Kaspersky Next
XDR Expert

Desvendando Kaspersky Next XDR Expert

O que é o Kaspersky Next XDR Expert?

Como o mais avançado dos três níveis de produtos do Kaspersky Next, o Kaspersky Next XDR Expert se integra perfeitamente à infraestrutura de segurança existente da organização, fornecendo visibilidade em tempo real e insights profundos sobre ameaças cibernéticas em evolução para oferecer detecção avançada de ameaças, resposta automatizada e uma ampla gama de recursos de XDR essenciais.

Por que o Kaspersky Next XDR Expert — e por que agora?

Cibercriminosos estão sempre aperfeiçoando suas táticas e desenvolvendo maneiras cada vez mais sofisticadas de atacar organizações. Os invasores de hoje estão cada vez mais adotando uma abordagem multivetorial, frequentemente envolvendo múltiplos pontos de entrada na infraestrutura e uma variedade de táticas e de técnicas.

Ameaças persistentes avançadas (APTs), por exemplo, contornam a detecção tradicional de endpoint e podem permanecer ativas por semanas ou meses, movendo-se lateralmente pela rede, obtendo permissões, exfiltrando dados e coletando informações das diferentes camadas da infraestrutura de TI em preparação para um ataque em larga escala ou uma violação de dados.

Alcançar uma segurança eficaz contra essas ameaças requer uma abordagem abrangente e proativa que combina tecnologias avançadas, políticas robustas, monitoramento vigilante, treinamento contínuo e mais.

Ao unificar as soluções específicas de cada camada, o XDR oferece a SOCs e equipes de segurança de TI a visibilidade e integração de ponta a ponta para identificar e responder a ameaças mais rápido, resolvê-las de forma mais eficaz e minimizar o dano que causam.

Como o XDR aborda esses problemas

O “estendida” em “detecção e resposta estendida” reflete o fato de que em XDR, uma solução de detecção e resposta de endpoint (EDR) é complementada e integrada de perto com uma variedade de outras ferramentas de segurança.

Com o XDR, soluções de segurança que não foram necessariamente projetadas para funcionar juntas podem interoperar na prevenção, detecção, investigação e resposta a ameaças. Isso poderia incluir, por exemplo, soluções projetadas para proteger o correio, a Web, a rede, a infraestrutura de nuvem, aplicativos, identidade etc., permitindo a detecção e investigação de outros tipos de cenários de ataque, e fortalecendo o processo de combate a ameaças cibernéticas complexas.

Ao fornecer uma única janela e visibilidade completa de ferramentas e de camadas de cibersegurança, XDR permite que equipes de segurança sobrecarregadas detectem e resolvam ameaças de forma mais rápida e eficiente; e capturem dados mais completos e contextuais para ajudá-los a tomar decisões de segurança melhores, evitando futuros ataques.

E os benefícios para a empresa?

Para combater ameaças cibernéticas cada vez mais sofisticadas, as organizações precisam de mais do que apenas um conjunto unificado de ferramentas de segurança do mesmo fornecedor.

Encontre o produto Kaspersky Next que é mais adequado para você com a ajuda de nossa ferramenta interativa: https://go.kaspersky.com/Kaspersky_Next_Tool

Para combater ameaças cibernéticas cada vez mais sofisticadas, as organizações precisam de mais do que apenas um conjunto unificado de ferramentas de segurança do mesmo fornecedor.

- Diante da escassez global de especialistas em segurança da informação, o XDR oferece proteção holística para uma infraestrutura de TI em expansão e em constante mudança contra um cenário de ameaças cibernéticas em rápida evolução.
- Ao automatizar tarefas de rotina, o XDR reduz o esforço manual e os tempos de resposta, simplifica as tarefas de recursos valiosos e escassos, como especialistas em segurança de TI e os liberta para se envolver no processo de lidar com incidentes complexos.
- Ao permitir a análise comportamental e de telemetria em tempo real em várias camadas de segurança, os analistas de segurança podem visualizar melhor as ameaças cibernéticas, eliminando-as com base na gravidade com que podem impactar a infraestrutura de TI da organização.
- O XDR ajuda a minimizar o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR); crucial para combater ameaças complexas e ataques direcionados.

Além disso, mesmo que sua organização tenha recursos especializados limitados, o XDR pode proteger contra ataques complexos por meio de recursos como:

- Maior automação de processos.
- Uso de um único console unificado.
- Livros técnicos e automação, possibilitando uma interação próxima entre as ferramentas de segurança de TI como parte do XDR e cenários conjuntos.
- Um único ambiente data lake.
- Integração embutida com dados confiáveis e relevantes de inteligência de ameaças.
- Menos falsos positivos e impacto minimizado das ameaças reais.

Como o Kaspersky Next XDR Expert pode ajudar

O que ele faz

Plataforma Open XDR se integra perfeitamente com a infraestrutura de segurança existente, ferramentas e aplicativos

Fornece visibilidade em tempo real e insights profundos sobre ameaças cibernéticas em evolução para oferecer detecção avançada de ameaças e resposta automatizada.

Como funciona

Detecta ameaças complexas por meio da correlação cruzada de múltiplas fontes de dados.

Inclui funcionalidade avançada de EDR com capacidades avançadas de detecção e resposta.

Permite uma caça proativa a ameaças para descobrir ataques bem escondidos.

Valor comercial

Abordagem de ecossistema, juntamente com design aberto, maximiza a eficiência das ferramentas de cibersegurança envolvidas, economiza recursos e reduz o risco.

Simplifica o trabalho dos especialistas em segurança de TI e os fornece o contexto adicional necessário para investigar ataques de multi-vetores.

Minimiza o MTTD e MTTR — crucial em combater ameaças complexas e ataques direcionados

Fornece proteção abrangente contra o cenário de ameaças em evolução.

Para quem isso é melhor

Organizações com grandes recursos de segurança que desejam uma única plataforma que ofereça:

- Uma imagem coerente do que está acontecendo em toda a infraestrutura protegida
- Caça às ameaças e inteligência de ameaça incorporadas
- Priorização superior de incidentes e menos alertas com falsos positivos

O que você recebe?

Proteção de endpoints

Antivírus de arquivos, de web e de e-mail, proteção de rede, detecção de comportamento, remediação, prevenção de exploits, HIPS, AMSI, anti-cryptor, prevenção de ataque BadUSB

Gerenciamento de segurança

Controle de firewall, da web, de dispositivo e de aplicativos, controle adaptativo de anomalias, descoberta e bloqueio na nuvem, monitoramento de integridade de arquivos, inspeção de registros, monitoramento de integridade do sistema

Proteção e gerenciamento de dispositivos móveis

Proteção, controle e gerenciamento, iOS MDM

Cenários de TI

Avaliação da vulnerabilidade, gerenciamento de patches, limpeza de dados, inventário de software/hardware, instalação de aplicativos de terceiros e sistema operacional, conexão remota

Criptografia

Criptografia e gerenciamento de criptografia

Recursos de EDR

Análise da causa raiz, verificação de IoC, clique único e resposta automatizada, orientação de resposta

Recursos Advanced EDR

Coleta de dados de telemetria, recursos de caça a ameaças, detecção de Indicador de Ataque (IoA), mapeamento MITRE ATT&CK

Recursos XDR

Agregação de alertas, sandbox, integração com AD, enriquecimento de inteligência contra ameaças/Kaspersky Security Network, gerenciamento de casos, livros técnicos manuais e automatizados, gráfico de investigação, conectores de terceiros, gerenciamento de registros e data lake, resposta totalmente automatizada, detecção de ameaças e correlação cruzada

E se você já estiver usando a segurança da Kaspersky?

Sua solução da Kaspersky	Migração recomendada	Mais recursos que você terá
Kaspersky Endpoint Detection and Response Standard / Advanced / Expert*	Kaspersky Next XDR Expert	• Cenários entre ativos • Agregação de alertas • Fluxo de trabalho de incidentes • Gráfico de investigação

* Você ainda pode adquirir ou usar o Kaspersky EDR Expert como uma solução independente ou atualizá-lo e usá-lo como parte do Kaspersky Next XDR Expert.

Saiba mais sobre o Kaspersky Next XDR Expert

Kaspersky Next XDR Expert

Kaspersky Next EDR Foundations — Saiba mais

Kaspersky Next EDR Optimum — Saiba mais

Saiba mais sobre o Kaspersky Next em:
https://go.kaspersky.com/next

Notícias sobre ciberameaças: securelist.com
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

kaspersky.com.br