Megatendências em cibersegurança e suas implicações para a proteção virtual

Repensando o EPP, EDR e XDR hoje, amanhã e no futuro

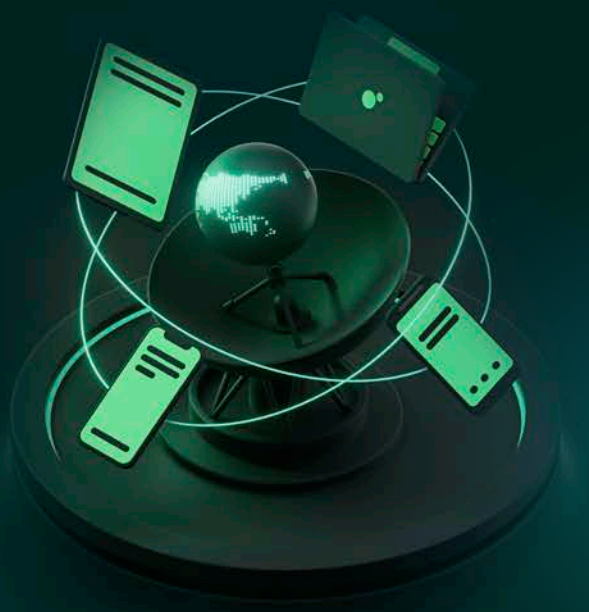
kaspersky

Sumário executivo

Todos os anos, analistas, comentaristas, associações comerciais e outros identificam as "megatendências" que podem influenciar significativamente o setor no curto prazo.

Não seria diferente com a segurança virtual. E por mais que esses insights sejam importantes para ajudar os executivos de nível C a prever as principais tendências e planejar o futuro de suas organizações, quando se trata de diretores de informação (CIOs), diretores de segurança da informação (CISOs), segurança e equipes de TI, é igualmente importante saber como suas implicações poderão ser acomodadas e operacionalizadas em termos práticos.

Para ajudar a lidar com esse processo, este e-book sintetiza algumas das tendências de segurança mais desafiadoras que causam impacto na indústria de TI contemporânea. E, particularmente, as implicações decorrentes do uso dessas soluções às organizações, desde plataformas de proteção de endpoints (EPP, na sigla em inglês), passando por detecção e resposta de endpoint (EDR, na sigla em inglês), até detecção e resposta estendidas (XDR, na sigla em inglês).



Conteúdo

- Sumário executivo
  página 2
- Você diz megatendência.
  Eu digo superfície de ataque expandida
  página 3
- Quais são as outras tendências específicas do setor de TI?
  página 4
- Como as megatendências mais recentes estão influenciando o cenário de ameaças
  página 6
- Como fazemos para sair da EPP para EDR ou XDR?
  página 7
- Quem precisa desse tipo de segurança?
  página 8
- Como avaliar os requisitos de segurança em evolução (EPP, EDR e MDR)
  página 9
- Como avaliar os requisitos de segurança cada vez mais dinâmicos – XDR
  página 15
- Expectativas quanto aos recursos e benefícios específicos de uma plataforma XDR
  página 17
- Como justificar o investimento em XDR
  página 21
- Como lidar com o cenário de ameaças mais amplo
  página 23
- A Kaspersky pode te ajudar
  página 25

Você diz megatendência.
Eu digo superfície de ataque expandida

Mesmo para os profissionais que trabalham na indústria de TI, às vezes pode ser difícil entender completamente a importância vital da segurança virtual dentro de um contexto de mercado mais amplo.

A Associação da Indústria de Segurança (SIA, na sigla em inglês), por exemplo, está liderando a associação de comércio para os provedores globais de solução de segurança, com mais de 1.400 membros. Na apresentação de sua visão para o setor, na edição de 2023, a SIA observa que "não é nem um pouco surpreendente ver a segurança virtual da segurança física brilhar novamente em nossa lista de megatendências de segurança de 2023".

> "As tendências predominantes no setor de segurança ainda envolvem a IA e segurança virtual, sendo evidente que a segunda ocupa a posição de prioridade principal para os líderes do setor. Além disso, tanto a IA quanto a segurança virtual foram avaliadas como as tendências mais significativas para o futuro."

Para entender esse contexto, os profissionais do setor de segurança consideram a segurança virtual e a IA muito mais críticas que as megatendências que poderiam ser consideradas dominantes no setor, como o desenvolvimento da força de trabalho, a mudança das condições econômicas e o uso ético/seguro de dados e da tecnologia.

Quais são as outras tendências específicas do setor de TI?

Analise os relatórios similares preparados pelos principais analistas, como a Gartner, IDC e Frost & Sullivan, para encontrar referências relacionadas a todos os aspectos: desde o aumento do dinamismo em ambientes de rede que dificulta a defesa das vulnerabilidades, até o volume acelerado e a sofisticação dos ciberataques que exploram essas vulnerabilidades.

Nas megatendências em segurança virtual de 2022, por exemplo, o IDC destaca "7 tendências da realidade da segurança virtual", entre elas:

- Transformação digital, trabalho híbrido e morte do perímetro
- Escassez dos profissionais de segurança da informação
- A sofisticação dos cibercriminosos está crescendo rapidamente
- A proliferação dos conjuntos de ferramenta de segurança e os processos em plataforma
- O crescimento contínuo das regulamentações de conformidade
- Novos compradores ou compradores com novas prioridades
- Confiança

Enquanto isso, o relatório Top Trends in Cybersecurity 2023 da Gartner afirma que "uma das principais tendências em segurança virtual neste ano é o aumento do reconhecimento da importância do envolvimento profissional no programa de segurança virtual, visando lidar com os riscos e manter uma função eficaz nessa área". A natureza cada vez mais distribuída do trabalho amplifica a adoção da nuvem. Isso, por sua vez, aumenta a dependência da visibilidade de ponta a ponta dos ecossistemas de expansão digital para garantir as cadeias de suprimentos resilientes. Além disso, os diretores de TI estão mudando os modelos operacionais para garantir a melhoria da agilidade dos negócios. O ambiente regulatório continua a evoluir, o que força os conselhos a atuarem mais ativamente no gerenciamento dos riscos de segurança virtual. Apesar da redução dos nos pagamentos decorrentes de ataques de ransomware, ainda persistem os ataques em grande escala desse tipo e os ataques direcionados aos sistemas de identidade.

Essas tendências globais estão levando os líderes em segurança e gerenciamento de riscos (SRM) a direcionar o foco para:

1. Orientar o foco para a função essencial das pessoas para o sucesso do programa de segurança e sustentabilidade.
2. Implementar recursos de segurança técnicos que fornecem muito mais visibilidade e responsividade em todo o ecossistema digital da organização.
3. Reestruturar o modo pelo qual a função de segurança opera para viabilizar a agilidade sem comprometer a segurança.

Para resolver esses problemas, a Gartner recomenda que os líderes em segurança e gerenciamento de riscos (SRM, na sigla em inglês) devem considerar os seguintes aspectos:

- Assimile a mentalidade do atacante para priorizar os esforços de mitigação de riscos cibernéticos ao adotar uma visão de ponta a ponta da superfície de ataque e consolidar os portfólios do fornecedor, conforme o caso.
- Otimize o alinhamento dos recursos de segurança virtual com as novas maneiras distribuídas de trabalho ao adotar novos modelos de segurança operacional e abordagens arquitetônicas que promovam a agilidade e segurança integrada pela concepção.
- Priorize e otimize os investimentos em melhoria comportamental de profissional para aprimorar e sustentar a eficácia da segurança da empresa.

Todas essas recomendações são um indicativo muito claro. Portanto, como é possível operacionalizar tudo isso dentro da organização?

Para responder a essa pergunta, precisamos analisar com mais detalhes o cenário de ameaças em evolução para entender o que isso significa no contexto da infraestrutura de segurança de TI, ferramentas e controles existentes.

"As vulnerabilidade de dia-zero são raramente a causa principal de uma violação. Em outras palavras, as violações poderiam ser evitadas se as organizações corrigissem a exposição à ameaça antes que o atacante pudesse explorá-las. Entretanto, corrigir cada vulnerabilidade conhecida sempre foi operacionalmente inviável."

Gartner: maiores tendências em segurança virtual em 2023

Como as megatendências mais recentes estão influenciando o cenário de ameaças

Em comparação com alguns poucos anos atrás, o cenário de ameaças está evoluindo mais rápido do que nunca. Neste momento, por exemplo, é raro passar uma semana sem haver um relatório sobre o ataque de ransomware, golpe, ou violação de dados mais recente, e os ciberataques não só aumentam em número, eles também estão cada vez mais sofisticados, mas também eles estão mais direcionados e são mais difíceis de detectar.

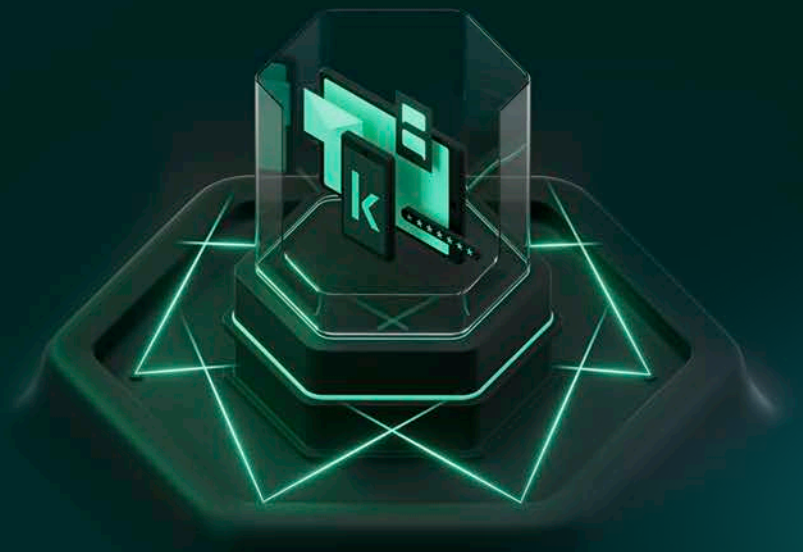
Muitos dos indivíduos que lançam ciberataques são criminosos de carreira, ou seja, o sucesso acontece com as tentativas. O popular equívoco de que os hackers são combatentes solitários não faz mais sentido.

Para ilustrar como exemplo um ransomware, os grupos envolvidos estão cada vez mais agindo como se fossem corporações descentralizadas, com redes complexas de filiais responsáveis pelas etapas individuais ao longo do processo. Ele vai desde o reconhecimento, acesso, criação de malware, distribuição e exfiltração de dados até a negociação do ransomware, publicação on-line dos dados roubados e lavagem de dinheiro originado do pagamento decorrente do ransomware.

Agora, a maioria dos ataques de ransomware tem tempo de permanência medidos em horas em vez de dias. Os grupos também oferecem ransomware como serviço e conduzem ataques mais parecidos com as ameaças persistentes avançadas (APTs, na sigla em inglês) em termos de escala. E os hacktivistas e os Estados-nação podem usar o ransomware e outras técnicas (como wipers) para difundir ataques destrutivos ou geopolíticos em vez de simplesmente lançar um ataque com objetivos comerciais.

Além disso, os TTPs (táticas, técnicas e procedimentos) usadas por criminosos virtuais estão se tornando cada vez mais sofisticados. Os exemplos incluem o uso de recursos de autodisseminação e autopropagação; a exploração de aplicativos públicos de leitura facial, o comprometimento de contas e e-mails maliciosos; além do uso de ferramentas como o PowerShell usadas extensivamente nas operações normais de TI, o que torna esses ataques muitos difíceis de serem detectados.

Consequentemente, estabelecer um nível ideal de proteção para sua organização, independentemente de estar usando EPP, EDR e/ou XDR, nunca foi tão importante.



Como fazemos para sair da EPP para EDR ou XDR?

Tradicionalmente, juntamente com a defesa dos perímetros com firewalls e proteção para e-mail, as organizações direcionaram o foco de seus esforços para os endpoints, como PCs, notebooks, servidores (físicos e virtuais) e estações de trabalho, como a principal estratégia de defesa contra as ameaças virtuais de modo que as plataformas de proteção de endpoints (EPP) se tornaram uma etapa fundamental no combate às ameaças complexas.

Mais recentemente, as organizações adicionaram a implantação de ferramentas mais avançadas para se defender dos ataques. Elas podem ser usadas para identificar e responder aos comportamentos anômalos em endpoints, por meio da detecção e resposta de endpoint (EDR), rede ou por meio da detecção e resposta de rede (NDR, na sigla em inglês).

No entanto, como acabamos de observar, os criminosos virtuais aprimoram constantemente suas estratégias e elaboram métodos mais sofisticados de ataques direcionados às empresas. 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.

Os agentes maliciosos potencializam as técnicas avançadas, como as de engenharia social (inclusive com phishing e comprometimento do e-mail corporativo), comprometimento de contas, aplicativos públicos de leitura facial e exploits de dia zero para violar as defesas das organizações, o que torna a proteção desses negócios um desafio considerável tendo em vista as ameaças em evolução.

APTs, por exemplo, burlam 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.

A enorme magnitude e complexidade destes ataques representam um desafio para as organizações manterem uma postura proativa. E sua superfície de ataque em constante expansão, inclusive os dispositivos móveis, ambientes de nuvem e trabalho remoto, assim como servidores e etc, aumentam ainda mais a dificuldade.

51% das organizações sofrem para detectar e investigar ameaças avançadas com as ferramentas atuais.

Relatório da ESG Research, Modernização do SOC e a importância do XDR

Além disso, as organizações necessitam gerenciar as ameaças internas, as vulnerabilidades na cadeia de suprimentos, os requisitos de conformidade regulatória e, ao mesmo tempo, enfrentar a persistente escassez de profissionais qualificados em segurança virtual. E o dano potencial para os sistemas corporativos, operações e reputações resultantes das violações de dados, ransomware, ataques de negação de serviço distribuída (DDoS), APTs, ciberespionagem, entre outros, podem ser imensos.

Portanto, chegar na segurança efetiva contra essas ameaças requer uma abordagem abrangente e proativa que combina tecnologias avançadas, políticas robustas, monitoramento vigilante, treinamento constante e muito mais, ou seja, uma visão em 360° exata do cenário de ameaças que o XDR está pronto para entregar.

Ao eliminar os obstáculos entre as soluções pontuais específicas de camada, o XDR oferece aos centros de operações de segurança (SOCs) e equipes de segurança de TI a visibilidade e integração de ponta a ponta para identificar e responder a ameaças mais rapidamente, resolvê-las eficazmente e minimizar o dano causado.

Quem precisa desse tipo de segurança?

A solução ideal é aquela que complementa a proteção de endpoints com segurança em nível de EDR e que diminui significativamente a carga de trabalho. Quanto mais ameaças são evitadas, menos ruído é criado para as equipes de segurança investigarem.

Por anos, PMEs e microempresas têm conseguido contar com a EPP para se protegerem de uma ampla gama de ameaças comuns. Entretanto, assim como foi discutido brevemente, os atacantes contemporâneos estão focados nas organizações de todos os tamanhos, setores e níveis de preparo, com PMEs e empresas menores com risco constante em face das ameaças evasivas e avançadas anteriormente direcionadas somente para as organizações muito maiores.

Em resposta a isso, as equipes de segurança de TI complementam a EPP existente com serviços de EDR e/ou detecção e resposta gerenciada (MDR), o que permite detectar e investigar incidentes de segurança, conter a ameaça no endpoint e receber uma resposta automática e/ou orientação de como remediar o incidente.

Dessa forma, a solução ideal é aquela que complementa a proteção de endpoints com segurança em nível de EDR e que diminui significativamente a carga de trabalho. Quanto mais ameaças são evitadas, menos ruído é criado para as equipes de segurança investigarem. Com isso, as equipes de segurança de TI podem otimizar os principais recursos e se concentrar nas tarefas de TI, em vez de perseguir falsos positivos e grandes volumes de alertas.

Ao migrar para um nível mais alto, de EDR para MDR, o elemento "estendido" na detecção e resposta estendidas reflete o fato de que, no XDR, uma solução de EDR é complementada e é estreitamente integrada com uma variedade de outras ferramentas de segurança que não necessariamente sejam desenvolvidas para trabalhar em conjunto. Em vez de usar diversas ferramentas de segurança como as soluções de ponto de barreira, o XDR viabiliza para as organizações a criação de um ecossistema de segurança abrangente, flexível e escalável que maximiza os benefícios das ferramentas existentes que podem ser personalizadas para as necessidades da organização, além de reduzir os riscos e torná-la mais segura.

Portanto, para responder a pergunta "qual é o tipo de segurança adequado a cada empresa?", é necessário levar em consideração os seguintes pontos fundamentais:

- Todas as organizações precisam de um fundamento sólido e moderno de segurança de endpoints.
- Além disso, o nível adicional de segurança requerido dependerá amplamente de uma combinação de tipos de ciberataque para os quais a organização está potencialmente exposta e das habilidades de segurança de TI encarregada de implementar e usar as ferramentas requeridas para evitar esses problemas.

Agora, analisaremos as cinco etapas que ajudarão a avaliar e operacionalizar os requisitos de segurança em relação a essas considerações.

Como avaliar os requisitos de segurança em evolução (EPP, EDR e MDR)

Etapa 1:

Analise a proteção de endpoints existente

Com tantas soluções avançadas de segurança virtual disponíveis no mercado, é fácil esquecer o papel vital desempenhado pela proteção de endpoints. Por que os endpoints são tão importantes? Eles são os pontos de entrada mais comuns para a infraestrutura de uma organização, e o alvo principal de criminosos virtuais, além de serem as principais fontes de dados necessários para a investigação eficaz de incidentes complexos.

Dessa forma, cada organização deve escolher uma EPP que forneça proteção automatizada contra o grande número de possíveis incidentes causados por ameaças comuns, inclusive ameaças sem arquivo e ransomware.

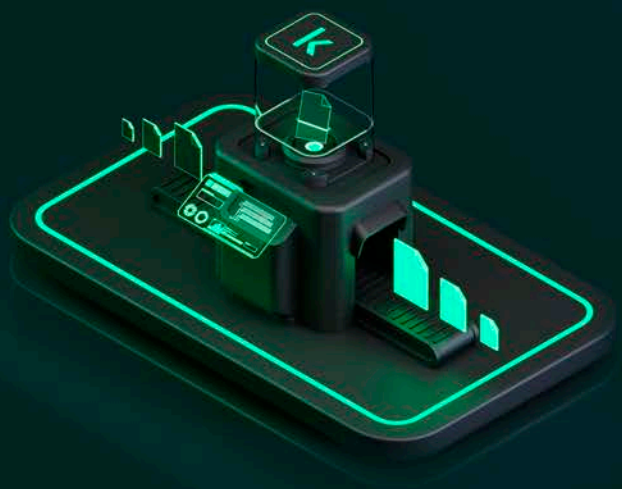
Como esse tipo de configuração requer conhecimento relativamente limitado ou uma pequena equipe especializada em segurança, ele atende às necessidades de segurança de endpoints de PMEs ou empresas de menor porte sem equipe de segurança dedicada, ou organizações com níveis muito baixos de experiência em segurança virtual.

Ele também é um estágio básico fundamental para empresas de médio e grande porte, em que, ao lidar automaticamente com um grande número de ameaças menores, a solução abre caminho para que as equipes de segurança se concentrem em defesas mais avançadas quando necessário.

Considerações principais

Ao receber a EPP para avaliar se ele está entregando os recursos necessários, considere os seguintes aspectos:

- Qual é o grau de eficiência?
- Quantos falsos positivos você está recebendo?
- Oferece recursos de redução eficaz da superfície de ataque, como arquivo, Web e antivírus de correio, proteção de rede, interface de verificação antimalware (AMSI, na sigla em inglês), prevenção contra exploit, remediação, detecção de comportamento e prevenção de invasões baseado em host (HIPS, na sigla em inglês)?
- Ajuda a automatizar tarefas de rotina?
- É fácil de operar e ajuda a minimizar custos e sobrecargas em sua equipe de TI?
- Oferece assistência com as tarefas críticas, como avaliação da vulnerabilidade, inventário de software/hardware, firewall, Web, controles de dispositivo e aplicativo e cloud discovery?



Etapa 2:

Identifique lacunas críticas em suas defesas de endpoint

Por que a EPP moderna requer recursos de EDR

Assim como foi discutido neste e-book, o cenário de ameaças em evolução indica que, ao longo do tempo, ameaças cada vez mais sofisticadas, que antes afetavam apenas grandes organizações, estão se propagando para impactar PMEs e empresas de menor porte sem recursos internos para lidar com elas de forma eficaz.

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 segurança virtual para organizações que usam soluções tradicionais de EPP.

Essas questões são ainda mais agravadas pela falta de transparência de EPP tradicional. Na verdade, essas soluções oferecem apenas uma representação positiva ou negativa de que uma invasão está ou não está ocorrendo. Por outro lado, o que uma equipe de TI com habilidades básicas de segurança necessita é a visibilidade sobre o que está acontecendo em cada endpoint para que seja possível analisar em mais detalhes e aumentar o entendimento sobre a ameaça.

As soluções modernas de EPP com recursos de EDR simples e integrados, portanto, oferecem um importante ponto de partida entre o EPP tradicional e mais avançado completamente integrado com as soluções de EDR.

Embora a EPP proteja contra uma ampla variedade de ameaças comuns, também é preciso considerar sua defesa contra ameaças novas, desconhecidas e evasivas que burlam a EPP.

Os ataques estão cada vez mais baratos para os cibercriminosos, colocando mais organizações em risco. E, além de ocorrerem com mais frequência, esses tipos de ataques se tornaram muito mais eficazes devido à combinação, teste e uso de técnicas variadas para burlar com eficácia a segurança do endpoint.

Lidar com essas ameaças também se tornou cada vez mais urgente devido a mudanças como a diluição de perímetros corporativos decorrentes do aumento do trabalho remoto. Todas essas tendências juntas estão criando uma necessidade de uso de EPP, cujos recursos vão além das soluções tradicionais de EPP oferecidas, que incluem, em particular, recursos básicos de EDR, como análise de causa raiz simples.

Considerações principais

Sendo assim, 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.

Para implementar uma solução eficaz de defesa contra essas ameaças, também será preciso considerar os aspectos de sua organização, incluindo porte, perfil corporativo, preparação de segurança, recursos existentes, experiência, e em particular, as habilidades de segurança de sua equipe ou segurança de TI.

Etapa 3:

Tenha clareza sobre o que deseja alcançar

Muitas organizações têm tempo e recursos limitados (ou um departamento de segurança de TI pequeno e sem planos de expansão), mas precisam entender o que está acontecendo em sua infraestrutura e ser capazes de responder a ameaças evasivas antes que ocorram danos.

Adicionar capacidades apropriadas de EDR à EPP moderna pode fornecer uma defesa eficaz contra ameaças evasivas mais avançadas. Isso deve permitir respostas automatizadas e/ou rápidas e precisas com um único clique, como colocar arquivos em quarentena, isolar hosts, interromper processos, excluir objetos etc. E, se houver especialistas de segurança de TI, a solução também deve fornecer informações, insights e ferramentas para investigações eficazes, como análise de causa raiz, criação de indicadores de comprometimento (IoCs) personalizados, importação de IoCs e verificação desses mesmos itens em todos os endpoints.

Além disso, contar com uma solução que faça o melhor uso de todas as funções realmente necessárias é o ideal sem ter que pagar por um monte de itens desnecessários, além de ter que recrutar especialistas de segurança de TI com as habilidades necessárias para trabalhar com elas.

5 equívocos comuns sobre EDR

1 Nossa proteção de endpoints está ótima e não precisamos de EDR

Equívoco: Nossos negócios não são atrativos para criminosos virtuais, não somos alvo de ataques que podem ser protegidos com EDR.

Realidade: Embora seja fácil pensar que as empresas menores não sejam visadas por criminosos virtuais, a realidade é que PMEs enfrentam muitas das mesmas ameaças enfrentadas pelas empresas de grande porte. Ainda que a grande maioria dos ciberataques sejam ameaças comuns, uma grande parte dos ataques restantes são novos, desconhecidos e evasivos que burlam a EPP tradicional. A detecção dessas ameaças é desafiadora devido à diversidade de técnicas de evasão empregadas, especialmente por meio do uso de ferramentas legítimas e recursos nativos do sistema. Além disso, por ficarem indetectáveis por um longo período, elas também têm o tempo necessário para explorar e se mesclarem à infraestrutura da empresa, causando grandes prejuízos, seja por meio de vazamento de dados, ataques de ransomware ou spyware, ou apagando e substituindo operações.

2 Precisamos de EDR para compensar uma EPP fraca

Equívoco: Nossa EPP não é eficaz o suficiente, por isso precisamos do EDR para fortalecê-lo.

Realidade: Tentar fortalecer a segurança de seu endpoint investindo em uma solução de EDR sem resolver problemas com a EPP é como tapar o sol com a peneira. Uma EPP fraca pode prejudicar muito a EDR, de modo que não produza os resultados necessários. Além disso, se a solução de EDR for especificada de forma exagerada para suas necessidades atuais, ela poderá ser muito cara e sua equipe poderá ter dificuldade para entendê-la e usá-la.

3 É preciso ter uma equipe de segurança de TI especializada para usar EDR

Equívoco: As SMBs ou microempresas não têm especialistas em segurança suficientes com as habilidades necessárias para entender e operar as ferramentas de detecção, investigação e resposta a ameaças evasivas.

Realidade: Quando o EDR foi introduzido pela primeira vez, os sistemas eram complicados e difíceis de usar. Mas com as soluções modernas, sempre que um alerta for recebido, a ferramenta de EDR ajudará a entender a origem da ameaça, como ela se desenvolveu, qual é sua causa e se ela chegou a outros hosts, ou seja, qual é sua escala. Ela também guiará você por um processo simples para lidar com incidentes, que inclui etapas como identificação, contenção, erradicação, recuperação e análise de lições aprendidas para ajudar você a se preparar para ataques futuros.

4 Não é possível combinar EDR e MDR

Equívoco: Se quiser segurança com EDR, será necessário investir em EDR para sua equipe interna usá-la ou terceirizar a detecção e resposta gerenciada (MDR, na sigla em inglês) para um provedor especializado.

Realidade: Escolher a segurança com EDR não exclui outras opções. A EDR e a MDR têm seus próprios benefícios, e a melhor opção geralmente é combinar as duas. Então, por exemplo, uma SMB ou microempresa pode usar a MDR para aumentar os recursos de segurança de TI e se proteger de ameaças evasivas sem precisar aumentar a equipe ou investir em recursos. Enquanto isso, uma empresa de grande porte pode utilizá-la para diminuir a carga dos processos de triagem e investigação de incidentes 24/7 e concentrar melhor os recursos de segurança de TI interna com o uso de EDR para investigar os detalhes e responder às ameaças.

5 A EDR gera alertas demais e não vale o esforço

Equívoco: O EDR é conhecido por gerar um grande número de alertas e falsos positivos, e as equipes de TI não têm tempo nem recursos para agir ou resolvê-los.

Realidade: As soluções de EDR modernas não apenas automatizam muitas tarefas, mas a EDR e/ou a MDR também podem reduzir o risco relativo a um ataque evasivo e renovar sua confiança na segurança de seu endpoint. Em vez de ficar inseguro quanto ao que está acontecendo em seu ambiente, você terá visibilidade e controle em todos os endpoints. E, em vez de ficar relutante em atualizar a segurança devido à complexidade, haverá uma solução simplificada e consolidada que ajuda a otimizarseus recursos.

Experimente nosso jogo simulado e interativo de ransomware para descobrir como proteger melhor a infraestrutura de TI:
https://www.kaspersky.com/response-game/en/

Etapa 4:

Pense em seus casos de uso

Antes de poder identificar a proteção que melhor atenda às suas necessidades, é preciso definir os requisitos claros para ela. Isso significa considerar os aspectos fundamentais do desempenho e do uso da solução, como os casos de uso que se precisa que ela cumpra e os resultados esperados que ela entregue.

Por exemplo, quando você recebe um alerta de segurança, a ferramenta de EDR e/ou MDR deve permitir que você responda a perguntas importantes, como:

- Qual é o contexto do alerta?
- Quais ações já foram realizadas no alerta?
- A ameaça detectada ainda está ativa?
- Há outros hosts sob ataque?
- Que caminho o ataque tomou?
- Qual é a principal causa da ameaça?

Também deve ajudar a compreender o escopo completo da ameaça. Por exemplo:

- Se sua empresa corre o risco de sofrer uma ameaça global, sua equipe de gerenciamento vai querer ser tranquilizada sabendo que o ataque não está acontecendo no momento. Para isso, é preciso encontrar um indicador de comprometimento (IoC) on-line, executar uma verificação e responder corretamente às preocupações.
- Se uma autoridade de regulamentação solicitar a execução de uma verificação para um IoC específico, será preciso ter a capacidade de importar IoCs de fontes confiáveis e fazer verificações periódicas em busca de sinais de um ataque.
- Se você investigou completamente um alerta e gerou um IoC com base na ameaça descoberta, em vez de executar varreduras em toda a rede para descobrir se outros hosts foram afetados, essa tarefa deve ser realizada automaticamente.

Da mesma forma, também será preciso ter a capacidade de responder rapidamente a ameaças crescentes e velozes:

- Contendo a ameaça isolando o host, colocando o arquivo em quarentena ou evitando que os arquivos sejam executados durante a investigação.
- Usando resposta de endpoint cruzada e automatizada, baseada em verificações de IoC, para viabilizar a resposta a ameaças evasivas assim que forem descobertas, ou guiada e cenários de resposta remota se estiver usando MDR.

Dentre os principais resultados esperados da sua solução, destacamos:

- Proteção contra ameaças evasivas mais frequentes e destrutivas.
- Economia de tempo e de recursos com uma ferramenta automatizada simples.
- Avaliação do alcance de um ataque com a verificação de IoCs em todos os endpoints.
- Compreensão da causa básica de cada ameaça e de que como ela realmente ocorreu.
- Prevenção de outros danos com a resposta automatizada rápida.

5 equívocos comuns sobre MDR

1 A MDR é apenas mais um serviço de segurança gerenciado

Equívoco: A MDR é como qualquer outro serviço de segurança gerenciado (MSS, na sigla em inglês) que envolve a gestão da sua infraestrutura de TI por parte do fornecedor.

Realidade: Os MSSs costumam abranger uma variedade de serviços de segurança virtual como avaliação de conformidade regulatória, VPNs e firewalls, testes de invasão, recomendações de ofertas etc. Enquanto a MDR é voltada para a detecção avançada e a resposta rápida a ameaças novas, desconhecidas e evasivas que burlam a EPP automatizada. Para isso, ela utiliza uma combinação de descoberta, detecção e análise de ameaças de acordo com TTPs.

2 A MDR é destinada apenas para grandes empresas

Equívoco: Como a MDR lida com recursos complexos, como descoberta de ameaças e indicadores de ataque (IoAs, na sigla em inglês), ela se adequa apenas às necessidades de grandes empresas.

Realidade: A MDR não é uma solução que funciona para todos. Ela fornece diferentes recursos para diferentes tipos de organizações. Uma PME ou microempresa poderia usar a MDR para melhorar instantaneamente a segurança de TI e garantir proteção contra ameaças evasivas, enquanto uma empresa de grande porte poderia usá-la para diminuir a carga da triagem e investigação de incidentes e direcionar melhor o foco interno de segurança de TI.

3 MDR com IA não precisa de pessoas especializadas

Equívoco: Com o grande avanço da inteligência artificial (IA) e do Machine Learning (ML), em breve, o trabalho de pessoas especializadas em MDR será uma coisa do passado.

Realidade: IA, ML e IoAs exclusivos costumam ser capazes de processar um grande número de alertas automaticamente, ativando a triagem inicial de incidentes, minimizando o tempo médio de detecção (MTTD, na sigla em inglês) e o tempo médio de resposta (MTTR, na sigla em inglês). Com isso, ocorre um aumento no rendimento do analista de MDR, e a garantia da proteção contínua até mesmo contra as ameaças mais inovadoras sem malware. Mas para os TTPs (táticas, técnicas e procedimentos) antes desconhecidos ou controlados por humanos que não automatizam a detecção, a descoberta gerenciada de ameaças ainda requer a proatividade e o esforço manual da equipe de busca de ameaças.

4 A MDR é difícil de implementar

Equívoco: A MDR é frequentemente comercializada como se oferecesse os recursos de um SOC 24/7, portanto o seu uso deve ser complicado.

Realidade: Como foi destacado acima, a MDR pode ser usada para tudo: desde a prevenção contra as ameaças que burlam as defesas cibernéticas até a oferta de uma segunda opção ou mesmo liberar os especialistas internos para que se concentrem nas tarefas mais importantes. Isso é resultado de um serviço turnkey de fácil implementação que oferece melhorias drásticas no MTTD e no MTTR, e quanto mais rápido o MTTD e o MTTR, menos interrupções causadas pelos incidentes e menores são os custos resultantes.

5 Mesmo com MDR, sua equipe ainda tem muito trabalho

Equívoco: Os serviços de MDR param após a investigação de incidentes e deixam os clientes com relatórios técnicos e recomendações para aplicar nos sistemas, além de aumentar ainda mais a pressão sobre os recursos de segurança de TI.

Realidade: Embora esse fosse o caso no passado, com os serviços de MDR modernos, é possível optar por autorizar o provedor a responder automaticamente, iniciar as ações de resposta recomendadas (como isolar o host, mover arquivos para quarentena, remover arquivos, encerrar processos, solicitar arquivos ou executar um programa no host, verificação de indicadores de comprometimento (IoC, na sigla em inglês) e etc) ou aproveitar os cenários de correção gerenciada que podem ser pré-aprovados ou aprovados manualmente para cada alerta.

O Security Operations Center (SOC) e o Global Emergency Response Team (GERT) da Kaspersky analisaram o impacto dos incidentes de cibersegurança do ano, abrangendo todos os setores, para desenvolver um panorama inigualável do cenário de ameaças.

Acesse os relatórios:
https://go.kaspersky.com/mdr-and-ir-reports-2022.html

Etapa 5:

Escolha a proteção que se ajuste às suas necessidades

Muitas organizações não têm recursos para dedicar funcionários especificamente à segurança de TI. Algumas outras podem estar ainda no processo inicial de desenvolvimento de um departamento de segurança de TI. E outros podem já ter equipes de segurança de TI totalmente formadas e qualificadas.

Muitas organizações não têm recursos para dedicar funcionários especificamente à segurança de TI. Algumas outras podem estar ainda no processo inicial de desenvolvimento de um departamento de segurança de TI. E outros podem já ter equipes de segurança de TI totalmente formadas e qualificadas. A experiência disponível dessas organizações em relação às defesas contra ameaças varia amplamente, assim como a quantidade de tempo que elas podem dedicar a essa tarefa.

Para lidar com essas circunstâncias diferentes, as organizações que não dispõem de uma equipe de segurança de TI dedicada, ou aquelas cuja equipe de segurança de TI está sobrecarregada com tarefas de rotina, precisarão fazer uso estratégico da automação para combater as ameaças evasivas mais recentes.

Isso significa complementar a EPP com ferramentas adicionais de EDR que, ao passo que protegem contra essas ameaças, também incorporam níveis apropriados de automação (total ou parcial).

Como alternativa, em vez de investir em uma solução de EDR excessivamente complexa para a qual as empresas podem não ter o tempo ou as habilidades necessárias, a MDR permite que as organizações acessem recursos como monitoramento de segurança 24/7 por especialistas do setor, descoberta automática e gerenciada de ameaças e cenários de resposta guiada e remota por um fornecedor, provedor de serviços gerenciados (MSP, na sigla em inglês) ou provedor de serviços de segurança gerenciados (MSSP, na sigla em inglês).

Uma terceira opção é combinar EDR e MDR. Muitas organizações não têm o conhecimento necessário para a descoberta de ameaças, portanto, terceirizar essa tarefa e, ao mesmo tempo, implementar recursos de detecção e resposta internamente é a solução ideal. E essa opção pode ser especialmente positiva para empresas que desejam desenvolver uma equipe de segurança virtual própria, mas carecem de recursos, pessoal e/ou habilidades para dar suporte a detecção e resposta de especialistas.

Mas, e se os recursos internos forem limitados?

Digamos que seus recursos internos de segurança de TI sejam limitados ou que a equipe seja pequena, com apenas um ou dois especialistas em segurança. Vamos supor também que você esteja tentando decidir se complementa sua EPP com EDR e/ou MDR. Quais tipos de benefícios podem ser esperados? E qual opção é a mais adequada para você?

Se preferir uma abordagem mais prática (e sua equipe de TI tiver habilidades de segurança suficientes), o EDR pode ajudar a evitar interrupções e danos comerciais ao eliminar os riscos apresentados por ameaças novas, desconhecidas e evasivas para fornecer à equipe de segurança a visibilidade necessária para a investigação, análise da causa raiz e a resposta.

Isso pode gerar eficiência de custos, permitindo que sua equipe de segurança trabalhe de modo mais eficaz sem ter de lidar com várias ferramentas e consoles, além de maximizar a capacidade ao automatizar uma ampla variedade de processos. Essas ferramentas também proporcionam mais tranquilidade ao facilitar o monitoramento e a detecção de ameaças e a resposta e a prevenção de ataques.

Se você deseja expandir sua capacidade de segurança de TI interna removendo a carga das principais tarefas de detecção e resposta, o MDR pode oferecer proteção avançada e ininterrupta contra ameaças que, de outra forma, poderiam burlar as barreiras de segurança automatizadas. Isso pode ajudar a capacitar sua empresa e solucionar a crise de talentos da segurança virtual ao fornecer todos os principais benefícios de um SOC 24/7.

A MDR também aumenta a eficiência de custos, concentrando os recursos internos nas tarefas críticas que realmente exigem o envolvimento da equipe ou de segurança de TI e maximiza a capacidade ao aproveitar os modelos avançados de ML para aumentar significativamente o rendimento do analista e minimizar o MTTR. Além disso, ela pode fornecer monitoramento de segurança contínuo por especialistas do setor juntamente com a descoberta automatizada e gerenciada de ameaças. Isso inclui a análise de ameaças complexas que não são malware e ameaças perigosas e difíceis de detectar usando ferramentas legítimas do sistema operacional em ataques.

Enquanto isso, a combinação de EDR e MDR permite que você adapte os recursos de classe de EDR às necessidades da sua empresa, por exemplo, terceirizando a descoberta de ameaças (tarefa para a qual você pode não ter o conhecimento necessário) enquanto implementa recursos internos de detecção e resposta de endpoint.

Como avaliar os requisitos de segurança cada vez mais dinâmicos – XDR

40% das organizações implementarão uma plataforma de XDR até 2027, ou seja, um aumento de 5% desde 2021

De acordo com o Estudo Cyber Resilient Organization 2021 da IBM, 32% das organizações relataram usar de 21 a 30 ferramentas de segurança individuais em resposta a cada ameaça, e 13% relataram usar 31 ferramentas ou mais.

Como consequência da quantidade de ferramentas envolvidas, as ameaças avançadas demoram muito para serem identificadas e contidas.

O relatório da IBM sobre os custos de uma violação de dados em 2022 revelou que se levou em média 277 dias para detectar e resolver um incidente de violação de dados, portanto uma violação que ocorreria em 01 de janeiro não seria contida até 04 de outubro.

O XDR em resumo

Se sua empresa tem porte médio ou grande, e se sua equipe de SOC ou TI ainda não o questionou sobre o uso do XDR, isso será apenas uma questão de tempo para que isso seja feito.

De acordo com a CRN (15.02.2023), "quando falamos em detecção e resposta contra ameaças, analisar o endpoint e a rede não é mais satisfatório. A abordagem que muitas das maiores empresas de segurança virtual do mundo estão colocando em prática nessa esfera é o XDR, ou seja, a detecção e resposta estendidas. Uma das categorias com o crescimento mais acelerado em segurança virtual atualmente, o XDR tem o objetivo de oferecer segurança aprimorada ao correlacionar os dados entre os ambientes e dispositivos das organizações, e em seguida, priorizar as ameaças mais sérias para oferecer uma resposta.

"Independentemente da forma como são definidas, todas as plataformas de XDR compartilham da intenção de capacitar equipes de segurança de TI com recursos limitados, buscando aprimorar a qualidade da detecção das ameaças e reduzir a sobrecarga de alertas."

Com o XDR, as soluções de segurança que podem não ter sido projetadas especificamente para funcionar em uníssono podem colaborar perfeitamente na prevenção, detecção, investigação e resposta a ameaças. E ao eliminar as lacunas de visibilidade entre as ferramentas de segurança virtual e suas camadas, o XDR permite que as equipes de segurança sobrecarregadas detectem e resolvam as ameaças mais rápida e eficientemente; e capturem dados mais completos e contextuais para ajudá-los a tomar decisões de segurança melhores, evitando futuros ataques.

Mas, o que o XDR faz exatamente, quais são seus benefícios, e por que ele pode ser considerado um dos investimentos mais significativos em segurança que sua organização fará?

EDR vs MDR vs XDR

EDR
Detecção e resposta de endpoint

- Identifica ameaças novas, desconhecidas e evasivas que estão burlando a proteção de endpoint e automatiza as tarefas rotineiras de segurança

MDR
Detecção e resposta gerenciadas

- Sobrecargas de detecção de ameaças, descoberta de ameaças e investigação de incidentes ou medidas existentes adicionais ao entregar proteção contra ameaças avançadas 24/7

XDR
Detecção e resposta estendidos

- Detecta proativamente as ameaças complexas entre múltiplos níveis da infraestrutura e automaticamente responde e contra-ataca estas ameaças

Como funciona

- Aprimora a visibilidade e visualização de ameaças
- Oferece mecanismos de detecção avançados (por exemplo, IoC e IoA)
- Simplifica a análise de causa raiz e oferece suporte a busca de ameaças
- Entrega uma resposta rápida, centralizada e automatizada

- Entrega a proteção contínua e especializada contra as ameaças mais complexas e inovadoras de não-malware

- Integra-se com diversas ferramentas de segurança, aplicativos e infraestrutura de segurança virtual existente
- Monitora os dados entre diversas fontes para detectar e eliminar as ameaças complexas

Valor comercial

- Permite que as equipes de segurança de TI trabalhem de forma mais eficaz sem precisar controlar várias ferramentas e consoles.
- Automatiza uma vasta gama de processos para evitar a dependência de processos tradicionais de remediação que possam resultar em tempo de inatividade
- Facilita o monitoramento e detecção de ameaças, a reunião centralizada de dados forenses, além de responder e evitar ataques

- Foco nos caros recursos internos para as tarefas críticas que realmente demandam o envolvimento da equipe de segurança de TI
- Potencializa os modelos proprietários de machine learning para aumentar significativamente o rendimento do analista e reduzir MTTD e MTTR
- Resolve a crise de talentos em segurança virtual
- Oferece todos os grandes benefícios de um SOC 24/7

- A abordagem do ecossistema maximiza a eficiência das ferramentas de segurança cibernética 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?

- Tecnologicamente conservador e com os negócios apresentando aversão aos riscos que desejam agregar visibilidade na proteção automática
- Usuários tradicionais de TI que desejam desenvolver processos de resposta a incidentes
- Organizações que usam a TI como uma vantagem competitiva e que necessitam capacitar os especialistas para encontrar e neutralizar ameaças complexas

- As empresas que procuram expandir a capacidade de segurança de TI interna ao descarregar as tarefas de detecção principal e de resposta
- As organizações que talvez não possam ter o orçamento ou equipe de especialistas disponíveis para desenvolver seu próprio SOC interno

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

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

Expectativas quanto aos recursos e benefícios específicos de uma plataforma XDR

Plataforma única que integra diversas ferramentas de segurança

Com o XDR, as soluções de segurança que podem não ter sido projetadas especificamente para funcionar em uníssono podem colaborar perfeitamente na prevenção, detecção, investigação e resposta a ameaças.

- Isso poderia incluir, por exemplo, soluções desenvolvidas para proteger o correio, a Web, a rede, a infraestrutura de nuvem, aplicativos, identidade e etc, para permitir a detecção e investigação de outros tipos de cenários de ataque e fortalecer o processo de combate a ameaças complexas.
- O XDR também pode integrar as ferramentas de inteligência contra ameaças, como os feeds de dados de ameaças e a plataforma usada para gerenciar esses dados, para oferecer às equipes de SOC um contexto complementar muito importante para a investigação de incidentes virtuais complexos.
- Além disso, dependendo do setor e dos requisitos da organização, o XDR pode integrar as ferramentas de segurança de tecnologia operacional (OT, na sigla em inglês) e Internet das Coisas (IoT, na sigla em inglês) para estender a abrangência da segurança entre os ambientes de TI/OT.

Une os diversos tipos de telemetria

Ao permitir a análise comportamental e de telemetria em tempo real em várias camadas de segurança, incluindo endpoint, rede e nuvem, os analistas de segurança podem visualizar melhor as ameaças virtuais, eliminando-as de acordo com a gravidade com que podem impactar a infraestrutura de TI da organização.

Entrega visibilidade contra ameaças de ponta a ponta

Ao eliminar os obstáculos entre as soluções pontuais específicas de camada, o XDR oferece ao SOC e equipes de segurança de TI a visibilidade e integração de ponta a ponta para identificar e responder a ameaças mais rapidamente, resolvê-las eficazmente e minimizar o dano causado.

Como o XDR pode vincular cada etapa ao longo de toda uma cadeia perigosa e apresentá-la como um único alerta ao detalhar o contexto completo dos ataques, isso reduz o volume de alertas, aumenta a sua qualidade e viabiliza a orquestração e resposta de ponta a ponta.

Dinamiza e centraliza a coleta de dados e aumenta a eficiência

Um único data lake entrega uma coleção de logs abrangente, gerenciamento e armazenamento ao oferecer uma plataforma centralizada para coletar, indexar e analisar os logs de diversas fontes, inclusive os das soluções de segurança (EPP, FW, NGFW, IAM, SIEM, SOAR e etc), sistemas operacionais, aplicativos corporativos (sistemas de RH, ferramentas do Office), segurança física (sistemas de controle de acesso automatizado) e outros dispositivos.

Assim, o SOC e as equipes de segurança de TI podem ter insights valiosos, detectar anomalias e identificar incidentes potenciais de segurança ao dinamizar a riqueza do log de abrangência de dados dos eventos no passado e presente (em tempo real). A integração com outras ferramentas e plataformas de segurança também aprimora a eficiência operacional ao centralizar o gerenciamento de segurança e oferecer uma visão unificada dos eventos e incidentes de segurança.

Acelera a detecção, investigação e resposta contra ameaças

Ao eliminar as lacunas de visibilidade entre as ferramentas de segurança virtual e suas camadas, o XDR permite que as equipes de segurança sobrecarregadas detectem e resolvam as ameaças mais rápida e eficientemente; e capturem dados mais completos e contextuais para ajudá-los a tomar decisões de segurança melhores, evitando futuros ataques.

Ao automatizar as tarefas de rotina, como a triagem de ameaças, contenção e remediação, as organizações podem otimizar os recursos de segurança e direcionar o foco em atividades mais estratégicas.

Reduz o MTTD e o MTTR

O XDR ajuda a minimizar o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR), fundamentais para o combate complexo das ameaças e ataques direcionados, onde as ações rápidas adotadas pelos especialistas de segurança de TI reduzem o tempo de permanência e as chances de os atacantes atingirem o objetivo de causar danos financeiros ou de reputação para a organização.

Melhora a busca de ameaças

Ao potencializar a inteligência contra ameaças mais recente, o XDR aprimora a busca e descoberta de ameaças, enquanto a automação das tarefas de rotina, os processos de investigação guiados e todas as detecções personalizáveis promovem a aceleração da resolução de incidentes. As ameaças avançadas são detectadas e neutralizadas com mais rapidez e precisão, ponto crucial para lidar com ataques complexos e do tipo APT.

Ajuda a enfrentar a escassez global de especialistas de segurança de TI

Diante da escassez global de especialistas em segurança de TI, o XDR oferece proteção holística para uma infraestrutura de TI em expansão e em constante mudança contra um cenário de ameaças virtuais em rápida evolução. O XDR simplifica os trabalhos valiosos e em escassez de recursos, como os especialistas de segurança de TI, reduz a necessidade de se envolver com as tarefas de rotina e libera os profissionais para que possam lidar com os processos de trabalho que envolvem incidentes complexos.

Compatível com conformidade regulatória e gerenciamento de risco

Ao fornecer a visibilidade abrangente, a inteligência contra ameaças e os recursos de geração de relatórios, as organizações podem demonstrar conformidade com as regulamentações do setor e estrutura, como a GDPR, PCI DSS, HIPAA, entre outras. Isso ajuda a mitigar os riscos legais e financeiros associados com a não conformidade.

O gerenciamento de log também representa um papel fundamental para garantir a conformidade com o setor ou os padrões e regulamentações regionais ao facilitar o armazenamento e a retenção de dados e logs para os períodos pré-determinados, e ao permitir que as organizações recuperem a analisem facilmente os logs quando houver necessidade.

Entrega de gerenciamento amigável para o usuário por meio de um console único

As soluções de XDR amigáveis oferecem insights abrangentes em relação às ameaças contínuas e atividades suspeitas por meio de um único console. Isso viabiliza a busca proativa de ameaças e uma resposta mais rápida aos incidentes, além de entregar uma visão holística que ajuda as equipes de SOC a identificar atividades suspeitas e potenciais incidentes de segurança mais eficientemente.

Opções de plataforma aberta e nativa

O XDR aberto é compatível com as integrações de terceiros para coletar formas específicas de telemetria e ativar a detecção, busca e investigação de ameaças entre as diferentes fontes de dados para executar ações de resposta. Isso evita a dependência de um único fornecedor e permite que as organizações potencializem as ferramentas de segurança de terceiros já implementadas, além de viabilizar a escolha dos produtos mais adequados de diferentes fornecedores.

O XDR nativo é uma solução construída por um único fornecedor e desenvolvido para trabalhar com os produtos do vendedor.

Implementação em nuvem e/ou on-premises

Enquanto a ampla maioria das plataformas de XDR são abertas e baseadas em nuvem, a implementação on-premises é ideal para as organizações que desejam ativar a completa soberania de dados, além de garantir a vigência dos requisitos de regulamentação e conformidade.

Integração com Zero Trust

Usados em conjunto, o XDR e o Zero Trust fornecem uma defesa poderosa contra as ameaças virtuais. O conceito de Zero Trust ajuda a evitar o acesso não autorizado a recursos e aplicativos, permitindo revogar o acesso concedido caso as condições se alterem. Por outro lado, o XDR atua na detecção e resposta a possíveis ameaças que conseguem contornar esses controles iniciais.

XDR vs. SIEM vs. SOAR

XDR
Detecção e resposta estendidos

- Detecta proativamente as ameaças complexas entre múltiplos níveis da infraestrutura e automaticamente responde e contra-ataca estas ameaças

SIEM
Segurança da informação e gerenciamento de eventos

- Coleta, agrega, analisa e armazena dados de log na infraestrutura de TI para diversos casos de uso, incluindo governança, conformidade e correspondência de correlação baseada em regras para atividades suspeitas

SOAR
Orquestração segura e resposta automática

- Coleta dados provenientes de diversas fontes na infraestrutura, abrangendo sistemas de gerenciamento e plataformas de inteligência de ameaças, visando oferecer análise de prioridades
- Permite que as equipes de segurança configurem respostas automatizadas em diversos estágios e entre as soluções para as ameaças apresentadas

Como funciona

- Integra múltiplas ferramentas e aplicativos de segurança
- Monitora os dados nos endpoints, redes, nuvens, servidores da Web, servidores de correio eletrônico e etc, para assim detectar e eliminar ameaças complexas

- Investiga qualquer padrão ou eventos que possam indicar comportamento suspeito e gera um alerta para o SOC ou equipe de segurança de TI

- Usa roteiros para automatizar uma ampla variedade de processos, incluindo a verificação de vulnerabilidades, análise de logs, administração de acessos de usuário, triagem de ameaças e outras tarefas operacionais
- Orquestra diversas ferramentas distintas, unindo elas em um fluxo de trabalho abrangente, e centraliza todos os dados relevantes em uma única plataforma para criar informações consolidadas e prontas para ação

Afinal, quais são as diferenças?

- A abordagem do ecossistema maximiza a eficiência das ferramentas de segurança cibernética 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

- O imenso conjunto de dados fornecidos pelo SIEM pode resultar em muitos alertas que deverão ser filtrados, processados e analisados manualmente
- Não fornece o contexto necessário para lidar com ataques novos, complexos ou sofisticados
- A solução passiva não conta com bloqueio, quarentena ou recursos de resposta
- É melhor usado em conjunto com as soluções de investigação e resposta proativas, como XDR ou SOAR

- Manter a plataforma SOAR devidamente configurada, integrada às ferramentas parceiras, exige esforço contínuo de um SOC altamente especializado e maduro
- Sem uma manutenção qualificada e vigilante, os analistas SOAR podem acabar com muitos alertas de baixa prioridade, falsos positivos e um conjunto de dados geralmente incoerente como consequência de toda a diversidade de ferramentas isoladas que alimentam a plataforma (exatamente o que eles tentam evitar)

Como justificar o investimento em XDR

Juntamente com os benefícios técnicos, há muitas boas razões para investir no XDR, como as razões relacionadas com a mitigação de ataque, a detecção de ameaças internas, nuvem e conformidade, a investigação e resposta a incidentes e muito mais.

Mitigação de ataque

Se uma organização tivesse sido vítima de ataque de ransomware que tivesse resultado na criptografia de dados críticos e na interrupção de operações, os recursos de detecção proativos de ameaças do XDR ajudariam a identificar e evitar esse tipo de ataque antes mesmo que ele pudesse causar estragos por meio da capacidade de detectar comportamentos suspeitos, isolar endpoints infectados e oferecer resposta a incidentes em tempo real, o que representa uma redução significativa do impacto do ataque e o pronto restabelecimento da continuidade dos negócios.

Detecção de ameaças internas

As ameaças internas são a maior preocupação para a maioria das organizações, sejam elas intencionais ou não. Entretanto, como o XDR entrega visibilidade abrangente entre os endpoints, redes, aplicativos e a nuvem, ele pode detectar sinais reveladores de ameaças internas, como o comportamento anômalo do usuário, as tentativas de exfiltração de dados e acesso não autorizado. Por outro lado, ao correlacionar e analisar os dados originados de diversas fontes, o XDR pode ajudar a identificar e mitigar as ameaças internas, proteger as informações confidenciais e manter a integridade de dados.

Nuvem e conformidade

Como muitas organizações estão passando a usar as tecnologias na nuvem, garantir uma segurança e conformidade robustas está se tornando cada vez mais importante. Ao oferecer a visibilidade unificada e a detecção contra as ameaças entre os ambientes híbridos e com diversas nuvens, o XDR permite que as organizações monitorem as cargas de trabalho na nuvem, detectem as configurações inadequadas e identifiquem as atividades suspeitas, enquanto elas mantêm a segurança e a conformidade com a infraestrutura na rede e mitigam os riscos associados com os ataques baseados na nuvem.

Resposta a incidentes e investigação

Respostas rápidas e investigações completas são elementos críticos para minimizar os danos e evitar incidentes futuros. O XDR dinamiza os processos de resposta a incidentes ao automatizar a detecção contra ameaças, a triagem de alertas e os fluxos de trabalho de investigação, e ao oferecer às equipes de segurança uma visão abrangente dos incidentes para que elas sejam capazes de responder pronta e eficazmente. As economias de tempo e recursos resultantes dos recursos de resposta automatizados do XDR fazem com que ele seja um trunfo na manga para o gerenciamento de incidentes.

Complementos EPP, EDR, SIEM e muito mais

Evitar as categorias de ameaças mencionadas é uma razão mais do que suficiente para investir em XDR. Além disso, para aqueles que utilizam EPP, EDR, SIEM e outras soluções, o XDR aprimora o desempenho de todas essas ferramentas.

- Para a EPP, o XDR aprimora os recursos de proteção de endpoints ao oferecer a detecção avançada contra ameaças, automação de respostas e visibilidade aprimorada entre a rede e os ambientes na nuvem, o que o torna o próximo passo logicamente viável nos roteiros de segurança, além de viabilizar para as organizações a conquista de um novo nível de proteção contra as ameaças em evolução.
- Para o EDR, o XDR (frequentemente construído no EDR) estende os recursos da solução além da detecção e resposta focadas em endpoint, ao oferecer visibilidade holística e detecção contra ameaças na infraestrutura protegida, inclusive na rede, máquinas virtuais, aplicativos e ambientes na nuvem, além de viabilizar os recursos eficientes de resposta a incidentes e a busca aprimorada de ameaças.
- Para o SIEM, o XDR complementa a solução ao oferecer detecção de ameaças em tempo real, recursos de resposta avançada, visibilidade aprimorada e correlação de eventos de segurança entre os endpoints, redes e nuvem, além de viabilizar a resposta mais rápida a incidentes e o menor tempo de investigação.

Para as organizações mais propensas a investir na tecnologia XDR no futuro próximo, a facilidade de uso é, de longe, o benefício percebido mais importante para a organização, seja planejando a integração da tecnologia com as ferramentas de segurança existentes, seja definindo um fornecedor único para que a infraestrutura esteja pronta para receber o XDR. As organizações também indicaram que outros investimentos de médio prazo em soluções para unificar a detecção e resposta e melhorar a visibilidade entre os produtos e serviços tinham a maior probabilidade de ser detecção e resposta de endpoint (EDR), detecção e resposta de rede (NDR), segurança da informação, gerenciamento de evento (SIEM) e inteligência contra ameaças.

CRA Business Intelligence, o XDR deverá se tornar um multiplicador de forças para a detecção contra ameaças, março de 2022

Como lidar com o cenário de ameaças mais amplo

Em muitas organizações, analistas de segurança passam mais da metade do tempo na triagem de falsos positivos ao invés da busca e resposta proativa a ameaças, o que aumenta significativamente os tempos de detecção

Threat intelligence

Para muitas organizações, especialmente as que são vulneráveis aos ataques direcionados e APTs, a inteligência de ameaças (TI, na sigla em inglês) é uma ferramenta vital para permitir a defesa proativa contra as ameaças. Mas, embora os usos e benefícios da TI sejam muitos e variados, assim como são seus recursos, isso significa que identificar o que funcionaria melhor para uma determinada organização pode ser um desafio por si só.

Em muitas organizações, os analistas de segurança passam mais de metade do seu tempo classificando falsos positivos ao invés da busca e resposta a ameaças proativa, levando a um aumento significativo nos tempos de detecção. Fornecer às operações de segurança informações sobre ameaças irrelevantes ou imprecisas aumentará ainda mais os falsos positivos, afetando negativamente a capacidade de resposta e a segurança geral. Então, como evitar esse cenário?

Apesar de não existir nenhum critério universalmente aceito para avaliar as ofertas comerciais de inteligência de ameaças, os aspectos a serem levados em consideração ao fazer isso incluem:

- Com uma extensa gama de provedores entre os quais escolher, as organizações devem examinar a TI que transforme o entendimento de seu ambiente específico de ameaças, por exemplo, mediante análise detalhada de ameaças históricas e emergentes que visam um determinado setor ou uma empresa específica para aprimorar o desempenho das funções, como o gerenciamento de vulnerabilidades, descoberta de ameaças, resposta a incidentes e muito mais.
- Para combinar de forma eficaz a TI com as ferramentas de segurança, controles e processos já usados e conhecidos por uma organização, ela deve procurar os métodos de entrega, mecanismos de integração e formatos que sejam compatíveis com uma integração tranquila da TI em suas operações existentes de segurança.
- Além disso, também é importante identificar a TI com a abrangência global. Como os ataques são ilimitados, o fornecedor obtém globalmente as informações e agrupa as atividades aparentemente desconexas em campanhas coesas, uma vez que esse tipo de inteligência é útil para adotar ações mais adequadas?
- Se as organizações estiverem procurando um conteúdo mais estratégico para informar seu planejamento de segurança a longo prazo, procure por um provedor de TI com um histórico comprovado de descoberta e investigação de ameaças complexas em sua região e/ou setor.
- A capacidade do fornecedor de adaptar seus recursos de pesquisa às especificidades da organização também é crítica.

A inteligência de ameaças (IA) é um recurso em constante evolução. E para ser eficaz, os programas internos de TI que a utilizam também devem ser. Defina seu desempenho atual com nossa ferramenta de avaliação interativa de TI e obtenha recomendações personalizadas de melhoria de acordo com suas respostas: https://go.kaspersky.com/ti_tool_2023.html

Além disso, usar o Portal do Kaspersky Threat Intelligence ajuda a organização a agregar, gerenciar e operacionalizar a TI, o que é vital quando as ferramentas de segurança estão usando TI de diversas fontes. Especificamente quando falamos do Portal do Kaspersky Threat Intelligence, ele deve ajudar a organização da seguinte maneira:

- Responda às ameaças mais efetivamente ao verificar qualquer indicador de ameaça que seja considerado suspeito, seja um arquivo, hash de arquivo, endereço IP ou endereço da Web.
- Análise de arquivos para detectar ameaças do tipo de commodity, evasiva e de APT.
- Envie endereços IP, hashes de arquivo, domínios ou endereços da Web considerados suspeitos para validar e priorizar rapidamente alertas e incidentes usando níveis de risco e informações contextuais de apoio para determinar quais são as ameaças reais.
- Recebimento de relatórios regulares sobre o comportamento de arquivos ou endereços da Web específicos.
- Automatize os fluxos de trabalho de segurança por meio da conexão de aplicativos com o Portal do Kaspersky Threat Intelligence.

Mais de 80% de todos os incidentes cibernéticos são causados por erro humano

Um treinamento de conscientização sobre segurança

Mais de 80% de todos os incidentes virtuais são causados por erros humanos, especialmente porque muitas das soluções de segurança estão em rápido desenvolvimento e se adaptando às ameaças complexas. Isso dificulta a vida dos criminosos virtuais, então, eles acabam se voltando para o elemento mais vulnerável da segurança virtual, o fator humano. Os exemplos dos impactos disso são os seguintes:

- 52% dos executivos de nível C afirmam que os profissionais são a maior ameaça à segurança operacional.
- 43% das empresas de pequeno porte sofreram um incidente de segurança devido à violação de políticas de segurança de TI por funcionários.
- 60% dos profissionais possuem dados confidenciais em seus dispositivos corporativos (dados financeiros, base de dados de e-mail etc).
- 30% dos funcionários admitem que compartilham o login e a senha de seus computadores corporativos com colegas.

Portanto, uma cultura de comportamento virtual seguro, com habilidades básicas no assunto e conscientização por toda a organização é importante para reduzir a superfície de ataque e o número de incidentes com os quais a equipe de TI precisa lidar.

A Kaspersky pode te ajudar

Kaspersky Next EDR Foundations

Proteção poderosa de endpoints baseada em ML do Kaspersky Next EDR Foundations, controles de segurança flexíveis e ferramentas de análise de causa-raiz de EDR fornecem todas as ferramentas necessárias para construir um núcleo forte para a segurança virtual. Uma implementação simples no console, na nuvem ou on-premises, e uma variedade de recursos que promovem a qualidade de vida no trabalho reduzem a complexidade e aumentam a eficiência.

Kaspersky Next EDR Optimum

O Kaspersky Next EDR Optimum fornece uma forte proteção de endpoints, controles aprimorados, treinamento, gerenciamento de patches e muito mais, tudo aprimorado pela funcionalidade essencial de EDR. A visibilidade, investigação e resposta a ameaças são simples, rápidas e guiadas, ajudando equipes de TI e de segurança de TI a repelir ataques rapidamente e gastando poucos recursos.

Kaspersky Next XDR Expert

O Kaspersky Next XDR Expert integra-se perfeitamente com a infraestrutura de segurança existente da organização para fornecer visibilidade em tempo real e insights profundos sobre ameaças virtuais em evolução e fornece detecção avançada de ameaças e resposta automatizada, além dos recursos essenciais de XDR descritos neste e-book.

Kaspersky Managed Detection and Response

O Kaspersky MDR fornece proteção avançada e ininterrupta contra o crescente volume de ameaças que burlam as barreiras de segurança automatizadas para proporcionar alívio às organizações com dificuldade de encontrar pessoal especializado ou com recursos internos limitados. Seus recursos superiores de detecção e resposta têm suporte de uma das equipes de busca de ameaças de maior sucesso e experiência do setor. Ao contrário das ofertas semelhantes no mercado, o Kaspersky MDR aproveita modelos patenteados de ML, exclusiva inteligência de ameaças (TI) contínua e um registro comprovado de pesquisas eficientes de ataques direcionados. Ele reforça automaticamente a resistência da sua empresa contra as ameaças virtuais, enquanto otimiza os recursos existentes e os investimentos futuros em segurança de TI.

Kaspersky Threat Intelligence

O portfólio de TI da Kaspersky abrange uma gama completa de cenários de segurança, inclusive prevenção, detecção, resposta e relatório estratégico, sendo que todos eles podem ser ajustados para as necessidades individuais de cada organização. Nosso Global Research and Analysis Team (GReAT) é um grupo de elite de especialistas em segurança que, por meio de suas habilidades em se infiltrar em comunidades fechadas e fóruns nebulosos ao redor do mundo, descobriu e dissecou mais de 50 dos ataques direcionados mais sofisticados do mundo. Seu conhecimento, a experiência e a profunda inteligência sobre todos os aspectos da segurança virtual fizeram com que nos tornássemos o parceiro de confiança das principais autoridades policiais e governamentais, inclusive a INTERPOL e as principais CERTs.

Os exemplos de nossas soluções e serviços de TI inovadores incluem mais de 20 tipos de ameaças de feeds de dados; uma gama extensiva de relatórios de TI; sandbox desenvolvida internamente para a detecção sofisticada e ameaças evasivas; portal aberto de inteligência contra ameaças; e serviços, como a análise do cenário específico de ameaças do cliente e o Kaspersky Digital Footprint Intelligence que analisa os rastros digitais para identificar possíveis ameaças e vulnerabilidades.

Kaspersky Security Awareness

A Kaspersky Security Awareness oferece uma variedade de soluções de treinamento envolventes e eficazes, fortalecendo a conscientização em todos os níveis profissionais, ajudando os indivíduos a desempenharem um papel abrangente na segurança virtual. Como mudanças sustentáveis de comportamento levam tempo, nossa abordagem envolve um ciclo de aprendizagem contínuo com diversos componentes, inclusive simulações de proteção criativa que abrangem uma gama de cenários do setor; ferramentas de avaliação lúdicas; uma plataforma automatizada de conscientização sobre segurança que aplica simulações de phishing; treinamentos para executivos em nível C e muito mais.

Kaspersky Professional Services

O portfólio do Kaspersky Professional Services de serviços de avaliação, implementação, manutenção e otimização ajuda as organizações com suas necessidades únicas, minimiza os riscos de segurança, maximiza o retorno do investimento, minimiza a pressão sobre os recursos, responde rapidamente às novas ameaças de segurança e extrai o máximo benefícios das soluções da Kaspersky.

Confiança

Proven. Transparent. Independent.

Em 2017, a Kaspersky lançou a Iniciativa de Transparência Global. Isso significa que, ao contrário de qualquer outro fornecedor de mesmo tamanho, se você ainda tiver dúvidas sobre nossos produtos, poderá revisar nosso código-fonte, atualizações de software e regras de detecção de ameaças, além de nossos processos seguros de ciclo de vida de desenvolvimento e estratégias de mitigação de riscos de software e supply chain. Para apoiar a iniciativa, abrimos mais de 10 centros de transparência ao redor do mundo. Assim, acabamos recebendo a visita de órgãos de regulamentação, provedores de infraestruturas críticas, clientes, parceiros, a mídia e muitos outros e outras. E para os clientes que exigem, somos passamos por auditoria SOC2 e temos certificação ISO/IEC 27001.

Kaspersky Next

Para mais informações sobre o Kaspersky Next acesse:
https://go.kaspersky.com/next_brasil

Notícias sobre ciberameaças: securelist.lat
Notícias sobre segurança de TI:
kaspersky.com.br/blog/category/business/
Segurança de TI para PMEs: kaspersky.com.br/business
Segurança de TI para grandes empresas: kaspersky.com.br/enterprise

kaspersky.com.br