Microsoft Security

Proteção da propriedade digital:

Uma abordagem integrada para o aumento da eficiência do SOC

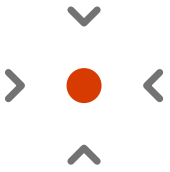
Os ambientes de TI complexos de hoje exigem uma abordagem mais eficiente, simples e integrada para o centro de operações de segurança.

Sumário

Pontos importantes deste artigo:

Cenários de ataque cada vez mais sofisticados e complexos fazem com que os SOCs tenham mais dificuldade em manter o ritmo.

A integração de sistemas SIEM e XDR aumenta a eficácia e a eficiência da segurança em toda a empresa.



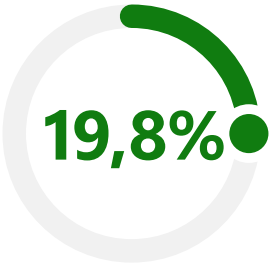
Automação e IA são componentes essenciais do kit de ferramentas de segurança, pois podem **detectar e corrigir ameaças proativamente,** liberando recursos da Operação de Segurança.

Uma abordagem de segurança nativa de nuvem melhora a performance e a escala dos atuais ambientes de TI híbridos.

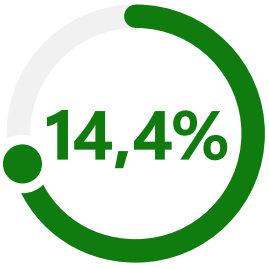
Introdução

As equipes de segurança ainda estão sentindo o impacto da mudança repentina para o trabalho remoto. Os CEOs estão exigindo experiências aprimoradas para os usuários a fim de acomodar políticas estendidas de trabalho em casa, ao mesmo tempo em que pedem aos CISOs que atualizem a segurança de TI para aumentar a resiliência, de acordo com a Pesquisa com CIOs sobre o impacto da pandemia nos negócios.

Enquanto isso, as ameaças estão em constante evolução. De acordo com o Relatório de Defesa Digital da Microsoft, o nível de sofisticação dos ataques continua a crescer e muitas vezes aumenta em tempos de crise.[1] O 2021 Phishing Benchmark Global Report da Terranova Security constatou que 19,8% dos funcionários norte-americanos clicaram em um link em uma simulação de phishing e 14,4% do total de participantes fizeram o download do documento na página de simulação de phishing.[2] Ao mesmo tempo, os centros de operações de segurança (SOCs) estão sobrecarregados pela quantidade de sinais que precisam analisar, incluindo muitos sinais de baixa fidelidade que são difíceis, se não impossíveis, de detectar manualmente e mitigar. À medida que as ameaças aumentam, as equipes dos SOCs já sobrecarregadas têm dificuldade para fazer o acompanhamento.



dos funcionários norte-americanos clicaram em um link em uma simulação de phishing.



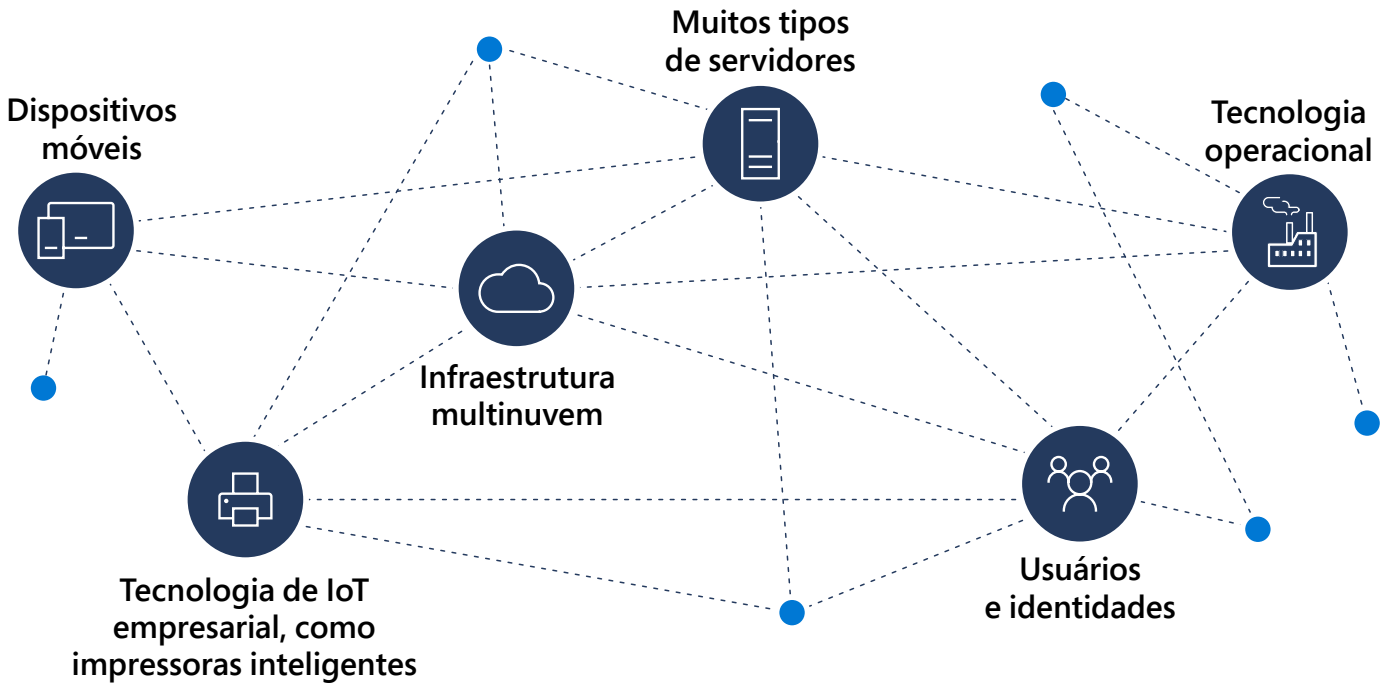
do total de participantes fez o download do documento na página de simulação de phishing.

O patchwork de ferramentas de segurança da atualidade fornece bolsões de proteção, mas dificulta a integração da amplitude dos sinais de segurança que envolvem a empresa. Como resultado, é difícil para as equipes de Operações de Segurança obter uma visão corporativa de toda a cadeia de ataques, o que explica por que as violações podem levar meses ou mais para serem descobertas sem os controles de segurança certos. Uma vez que os autores dos ataques conseguem invadir sem serem detectados, o dano pode se agravar rapidamente. Alocar mais recursos para preencher as lacunas não é a resposta, já que encontrar profissionais de segurança qualificados o suficiente é um desafio constante. Isso sobrecarrega as equipes de segurança.

[1]"Relatório de Defesa Digital da Microsoft", 2021, Microsoft.

[2]"Free Phishing Benchmarking Data to Train Your Cyber Heroes", 2021, Terranova.

A crescente propriedade digital é difícil de gerenciar e proteger



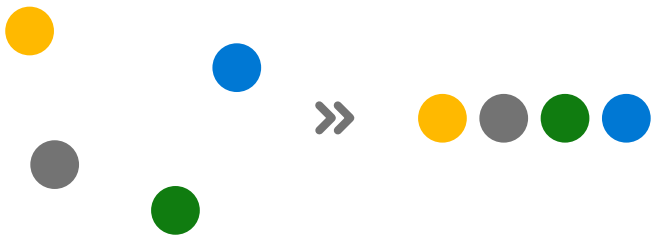
Apesar de o escopo dos desafios de segurança atuais parecer amedrontador, ainda é possível manter-se otimista pela situação dos CISOs que buscam melhorar a eficiência e a eficácia de suas operações de segurança. A resposta está em uma abordagem integrada e completa da proteção contra ameaças que ajudará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

- ✓ **Combater os ataques antes que eles aconteçam** reduzindo a superfície de ataque e eliminando ameaças persistentes.
- ✓ **Detectar ameaças em todos os domínios,** integrando dados de ameaças para obter respostas rápidas e completas.
- ✓ **Liberar recursos da equipe de segurança** com ferramentas que consigam identificar proativamente ataques sofisticados em todos os domínios.

É possível habilitar essa abordagem integrando a solução de detecção e resposta estendida (XDR) com sistemas SIEM nativos de nuvem que aplicam recursos de Inteligência Artificial (IA) e automação para ajudar o SOC a se tornar mais preditivo, proativo e preventivo contra ataques em toda a empresa.

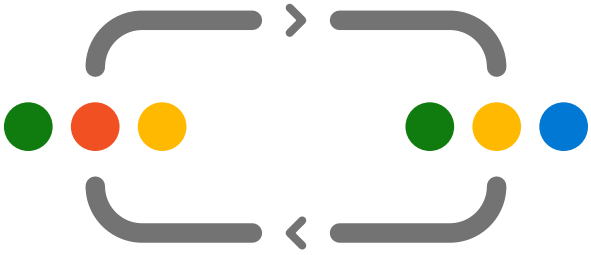
A mudança para proteção integrada contra ameaças

Uma abordagem integrada pode ajudar um SOC de três formas importantes:



Redução da complexidade, consolidando ferramentas para ajudar a simplificar a segurança enquanto fortalece sua postura de segurança.

Detecção automatizada e correlação de alertas e dados em incidentes gerenciáveis.

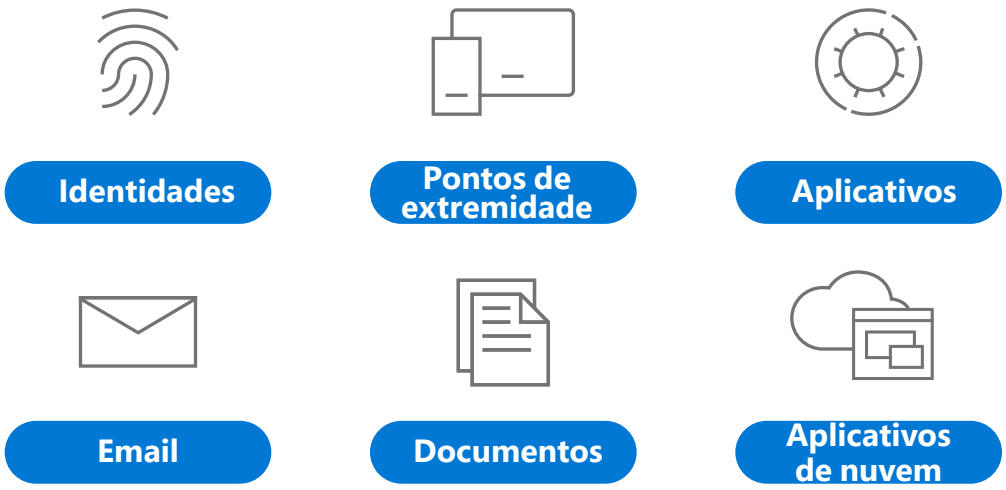


Recursos automatizados de "autorrecuperação", que faz com que as equipes de SOC economizem tempo na busca de ameaças.

Uma abordagem nativa de nuvem para proteção contra ameaças fornece a performance, a escala e a visibilidade necessárias para lidar com todos os tipos de ameaças para usuários, aplicativos, dados, dispositivos e infraestrutura. Ela aplica recursos de Inteligência Artificial e automação para ajudar as equipes do SOC a priorizar quais ameaças são as mais importantes. O estudo de 2021 Security Priorities do IDG constatou que os líderes de segurança de TI planejam aumentar os gastos com a proteção de dados na nuvem (30%), controles de acesso (29%), serviços de segurança cibernética baseados em nuvem (28%) e muito mais, o que indica claramente que a segurança na nuvem e em ambientes interligados é uma prioridade.[3]

A proteção integrada contra ameaças é fundamental porque os maus atores não respeitam os perímetros; eles explorarão qualquer vulnerabilidade que puderem encontrar em dispositivos, aplicativos e, até mesmo, usuários. Quando descobrem ou criam uma abertura, eles a usam como ponto de partida para se mover lateralmente até encontrar seu alvo, muitas vezes na forma de sistemas ou dados confidenciais que podem usar para chantagear ou divulgar.

Os invasores buscam vulnerabilidades em toda a organização



Por exemplo, o agente estado-nação BISMUTH foi capaz de passar em grande parte sem ser detectado aproveitando-se de alertas de baixa prioridade causados por mineradores de criptomoedas.
Seu objetivo: estabelecer monitoramento e espionagem contínuos a fim de exfiltrar informações úteis.

[3]"IDG Security Priorities Study", 2021, IDG.

Esse nível de sofisticação e complexidade é surpreendente e alarmante. É por isso que é fundamental alinhar SIEM e XDR para correlacionar alertas, priorizar as maiores ameaças e coordenar ações em toda a empresa. Em última análise, essas soluções fornecem eficiência do SecOps e reduzem o risco de violações de dados prejudiciais.

Por exemplo, integrar SIEM e XDR oferece às equipes de Operações de Segurança muito mais contexto, graças aos recursos de Inteligência Artificial integrados. Além disso, a automação implanta e aprimora proativamente as técnicas de prevenção, ao mesmo tempo em que permite que as equipes se concentrem em tarefas mais sofisticadas, como a busca de ameaças e a criação de ferramentas personalizadas que reduzam o tempo de resposta.

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.

O sistema então normaliza, analisa e correlaciona os dados, ao mesmo tempo em que fornece contexto sobre como o ataque 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.

Fortalecimento da postura de segurança com proteção inteligente e integrada contra ameaças

As soluções de proteção contra ameaças da Microsoft oferecem segurança integrada e abrangente com automação interna e recursos de Inteligência Artificial como parte de uma pilha completa de SIEM e XDR. Essa estratégia concede às equipes de SOC a funcionalidade certa para combater até mesmo os ataques mais sofisticados entre domínios em todos os aplicativos da Microsoft, de terceiros e personalizados.

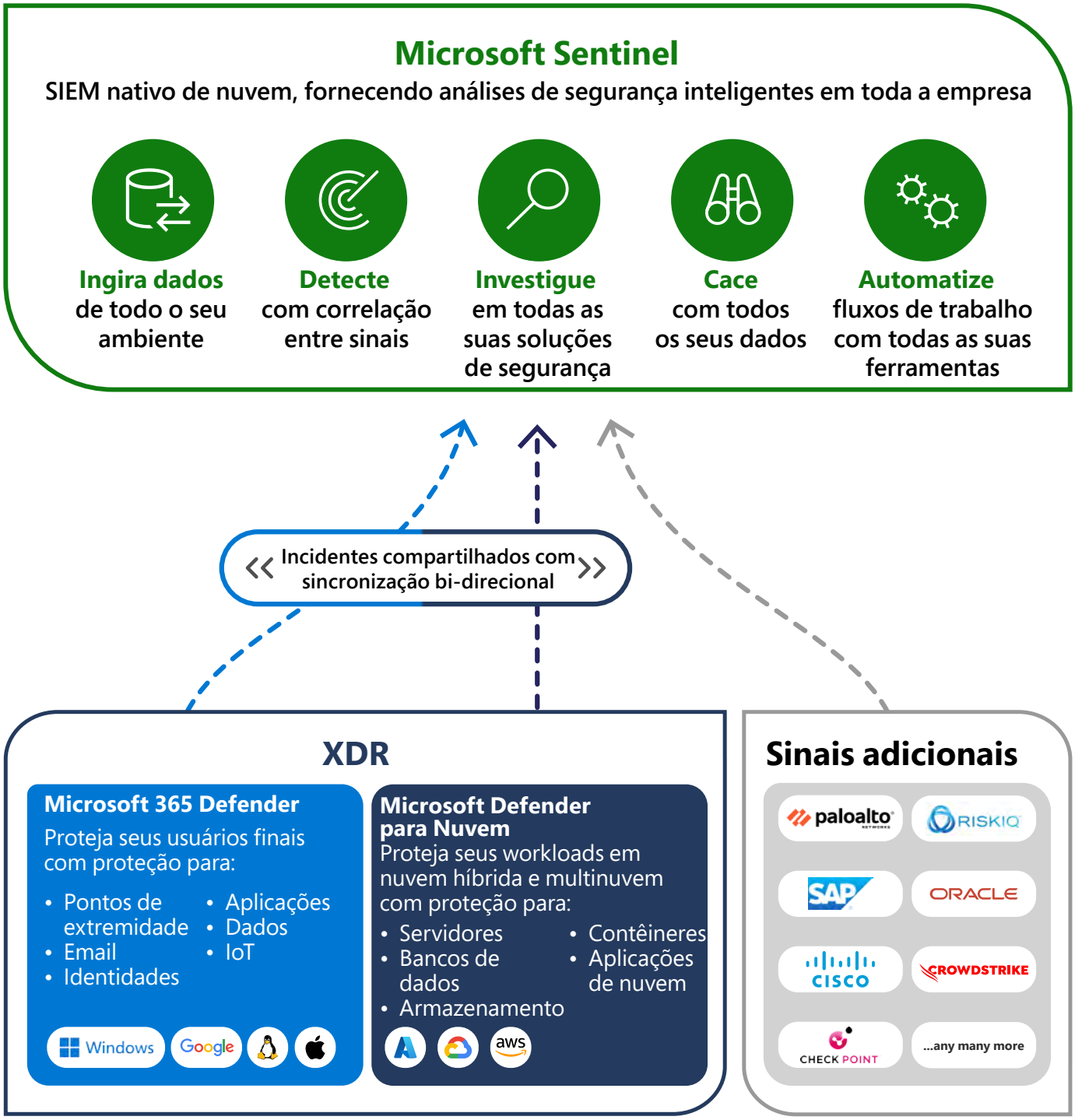
O Microsoft 365 Defender aborda a segurança do usuário final e na infraestrutura local em todo o ecossistema do Microsoft 365, protegendo identidades, pontos de extremidade, emails e aplicações. O recurso usa ferramentas de Inteligência Artificial para consolidar alertas e corrigir ataques simples.

O Microsoft Defender para Nuvem protege ambientes de nuvem híbrida e multinuvem em bancos de dados, máquinas virtuais, contêineres, armazenamento e muito mais. Ele encontra pontos fracos em toda a sua configuração de nuvem, ajuda a fortalecer a postura geral de segurança do seu ambiente e pode proteger os workloads de ameaças em evolução.

O Microsoft Sentinel fornece uma experiência abrangente de comando e controle de SecOps em toda a empresa. Ele reúne e integra dados de ameaças de todos os recursos de segurança da empresa, incluindo firewalls e ferramentas existentes, além de sistemas e plataformas de terceiros. Ele também ajuda a reduzir o ruído de eventos legítimos com Machine Learning integrado e conhecimento baseado na análise de trilhões de sinais diariamente.

Com a integração entre esses produtos, as equipes de SOC ficam preparadas para enfrentar os desafios do trabalho híbrido e os números esmagadores de sinais, além de poderem prevenir violações.

Esteja um passo à frente dos invasores com uma experiência unificada de SecOps



Dê o próximo passo

O cenário de ataque, juntamente com a necessidade contínua de um trabalho remoto seguro, exige uma abordagem moderna e integrada para a proteção contra ameaças. A integração completa capacita os defensores de sua organização colocando as ferramentas e a inteligência ideais nas mãos das pessoas certas. Com soluções integradas de SIEM e XDR, os defensores estão munidos com todo o contexto e automação necessários para combater até mesmo os ataques mais sofisticados entre domínios.

Como próximo passo, considere uma avaliação para ter uma visão completa de sua postura de segurança. O Microsoft Secure Score ajuda os CISOs a entender o estado atual da organização. Ele faz recomendações para melhorar a proteção contra ameaças e estabelece os principais indicadores de performance para ajudar as empresas a monitorar seu progresso.

Saiba mais sobre proteção integrada contra ameaças com SIEM e XDR.

Microsoft Security