kaspersky BRING ON THE FUTURE

Kaspersky Optimum Security

Atinja o nível ideal de cibersegurança com proteção gerenciada e detecção e resposta de endpoint habilitadas na nuvem

O desafio

Você precisa defender a sua empresa de forma eficaz contra ameaças novas, desconhecidas e evasivas sem sobrecarregar seus recursos e tempo limitados.

30% dos ciberataques bem-sucedidos envolveram ferramentas legítimas do sistema[1]

Os ataques avançados estão aumentando

As ameaças evasivas atuais, criadas para contornar de forma eficaz a proteção de endpoints tradicional, representam riscos mais significativos para as empresas agora que os ataques estão se tornando mais difíceis de detectar, analisar e responder. Se uma ameaça não detectada criar raízes em sua infraestrutura, você poderá enfrentar perdas significativas que afetarão o desempenho da empresa:

- interrupção de processos de negócios críticos
- danos significativos à reputação e perda de clientes
- multas, penalidades e lucros cessantes.

A proteção de endpoints deve ser fortalecida

Os ataques evasivos atuais tornaram-se muito mais eficazes. Os criminosos usam ferramentas legítimas do sistema, além de outros métodos e tecnologias prontamente disponíveis, para obter acesso, persistir e agir de forma mal-intencionada, mais rápida e sem serem detectados dentro da sua infraestrutura.

Essa situação é ainda mais exacerbada com a dissolução do perímetro e a expansão do trabalho remoto, o que coloca os endpoints – tradicionalmente, as entradas mais atraentes para a sua infraestrutura – ainda mais em destaque.

E os recursos já são muito escassos como estão

Para fornecer a vantagem a mais que a segurança de endpoints agora requer, recursos adequados para resposta a incidentes precisam ser desenvolvidos dentro da sua organização.

Mas os custos associados a um projeto como esse podem rapidamente sair do controle:

- 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.

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.

45% dos ataques foram detectados devido a arquivos suspeitos ou atividades de endpoints suspeitas[1]

Proteção avançada contra ameaças

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 ameaças novas, desconhecidas e evasivas. Assim, você estará pronto para enfrentar o cenário de ameaças em rápida evolução dos dias de hoje.

Solução pronta, rápida e dimensionável

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 rápida – todos fornecidos via nuvem. Seus engenheiros de cibersegurança podem agora lidar até mesmo com ameaças que costumavam mantê-los acordados à noite, com velocidade e precisão.

Níveis de investimento ideais

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

Ele se adapta às suas necessidades com opções locais e na nuvem e um conjunto de ferramentas de segurança prontas e dimensionáveis que ajudam você a diminuir a complexidade do sistema de TI, manter elevada a produtividade dos usuários e manter os custos de implementação transparentes.

Principais benefícios

- Fique à frente da concorrência e 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
- Riscos de infecção significativamente menores ao treinar seus funcionários e conscientizá-los em segurança
- Preserve recursos importantes por meio da automação de operações e funcionalidade gerenciada
- Economize tempo e esforços com uma solução cujos diversos recursos são gerenciados em um único console em nuvem ou local

Principais recursos

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

55% dos ataques levaram semanas ou mais para serem detectados[1]

Detecção avançada

- Algoritmos de análise de comportamento baseados em machine learning para expor de forma rápida e precisa comportamentos suspeitos
- Buscas de ameaças automatizadas com base em Indicadores de Ataque proprietários para encontrar ameaças complexas ocultas – com suporte de especialistas da Kaspersky
- Controle de anomalias adaptativo para ajustar automaticamente a configuração das ferramentas de redução da superfície de ataque para perfis de usuários

Investigação simplificada

- Todas as informações pertinentes a um incidente serão automaticamente reunidas em uma única ficha 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 endpoints ajuda você a encontrar e responder a ameaças analisadas ou importadas em toda a rede

Como aplicá-las

Como o Kaspersky Optimum Security inclui várias ferramentas e recursos avançados que juntos podem efetivamente ser usados para prevenir, detectar e responder a ameaças em vários estágios de um ataque:

Penetração

O usuário recebe um email de phishing ou acessa um recurso da Web mal-intencionado, contaminando seu host

Instalação

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

Rooting

Um conjunto de ferramentas é usado, incluindo ferramentas legítimas e nativas do sistema, para persistir e iniciar um movimento horizontal se necessário

Conscientização sobre segurança dos funcionários

Mecanismos de detecção avançados, incluindo análise comportamental baseada em machine learning e sandbox

Redução da superfície de ataque

Busca de ameaças automatizada com IoAs[2]

Análise de causa-raiz e varredura de IoC[3]

Prevenção de ameaças automática

Cenários de respostas guiadas e remotas

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

Mais proteção

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

Emails mal-intencionados fizeram parte de 31% dos ciberataques bem-sucedidos, o que significa que muitos deles poderiam ter sido evitados pelos próprios funcionários[1]

Camada de detecção adicional

Exponha ameaças novas e desconhecidas de forma ainda mais rápida e confiável com o **Kaspersky Sandbox** – analisando ameaças automaticamente em um ambiente isolado, usando algoritmos de detecção patenteados e técnicas antievasão. Respostas configuradas são aplicadas automaticamente às ameaças descobertas, aumentando significativamente seus recursos de detecção sem necessitar de qualquer gerenciamento além da implantação inicial.

Vantagens adicionais em investigações

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 ajuda extra sem custo adicional no **Kaspersky Threat Intelligence Portal** fácil de usar.

Pessoas são a chave para a sua segurança

A chave para reduzir a sua superfície de ataque e o número de incidentes é treinar seus funcionários para que conheçam 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.

Como ele funciona

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:

Kaspersky Security Awareness
Programas de treinamento online para desenvolver as habilidades em segurança cibernética dos funcionários

Kaspersky Endpoint Detection and Response Optimum
Visibilidade de ameaças aprimorada
Análise de causa-raiz
Resposta automatizada

Kaspersky Managed Detection and Response Optimum
Monitoramento de segurança ininterrupto
Busca de ameaças automatizada
Cenários de respostas guiadas e remotas

Kaspersky Sandbox
Detecção automática de ameaças evasivas melhorada

Kaspersky Threat Intelligence Portal
Dados avançados para investigação

Em operação

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

56% dos participantes disseram que suas organizações estão em risco devido à escassez de funcionários de cibersegurança[2]

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
- Uma solução com várias camadas de proteção, abordando ameaças evasivas e de commodity, bem como oportunidades para erros humanos

Facilidade de gerenciamento

- O console de gerenciamento na nuvem possibilita o controle rápido e eficiente de qualquer lugar do mundo
- Opções locais e na nuvem fornecem a mesma experiência administrativa
- A implantação é rápida e sem complicações, não importa se você já usa ou não soluções 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 ajuda organizações com falta de profissionais ou conhecimento em segurança de TI a desenvolver recursos de detecção e resposta sem investimentos associados à segurança
- Processos de cibersegurança cruciais são automatizados, tornando a resposta a 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!

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 a 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

- Prevenção automatizada multivetor de incidentes causados por ameaças de commodity – a grande maioria dos ciberataques.
- O estágio base para organizações de qualquer tamanho e complexidade no desenvolvimento de uma estratégia de defesa integrada
- Proteção de endpoints confiável para quem tem equipes de TI pequenas e pouca experiência em segurança

Kaspersky Optimum Security

Desenvolvimento de defesas contra ameaças evasivas para aqueles que:

- Têm uma equipe de segurança de TI pequena com conhecimento básico em segurança cibernética
- Têm um ambiente de TI que está crescendo em tamanho e complexidade, aumentando a superfície de ataque
- Enfrentam uma falta de recursos de cibersegurança – em contraste com uma necessidade de melhor proteção
- O desenvolvimento de capacidade de resposta a incidentes tem se tornado cada vez mais importante

Kaspersky Expert Security

Prontidão para ataques complexos e do tipo APT onde:

- Os ambientes de TI são complexos e distribuídos
- A equipe de segurança de TI é madura ou um Centro de Operações de Segurança (SOC) foi estabelecido
- A propensão a riscos é baixa devido a custos mais altos de incidentes de segurança e violações de dados
- A conformidade regulatória é uma preocupação

Para obter mais informações sobre como o Kaspersky Optimum Security aborda ameaças cibernéticas ao mesmo tempo que alivia a sua equipe e os recursos de segurança, visite: http://go.kaspersky.com/optimum.

1 Relatório de Análise de Respostas a Incidentes Kaspersky 2019, Kaspersky, 2020
2 (ISC)2 Estudo sobre Mão de Obra de Cibersegurança, (ISC)2, 2020

Notícias sobre Ciberameaças: www.securelist.com
Notícias sobre Segurança de TI: business.kaspersky.com

www.kaspersky.com.br