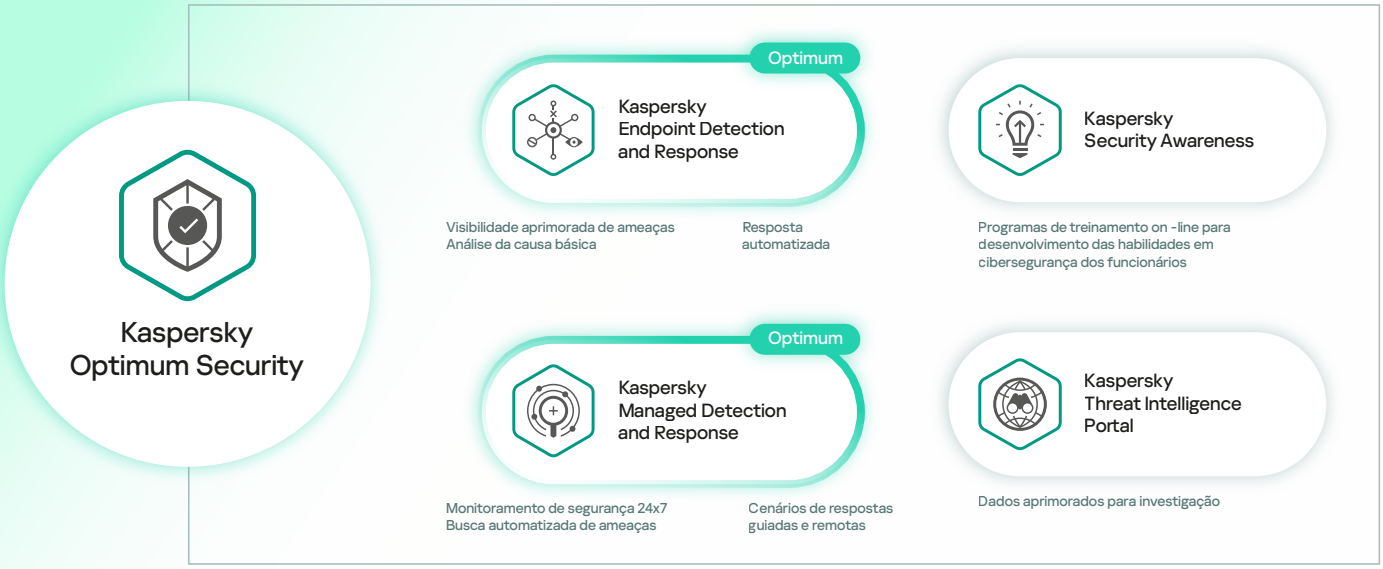
- Todas as informações pertinentes a um incidente são automaticamente reunidas em **um único cartão de incidente**.
- **A visualização e um processo de investigação simples** permitem que você analise de forma rápida e eficaz o incidente em um único ambiente e decida sobre um curso de ação adicional.
- Ao mesmo tempo, todas as detecções por Indicadores de Ataque são **priorizadas e investigadas pela Kaspersky para fornecer a você recomendações personalizadas**.

Resposta automatizada

- **A resposta com um "clique único"** permite conter rapidamente um incidente individual
- **A resposta guiada** com base na experiência de especialistas da Kaspersky significa que você pode lidar até mesmo com as ameaças mais perigosas e complexas
- **A resposta cruzada automatizada de endpoint** ajuda você a encontrar e responder a ameaças analisadas ou importadas em toda a rede

O que há dentro?

Você escolhe como usar o Kaspersky Optimum Security – como uma solução gerenciada para obter proteção ininterrupta, como um conjunto de ferramentas de EDR fácil de usar ou como uma mistura de ambos, aproveitando a experiência e o conhecimento de especialistas da Kaspersky ao desenvolver seus recursos de detecção e resposta internos. O Kasperky Optimum Security une vários produtos sob uma única solução:



Emails mal-intencionados fizeram parte de 31% dos ciberataques bem-sucedidos, o que significa que muitos deles poderiam ter sido evitados pelos próprios funcionários

Como acima

Mas espere, tem mais...

Você pode aprimorar ainda mais suas defesas com várias ferramentas voltadas para diferentes aspectos da segurança – detecção, investigação e conscientização.

Eduque seus usuários

A chave para reduzir a sua superfície de ataque e o número de incidentes é treinar seus funcionários para que conheçam as ameaças cibernéticas que podem ser desencadeadas em sua infraestrutura através de negligência ou de uma simples falta de conhecimento. **O Kaspersky Security Awareness** desenvolve o conhecimento e as habilidades necessários a todos os funcionários para que eles ajudem a proteger a sua infraestrutura e trabalhem ativamente com você para manter um ambiente cibernético seguro.

Obtenha as informações mais recentes

Ajude seus especialistas em cibersegurança a analisar e compreender ameaças de forma mais rápida e completa com as últimas informações sobre arquivos, hashes, IPs e URLs associados às ameaças. Obtenha essa percepção extra sem custo adicional no **Portal Kaspersky Threat Intelligence** fácil de usar.

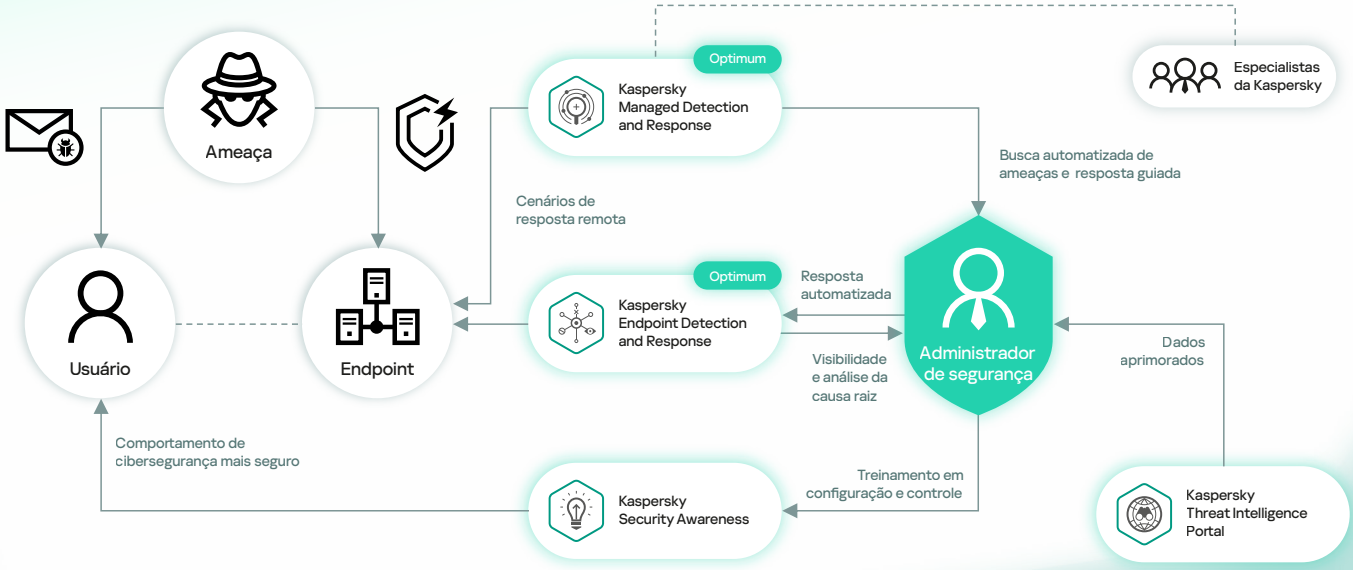
Nos permita ajudar-lhe

Para garantir uma proteção eficiente para sua infraestrutura de TI, você precisa implementar e configurar seus produtos de acordo com as melhores práticas e seus requisitos de segurança únicos.

Minimize o retorno sobre o investimento de sua solução de segurança e assegure qie esteja desempenhando em 100% de sua capacidade, ao deixar que nossos especialistas do **Kaspersky Professional Services** lhe ajudem a verificar a integridade, implementar, manter e otimizar sua solução de segurança.

Como isso tudo funciona em conjunto

A prevenção, detecção, análise, resposta e treinamento do funcionário estão todas unidas no Kaspersky Optimum Security. Qualquer componente traz seu próprio valor e pode ser suado separadamente, mas todos trabalham juntos para cobrir todas as necessidades de proteção evasiva de endpoint em uma única solução integrada.



4% das organizações veem o custo de assegurar ambientes complexos em crescimento como uma das principais questões

Relatório "IT security economics 2021", Kaspersky

Facilidade de operação

Você achará o Kaspersky Optimum Security simples de administrar por um único console, aproveitando ao máximo seu tempo e recursos limitados.

Pacote completo

- Parte do ecossistema de segurança da Kaspersky, desenvolvendo suas defesas de fundações de segurança para recursos avançados otimizados
- Os diversos recursos do Kaspersky Optimum Security podem ser gerenciados por meio de um único console em nuvem.
- Múltiplas camadas de proteção, abordam as ameaças às comodities e evasivas, assim como o risco de erro huamano.

Facilidade de gerenciamento

- Nosso console de gerenciamento na nuvem possibilita o controle rápido e eficiente de qualquer lugar do mundo
- Opções locais e no lacal e SaaS fornecem a mesma experiência administrativa.
- A implementação é rápida e sem complicações, não importa se você já usa ou não soluções da Kaspersky
- Todas as ferramentas podem ser controladas e gerenciadas de forma fácil e intuitiva, sem a necessidade de longos períodos de familiarização ou novos treinamentos

Economize tempo e recursos

- A proteção gerenciada lhe ajuda a desenvolver as capacidades de detecção e resposta sem níveis associados de investimento em segurança, mesmo que lhe falte equipe de cibersegurança ou especialização.
- Processos de cibersegurança cruciais são automatizados, tornando a resposta aos incidentes ainda mais rápida, precisa e eficiente.
- A melhor conscientização dos funcionários em segurança significa que menos ameaças penetrarão em suas defesas, gerando menos incidentes para você processar!

Na prática

Como tudo se junta na prática.

Testes de

O usuário recebe um e -mail de phishing ou acessa um recurso da Web malicioso, contaminando o seu host

- Conscientização dos funcionários sobre segurança
- Redução da superfície de ataque
- Prevenção automática de ameaças

Instalação

A infecção inicial implementa os componentes necessários, se comunica com o C&C [1] e explora as redondezas

- Mecanismos de detecção avançada, incluindo análise de comportamento com base em Aprendizado de Máquina e Sandbox na nuvem
- Busca automatizada de ameaças com IoAs[2]
- Cenários de respostas automatizadas guiadas e remotas

Rooting

Um conjunto de ferramentas é usado sistema para persistir e iniciar um movimento horizontal se necessário

- Análise da causa-raiz e verificação de IoC[3]

[1] Comando e controle
[2] Indicadores de ataque
[3] Indicador de comprometimento

Abordagem em estágios da Kaspersky

Juntos, podemos desenvolver suas defesas com base em proteção confiável com o Kaspersky Security Foundations, intensificar suavemente sua resposta essencial aos incidentes com o Kaspersky Optimum Security, além de, eventualmente, expandir a aplicação de ferramentas poderosas destinadas a oferecer proteção contra as ameaças mais avançadas com o Kaspersky Expert Security. Escolha o estágio certo para você:

Kaspersky Security Foundations

Bloqueie automaticamente a grande maioria das ameaças.

» Saiba mais

Kaspersky Optimum Security

Desenvolve suas defesas contra ameaças evasivas.

» Saiba mais

Kaspersky Expert Security

Disposição imediata para ataques complexos e semelhantes a APT.

» Saiba mais

Quem somos

Nós somos um empresa privada cibersegurança global com centenas de clientes e parceiro ao redor do mundo, comprometidos com a transparência e independência. Por 25 anos nós estamos desenvolvendo ferramentas e fornecendo serviços para mantê-lo seguro com nossas **tecnologias mais testadas e mais premiadas**.

IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprise e SMB 2021 Vendor Asseccinents

Principal atuante

AV-Test

Proteção Avançada de Endpointo: Teste de Proteção Conta Ransomware

100% de proteção

Radicati Group

Quadrante de mercado de ameaças persistentes avançadas (APT)

Principal atuante

Examine mais de perto

Para saber mais sobre como o Kaspersky Endpoint EDR Optimum enfrenta ameaças cibernéticas e facilita a vida da sua equipe de segurança e dos seus recursos, visite https://www.kaspersky.com/enterprise-security/edr-security-software-solution

[1] Detecção e Resposta de Endpoint
[2] Detecção e Resposta Gerenciada

Notícias sobre ciberameaças: securelist.lat
Notícias sobre segurança de TI: business.kaspersky.com
Segurança de TI para PMEs: kaspersky.com.br/business
Segurança de TI para Grandes Empresas: kaspersky.com.br/enterprise

www.kaspersky.com

© 2022 AO Kaspersky Lab.
As marcas registradas e de serviço pertencem aos seus respectivos proprietários.