Kaspersky Next XDR Expert

Visão incomparável. Proteção Total.

kaspersky

A complexidade da cibersegurança empresarial

O cenário de ciberameaças torna extremamente desafiador para as organizações manterem o controle de todas suas necessidades de cibersegurança enquanto focam nas operações essenciais de negócios. Adicione a essa lista uma superfície de ataque em constante expansão, requisitos regulamentares rígidos e a falta de especialistas em cibersegurança e é fácil ver por que as empresas modernas estão sob tanta pressão, e por que ciberataques causam tantos problemas.

51%

das empresas sofrem para deter e investigar ameaças avançadas usando as ferramentas que dispõem atualmente.

68%

das empresas enfrentaram um ataque direcionado em suas redes e sofreram perda de dados como principal consequência direta

US$ 6 trilhões

por ano: custo globlal anual do cibercrime

400000

novos malware são detectados por dia

Fontes: Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Extended Detection and Response

Visibilidade completa. Proteção imbatível.

Como parte da linha de produtos Kaspersky Next, introduzimos o Kaspersky Next XDR Expert, uma solução que representa a abordagem da XDR da Kaspersky e fornece uma visão universal da segurança da empresa.

Kaspersky XDR é uma solução de cibersegurança robusta que defende sistemas contra as ciberameaças mais sofisticadas. A solução fornece total visibilidade, correlação e automação, tirando proveito de uma ampla gama de fontes de dados, incluindo de endpoints, redes e nuvem.

O produto é uma evolução da plataforma Kaspersky Anti-Targeted Attack como Native XDR em 2016 para o Open XDR em 2023, fornecendo uma visão de segurança abrangente e completa. Facilmente gerenciável via Plataforma de Gerenciamento Open Single, o Kaspersky XDR oferece uma segurança abrangente local, garantindo que os dados confidenciais dos clientes permanecem na sua própria infraestrutura, atendendo ainda aos requisitos imperativos de dados.

XDR aberta

As soluções Open XDR são projetadas para funcionar com uma variedade de produtos de segurança, permitindo às organizações integrar vários produtos de diferentes fornecedores, oferecendo mais flexibilidade e recursos independente do fornecedor.

Soluções XDR nativas

Soluções nativas XDR geralmente funcionam sem problemas com o ecossistema de ferramentas de segurança do próprio fornecedor, proporcionando uma experiência coesiva e mais unificada. Essas soluções são criadas com a finalidade de funcionarem juntas, oferecendo integração aprofundada, automação e fluxos de trabalho racionalizados dentro da suíte de produtos de segurança do fornecedor.

Principais tecnologias

Oferecemos a Open XDR como uma única plataforma de código aberto, uma ferramenta universal para criar um ecossistema unificado de produtos de cibersegurança. No epicentro o Kaspersky XDR estão nossas soluções líderes de mercado - Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Next EDR Foundations e Kaspersky Endpoint Detection and Response Expert. Para a gestão de rede avançada, o KATA é uma opção adicional.

Monitoramento e Análise

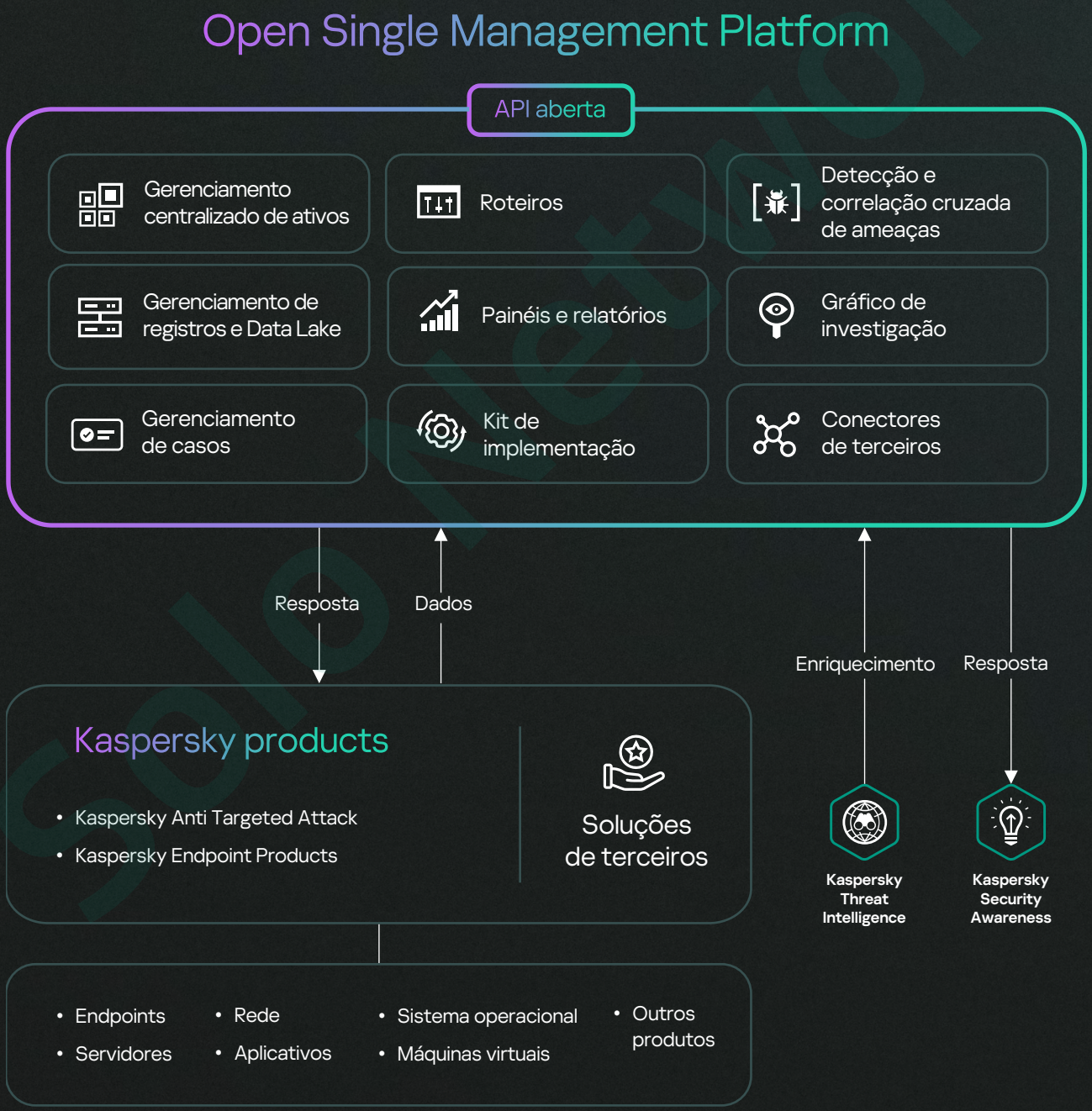
Fornece coleta e análise centralizada de logs, correlação de eventos de segurança em tempo real e notificação de incidentes em tempo real. Inclui um conjunto pronto para usar de regras de correlação e acesso a um rico porfólio dos serviços Kaspersky Threat Intelligence para identificar e priorizar ameaças, ataques e IoCs.

Proteção de endpoints

Fornece proteção reforçada de endpoits, protegendo contra ataques de ransomware, malware e ataques fileless. Seja em servidores locais do cliente ou na nuvem, nossa proteção de endpoints utiliza o aprendizado de máquina e análise de comportamento para proteger todos os tipos de endpoints que executam qualquer sistema operacional padrão.

Detecção e Resposta de Endpoints

Oferece visibilidade abrangente e ferramentas de defesa robustas para todos os endpoints de uma empresa. A busca e a descoberta aprimoradas de ameaças utilizam a inteligência de ameaças exclusiva da Kaspersky, enquanto a automação de tarefas rotineiras, processos de investigação guiados e detecções personalizáveis promovem a resolução rápida de incidentes.



Recursos poderosos, benefícios significativos

Fusão de dados de terceiros em tempo real

A capacidade de integrar dados de fontes de terceiros vai além de apenas endpoints e é aprimorada pela correlação cruzada de dados em tempo real.

Resposta e remediação automatizadas

Coloque em quarentena ou isole endpoints comprometidos, bloqueie atividades maliciosas e corrija vulnerabilidades, reduzindo o esforço manual e o tempo de resposta.

O melhor EPP/EDR da categoria

Reconhecida como líder global, a Kaspersky é referência para soluções EPP/EDR em todo o mundo. O Kaspersky EDR se destaca em escala global, apoiado por prêmios e participação ativa em comitês internacionais como Interpol e MAPP.

Escalabilidade inigualável

Capaz de comportar cargas de centenas de milhares de endpoints em uma única instância, o Kaspersky XDR rastreia diligentemente as ameaças em tempo real, garantindo alta disponibilidade.

Soberania de dados

O Kaspersky XDR é um dos poucos produtos que oferece uma solução abrangente de XDR local, garantindo que os dados confidenciais dos clientes permaneçam dentro das suas próprias infraestruturas, atendendo ainda aos requisitos de soberania de dados.

Integração harmoniosa e sólida para todos os produtos Kaspersky

A interação entre produtos atinge um nível imbatível para soluções de terceiros, com um sistema de suporte unificado e design perfeitamente integrado.

Multilocação que permite cenários MSSP

Forneça a XDR como um serviço com locatários completos - os usuários de um locatário não podem visualizar os dados de outros locatários, mas o administrador principal (o MSSP) pode criar processos de detecção e resposta para todos os clientes.

Personalização avançada de cenários de segurança e análise de dados em toda a infraestrutura

Possibilita os usuários a configurar cenários de segurança intrincados com a capacidade adicional de analisar dados em toda a infraestrutura.

Recursos de integração

A ampla gama de integrações com o Kaspersky XDR fornece uma visão unificada e contextualizada de ameaças potenciais, fornecendo a sua equipe de segurança todas as ferramentas e informações necessárias para proteger sua organização de cibercriminosos e seus ataques.

Os recursos de integração do produto incluem a capacidade de receber dados (logs) de outros sistemas e dispositivos, bem como configurar respostas automatizadas em outros produtos. O Kaspersky XDR dispõe de uma ampla gama de integrações prontas para uso, com a Kaspersky e produtos de terceiros. Também é possível adicionar integrações que podem ser desenvolvidas pelos Serviços Profissionais Kaspersky ou pelos próprios parceiros ou clientes (incluindo o uso dos recursos de API de produtos conectáveis). A integração é possível com sistemas de vários domínios e diferentes fornecedores, e vários protocolos e formatos de dados são compatíveis.

Por domínio de segurança

Endpoint Security

- Soluções EPP & EDR

Segurança de rede, web e e-mail

- Proteção de e-mail
- Resposta e Detecção de Rede (NDR)
- Firewalls (FW) e Firewalls de próxima geração (NGFW)
- Gerenciamento unificado de ameaças (UTM)
- Sistema de Detecção de Invasões (IDS)

Segurança em nuvem

- Cloud Access Security Brokers (CASB)
- Plataformas de Proteção de Carga de Trabalho na Nuvem (CWPP)

Inteligência de ameaças

- Inteligência contra Ciberameaças (CTI)

Segurança de identidade

- Gerenciamento de acesso e identidade (IAM)
- Gerenciamento de acesso privilegiado (PAM)

Conscientização de segurança de OT / IoT

Por tipo de transporte

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- Arquivo
- 1c-log e 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

Por tipo de dados

- XML
- Syslog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

Por fornecedor

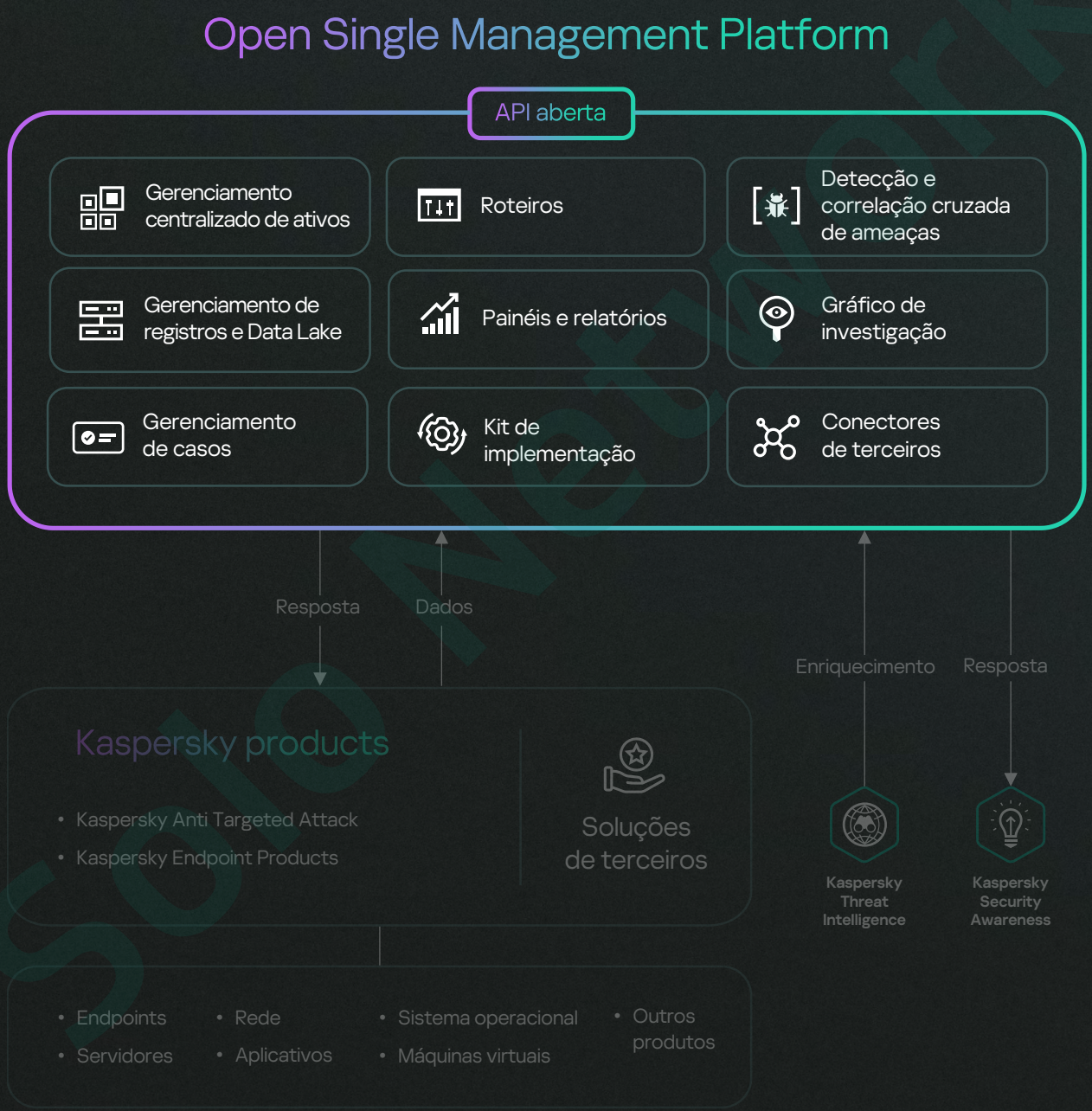
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexo
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard - Firebox
- Winchill Fracas
- Zettaset
- Zscaler e etc.

O que oferecemos

O Kaspersky XDR está disponível em duas opções.

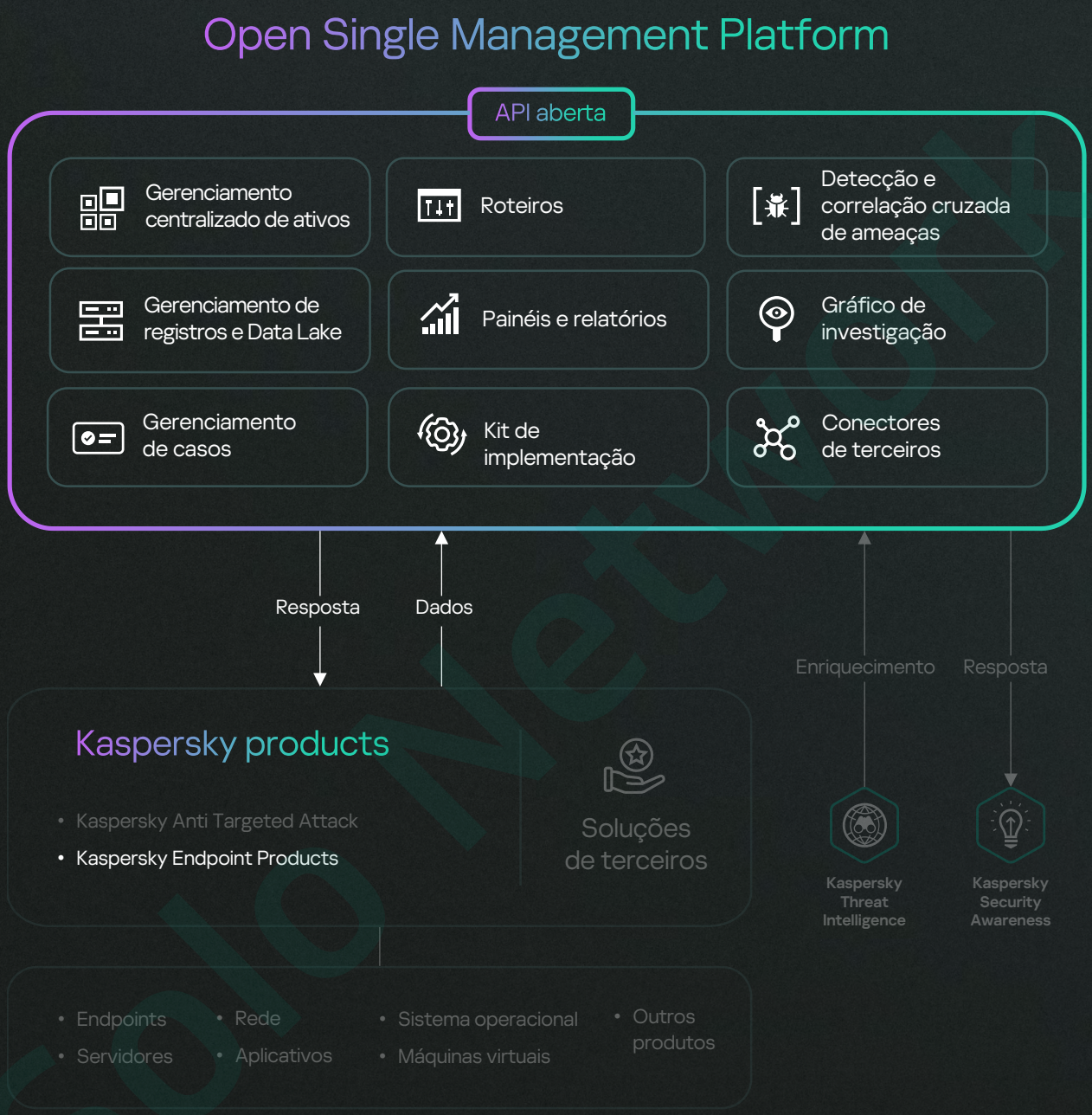
Kaspersky XDR Core

O Kaspersky XDR Core se destina aos a clientes que já possuem soluções de Endpoint e EDR implementados e não querem substituí-las, preferindo ampliar a funcionalidade com um mecanismo de correlação, respostas automatizadas e conectores de terceiros.



Kaspersky Next XDR Expert

O Kaspersky Next XDR Expert combina a melhor proteção de endpoints da categoria com os recursos avançados de detecção do Kaspersky EDR Expert, um mecanismo de correlação e resposta automatizadas. Conectores de terceiros podem ser adicionados para extração de todos os dados.



Valor agregado com sensores complementares

O Kaspersky XDR comporta a integração perfeita de sensores suplementares projetados para proteger ativos específicos, integrando-se perfeitamente ao XDR para oferecer uma camada adicional de valor e transformando o XDR em uma plataforma coesa que oferece aos analistas um espaço de trabalho centralizado que abrange todas as soluções integradas.

O Kaspersky XDR aumenta as suas defesas graças ao EDR, e ainda oferece recursos de integração flexíveis, para que os clientes possam adicionar produtos ao ecossistema a qualquer momento.

		Kaspersky XDR Core	Kaspersky Next XDR Expert
Open Single Management Platform e componentes	Mecanismo de correlação cruzada • Conectores de terceiros • Gerenciamento de registos & Data Lake • Detecção e correlação de ameaças • Gerenciamento de ativos • Painéis e relatórios	●	●
	Componentes XDR • Gerenciamento de casos • Automação e orquestração de respostas (roteiros) • Investigação • Kit de implementação • API aberta	●	●
Funcionalidade do Kaspersky Endpoint*	Detecção manual, automatizada e semi-automatizada		●
	Monitoramento entre os endpoints protegidos		●
	Contenção de ameaças		●
	Opções de recuperação		●
	Proteção e gerenciamento de dispositivos móveis		●
	Cloud Discovery e bloqueio		●
	Segurança para MS O365, descoberta de dados		●
	Treinamento em cibersegurança para administradores de TI		●

* A disponibilidade dos recursos varia conforme o método de implementação

Kaspersky XDR Core

- Kaspersky Unified Monitoring and Analysis Platform
- Componentes XDR

Kaspersky Next XDR Expert

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Next EDR Foundations
- Kaspersky Endpoint Detection and Response Expert
- Componentes XDR

Apresentamos o Kaspersky Next

Kaspersky Next EDR Foundations

Segurança robusta para todos

Proteja todos os seus endpoints

Caso precise de

- Proteção robusta para endpoints
- Controles básicos de segurança
- Automação máxima

Kaspersky Next EDR Optimum

Construa suas defesas

Fortaleça a segurança com investigação e resposta essenciais

Caso precise de

- Recursos de visibilidade e resposta aprimorados
- Segurança de nuvem expandida
- Controles de nível empresarial

Kaspersky Next XDR Expert

Equipar seus especialistas

Proteja os negócios contra as ameaças mais complexas e avançadas

Caso precise de

- Detecção avançada de ameaças
- Integração perfeita
- Ferramentas poderosas de caça a ameaças

Por que escolher o Kaspersky XDR

A mais testada. A mais premiada. Proteção Kaspersky.

A Kaspersky é uma empresa líder global em cibersegurança que conta com um extenso histórico de experiência em segurança. Protegemos organizações em todo o mundo há mais de 25 anos e recebemos inúmeros prêmios e reconhecimentos por nossos produtos e serviços. Entre 2013 e 2022, os produtos Kaspersky:

827
participaram de 62 testes e análises independentes

587
conquistou 587 primeiros lugares

685
conquistou um lugar entre os três melhores

Em 2023, a Kaspersky foi nomeada líder no mercado de soluções XDR pela empresa líder global de pesquisa e consultoria em tecnologia ISG. O ISG define "líderes" como aqueles com uma oferta abrangente de produtos e serviços e representam força inovadora e estabilidade competitiva.

Saiba mais

Kaspersky Extended Detection and Response

www.kaspersky.com.br

#kaspersky
#bringonthefuture