



Kaspersky Next
EDR Foundations

Desvendando Kaspersky Next EDR Foundations



O que é o Kaspersky Next EDR Foundations?

O Kaspersky Next EDR Foundations oferece uma poderosa proteção de endpoint baseada em ML, controles flexíveis de segurança e análise de causa raiz. Com implementação fácil e recursos que melhoram a qualidade de vida no trabalho, ele constrói uma base sólida para a cibersegurança, reduzindo a complexidade e aumentando a eficiência.



Por que o Kaspersky Next EDR Foundations — e por que agora?

Desmerecer o papel da EPP está se tornando um problema sério

As plataformas de proteção de endpoint (EPPs) se tornaram tão familiares para as equipes de TI que muitas vezes são basicamente “parte da decoração”. Isso ocorre porque, além do foco em defesa de perímetro com firewalls e proteção de e-mail, a grande maioria das organizações tem concentrado seus esforços nos endpoints — incluindo PCs, notebooks, servidores (físicos e virtuais) e estações de trabalho — como sua defesa primária contra ameaças cibernéticas.

Como resultado, EPPs se tornaram fundamentais para combater ataques. No entanto, é importante entender que a definição do que constitui uma EPP está evoluindo e trazendo novas demandas sobre o que tal plataforma deve oferecer. Isso se deve ao aumento do número de ameaças que estão contornando a EPP tradicional.

O problema com a EPP tradicional

Por anos, pequenas e médias empresas, assim como empreendimentos de baixo custo, têm conseguido contar com EPP para se proteger de diversas ameaças “commodities”. Mas os invasores de hoje em dia têm visado organizações de todos os tamanhos, setores e níveis de preparo.

Essa evolução significa que, ao longo do tempo, ameaças cada vez mais sofisticadas, que antes afetavam apenas grandes organizações, estão se propagando para impactar pequenas e médias empresas e empreendimentos menores sem recursos internos para lidar com elas de forma eficaz.

O que uma equipe de TI com habilidades básicas de segurança requer é visibilidade do que está acontecendo em cada endpoint, possibilitando uma análise mais aprofundada e mais entendimento da ameaça.

Em particular, ocorreu o surgimento de ameaças evasivas, que utilizam ferramentas legítimas em ataques, incluem cenários prontos para contornar a EPP, têm baixo custo e estão disponíveis na dark web. Isso aumentou os riscos à cibersegurança para organizações que utilizam soluções tradicionais de EPP.

Essas questões são ainda mais agravadas pela falta de transparência da EPP tradicional. Na verdade, essas soluções oferecem apenas uma representação positiva ou negativa de que uma invasão está ou não está ocorrendo. Mas o que uma equipe de TI com habilidades básicas de segurança requer é visibilidade do que está acontecendo em cada endpoint, possibilitando uma análise mais aprofundada e mais entendimento da ameaça.

Então como saber se é hora de aumentar suas defesas?

Como saber se a EPP não está mais de acordo com suas necessidades

Os sinais que indicam que chegou hora de expandir suas defesas além da EPP tradicional incluem:

- Sua EPP não está conseguindo impedir um número crescente de ameaças novas, desconhecidas e evasivas.
- Você tem visibilidade limitada sobre o que está acontecendo em seus endpoints. Isso inclui a impossibilidade de realizar análise de causa raiz, investigação e resposta a ameaças em tempo real ou ter que fazer isso manualmente, com ferramentas padrão do sistema operacional (SO), caso a caso, o que é lento, complexo e propenso a erros.
- Você não tem as habilidades especializadas de segurança de TI ou a capacidade necessária para lidar com ameaças cada vez mais sofisticadas.
- Você está preocupado com possíveis multas ou com a ameaça à reputação de sua empresa resultante de um grande incidente de segurança.

Se estiver passando por qualquer um desses problemas, uma solução moderna de EPP como o Kaspersky Next EDR Foundations é a chave. Incorporar uma simples resposta e detecção de incidentes (EDR) também pode ser um grande marco da EPP tradicional para soluções profissionais e avançadas de detecção e resposta estendida (XDR), tornando o recurso muito mais do que apenas “decorativo”.

Como o Kaspersky Next EDR Foundations pode ajudar



O que ele faz

Oferece uma poderosa proteção de endpoint baseada em ML, controles de segurança flexíveis e análise da causa raiz EDR para a maneira mais direta de construir um núcleo de cibersegurança forte



Como funciona

Garante proteção eficaz para todos os endpoints.

Incorpora capacidades básicas de EDR para aumentar a compreensão das ameaças e ataques.

Console na nuvem ou local



Valor comercial

Oferece proteção robusta para endpoints juntamente com maior visibilidade, funcionalidade básica de EDR e cenários de TI, incluindo avaliação da vulnerabilidade e inventário de software/hardware.



Para quem isso é melhor

Empresas com um administrador de TI, mas com recursos limitados de segurança especializados em TI

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

Firewall, Web, dispositivo, controles de aplicativos, Cloud Discovery



Proteção e gerenciamento de dispositivos móveis

Proteção, controle e gerenciamento, iOS MDM



Cenários de TI

Avaliação de vulnerabilidade, inventário de software/hardware



Recursos de EDR

Análise de causa-raiz



Kaspersky Next EDR Foundations combina os pontos fortes e os principais recursos do Kaspersky Endpoint Security Cloud, Cloud Plus e Kaspersky Endpoint Security for Business Select.

E se você já estiver usando a segurança da Kaspersky?

Kaspersky Next EDR Foundations combina as principais forças e capacidades do Kaspersky Endpoint Security Cloud, Cloud Plus e Kaspersky Endpoint Security for Business Select para criar uma única solução forte de proteção e controle de endpoint que requer pouco ou nenhum esforço para instalar e usar. Controles importantes (especialmente controle de aplicativos, BadUSB etc.) trazem novos benefícios para os usuários do Kaspersky Endpoint Security Cloud e Cloud Plus, enquanto os usuários do Kaspersky Endpoint Security for Business Select ganham o valor adicional de um console na nuvem e descoberta na nuvem. E todos esses usuários também ganham capacidades EDR com funcionalidade de análise de causa raiz.

Sua solução da Kaspersky

Migração recomendada

Mais benefícios pra você



Kaspersky Endpoint Security Cloud



Kaspersky Next EDR Foundations

- Prevenção de ataques BadUSB
- Controles de dispositivos, da Web e de aplicativos
- Análise de causa-raiz



Kaspersky Endpoint Security Cloud Plus



Kaspersky Next EDR Foundations

- Prevenção de ataques BadUSB
- Controle de aplicativos



Kaspersky Endpoint Security for Business Select



Kaspersky Next EDR Foundations

- Console simples na nuvem
- Análise de causa-raiz
- Cloud discovery

Saiba mais sobre o [Kaspersky Next EDR Foundations](#)



Kaspersky Next EDR Foundations



Kaspersky Next EDR Optimum

Saiba mais



Kaspersky Next XDR Expert

Saiba mais

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

© 2024 AO Kaspersky Lab.
As marcas registradas e de serviço pertencem aos seus respectivos proprietários.

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

Escolha o nível que melhor se adequa a você e responda a uma breve pesquisa em nossa ferramenta interativa:
https://go.kaspersky.com/Kaspersky_Next_Tool

