



A resposta para a mitigação de riscos de cibersegurança em uma era de transformação digital

A transformação digital é o segredo para o crescimento corporativo e a eficiência institucional em todo o mundo. Mas proteger a infraestrutura da organização digital representa um enorme desafio. Ameaças avançadas e ataques direcionados em elementos únicos de rede, ocultos e inertes até serem ativados, se somam aos fatores de risco que a transformação digital envolve, afetando o crescimento de negócios e iniciativas de desenvolvimento. Embora as técnicas usadas por criminosos virtuais evoluam constantemente, e estejam cada vez mais focadas em ambientes direcionados de forma específica, um número altíssimo de organizações ainda conta com tecnologias convencionais de segurança para se proteger contra ameaças atuais e futuras.

Transformação digital - um novo papel para a cibersegurança

A cibersegurança, juntamente com uso de dados e compliance, se tornou uma prioridade estratégica de grande importância para negócios digitais. As organizações buscam abordagens de segurança que facilitem um foco claro em necessidades de negócios.

Novos desafios empresariais:

- Alto volume de tarefas manuais necessário para resposta a incidentes
- Falta de pessoal de equipe de segurança de TI e carência de expertise de alto nível
- Número muito alto de eventos de segurança para processar, analisar, separar e responder de forma efetiva com um prazo limitado
- Problemas de compliance em compartilhamento de dados e confiança conforme a infraestrutura digital é ampliada
- Desafios de falta de visibilidade e coleta de evidências para análise pós-violações

Benefícios empresariais

- Redução nos danos operacionais e financeiros causados por crimes virtuais
- Menor complexidade através de uma interface de gestão descomplicada e orientada para negócios
- Redução de custos administrativos através de automação de tarefas e processos descomplicados de compliance de segurança
- Maior retorno sobre o investimento através de automação de fluxo de trabalho integrada e sem interrupções aos processos de negócios
- Riscos mitigados de ameaças avançadas através de detecção rápida

Uma solução unificada para acelerar a inovação em transformação digital

O Kaspersky Threat Management and Defense compõe uma combinação única das principais tecnologias de segurança, suporte e serviços de cibersegurança que são altamente adaptativos aos detalhes específicos da organização e adotam uma abordagem estratégica, proporcionando processos unificados para proteção contra ameaças avançadas e ataques direcionados únicos.



Produtos

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Private Security Network

Serviços

- Treinamento de segurança virtual Kaspersky
- Portal de Inteligência sobre Ameaças Kaspersky
- Kaspersky Managed Detection and Response
- Resposta a incidentes da Kaspersky

Suporte

- Contrato de Serviço de Manutenção da Kaspersky
- Kaspersky Security Account Manager
- Serviços profissionais Kaspersky

Consagrado como a solução
mais eficaz da indústria



**Escolha do cliente
para detecção
e resposta em
endpoints do Gartner
Peer Insights, 2020**

MITRE | ATT&CK®

**Qualidade de detecção confirmada
pela avaliação MITRE ATT&CK**



SE Labs Teste de
resposta a violação:
AAA Awards



ICSA Labs, teste
de defesas contra
ameaças avançadas
(3º trimestre de 2019):
**taxas de detecção
de 100%, sem falso-
positivos**



**Principal nome no Radicati APT
Protection Market Quadrant 2020**

Seleção do equilíbrio ideal de tecnologias e serviços

Para aumentar a experiência da equipe, a Kaspersky também oferece uma variedade de programas de treinamento de habilidades, além de dados de inteligência de ameaças com os quais enriquecer os resultados de investigação interna. Nosso Managed Detection and Response Service significa que os recursos de segurança de TI podem ser conservados transferindo-nos as tarefas de processamento relacionadas a incidentes ou consultando a Kaspersky para fornecer julgamentos especializados e conhecimento exclusivo em busca de ameaças. Tudo o que sua empresa precisa agora ou no futuro em termos de segurança de TI - nós temos a solução.

Defesas estendidas com uma perspectiva mais ampla

Basicamente, o Kaspersky Anti Targeted Attack Platform com o Kaspersky EDR protege vários pontos de entrada de ameaças em potencial nos níveis da rede e do endpoint, além de fornecer recursos estendidos de detecção e resposta. O especialista em segurança de TI possui um kit de ferramentas abrangente para descoberta multidimensional de ameaças, investigação aprofundada, busca proativa de ameaças e uma resposta centralizada a incidentes complexos. Ela se integra totalmente ao Kaspersky Endpoint Security for Business, que compartilha um único agente com o Kaspersky EDR, Kaspersky Hybrid Cloud Security e com ambos Kaspersky Security for Mail Server e Kaspersky Security for Internet Gateway para fornecer respostas automatizadas no nível do gateway a ameaças complexas. A natureza multifuncional dessa solução reduz significativamente o tempo e o esforço que as equipes de segurança de TI precisam gastar em proteção contra ameaças, graças à automação máxima de ações defensivas nos níveis de rede e do endpoint e a representação contextual de incidentes no único console da Web.

Uma solução de segurança confiável que assegura total privacidade

Para empresas com políticas de privacidade rigorosas, a análise de objetos é realizada no local, sem fluxo de dados externos com a integração com a Kaspersky Private Security Network. Isso oferece atualizações de reputação internas em tempo real enquanto preserva o total isolamento dos dados corporativos.

Fortalecimento do Centro de Operações de Segurança

Para combater as ameaças virtuais contemporâneas mais sofisticadas e se adaptar aos desafios atuais em um ambiente de ameaças em constante mudança, o Centro de Operações de Segurança (SOC, Security Operations Center) deve estar equipado com tecnologias avançadas, alimentadas com inteligência de ameaças e com profissionais equipados com todo o conhecimento e experiência necessários. O resultado é um ciclo completo de defesas contra os ataques mais complexos do tipo APT e campanhas direcionadas. Na estrutura do Kaspersky Threat Management and Defense, oferecemos um arsenal completo de tecnologias e serviços avançados de defesa para aumentar a eficácia do SOC.

Kaspersky Managed Detection and Response

Se você está buscando expertise ampla na detecção de ameaças, pode ampliar seus próprios recursos com as competências e experiência de nossos profissionais, que vão:

- Avaliar os dados coletados no seu ambiente
- Notificar rapidamente sua equipe de segurança se atividades maliciosas forem detectadas
- Proporcionar orientações sobre como responder e remediar

Notícias sobre ameaças virtuais: securelist.com
Notícias sobre segurança de TI: business.kaspersky.com
Segurança de TI para PMEs: kaspersky.com.br/business
Segurança de TI para empresas: kaspersky.com.br/enterprise

www.kaspersky.com

2020 AO Kaspersky Lab.
As marcas registradas e marcas de serviço pertencem
aos seus respectivos proprietários.



Somos comprovados. Somos independentes. Somos transparentes. Estamos empenhados em construir um mundo mais seguro, onde a tecnologia melhora as nossas vidas. É por isso que criamos soluções de segurança. Para que todas as pessoas, em todos os lugares, possam aproveitar as infinitas oportunidades que a tecnologia oferece. Leve a segurança virtual para um amanhã mais seguro.

Saiba mais em kaspersky.com.br/transparency



**Proven.
Transparent.
Independent.**