kaspersky preparados para o futuro

Como proteger empresas contra ataques cibernéticos complexos

Você já ficou acordado à noite, preocupado que algum tipo de ameaça cibernética avançada pudesse estar à espreita em sua infraestrutura, apenas esperando o momento certo para roubar sua propriedade intelectual ou manter sua empresa ou seus negócios como refém?

Se sim, você tem um bom motivo. Como o nome sugere, ameaças persistentes avançadas (APTs) usam técnicas sofisticadas de hacking para obter acesso aos seus sistemas. Depois que elas violam suas defesas, podem permanecer indetectáveis por meses ou até anos, obtendo privilégios de acesso de nível mais alto e coletando e exfiltrando seus dados com resultados possivelmente devastadores.

Quem está correndo risco?

Não é de surpreender que seja preciso uma quantidade significativa de habilidade, esforço e recursos para montar uma APT ou ataque direcionado, pois seus principais alvos geralmente são setores governamentais ou grandes corporações com dados confidenciais ou proprietários que justificam o investimento.

Mas, apesar disso, APTs são um método de ataque que deve estar no radar de empresas em todos os lugares – até mesmo empresas de médio porte podem estar em risco.

Os invasores de APT estão, por exemplo, cada vez mais visando empresas menores que compõem as cadeias de suprimentos de seus alvos finais. Como essas empresas geralmente são menos bem defendidas, elas podem atuar como trampolim para obter acesso a organizações maiores com as quais trabalham.

Como resultado, seja você uma grande empresa ou uma empresa menor que poderia ser explorada para atingir uma organização maior, é importante **compreender a natureza das ameaças** que você pode estar enfrentando. Isso inclui APTs e outros ataques direcionados – e os recursos necessários para se defender contra eles.

Todos os setores visados

Durante os últimos dois anos, ataques direcionados conduzidos por humanos foram observados em todos os setores. Em 2024, os setores de TI e governo lideraram com 14,7% e 13,8%, respectivamente.

Fonte: Kaspersky Managed Detection and Response 2024 Analyst Report

US$ 4.88 milhões

O custo médio global de uma violação de dados em 2024 – marcando um aumento de 10% em relação a 2023 e o maior total de todos os tempos. Na região do Oriente Médio, esse indicador é significativamente maior, chegando a US$ 8,75 milhões.

Fonte:IBM 2024 Cost of a Data Breach Report

258 dias

É hora de identificar e conter uma violação. Esse período de recuperação prolongado não apenas agrava perdas financeiras, mas também deixa as organizações vulneráveis a novos ataques.

Fonte:IBM 2024 Cost of a Data Breach Report

Como as APTs funcionam?

O objetivo de uma APT é obter acesso persistente ou contínuo aos sistemas de TI e/ou OT (tecnologia operacional) do alvo, o que os hackers geralmente conseguem por meio de um processo de cinco etapas.

Figura 1: Estágios de uma APT em evolução

Estágio 1

Obter acesso

Assim como um ladrão arromba uma porta com um pé de cabra, geralmente, os criminosos cibernéticos obtêm acesso inicial com um "pé de cabra digital", como um arquivo infectado, um e-mail de spam ou phishing ou uma vulnerabilidade em aplicativo, para inserir malware na rede alvo.

Estágio 2

Estabelecer uma posição

Feito isso, eles implantam malware, o que lhes permite criar backdoors e túneis que podem ser usados para se movimentar em sistemas sem que sejam detectados.

Estágio 3

Aprofundar acesso

Uma vez na rede, os hackers usam técnicas como quebra de senhas para obter acesso com direitos de administrador, ter mais controle sobre o sistema e obter níveis de acesso ainda mais elevados.

Estágio 4

Mover-se lateralmente

Mais profundamente no sistema, e com os mesmos direitos do administrador de rede, eles podem se movimentar à vontade. Isso permite a eles acessar vários servidores e outras partes seguras da rede.

Estágio 5

Olhar, aprender e permanecer

Com acesso mais profundo ao seu sistema, os criminosos cibernéticos podem obter uma compreensão completa de como o ambiente funciona e suas vulnerabilidades, o que lhes permite coletar as informações desejadas quando quiserem. Eles também podem tentar manter esse processo em execução — talvez indefinidamente — ou sair quando atingirem seus objetivos.

Quais são as possíveis consequências de ser vítima de um ataque APT?

Leia a cobertura da mídia sobre qualquer organização que tenha sofrido um ataque direcionado e ficará claro que os efeitos podem ser graves e duradouros. Embora os impactos imediatos normalmente incluam danos financeiros causados pela perda de dados e interrupção dos negócios, os efeitos de longo prazo podem incluir danos à reputação da organização, à confiança de clientes e possíveis processos legais.

Depois, é claro, há a questão de reparar os danos à infraestrutura de TI da organização, o que geralmente leva meses ou até anos para ser concluído. E, dependendo do setor em que você atua, também pode haver consequências específicas.

Figura 2: Compreendendo o impacto das APTs na segurança empresarial

Financeiro

- Interrupção de serviços críticos
- Transações não autorizadas
- Ataques de saque
- Consequências legais de roubo de identidades

Governo

- Possíveis efeitos de espionagem cibernética
- Danos a infraestrutura crítica
- Interrupção de serviços governamentais eletrônicos
- Exposição de dados pessoais de cidadãos

Comércio eletrônico

- Implicações legais de apropriação indébita de contas por meio de roubo de identidade
- Transações fraudulentas
- Negação de serviços de TI, perdas de receita
- Possíveis multas sob GDPR, PCI DSS etc.

Transportes

- Interrupção operacional e paralisações
- Atrasos em cadeia de suprimentos e aumento de custos
- Ameaça à vida
- Danos a infraestrutura crítica

Alimentício

- Escassez de estoque e paralisações de produção
- Qualidade alimentar comprometida
- Possível contaminação com produtos químicos, toxinas etc.
- É necessário recorrer a operações manuais

Serviços de saúde

- Interrupção de serviços críticos
- Exposição de dados pessoais de pacientes
- Confiança pública minada
- Possível ameaça à vida

TI e telecomunicações

- Perda de clientes
- Perda de vendas
- Tempo de inatividade de rede não planejado
- Interrupção de serviços fixos e móveis

Industrial

- Desastres ambientais
- Interrupção operacional
- Aumento de tempo de inatividade não planejado
- Falhas em cascata ou apagões em todo o sistema

Mais de 2

incidentes de alta gravidade acontecem todos os dias.

43%

de todos os incidentes de alta gravidade detectados pela Kaspersky em 2024 foram ataques direcionados conduzidos por humanos (APTs).

Fonte: Kaspersky Managed Detection and Response 2024 Analyst Report

O que isso significa para a segurança cibernética?

Um grande perigo das APTs e outros ataques direcionados é que, mesmo quando eles são descobertos e a ameaça imediata parece ter passado, os hackers podem ter deixado várias backdoors, permitindo que eles retornem quando quiserem.

Outro problema é que muitas defesas cibernéticas tradicionais, como antivírus e firewalls, geralmente não conseguem proteger contra esses tipos de ataques.

A partir do breve resumo acima das etapas envolvidas na montagem de uma APT ou de um ataque direcionado, deve ficar claro que a defesa contra essas ameaças requer uma abordagem multinível – incorporando soluções capazes de proteger endpoints, redes, nuvem, e-mail, acesso à Internet e muito mais.

Isso não só ajudará a prevenir e reduzir o risco de ataques sofisticados, como também ajudará a minimizar a interrupção e os custos desses tipos de incidentes, caso ocorram.

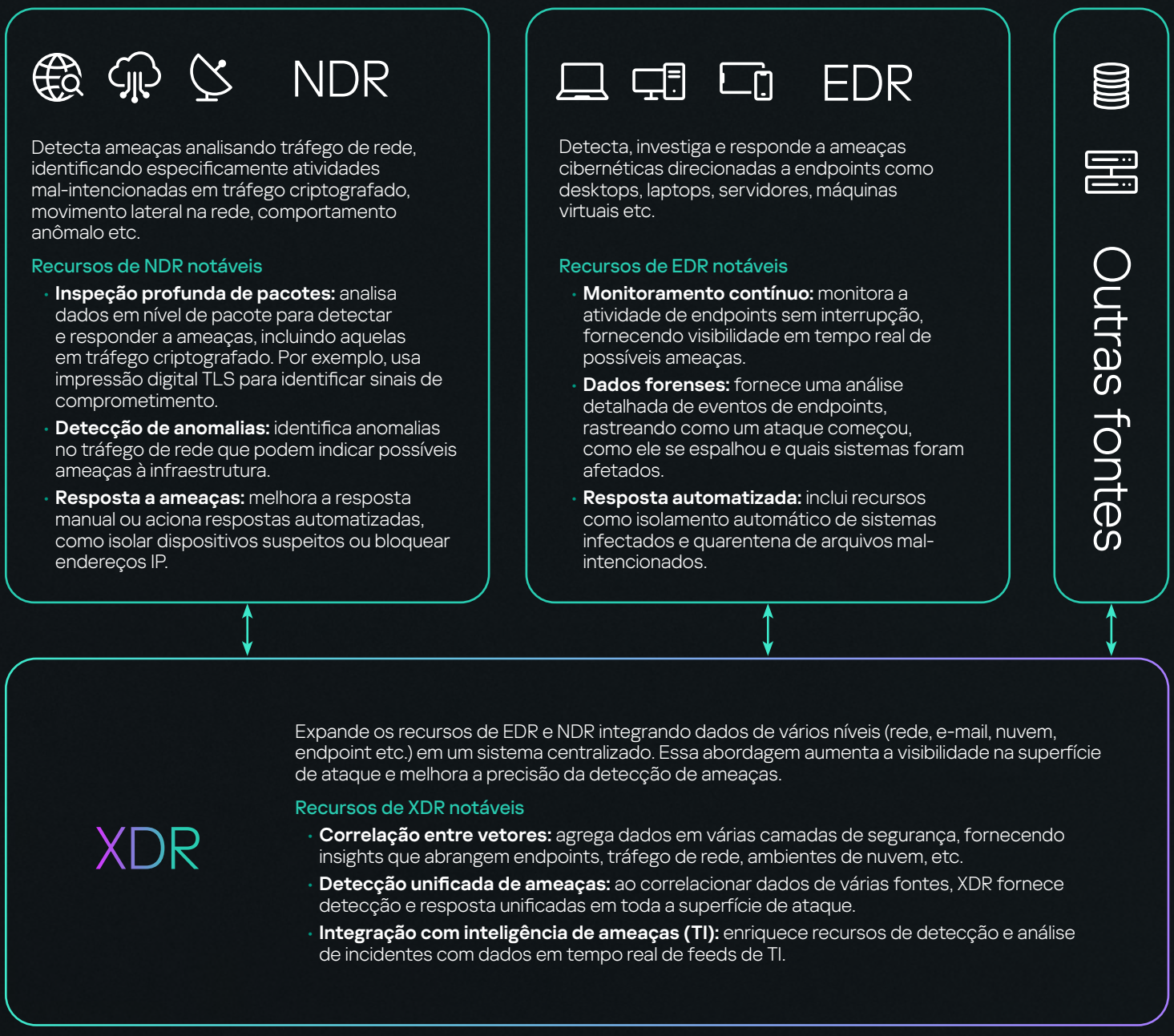
Então, quais tipos de soluções isso envolve e como você deve tentar implementá-las?

Como proteger empresas contra ataques cibernéticos complexos

Embora uma plataforma de proteção de endpoints (EPP) por si só não proteja contra ataques direcionados, ela fornecerá uma fonte vital de dados a serem usados na análise de ataques novos, contínuos ou históricos. Como resultado, ela deve ser usada como parte de um conjunto de soluções que também inclua:

- Detecção e resposta de endpoints (EDR) – Fornece proteção de endpoints e visibilidade no nível do dispositivo, identifica e responde a ameaças em estações de trabalho, servidores etc.
- Detecção e resposta de rede (NDR) – Monitora e analisa o tráfego de rede, detecta anomalias e responde a possíveis ameaças no nível de rede.
- Detecção e resposta estendidas (XDR) – Integra EDR, NDR e outras camadas de segurança para aumentar a visibilidade e automatizar a resposta a ameaças.

Figura 3: EDR, NDR, XDR: Como isso funciona?



Em 2024, o tempo médio para investigar e relatar incidentes de alta gravidade aumentou 48%, indicando um aumento na complexidade média dos ataques em comparação a 2023. Isso é apoiado pelo fato de que a grande maioria das regras de detecção e IoAs acionadas foram feitas por ferramentas de XDR especializadas, em vez de logs do sistema operacional, como nos anos anteriores.

Fonte: Kaspersky Managed Detection and Response 2024 Analyst Report

Então quais soluções você deve escolher?

A seleção das soluções corretas depende das necessidades específicas da sua organização, da infraestrutura e do cenário de ameaças:

- Escolha EDR se ferramentas tradicionais de proteção de endpoints não forem mais suficientes e você precisar de proteção mais avançada contra ameaças cibernéticas (como malware, ransomware, phishing e mais) direcionada a endpoints.
- Escolha NDR se ameaças baseadas em rede são sua principal preocupação e você precisa de recursos avançados para analisar e responder a anomalias de tráfego de rede.
- Escolha XDR se você deseja proteção abrangente em vários vetores e a capacidade de correlacionar ameaças em toda a sua infraestrutura de TI.
- Melhor ainda, combine EDR, NDR e XDRem um único ecossistema de segurança para fornecer defesa abrangente contra uma ampla gama de ameaças cibernéticas invasivas e avançadas.

Figura 4: EDR, NDR, XDR – para quem é melhor?

Soluções de segurança cibernética	Para qual organização é mais indicada?
EDR	• Organizações que priorizam proteção de endpoints e precisam de insights em tempo real sobre a atividade de endpoints. • Organizações com muitos endpoints distribuídos, como instituições financeiras ou provedores de assistência médica, que se beneficiarão muito da capacidade de EDR em detectar e responder a ameaças baseadas em endpoints em tempo real.
NDR	• Organizações que dependem fortemente do tráfego de rede e precisam de recursos avançados para detectar ameaças baseadas em rede. • Empresas com uma equipe dedicada de segurança de TI ou negócios altamente regulamentados, como data centers, provedores de serviços ou agências governamentais, podem se beneficiar da capacidade de NDR em detectar e responder a ameaças baseadas em rede.
XDR	• Organizações que exigem uma plataforma de segurança unificada com recursos abrangentes de detecção e resposta a ameaças em toda a sua infraestrutura de TI. • Grandes organizações com ambientes de TI complexos que precisam de uma abordagem abrangente de segurança. Por exemplo, uma empresa multinacional com data centers locais e ambientes de nuvem se beneficiaria da capacidade de XDR em fornecer detecção unificada de ameaças em várias plataformas, ao mesmo tempo em que reduz a complexidade operacional ao centralizar a resposta a incidentes.

Kaspersky Anti Targeted Attack

A Kaspersky pode te ajudar

O Kaspersky Anti Targeted Attack (KATA) oferece proteção anti-APT abrangente contra ameaças cibernéticas complexas. Ele ajuda as organizações a:

- Detectar, analisar e responder rapidamente a ataques direcionados.
- Habilitar segurança robusta em todos os principais pontos de entrada de ataques, incluindo redes, e-mails, Web e endpoints.
- Proteger ativos críticos.
- Garantir conformidade com as regulamentações do setor.

O acima exposto é possível graças à alavancagem de poderosas tecnologias NDR e EDR disponíveis nos três níveis do Kaspersky Anti Targeted Attack.

Os três níveis do KATA oferecem proteção contra ameaças persistentes avançadas (APT), desde NDR essencial e avançada até XDR nativa.

- KATA: serve como uma solução NDR essencial e oferece recursos básicos para detectar e responder a ameaças cibernéticas.
- KATA NDR Enhanced: baseia-se nos recursos fundamentais do nível KATA, oferecendo recursos avançados de NDR.
- KATA Ultra: combina recursos de NDR e EDR para fornecer funcionalidade XDR nativa. Ele protege vários pontos de entrada de ameaças, incluindo redes, Web, e-mail, endpoints, servidores e máquinas virtuais.

Figura 5: Kaspersky Anti Targeted Attack. Uma escolha flexível.

Critérios comparativos	KATA	KATA NDR Enhanced	KATA Ultra
Descrição	NDR essencial	NDR avançado	NDR+EDR (XDR nativo)
Nova funcionalidade de NDR	•	•	•
Sandbox avançada	•	•	•
Kaspersky Threat Intelligence e enriquecimento de MITRE ATT e CK	•	•	•
Função de NDR melhorada		•	•
Funcionalidade especializada de EDR			•
Funcionalidade XDR nativa			•

Escolha entre a funcionalidade NDR de nível essencial ou avançado, ou opte pela solução combinada de NDR e EDR para cenários XDR nativos, protegendo você contra as ameaças cibernéticas mais sofisticadas, tudo em uma única plataforma. No nível KATA Ultra, você obtém proteção APT plena e completa, além de visibilidade em toda a sua infraestrutura de TI.

Por que escolher o Kaspersky Anti Targeted Attack

Visibilidade total em toda a sua infraestrutura de TI.

Fornece um conjunto completo de tecnologias exclusivas para eliminar pontos cegos e controlar todos os pontos de entrada de possíveis ameaças, incluindo rede, Web, endpoints e e-mail – tudo em uma única plataforma unificada.

Proteção enriquecida por inteligência global sobre ameaças

Enriquece a análise e resposta a ameaças por meio de acesso direto ao banco de dados global de reputação da Kaspersky Private Security Network, Kaspersky Threat Intelligence e mapeamento para a estrutura MITRE ATT&CK.

Tecnologias testadas e comprovadas de forma independente

Usa tecnologias inovadoras para detecção avançada de ameaças orientada por ML, investigações aprofundadas e resposta rápida a incidentes, o que é reconhecido pelas principais agências analíticas e de confiança de grandes clientes no mundo todo.

Kaspersky Anti Targeted Attack

Saiba mais

Kaspersky Anti Targeted Attack Ultra

Assista agora

As previsões avançadas de ameaças

Leia agora

www.kaspersky.com.br