kaspersky

Kaspersky Security for Enterprise

Sobre o Portfólio Empresarial da Kaspersky

Criar uma base de segurança para sua empresa escolhendo o produto ou serviço certo é o primeiro passo. Mas desenvolver uma estratégia de cibersegurança corporativa com visão de futuro é fundamental para o sucesso a longo prazo.

O Portfólio Empresarial da Kaspersky reflete as demandas de segurança das empresas atuais, respondendo às necessidades de organizações em diferentes níveis de desenvolvimento com uma abordagem passo a passo. Essa abordagem combina diferentes camadas de proteção contra todos os tipos de ameaças cibernéticas para detectar ataques mais complexos, responder de forma rápida e adequada a qualquer incidente e impedir futuras ameaças.

O papel da segurança de endpoints no planejamento a longo prazo

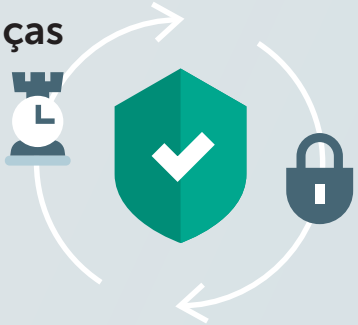
Processo tradicional de evolução de seguranças

Tomada de decisão

- Tendências de mercado
- Solução de segurança em silos
- Abordagem 'Apagar incêndios'
- Orientada à conformidade

Aproveitando produtos tradicionais:

- EPP
- Firewalls/NGFW
- Firewalls de Aplicações Web Prevenção
- de Perda de Dados
- SIEM

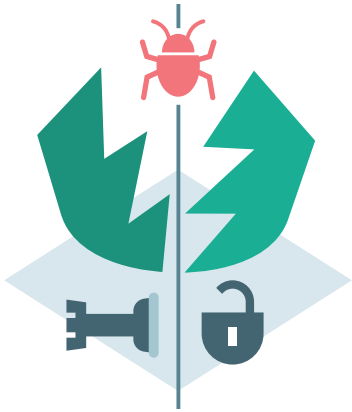


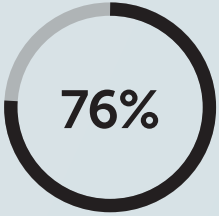
Atributos

- Planejamento de segurança a curto prazo
- Confiança em tecnologias e recursos
- Defesa de rede baseada em perímetro

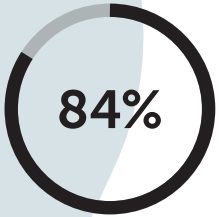
Por que as abordagens tradicionais falham

- Crescente complexidade das ameaças e o cenário de ameaças Complexidade das
- tecnologias de cibersegurança
- Necessidades da empresa de uma estratégia de cibersegurança a longo prazo





De todos os alertas são gerados por endpoints



De todas as violações de endpoint envolvem mais de um endpoint

Os endpoints são os pontos de entrada mais comuns na infraestrutura de uma organização, o principal alvo dos cibercriminosos e as principais fontes de dados necessários para a investigação eficaz de incidentes complexos.

3 passos de um plano avançado de cibersegurança para empresas

2

Ameaças avançadas e ataques direcionados

Defesa avançada

Focar na detecção avançada e resposta rápida às ameaças complexas perdidas pela proteção preventiva.

Endpoints

Kaspersky Endpoint Detection and Response

Serviços

Kaspersky Targeted Attack Discovery Service

1

Cenário mais amplo de ameaças

Bases de segurança

Fortalecer sistemas e bloquear o máximo número possível de ameaças de forma automática.

Endpoints

Kaspersky Endpoint Security for Business

Kaspersky Embedded Systems Security

Network

Kaspersky Secure for Mail Server

Kaspersky Security for Internet Gateway

3

Campanhas direcionadas e armas cibernéticas

Abordagem integrada de cibersegurança

Prontidão para ataques em nível de APT. Alto nível de especialização, recursos avançados de inteligência contra ameaças e caça permanente a ameaças.

Kaspersky Threat Management & Defense

Rede

Kaspersky Anti Targeted Attack

Inteligência

Kaspersky Threat Intelligence

Pessoas

Kaspersky Cybersecurity Training

Privacidade

Kaspersky Private Secutity Network

Nuvem

Kaspersky Hybrid Cloud Security

Suporte

Kaspersky Premium Support and Professional Services

Dados

Kaspersky Security for Storage

Pessoas

Kaspersky Security Awareness

4 benefícios desta abordagem para a empresa

Forma a base para o desenvolvimento de uma estratégia de cibersegurança a longo prazo, levando em conta as especificidades do negócio e as tendências no cenário de ameaças.

Investimento otimizado em tecnologia de segurança e redução de TCO.

Danos financeiros e operacionais reduzidos causados pelo cibercrime.

Maior ROI pela automatização integrada do fluxo de trabalho e não interrupção dos processos de negócios.

1 Bases de segurança

Tecnologias de automatizadas de prevenção e conscientização sobre segurança

Bloquear o máximo número possível de ameaças

Ideal para empresas menores que não têm equipe de segurança dedicada ou com experiência muito limitada em cibersegurança

- Prevenção automatizada multivetor de um grande número de possíveis incidentes causados por ameaças a commodities
- O passo fundamental para empresas de médio a grande porte na criação de uma estratégia de defesa integrada contra ameaças complexas

Endpoints

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Nuvem

- **Kaspersky Hybrid Cloud Security**

Rede

- **Kaspersky Secure Mail Gateway**
- **Kaspersky Security for Internet Gateway**

Pessoas

- **Kaspersky Security Awareness**

Dados

- **Kaspersky Security for Storage**

Suporte

- **Kaspersky Premium Support**
- **Kaspersky Professional Services**

Kaspersky Endpoint Security for Business

A maioria dos ataques cibernéticos contra empresas começa em um endpoint. Capacidades limitadas de prevenção e automação resultam em especialistas sobrecarregados com incidentes de segurança. Cada endpoint tem o potencial de se tornar a principal causade interrupção de negócios; o Kaspersky Endpoint Security para Empresas impede ameaças e fortalece os endpoints, combinando a segurança adaptativa com ferramentas de controle estendidas. As ameaças são bloqueadas antes que possam danificar os dados ou prejudicar a produtividade do usuário, mesmo quando o endpoint não está dentro do perímetro corporativo.

Ideal para

Empresas cujas expectativas de TI estão crescendo e se diversificando
Empresas que querer reduzir as oportunidades e a frequência de erros de usuários que levam a violações de segurança

Business benefits

Prevents business interruption and human error

Supports digital transformation and secures mobile workforces

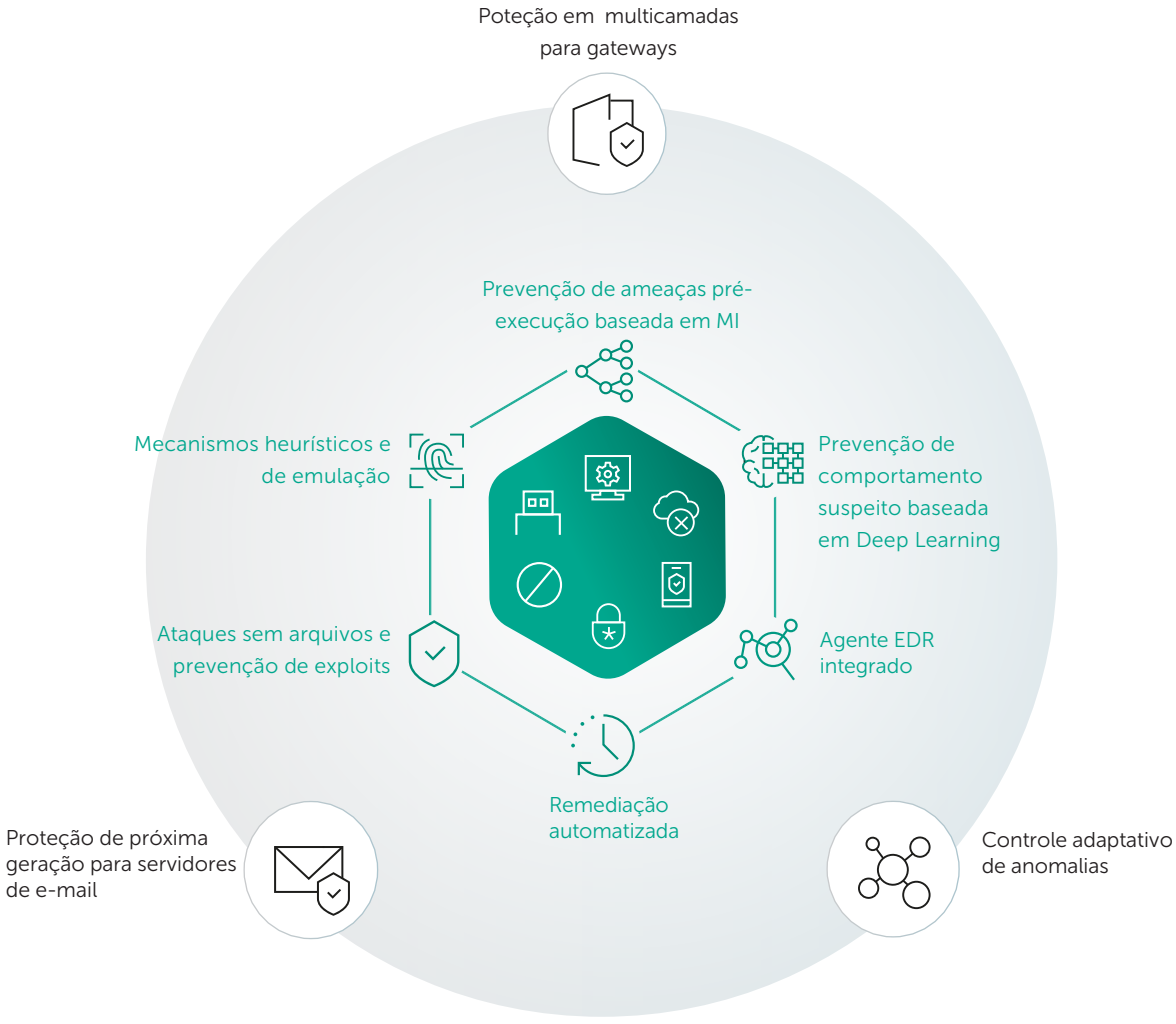
Improves audit-readiness – hunts and fixes vulnerabilities, 'configuration drift', and unencrypted devices

Maximizes ROI by reducing the attack surface and the number of incidents to manage

Enables control of every endpoint, thanks to an integrated console and unified agent

Casos de uso

- Reduz a exposição ao ataque aplicando proteção adaptativa, protegendo endpoints, servidores de e-mail e arquivos e gateways de internet
- Garante a conformidade dos endpoints com os requisitos regulatórios
- Automatiza tarefas de detecção, resposta e implantação de software, liberando tempo dos especialistas em segurança
- Simplifica a integração e adoção de outras tecnologias de segurança


Poteção em multicamadas
para gateways
Prevenção de ameaças pré-
execução baseada em MI
Mecanismos heurísticos e
de emulação
Prevenção de
comportamento
suspeito baseada
em Deep Learning
Ataques sem arquivos e
prevenção de exploits
Agente EDR
integrado
Remediação
automatizada
Proteção de próxima
geração para servidores
de e-mail
Controle adaptativo
de anomalias

Kaspersky Hybrid Cloud Security

O Hybrid Cloud Security é a solução que simplificae protege a transformação digital, à medida que as organizações virtualizam ou transferem cargas de trabalho para a nuvem. A tecnologia patenteada Light Agent permite a centralização e a otimização inteligente das funções de segurança, diminuindo de forma significativa o uso de recursos do hypervisor. A integração nativa com uma ampla variedade de plataformas de virtualização, contêiner e nuvem pública fornece visibilidade e controle consistentes em toda a infraestrutura. Um pacote completo de tecnologias de segurança gerenciadas a partir do mesmo consogarante a gestão simplificada de riscos em diversos ambientes no dia a dia.

Ideal para

Empresas que virtualizam cargas de trabalho de servidor e desktop
Empresas que estão transferindo ou mantêm infraestruturas em nuvens públicas
Empresas aproveitando nuvens públicas e contêineres para DevOps

Benefícios para a empresa

Garante visibilidade e controle consistentes em implantações de datacenter e nuvem

Reduz a superfície de ataque e o tempo de permanência, complicando o movimento lateral

Libera até 30% dos recursos do hypervisor e reduz o tempo de login de minutos para segundos

Oferece suporte à conformidade

Garante eficiente colaboração entre as equipes de TI, Segurança da Informação e Desenvolvimento, reduzindo os riscos e as falhas de segurança

Casos de uso

- Proteção cautelosa de recursos para infraestruturas de servidores virtualizados
- Segurança para VMWare e Citrix VDI
- Permite conformidade, atendendo aos principais requisitos de segurança
- Proteção de carga de trabalho na nuvem para instâncias da AWS e do Azure com implantação automatizada e visibilidade consistente por meio da integração nativa de API

Kaspersky Security for Mail Server

O Kaspersky Security for Mail Server protege contra ameaças baseadas em e-mail, impedindo que elas atinjam o endpoint em que a maioria das engenharias sociais e malwares atuam. Todos os tipos de malware, incluindo ransomware e mineradores, são bloqueados, além de tentativas de phishing, com especial atenção para a prevenção do Comprometimento de E-mail Corporativo. A solução também bloqueia malas diretas indesejadas e impede transmissões de dados suspeitas.

Ideal para

Qualquer empresa com TI bem desenvolvidae preocupações com privacidade e segurança de dados

Qualquer empresa que dependa muito de comunicações por e-mail e exija gerenciamento granular

Empresas que querem enriquecer seus dados de detecção APT com contexto de e-mail e bloquear componentes APT enviados por e-mail

Benefícios para a empresa

Aumenta a produtividade, bloqueando malas diretas indesejados

- incluindo spam - e oferecendo categorias de e-mail para gerenciamento mais conveniente de comunicações

Ajuda a impedir a interrupção de negócios, bloqueando ameaças baseadas em e-mail

Aumenta a segurança de dados, impedindo a transferência de tipos de dados indesejáveis

Ajuda a diminuir as despesas gerais de serviço, reduzindo os incidentes em nível de usuário

Aumenta a eficiência da segurança do atual gateway de correio, incluindo recursos de detecção mais avançados, sem adicionar falsos positivos

Casos de uso

- Funciona com uma ampla variedade de Agentes de Transferência de E-mail externos ou como um dispositivo virtual multifuncional.
- Oferece segurança de e-mail integrada à API para servidores Microsoft Exchange, operando em níveis de gateway e de caixa de correio
- Bloqueia a transferência de tipos de arquivos indesejáveis
- Integra-se ao Kaspersky Anti Targeted Attack para bloquear componentes do APT transmitidos por e-mail

Kaspersky Security for Internet Gateway

O Kaspersky Security for Internet Gateway oferece proteção contra ameaças baseadas na Web no níveldo perímetro de defesa corporativo, impedindo-as de atingir o principal alvo final de todas as formas de ataque: o endpoint. A solução ajuda a evitar ataques baseados em engenharia social e bloqueia todos os tipos de malware, incluindo ransomware e mineradores,além de tentativas de phishing. Combine com seu atual proxy corporativo para melhor desempenho ou implante como um dispositivo virtual multifuncional pronto para ser usado.

Ideal para

Qualquer empresa com TI desenvolvida e com preocupações sobre privacidade e segurança de dados

MSPs e xSPs (incluindo provedores de telecomunicações)

Benefícios para a empresa

Evita a interrupção de negócios, bloqueando ameaças baseadas na Web antes que alguém clique e permita que elas entrem
Aumenta a eficiência da atual segurança de gateway da web, incluindo recursos de detecção mais avançados, sem adicionar falsos positivos

Ajuda a diminuir as despesas gerais de serviço, reduzindo os incidentes em nível de usuário

Aumenta a produtividade e reduz os riscos, controlando o uso da Internet e a transmissão de tipos de arquivo específicos

Use cases

- Bloqueia recursos da Web maliciosos e de phishing, e malwares baixados
- Impede o uso de recursos indesejados da Web
- Permite o gerenciamento de espaços de trabalho separados com seus próprios conjuntos de regras
- iltra os tipos de arquivos indesejados que trafegam nos dois sentidos, com base em diversos critérios
- Integra-se ao Kaspersky Anti Targeted Attack como um sensor da Web e bloqueia os componentes de ataques direcionados, de acordo com os resultados avançados de detecção

Kaspersky Security for Storage

O armazenamento conectado de fácil acesso pode prontamente se tornar uma fonte de infecção em toda a infraestrutura e um alvo de ameaças, como ransomware. O Kaspersky Security for Storage protege os dados corporativos e evita o contágio da rede com um sólido pacote de tecnologias de proteção alimentadas pela inteligência global contra ameaças. Inclui recursos exclusivos, como anticriptografia remota, ativados pela integração com APIs do sistema de armazenamento.

Ideal para

Qualquer empresa com TI desenvolvida e preocupações sobre privacidade ou segurança de dados
Empresas como bancos, comércio eletrônico e seguros, que trabalham com grandes volumes de dados confidenciais/privados

Benefícios para a empresa

Protege os dados na conexão de armazenamentos, sem invadir o software de armazenamento
Reduz os problemas administrativos e aumenta a segurança graças a um console de gerenciamento com ponto único de visualização
Preserva a continuidade dos negócios, mantendo os dados armazenados protegidos contra ransomware e limpadores de criptografia de execução remota
Dá suporte à conformidade, oferecendo segurança para uma ampla variedade de modelos que podem ser usados como armazenamento regulamentado

Casos de uso

- Protege os armazenamentos conectados em rede e o servidor em que é executado
- Sempre que um novo arquivo é exibido no armazenamento seguro ou um arquivo existente é alterado, é verificado se são maliciosos. Também são possíveis verificações sob demanda
- Quando arquivos começam a ser criptografados de longe, a solução detecta e bloqueia a origem na rede, evitando mais danos*

* Apenas com integração de API disponível para alguns armazenamentos

Kaspersky Embedded Systems Security

Com avançada inteligência contra ameaças, detecção de malware em tempo real, controles abrangentes de aplicativos e dispositivos, e gerenciamento flexível, o Kaspersky Embedded Systems Security oferece segurança multifuncional desenvolvida especificamente para sistemas integrados.

Ideal para

Serviços Financeiros

Varejo e Transporte

Provedores de serviços de caixas eletrônicos e PDV

Benefícios para a empresa

Mitiga os riscos associados a ameaças direcionadas a infraestruturas financeiras específicas
Atende aos requisitos de conformidade de regulamentos como PCI/DSS, SWIFT, etc.
Otimiza os custos administrativos por meio de um único console de gerenciamento

Casos de uso

- Protege sistemas integrados geograficamente dispersos e raramente atualizados que apresentam preocupações de segurança específicas e exclusivas
- Proteção para Windows XP não suportado, ainda amplamente usado em hardwares low-end
- O design eficiente oferece avançada segurança, sem risco de sobrecarga de sistemas

Kaspersky Premium Support (MSA) serviço

Quando um incidente de segurança ocorre, o tempo necessário para identificar a causa e eliminá-la é crítico. Detectar e resolver rapidamente um problema pode poupar custos significativos para as empresas. Nossos planos de Maintenance Service Agreement (MSA) são desenvolvidos especificamente para atingir esse objetivo. Acesso 24 horas por dia aos nossos especialistas, priorização de problemas adequada e bem informada com tempos de resposta garantidos e patches privados - tudo o que você precisa para garantir que seu problema seja resolvido o mais rápido possível.

Ideal para qualquer empresa que use produtos Kaspersky

Benefícios para a empresa

Garante a continuidade dos negócios com especialistas alocados em espera, encarregados de apropriar-se do problema e chegar a uma solução da maneira mais rápida possível

Custo reduzido de um incidente de segurança devido ao acesso a uma linha de suporte prioritário, tempos de resposta garantidos e patches privados

Um gerente técnico de contas dedicado atuará como seu representante dentro da Kaspersky com autoridade para mobilizar toda a experiência necessária para resolver rapidamente o problema

Use cases

- Encaminhe de maneira rápida os problemas críticos diretamente para os especialistas nos bastidores da sede da Kaspersky, melhor equipados para fornecer a solução certa para você, em alta velocidade
- Medidas proativas adaptadas ao seu sistema, incluindo hot fixes priorizados e patches personalizados, mantendo você totalmente protegido
- Reduza o tempo gasto em manutenção e solução de problemas por seus valiosos recursos internos

Kaspersky Professional Services serviço

A cibersegurança é um grande investimento. Aproveite o seu ao máximo com especialistas que entendem exatamente como você pode otimizar sua segurança para atender às necessidades exclusivas da sua empresa. Trabalhando de acordo com nossas melhores práticas e metodologias estabelecidas, nossos especialistas em segurança estão disponíveis para ajudar em todos os aspectos da implantação, configuração e atualização de produtos Kaspersky em toda a infraestrutura de TI de sua empresa.

O Kaspersky Professional Service inclui:

- Implementation and Upgrade
- Configuration
- Product Training

Ideal para qualquer empresa que use produtos Kaspersky

Business benefits

Maximiza o ROI de suas soluções de segurança, garantindo que elas funcionem com 100% da capacidade

Reduz custos de equipes internas de TI

Minimiza os riscos de inatividade por meio de auditorias periódicas das configurações do produto, garantindo que os mais atualizados mecanismos de defesa estejam em vigor

Reduz o período de adoção do produto, permitindo que todos os benefícios sejam extraídos mais rapidamente do produto implantado

Use cases

- Reduz os riscos de implantação que possam diminuir a proteção, afetar negativamente a produtividade e até mesmo levar à inatividade
- Minimiza o impacto da implantação de sua nova solução de segurança nas operações diárias da empresa e reduz os custos gerais de implantação
- Prepara sua equipe para assumir a manutenção de produtos utilizados com nossos programas de treinamento de produtos, ajudando a evitar erros, demonstrando compatibilidade de produtos e explicando os princípios operacionais

Kaspersky Security Awareness

Nossos programas de treinamento em computador mudamhábitos e formam novos padrões de comportamento, quesão o verdadeiro objetivo do treinamento de conscientização. O portfólio de treinamento Kaspersky Security Awareness inclui: Automated Security Awareness Platform (ASAP) – treinamento de conscientização para todos os funcionários,que desenvolve habilidades concretas de ciberhigiene diaapós dia; Cybersecurity for IT Online (CITO) - treinamento para especialistas em TI generalistas que desenvolve habilidades práticas sobre como reconhecer um possível cenário de ataque e coletar dados de incidentes; e o Kaspersky Interactive Protection Simulation (KIPS) – jogo de cibersegurança para tomadores de decisão.

Ideal para

Empresas cujas expectativas de TI estão crescendo e se diversificando
Empresas que querem reduzir as oportunidades e a frequência de erros de usuários que levam a violações de segurança

Benefícios para a empresa

Protege as empresas a partir do lado de dentro

Mantém alta 'mentalidade cibersegura' em toda a cultura corporativa

Reduz os erros humanos em até 80%

Use cases

- Desenvolve o comportamento ciberseguro em situações e cenários típicos, simulações de ataques cibernéticos, diferentes tarefas e explicações
- Cria uma compreensão das ameaças potenciais e oferece as habilidades necessárias para lidar com elas
- Desenvolve habilidades práticas essenciais para reconhecer um possível ataque em um incidente de PC aparentemente benigno e coletar dados de incidentes para entregar à Segurança de TI
- Estabelece um melhor entendimento sobre segurança entre gerentes seniores e tomadores de decisão

2 Defesa avançada

Tecnologia de detecção avançada e resposta centralizada

Automação máxima no estágio de detecção e resposta a ameaças complexas perdidas por tecnologias de prevenção

- Ambientes de TI em crescimento, cada vez mais complexos, com maior superfície de ataque
- Possui pequena equipe de segurança com conhecimento limitado
- Tem recursos básicos de resposta a incidentes

Ideal para médias empresas:

Endpoint

Kaspersky Endpoint Detection and Response

Pessoas

Kaspersky Cybersecurity Training

Serviços

Kaspersky Targeted Attack Discovery

Rede

Kaspersky Anti-Targeted Attack

Privacidade

Kaspersky Private Security Network

Inteligência

Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

Para se defender com sucesso de ameaças avançadas o mais cedo possível, é essencial complementar as tecnologias de prevenção com recursos avançados de detecção de endpoints e resposta. O Kaspersky EDR é uma solução especializada que aborda avançadas ameaças a seus endpoints, compartilhando um único agente com a nossa solução de proteção líder mundial Kaspersky Endpoint Security. O Kaspersky EDR fornece uma visibilidade abrangente de todos os endpoints da rede corporativa, permitindo a automação de tarefas rotineiras para descobrir, priorizar, investigar e neutralizar rapidamente ameaças complexas.

Ideal para

Empresas

Organizações que já usam o Kaspersky Endpoint Security

SOCs e equipes de resposta a incidentes

Benefícios para a empresa

Mitiga os riscos associados a ameaças avançadas e ataques direcionados

Otimiza custos administrativos por meio da automação de tarefas e de uma interface única, simplificada, orientada para os negócios

Increases the speed and effectiveness of incident processing, at no extra cost

Aumenta a produtividade liberando o tempo de suas equipes de TI e segurança para outras tarefas

Dá suporte à conformidade com políticas de segurança interna e requisitos regulatórios

Casos de uso

- Aborda o ciclo completo de proteção de endpoints, desde o bloqueio automático de ameaças até a resposta complexa a incidentes contra ameaças avançadas usando um único agente
- Oferece acesso rápido aos dados de endpoint, mesmo quando as estações de trabalho comprometidas não estão disponíveis ou os dados estão criptografados
- Complementa investigações de incidentes com caça a ameaças, análise IoA e mapeamento MITRE ATT&CK
- Permite uma resposta eficiente em infraestruturas distribuídas, por meio de ações automatizadas de grande alcance

Kaspersky Anti Targeted Attack

O número e a qualidade dos ataques direcionados estão sempre crescendo. Para combater essas novas ameaças emergentes, é necessário adaptar constantemente seus sistemas de segurança. O Kaspersky Anti Targeted Attack concentra-se na detecção avançada de ameaças no nível de rede, com coleta, análise e correlação de dados totalmente automatizada, e possibilita uma compreensão detalhada do escopo da ameaça. O resultado é a eficiente proteção de sua infraestrutura corporativa contra ameaças complexas e ataques direcionados, sem a necessidade de recursos adicionais.

Ideal para

Enterprises

SOC teams

MSSPs

Empresas sujeita a regras de conformidade

Benefícios para a empresa

Mitiga os riscos associados a ameaças avançadas e ataques direcionados

Reduz danos financeiros e operacionais introduzindo um único sistema confiável para a proteção contra ataques complexos

Otimiza custos administrativos por meio da automação de tarefas e de uma interface única e simplificada orientada aos negócios

Agiliza tarefas tpor meio da automação integrada do fluxo de trabalho, sem interrupção dos processos da empresa

Casos de uso

- Rápida descoberta das ações de cibercriminosos que contornam tecnologias de prevenção, por meio do monitoramento e controle centralizados de possíveis pontos de entrada na infraestrutura
- Detecção de sinais de ameaça e correlação de eventos multivetores em um ataque numa única imagem, para permitir investigação mais eficaz
- Provisão oportuna para a equipe de resposta a incidentes com todas as informações necessárias sobre ameaças detectadas

Kaspersky Private Security Network

O Kaspersky Private Security Network permite que as empresas desfrutem da maior parte dos benefícios da inteligência global contra ameaças baseada na nuvem, sem liberar quaisquer dados fora de seu perímetro controlado. É uma versão pessoal da empresa, local e completamente privada do Kaspersky Security Network.

Ideal para

Empresas com requisitos rigorosos de controle de acesso a dados

Infraestruturas críticas com redes fisicamente isoladas

Telecom, segurança gerenciada e outros provedores de serviços

Benefícios para a empresa

Possibilita detecção mais avançada das ameaças direcionadas ao seu negócios

Garante tempos de resposta mais rápidos devido ao acesso em tempo real a estatísticas de ameaças e reputação

Aumenta a eficiência operacional minimizando falsos positivos

Suporta conformidade total com requisitos regulamentares para a segurança de sistemas e ambientes isolados

Casos de uso

- Todos os benefícios de segurança assistida em nuvem, sem a necessidade de compartilhar informações fora de sua infraestrutura controlada
- Permite a criação de proteção personalizada, adicionando seus próprios 'vereditos'
- Adaptado para redes críticas isoladas

Kaspersky Targeted Attack Discovery service

O Kaspersky Targeted Attack Discovery é um serviço abrangente de avaliação de comprometimento que determina se você está atualmente sob ataque, o que está acontecendo e quem é o agente da ameaça. Nossos especialistas detectam, identificam e analisam incidentes em andamento, bem como os que ocorreram anteriormente, e elaboram uma lista de sistemas afetados por esses ataques. Ajudamos você a descobrir atividades maliciosas, identificar as possíveis fontes de um incidente e planejar as ações corretivas mais eficientes.

Ideal para

Empresas com equipes de segurança inexistentes ou imaturas

Instituições governamentais

Infraestruturas críticas

1 Habilidades necessárias

5 Personalização e escalabilidade

3 Custo

Benefícios para a empresa

Previne e minimiza os danos resultantes de um comprometimento de sistemas, reduzindo significativamente o custo

Ajuda a manter a relação de confiança com seus clientes, parceiros e investidores para promover ainda mais as oportunidades de negócios

Garante que você evite penalidades e multas regulatórias

Fortalece suas defesas contra incidentes futuros por meio de recomendações corretivas

Casos de uso

- Compreenda o impacto digital da sua organização e seus riscos associados
- Ajuda a avaliar o risco realizando inspeções detalhadas de sua infraestrutura de TI e de dados (como arquivos de log) e analisando suas conexões de rede de saída
- Identifica sinais de intrusões atuais ou passadas em suas redes
- Reconheça como o ataque está afetando seus sistemas e o que você pode fazer

Kaspersky Threat Intelligence

Contra-atacar as ameaças cibernéticas de hoje exige uma visão 360 graus das táticas e ferramentas usadas pelos agentes das ameaças. Gerar essa inteligência e identificar as medidas mais eficientes exige vigilância constante e altos níveis de especialização. Com petabytes de ricos dados sobre ameaças para explorar, tecnologias avançadas de machine learning e uma equipe exclusiva de especialistas mundiais, a Kaspersky oferece as mais recentes informações sobre ameaças de todo o mundo, ajudando você a manter-se imune até mesmo contra ataques cibernéticos inéditos.

Ideal para

Empresas:

Instituições governamentais

SOCs e equipes de resposta a incidentes

MSSPs

Benefícios para a empresa

Detecção imediata de ameaças para evitar a interrupção das operações da empresa

Minimiza potenciais perdas financeiras causadas por incidentes

Assegura investimentos econômicos em determinadas tecnologias e na equipe certa, com base em informações atualizadas sobre ameaças direcionadas à sua empresa.

Impede que os concorrentes obtenham uma vantagem competitiva injusta por meio da exfiltração de propriedade intelectual

Ajuda a criar uma defesa proativa e adaptável

Casos de uso

- Reforce as soluções de segurança de rede com **Threat Data Feeds** atualizados constantemente
- Priorize de forma eficiente uma enorme quantidade de alertas de segurança e identifique imediatamente aqueles que devem ser encaminhados para equipes de resposta a incidentes com **Threat Data Feeds e o CyberTrace**
- Tenha **"consciência situacional"** em tempo real e aproveite melhor os feeds de inteligência sobre ameaças com o **CyberTrace**
- Identifique o impacto digital da sua empresa e reduza os riscos associados com o **Tailored Threat Intelligence Reporting**

Kaspersky Cybersecurity Training: Incident Response

serviço

A formação em cibersegurança é fundamental para empresas que enfrentam um volume crescente de ameaças em constante evolução. A equipe de segurança de TI deve estar capacitada nas técnicas avançadas mais importantes para estratégias eficientes de gerenciamento e mitigação de ameaças à empresa. O Kaspersky Cybersecurity Training ajuda a munir sua equipe interna de segurança com todo o conhecimento necessário para lidar com um ambiente de ameaças em constante evolução.

Benefícios para a empresa

Mitiga, de forma rápida e eficiente potenciais danos do incidente de segurança, para reduzir significativamente seu custo

Ensures you avoid regulatory penalties and fines

Helps maintain the relationship of trust with your customers, partners, and investors, to further foster business opportunities

Strengthens your defenses against future incidents through the lessons learned

Casos de uso

- Diferencie os APTs de outras ameaças
- Entenda várias técnicas de invasores e a anatomia de ataques direcionados
- Aplique métodos específicos de monitoramento e detecção
- Crie regras eficazes de detecção
- Reconstrua a lógica e a cronologia do incidente, e siga o fluxo de trabalho de resposta

Ideal para

Empresas
Instituições governamentais
SOCs e equipes de resposta a incidentes
MSSPs

3 Abordagem integrada de cibersegurança

Gestão de Ameaças e Defesa

Esteja preparado para ataques em nível de APT Ideal para empresas com alto nível de especialização, acostumadas a trabalhar com inteligência de ameaças e a caçar ameaças

- Ambientes complexos e distribuídos
- Equipe de segurança interna ou SOC
- Custos mais altos de incidentes e violações de dados
- Sujeito à conformidade

Serviços

Kaspersky Managed Protection

Kaspersky Incident Response

Pessoas

Kaspersky Cybersecurity Training

Inteligência

Kaspersky Threat Intelligence

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense é uma solução especializada que oferece uma estrutura abrangente para rápida descoberta de ameaças, investigação de incidentes, resposta e correções. Consiste de inteligência global sobre ameaças, tecnologias avançadas de detecção e resposta a ameaças, vários treinamentos de cibersegurança, caça permanente a ameaças e resposta a ameaças que contornam as barreiras de segurança existentes. A solução pode ser integrada à sua atual estratégia organizacional para combater ameaças complexas, complementando as tecnologias de proteção existentes e oferecendo a você suporte com conhecimento especializado quando necessário.

Ideal para

Empresas
Instituições governamentais
SOCs equipes de resposta a incidentes
MSSPs

5 Habilidades necessárias

5 Personalização e escalabilidade

5 Custo

Benefícios para a empresa

Minimiza os danos financeiros e operacionais causados por crimes cibernéticos e ajuda a manter a estabilidade da empresa

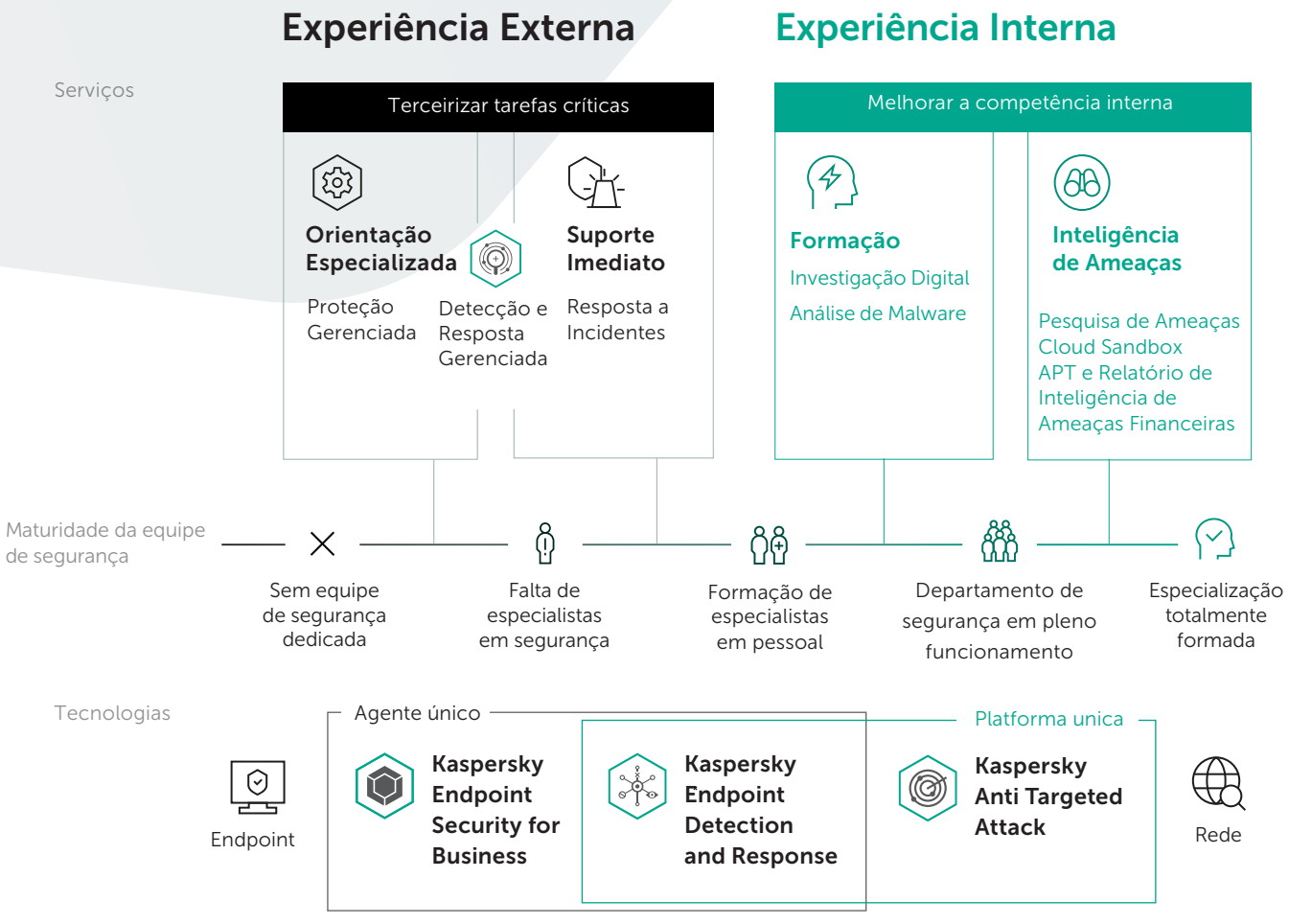
Aumenta o ROI por meio da automação e evitando interrupções nos processos da empresa

Reduz as taxas de rotatividade de pessoal e eleva a eficiência operacional, aumentando o conhecimento interno

Implanta estratégias de segurança de informações econômicas e totalmente informadas, baseadas em modelos de ameaças sob medida

Casos de uso

- A plataforma tecnológica multifuncional automatiza a demorada coleta de evidências e as tarefas manuais de rotina
- Inteligência proativa contra ameaças fornece o contexto necessário para prontamente detectar, priorizar, investigar e responder a ameaças
- Estratégia de gerenciamento das ameaças à empresa por meio do fornecimento de habilidades avançadas
- Caça a ameaças permite detecção de ameaças desconhecidas e avançadas, criadas para driblar as tecnologias de prevenção
- Acesso à experiência de terceiros dá suporte à investigação e resposta eficientes a incidentes complexos


Experiência Externa
Experiência Interna
Serviços
Terceirizar tarefas críticas
Melhorar a competência interna
Orientação Especializada
Proteção Gerenciada
Detecção e Resposta Gerenciada
Suporte Imediato
Resposta a Incidentes
Formação
Investigação Digital
Análise de Malware
Inteligência de Ameaças
Pesquisa de Ameaças
Cloud Sandbox
APT e Relatório de Inteligência de Ameaças Financeiras
Maturidade da equipe de segurança
Sem equipe de segurança dedicada
Falta de especialistas em segurança
Formação de especialistas em pessoal
Departamento de segurança em pleno funcionamento
Especialização totalmente formada
Tecnologias
Agente único
Platforma unica
Endpoint
Kaspersky Endpoint Security for Business
Kaspersky Endpoint Detection and Response
Kaspersky Anti Targeted Attack
Rede

Coisas a lembrar ao criar uma estratégia de cibersegurança de longo prazo

Uma abordagem em silos para cibersegurança coloca as empresas em risco

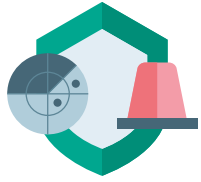
Os crescentes custos de violações de rede e dados colocam sérias pressões financeiras sobre as empresas que querem se transformar, e é por isso que a cibersegurança é questão importantíssima. Para ter sucesso neste ambiente, as empresas devem tornar a cibersegurança uma parte integral da sua estratégia global de negócios, desempenhando um papel fundamental na gestão de riscos e no planejamento de longo prazo.

A cibersegurança não é apenas um destino - é uma jornada permanente

O plano de segurança de uma empresa deve ser revisado e ajustado regularmente à medida que novos conhecimentos e ferramentas são disponibilizados. Todo incidente de segurança deve ser submetido a uma análise aprofundada e resultar na criação de novos procedimentos para lidar com ataques e medidas para evitar incidentes similares no futuro. As defesas existentes devem ser constantemente aprimoradas.

Conscientização, comunicação e cooperação são a chave para o sucesso em um mundo de ameaças cibernéticas em constante mudança

Mais de 80% de todos os incidentes cibernéticos são causados por erros humanos. O treinamento de equipes em todos os níveis é essencial para aumentar a conscientização sobre segurança em toda a organização e motivar todos os funcionários a prestarem atenção às ameaças cibernéticas e suas contramedidas, mesmo que eles não achem que isso faça parte de suas responsabilidades profissionais.



Uma mentalidade proativa de "detecção e resposta" é a melhor maneira de combater as ameaças atuais em constante evolução

Os sistemas tradicionais de prevenção devem funcionar em harmonia com tecnologias avançadas de detecção, análise de dados de ameaças, recursos de resposta e técnicas preditivas de segurança. Isso ajuda a criar um sistema de cibersegurança que constantemente se adapta e responde aos desafios emergentes enfrentados pelas empresas.

Por que escolher a Kaspersky

A mais testada. A mais premiada

A Kaspersky alcançou mais primeiros lugares em testes independentes do que qualquer outro fornecedor de segurança.
E fazemos isso ano após ano.

https://www.kaspersky.com.br/top3

Uma dos mais altamente recomendadas

A Kaspersky, mais uma vez, foi indicada a Escolha dos Clientes da Gartner Peer Insights para Plataformas de Proteção de Endpoints, tendo recebido um alto índice de satisfação do cliente de 4,6 de 5 em 28 de maio de 2019.*

A mais transparente

Com o nosso primeiro Centro de Transparência agora em atividade e processamento estatístico com base na Suíça, a independência de seusdados é garantida de forma que nenhum outro fornecedor pode igualar.

*A escolha dos clientes do Gartner Peer Insights constitui as opiniões subjetivas de avaliações, classificações e dados de usuários finais individuais aplicados de acordo uma metodologia documentada; eles não representam os pontos de vista nem o endosso da Gartner ou suas afiliadas. Leia no site

Fale conosco

Encontre um parceiro perto de você: https://www.kaspersky.com.br/partners
Kaspersky for Business: https://www.kaspersky.com.br/small-to-medium-business-security
Enterprise Cybersecurity: https://www.kaspersky.com.br/enterprise-security
Notícias sobre segurança de TI: https://www.kaspersky.com.br/blog/
Nossa abordagem exclusiva: https://www.kaspersky.com.br/enterprise-security/services

#bringonthefuture

www.kaspersky.com

kaspersky

Bring on the future

www.kaspersky.com.br