Microsoft Security

3 motivos para migrar para a proteção integrada contra ameaças

Sumário

Introdução

Uma empresa média usa atualmente mais de 30 ferramentas de segurança diferentes, muitas vezes desarticuladas e "adicionadas".

A segurança está em um ponto de inflexão. Os ciberataques estão cada vez mais sofisticados à medida que as organizações continuam a lidar com desafios que vão da escassez de talentos e do equilíbrio de custos ao controle das pressões do trabalho híbrido.

Enquanto isso, o mercado de segurança está mais fragmentado e complexo do que nunca. Uma empresa média usa atualmente mais de 30 ferramentas de segurança diferentes, muitas vezes desarticuladas e "adicionadas", fornecendo visibilidade limitada e insights inadequados para centros de operações de segurança (SOCs).

Os líderes de segurança e conformidade querem entender melhor os riscos e as ameaças mais recentes, mas também precisam saber o que está funcionando, o que não está e onde estão as lacunas.

Apesar de o escopo dos desafios de segurança atuais parecer amedrontador, ainda é possível manter-se otimista pela situação dos CISOs que buscam melhorar a eficiência e a eficácia das operações de segurança. A resposta está em uma abordagem integrada e completa da proteção contra ciberameaças que ajudará as organizações a:

Razão 1: Fazer mais com menos

Consolide soluções pontuais e reduza a sobrecarga do departamento das operações de segurança (SecOps).

Razão 1: Capacitar o departamento de SecOps para que se concentre em tarefas de alto valor

Use ferramentas que aumentem a eficiência e tornem até mesmo os analistas juniores mais capazes do que nunca.

Razão 1: Aumentar a produtividade dos funcionários

Proteja sua organização de modo a permitir que seu pessoal sejam destemido ao criar e inovar.

Essa abordagem é possibilitada pela integração de uma solução de detecção e resposta estendida (XDR) com um sistema de informações de segurança e gerenciamento de eventos (SIEM) nativo de nuvem que usa inteligência artificial (IA) e recursos de automação. A solução integrada pode ajudar seu SOC a se tornar mais preditivo, proativo e preventivo contra ataques em toda a empresa.

Razão 1

Fazer mais com menos

Ao consolidar ferramentas com a solução integrada da Microsoft, você também poderá economizar ao pagar apenas pelo que usar.

Muitas organizações abordaram as ferramentas de segurança com foco nas melhores soluções pontuais da categoria. Infelizmente, essa abordagem pode acabar dificultando o processo de identificação e resposta rápidas a ameaças pelos profissionais de segurança. Também pode acabar tendo um impacto negativo sobre os gastos com TI e a produtividade do usuário final.

À medida que as organizações buscam fazer mais com menos, uma abordagem integrada, como o SIEM e a XDR da Microsoft, pode ajudar. Ela pode reduzir a complexidade consolidando as ferramentas individuais — e, como é nativa da nuvem, uma solução integrada também pode melhorar a performance e escalar.

Ao consolidar ferramentas com a solução integrada da Microsoft, você também poderá economizar ao pagar apenas pelo que usar. Você também pode reduzir a sobrecarga exigida do departamento de SecOps para gerenciar as soluções ao aumentar a automação e a integração.

> É fácil iniciar o processo de adoção de novas ferramentas de segurança porque você espera que as lacunas sejam amplas. Progredindo a partir daí, você logo perceberá que ferramentas de diferentes fornecedores podem potencialmente se sobrepor em suas funções. Essa sobreposição pode ser desejável para verificações e saldos, **mas também pode ter um custo elevado.**"
>
> **Jonathan Cassar**
> Diretor de tecnologia, MITA

USD 1,6 milhões

de economia anual obtida da consolidação de fornecedores

A Microsoft encomendou à Forrester Consulting o estudo Total Economic Impact™ (TEI) e a análise do possível retorno sobre o investimento (ROI) que as empresas podem ter ao implantar o SIEM e a XDR da Microsoft. Estas foram algumas das principais conclusões obtidas para uma organização composta fictícia com 8 mil funcionários e 10 profissionais de segurança:

- **Economia de quase USD 1,6 milhão por ano com a consolidação de fornecedores.** O investimento no SIEM e na XDR da Microsoft permite que a organização composta reduza o custo de seu SIEM anterior (USD 560 mil), a infraestrutura local associada (mais de USD 360 mil), três soluções pontuais da XDR (USD 192 mil) e o custo contínuo com mão de obra para gerenciamento (USD 480 mil).

- **Redução do risco de violação material em 60%.** Com fluxos de trabalho de pesquisa e resposta de segurança mais eficientes, automação de resposta de segurança aprimorada e maior capacidade de proteger todos os ambientes de computação, incluindo proteção multinuvem, a organização composta reduz o risco de violações com economia anual de USD 1,6 milhão.

- **ROI de 207%.** As entrevistas representativas e a análise financeira revelaram que uma organização composta usufrui de USD 17,68 milhões em benefícios ao longo de três anos contra USD 5,76 milhões em custos, gerando um valor presente líquido (VPL) de USD 11,92 milhões.

Razão 2

Capacitar o departamento de SecOps para que se concentre em tarefas de alto valor

É fundamental integrar o SIEM e a XDR para correlacionar alertas, priorizar as maiores ameaças e coordenar ações em toda a empresa.

As equipes de SecOps são sobrecarregadas pela quantidade de sinais que têm para analisar, incluindo muitos sinais de baixa fidelidade que são difíceis, se não impossíveis, de detectar manualmente e mitigar. À medida que as ameaças aumentam, fica cada vez mais difícil para um SOC sobrecarregado acompanhá-las, especialmente ao tentar analisar dados de várias soluções pontuais. Alocar mais recursos para preencher as lacunas não é a resposta, já que encontrar profissionais de segurança qualificados o suficiente é um desafio constante.

Por isso é fundamental integrar o SIEM e a XDR para correlacionar alertas, priorizar as maiores ameaças e coordenar ações em toda a empresa, com Inteligência Artificial e automação avançadas para detectar e remediar ameaças de maneira proativa.

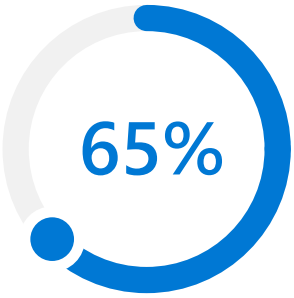
Considere, por exemplo, que um único sinal de nível baixo de segurança pode não atrair a atenção de um SIEM tradicional. No entanto, ao usar a Inteligência Artificial, um SIEM nativo de nuvem poderia comparar automaticamente esse sinal com sinais de outras fontes em toda a organização, relacionando-o com diversos conjuntos de dados para encontrar ataques em vários estágios.

A integração de o SIEM e a XDR libera os recursos do departamento de SecOps, além de capacitar até mesmo os analistas juniores com mais recursos e confiança.

O sistema então normaliza, analisa e correlaciona os dados, ao mesmo tempo em que fornece contexto sobre como o ciberataque entrou na infraestrutura, juntamente com a linha do tempo de como ele se espalhou. Isso permite que as equipes do SOC visualizem a violação a partir de um único console e lidem com ela de forma eficiente.

> Muitos CISOs não percebem **a sobrecarga que impõem às suas equipes com 20 painéis** ou soluções pontuais diferentes, e os custos anuais associados... Nós eliminamos grande parte da fadiga associada a ferramentas ao optar por um único fornecedor."
>
> **Terence Jackson**
> Diretor de segurança e privacidade da informação, Thycotic

Uma organização não deve precisar de experiência profunda para revelar o valor de uma solução de segurança. A integração de o SIEM e a XDR libera os recursos do departamento de SecOps, além de capacitar até mesmo os analistas juniores com mais recursos e confiança.



A abordagem integrada do SIEM e da XDR da Microsoft reduziu o tempo de investigação de ameaças em 65%.

O estudo Forrester Total Economic Impact™ (TEI) encomendado pela Microsoft mostrou esse tipo de eficiência de SecOps em sua organização composta:

- **Redução de 65% no tempo para investigar ameaças e redução de 88% no tempo para responder às ameaças.** A abordagem integrada do SIEM e da XDR da Microsoft para investigação e resposta contra ameaças de segurança tornam esses fluxos de trabalho mais eficientes para os profissionais de segurança da organização composta. Eles não precisam mais passar por várias ferramentas para identificar ameaças, enquanto os recursos de automação de segurança melhoram ainda mais os fluxos de trabalho de resposta.

- **Redução de 90% no tempo para criar uma pasta de trabalho e redução de 91% no tempo para integrar novos profissionais de segurança.** A abordagem integrada do SIEM e da XDR da Microsoft também torna os fluxos de trabalho dos profissionais de segurança mais eficientes. Como os logs do SIEM são integrados em todo o conjunto de soluções, a criação de pastas de trabalho é quase automatizada, enquanto um login único permite que novos profissionais de segurança sejam integrados quase 16 semanas mais rápido.

Razão 3

Aumentar a produtividade dos funcionários

Uma solução integrada do SIEM e da XDR pode ajudar sua organização a aumentar a produtividade dos usuários finais.

Além de fazer mais com menos e aumentar a eficiência do departamento de SecOps, uma solução integrada do SIEM e da XDR pode ajudar sua organização a aumentar a produtividade dos usuários finais.

As equipes de SecOps sabem que quando a segurança é dificultada, as pessoas sempre dão um jeito de burlá-la. Assim, quando as experiências dos usuários finais dificultam em vez de promover a produtividade dos funcionários, a organização pode ficar propensa a mais riscos de segurança e custos mais altos. Senhas fracas ou perdidas, acesso sem segurança em dispositivos pessoais ou compartilhamento sem restrições de dados confidenciais são apenas alguns dos desafios.

> [No passado] usávamos instrumentos contundentes quando alguém suspeitava de um problema. Encerrávamos tudo e retirávamos o acesso, o que afetava negativamente nossos negócios. E todos sabiam o que estava acontecendo porque as coisas simplesmente paravam de funcionar temporariamente. Com o Microsoft Sentinel, conseguimos reagir de maneira cirúrgica ao que está acontecendo. **A empresa geralmente nem percebe quando estamos respondendo a uma ameaça**, e essa é uma medida muito importante do nosso sucesso."
>
> **Rick Gehringer**
> Diretor de informações, Wedgewood

Quase
68.000
O SIEM e a XDR da Microsoft aumentaram a produtividade de outros funcionários em quase 68 mil horas por ano.

Uma abordagem integrada do SIEM e da XDR da Microsoft ajuda você a proporcionar experiências de usuário perfeitas que mantêm seu pessoal tanto produtivo quanto seguro em todas as facetas das experiências diárias. Ela pode reduzir os impactos negativos na produtividade, como ter que desativar os serviços ou isolar e recriar a imagem das máquinas. Mas a integração do SIEM e da XDR também pode criar oportunidades para ganhos de produtividade do usuário final, como o aumento do autosserviço para suporte de segurança, painéis e relatórios melhores e maior capacidade de resposta e tempos de inicialização mais rápidos proporcionados pela operação de menos agentes de segurança.

No estudo Forrester Total Economic Impact™ (TEI) encomendado pela Microsoft, a organização composta fictícia com 8 mil funcionários mostrou que a implantação do SIEM e da XDR da Microsoft gerou um aumento na produtividade dos funcionários:

- **Aumento da produtividade de outros funcionários em quase 68 mil horas por ano.** O SIEM e a XDR da Microsoft impedem que processos de segurança ineficientes afetem negativamente outros funcionários. Por exemplo, a organização composta economiza 4 mil horas por ano graças à nova capacidade de autosserviço dos profissionais de TI para atualizações e recomendações de segurança. Também oferece solução remota de problemas de segurança nas máquinas dos funcionários e reduz o número de agentes de segurança nelas, economizando quase 64 mil horas por ano em produtividade do usuário final.

A segurança se tornou um facilitador essencial do sucesso tecnológico. É por isso que as organizações precisam de medidas de segurança que gerem o máximo de resiliência possível em relação aos ataques modernos — para proteger e possibilitar a produtividade e a inovação que impulsionam o crescimento.

Obtenha proteção integrada contra ciberameaças com o SIEM e a XDR

Essa integração de produtos líderes da indústria oferece prevenção, detecção e resposta contra ciberameaças em uma única solução abrangente.

A Microsoft oferece a primeira e única solução integrada de SIEM e XDR, proporcionando visibilidade de ponta a ponta em todas as nuvens e plataformas. Essa integração de produtos líderes da indústria oferece prevenção, detecção e resposta contra ciberameaças em uma única solução abrangente.

O SIEM e a XDR da Microsoft exploram o poder da Inteligência Artificial e da automação, bem como investimentos profundos e contínuos em detecção e análise de ciberameaças, com insights especializados e visibilidade de 43 trilhões de sinais todos os dias. Com a integração desses produtos, as equipes do SOC estão equipadas com mais contexto do que nunca para caçar e resolver ciberameaças críticas mais rapidamente:

Microsoft Sentinel

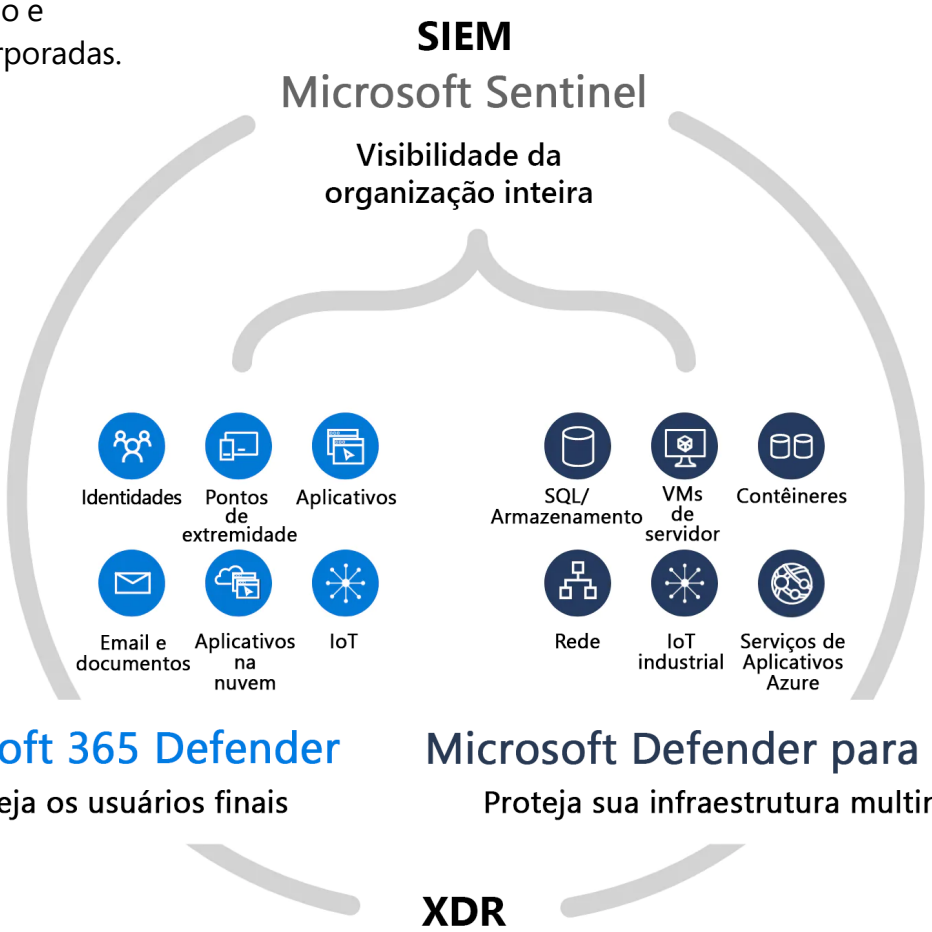
Obtenha uma visão panorâmica de toda a empresa com o SIEM nativo de nuvem da Microsoft. Agregue dados de segurança de praticamente qualquer fonte e aplique Inteligência Artificial para separar ruído de eventos legítimos, correlacionar alertas em cadeias de ciberataques complexas e acelerar a resposta contra ciberameaças com orquestração e automação incorporadas.

Microsoft Defender XDR

Impeça e detecte ciberataques em suas identidades, pontos de extremidade, aplicativos, email, dados e aplicativos de nuvem com recursos da XDR. Investigue e responda aos ciberataques com a melhor proteção da categoria, pronta para ser usada. Procure ameaças e coordene facilmente sua resposta de um único painel.

Microsoft Defender para Nuvem

Proteja suas cargas de trabalho de nuvem híbrida e multinuvem com os recursos da XDR incorporados. Proteja seus servidores, armazenamento, bancos de dados, contêineres e muito mais. Concentre-se no que mais importa com os alertas priorizados.



Não deixe a segurança para depois. Integre-a.

Coloque as ferramentas e a inteligência certas nas mãos das pessoas certas. Defenda-se de ataques modernos com uma solução integrada, completa e nativa de nuvem.

Saiba mais sobre a proteção integrada contra ciberameaças com as soluções de SIEM e XDR da Microsoft >

Microsoft Security