DOCUMENTO TÉCNICO

# Sistemas de defesa cibernética explicados

Como o novo modelo de defesa cibernética oferece resiliência para a era da IA agêntica.

SOPHOS

# Sumário executivo

Em teoria, a cobertura de segurança para a maioria das organizações parece sólida. Ao longo dos anos, eles acumularam dezenas de produtos de segurança. No entanto, de acordo com a Gartner, "Em média, as organizações possuem 45 ferramentas de segurança que frequentemente operam isoladamente, criando complexidade, pontos cegos e vulnerabilidades ainda não identificadas que são exploradas pelos adversários".[1] Portanto, embora não faltem ferramentas, há uma carência de conectividade entre elas.

Os invasores já estão explorando as brechas entre as ferramentas, transitando entre e-mail, identidade, endpoint e rede em questão de minutos. A inteligência artificial está aumentando a velocidade, a escala e o alcance das ameaças cibernéticas a uma taxa sem precedentes, permitindo que ataques sofisticados e multicamadas sejam executados em larga escala.

Auditores, reguladores e seguradoras de proteção digital agora esperam ver um conjunto de evidências que os produtos cibernéticos fragmentados têm dificuldade em produzir. A maioria das organizações ainda tem dificuldade em responder a três perguntas básicas: se estamos protegidos, onde está o nosso maior risco e se os nossos investimentos estão dando resultado.

Um novo modelo de defesa cibernética está se consolidando para garantir a segurança na era da IA. A plataforma de segurança está evoluindo para um sistema de defesa cibernética. Estes são os seus traços característicos:

- **Uma única exibição em tempo real do ambiente** alimentada por todos os pontos de controle de todo e qualquer fornecedor.
- **As respostas se coordenam automaticamente,** em todos os pontos de controle: e-mail, identidade, endpoint, rede e outros.
- **A IA agêntica responde à velocidade e ao volume dos ataques modernos,** enquanto especialistas humanos definem os limites e permanecem responsáveis pelos resultados.
- **Aprendizagem contínua** com cada nova descoberta e cada ameaça interrompida na base total de usuários que fortalece as defesas em todos os lugares, automaticamente.
- **A unidade de defesa passa de produtos individuais para uma arquitetura que os conecta**, incluindo a arquitetura tecnológica e uma rede de especialistas humanos.

# Um sistema de defesa cibernética é...

Uma arquitetura de segurança unificada onde cada ponto de controle compartilha uma mesma exibição em tempo real, responde como uma entidade única, aprende continuamente e opera na velocidade da máquina sob responsabilidade humana.

1. *Gartner, "Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System", Neil MacDonald, 12 de dezembro de 2025*

## As ameaças da era da IA agêntica já chegaram

No final de 2025, pesquisadores documentaram a primeira campanha de espionagem cibernética conhecida, conduzida principalmente por IA em vez de pessoas. Estima-se que a IA tenha realizado entre 80 e 90% da operação de forma autônoma, em uma velocidade e escala que nenhuma equipe humana conseguiria igualar.

*Fonte: Anthropic,*

*novembro de 2025*



SOPHOS

# Seus desafios de segurança na era da IA

Anos de decisões de compra ponderadas, baseadas em ameaças específicas, resultaram em um ambiente tão complexo que a sua própria complexidade se tornou a exposição. Agora, esse conjunto de produtos descoordenados está enfrentando invasores que agem na velocidade da IA e não está conseguindo acompanhar o ritmo. Como chegamos a essa situação?

## Limitações da abordagem de plataforma

Quase todos os grandes fornecedores de segurança cibernética afirmam que suas plataformas podem fazer tudo o que você precisa. Eles vendem soluções direcionadas para o comprador que busca soluções individuais para ameaças individuais, soluções essas que visam operar em conjunto como uma única plataforma.

A filosofia da plataforma de construir um sistema unificado estava no caminho certo, mas, muitas vezes, se assemelha a uma colcha de retalhos, com ferramentas construídas ou adquiridas às pressas, destinadas a atender a hypes passados ou a inflar o preço das ações. As promessas não se concretizam:

- **Elas prometem um "painel de controle único"**, mas quando são testadas no mundo real, as equipes de resposta continuam precisando alternar entre diferentes painéis.
- **Elas prometem dados compartilhados**, mas os produtos da plataforma não conseguem analisar esses dados em conjunto para detectar um ataque que abrange identidade, nuvem e endpoint.
- **Elas prometem integração**, mas cada produto mantém seu próprio modelo de dados, e as ações de resposta ficam isoladas entre os domínios.

Todo o trabalho da plataforma — configuração, personalização e criação de fluxo de trabalho que consolide o uso de todas as partes — fica a cargo do cliente.

**Segundo a Gartner®, "Simplesmente adicionar mais ferramentas à pilha não fornecerá a estrutura de defesa cibernética inteligente que as organizações precisam para mitigar ataques orquestrados por IA, como o que a Anthropic identificou recentemente".**

**Neil MacDonald**
Gartner | VP, Distinguished Analyst e Gartner Fellow Emeritus

*Gartner, Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System, Neil MacDonald, 12 de dezembro de 2025*
*GARTNER é uma marca registrada da Gartner, Inc. e/ou suas afiliadas*

## Ataques a domínios diferentes vencem defesas fragmentadas

Modelos de dados fragmentados e análises deficientes em plataformas de produtos são um cenário perfeito para os adversários. Este tipo de ataque demonstra por quê:

- **Passo 1:** Um e-mail convincente surge na caixa de entrada.
- **Passo 2:** O destinatário insere sua senha em uma página de login falsa.
- **Passo 3:** O adversário faz login a partir de um local desconhecido.
- **Passo 4:** O invasor adiciona silenciosamente uma regra de caixa de correio para monitorar o tráfego.
- **Passo 5:** O invasor usa esse acesso para alcançar um compartilhamento de arquivos e extrair dados.

Cinco passos, cada um deles levando a um domínio diferente.

- **A segurança de  e-mail** vê a mensagem.
- **A solução de identidade** vê um login estranho.
- **A proteção de endpoint** observa uma pequena anomalia.
- **O firewall** registra a conexão de saída.

Cada produto registra a sua própria atuação e, tecnicamente, cada produto está desempenhando a sua função. No entanto, **nenhum deles consegue enxergar o quadro completo**, porque nenhum deles transmite o que sabe aos outros enquanto o ataque está em andamento. Parece apenas ruído, não uma narrativa de ataque coerente. A cadeia de eventos só se torna óbvia mais tarde, quando já é tarde demais.

Esse tipo de movimento lateral é comum em ataques modernos, e também costuma passar despercebido. O relatório O Estado do Ransomware de 2026 da Sophos mostrou que 55% dos criminosos conseguiram criptografar dados mesmo quando o firewall detectou o ataque.

## Ataques na velocidade da máquina, resposta na velocidade humana

Agora, imagine esse ataque entre domínios e reduza o tempo de duração do ataque de dias para minutos. Foi isso que a IA fez. Uma defesa que espera que uma pessoa perceba um alerta em um produto e faça uma comparação com outro produto é tardia demais. O problema não são equipes de defesa lentas, mas, sim, respostas lentas, que utilizam uma ferramenta de cada vez. Fluxos de trabalho altamente manuais não conseguem acompanhar um ataque automatizado. Quando um operador consegue formular a resposta, o invasor já passou para a próxima etapa.

## A experiência é escassa. O ruído, não.

Alocar pessoas para resolver o problema não é realmente uma opção, porque as pessoas não estão lá. A escassez de profissionais qualificados em segurança cibernética é real e não está diminuindo. No estudo da ISC2 sobre a força de trabalho em 2025, 95% das equipes de segurança relataram pelo menos uma lacuna de habilidades, e 59% a consideraram crítica ou significativa, um aumento em relação aos 44% do ano anterior.

Ao mesmo tempo, a quantidade de trabalho continua aumentando. Uma equipe pequena pode acabar responsável por mais produtos, alertas e painéis do que jamais conseguiria monitorar de forma razoável. A maioria desses alertas não passa de ruído, mas alguém precisa encontrar o sinal que eles escondem.

A IA deveria aliviar essa pressão, mas, em alguns ambientes, ela fez exatamente o contrário.

Adicionar a IA como outro produto avulso cria os mesmos problemas: mais ruído e alertas, porque ela não foi desenvolvida para interagir nativamente com o restante dos produtos da plataforma. Agora, a equipe de segurança cibernética não precisa apenas filtrar falsos positivos, mas precisa também lidar com alucinações causadas pela IA.

# A linha da pobreza em segurança cibernética é real

A linha da pobreza em segurança cibernética é a linha abaixo da qual uma organização não pode ser protegida eficientemente. Ela não é definida pelo tamanho da organização, por seu orçamento ou pelo fato de ela ter ou não um CISO. Na verdade, existem muitas organizações com bom respaldo econômico que estão abaixo dessa linha.

**A linha da pobreza em segurança cibernética é um limiar da capacidade estratégica.**

Sua organização apenas possui a tecnologia de segurança ou ela é capaz de executá-la como um sistema? Grandes equipes podem gastar grandes quantias em ferramentas que ninguém tem perícia para operar, enquanto uma pequena empresa com cerca de 200 funcionários e bem disciplinada pode operar um sistema de defesa que supera o de organizações muito maiores. Muitas organizações, sem saber, estão abaixo da linha da pobreza porque presumem que a capacidade de executar a segurança como sistema já estava implementada internamente.

Para essas organizações, a maior lacuna não é a falta de uma ferramenta. Trata-se da falta de uma estratégia clara e da orquestração necessária para que os controles existentes funcionem em conjunto contra ameaças aceleradas por IA. Elas continuam investindo, mas ainda têm dificuldade para responder a três perguntas básicas:

- Estamos protegidos?
- Onde estão os nossos maiores riscos?
- Será que nossos investimentos estão realmente dando resultado?

## Órgãos reguladores estão exigindo mais provas de resiliência

Órgãos reguladores e seguradoras de proteção digital não se importam se você possui os produtos certos. Na verdade, eles estão forçando as organizações a demonstrar cada vez mais:

- Controle coordenado entre domínios.
- Evidências retidas e auditáveis.
- Divulgações consistentes e oportunas.
- Resiliência testada e comprovada no mundo real.

Essas novas regulamentações representam um fardo pesado para organizações que ainda têm um patrimônio de segurança distribuído por dezenas de produtos, cada um com seu próprio modelo de dados e período de retenção. Produzir as provas solicitadas por um auditor ou seguradora pode se transformar um trabalho de tempo integral: exportar registros de sistemas separados, reuni-los manualmente e torcer para que o resultado trace uma história coerente. Um controle que não pode ser demonstrado é, para fins de conformidade, um controle desconsiderado.

## O fio condutor

Nenhum desses problemas é resolvido adicionando-se outro produto ou botão ao painel de controle. Eles apresentam a mesma causa primária: defesas que operam em isolamento e que falham quando as ameaças contra elas operam em consonância. Preencher essa lacuna exige algo diferente, não apenas mais um produto novo.

# Sistemas de defesa cibernética: uma abordagem moderna à segurança

Se o problema é a fragmentação, a resposta não é a consolidação por si só. Comprar um produto que tenta fazer tudo e que falha em seu intuito não é melhor do que ter vários bons produtos que não se congregam bem.

Em vez disso, as organizações deveriam procurar um sistema de defesa cibernética: um conjunto de produtos e serviços de segurança projetados para funcionar como um sistema unificado. Cada ponto de controle deve contribuir para uma compreensão compartilhada do ambiente e responder coordenadamente como parte de um todo. O sistema deve ser bem conectado, sincronizado, automatizado, inteligente e adaptável. Cinco princípios descrevem como isso se traduz na prática.

## 1 Pontos de controle autônomos e sincronizados

Um sistema de defesa cibernética começa com pontos de controle. Essas são as tecnologias e os serviços onde a telemetria de segurança é observada e as regras de segurança são impostas. Os pontos de controle podem ver e agir sobre o que está acontecendo com eles. Endpoint, firewall, e-mail, identidade, ferramentas de produtividade e outros mais são todos pontos de controle.

## 2 Uma visão compartilhada, em tempo real

Um sistema de defesa difere de uma plataforma por ter um entendimento comum do que está acontecendo em todo o ambiente. Cada ponto de controle envia as informações que observa para uma camada de dados comum em tempo real, sem atrasos causados por cópias ou reconciliações. Isso proporciona ao sistema uma visão única e compartilhada dos eventos em tempo real. Sem pontos cegos nem lacunas na resposta.

## 3 Resposta coordenada em todas as camadas

Uma resposta coordenada começa com uma detecção em uma camada que pode disparar automaticamente uma ação nas outras camadas sem que um analista precise retransmitir o sinal de um painel para o outro.

Um login suspeito pode levar a uma análise mais rigorosa tanto no endpoint quanto na camada de e-mail. Um arquivo malicioso em um dispositivo pode fazer com que o firewall ou a rede bloqueie a conexão que está tentando estabelecer. O sistema responde como tal porque já reconhece o ataque como tal. E quando um ataque se move rapidamente, esse tipo de coordenação é importante.



SOPHOS

## 4 IA agêntica com responsabilidade humana

A velocidade é o fator decisivo. Ataques que se desenrolam em minutos não podem ser interrompidos por defesas que esperam que um humano os perceba. É por isso que a IA precisa estar no centro do sistema, não nas margens.

Em um sistema de defesa cibernética, a IA é a arquitetura; e ela é integrada, não adicionada posteriormente. A IA correlaciona sinais em todas as camadas, identifica o formato de um ataque assim que ele surge e impulsiona a detecção, a investigação e a resposta na velocidade da máquina. Esse sistema nativo de IA é diferente da IA que é acoplada a um produto unitário e só consegue ver os dados desse produto.

A inteligência artificial integrada a um sistema de defesa pode raciocinar sobre tudo o que o sistema observa. No entanto, a resposta na velocidade da máquina sem responsabilidade humana é uma desvantagem, não uma vantagem. Os sistemas de defesa cibernética não retiram as pessoas da segurança. Em vez disso, eles as direcionam para onde o discernimento humano tem maior peso: definir limiares, lidar com questões inéditas ou decisões de alto risco, analisar incidentes e manter a responsabilidade pelos resultados.

**A IA lida com a velocidade e o volume.** A triagem de rotina e as ações rápidas e de alta confiabilidade.

**Especialistas humanos definem o limite da confiança:** o que a IA pode decidir sozinha e quando precisa de ajuda. Eles intervêm quando o contexto é desconhecido ou quando os riscos são altos.

À medida que o sistema conquista a confiança, esse limite pode se expandir. Mas a responsabilidade está sempre nas mãos dos especialistas humanos.

A IA lida com a velocidade e o volume.

Especialistas humanos definem o limite de confiança.

## 5 Inteligência composta

Os sistemas de defesa aprendem. Uma ameaça encontrada em qualquer lugar se torna conhecimento em todo lugar. O endpoint vê o que o firewall viu. O gateway de e-mail diz à camada de identidade o que capturou. Cada ferramenta aprende juntamente com as outras e se baseia no que ocorreu antes. Tudo isso acontece sem qualquer configuração manual. A inteligência do sistema de defesa se aprimora com o aumento do número de usuários e padrões observados, permitindo que o sistema evolua tão rapidamente quanto os ataques impulsionados por IA.

## De plataformas a sistemas de defesa cibernética

Considerados em conjunto, esses cinco princípios definem uma categoria própria. Os sistemas de defesa são a evolução da plataforma, otimizados para a era da IA. Uma plataforma é, geralmente, apenas um conjunto de produtos por trás de um painel compartilhado, interligados por um contrato de licenciamento e login, não por design.

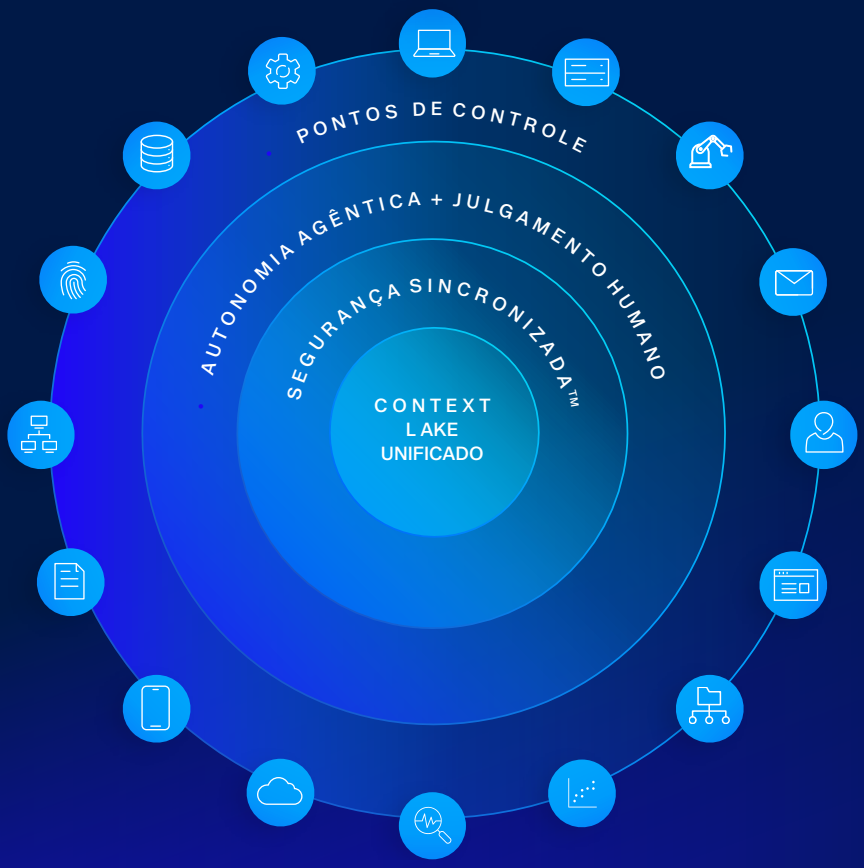
Um sistema de defesa cibernética é diferente. Os dados são compartilhados, a IA está integrada, a resposta é coordenada e especialistas humanos permanecem no comando. Trata-se de uma arquitetura projetada para funcionar como um único produto, em vez de uma coleção de produtos organizados para parecerem uma só unidade.

# Sophos Fusion: o sistema de defesa cibernética da Sophos

O Sophos Fusion é o sistema de defesa cibernética mais completo do setor, projetado para um mundo onde as ameaças se movem na velocidade da IA. Viabilizada pela arquitetura Sophos AI-Native Cybersecurity Defense System e por mais de 500 integrações da Sophos e de terceiros, a solução enxerga tudo, conecta tudo e permite que suas defesas respondam de forma unificada.

O Sophos Fusion transforma os princípios dos sistemas de defesa cibernética em prática: uma arquitetura única e aberta, em que os pontos de controle operam em unidade, impulsionados por IA agêntica, com discernimento humano para proteger as organizações contra ameaças habilitadas por IA que se movem mais rápido do que as defesas conseguem rebater.

Quanto mais produtos do portfólio Sophos um cliente ativar, mais valor o Sophos Fusion proporcionará.



## Pontos de controle autônomos e sincronizados

Cada ponto de controle que você já possui fornece inteligência de ameaças em tempo real e executa ações de resposta. A arquitetura é totalmente aberta: integra-se nativamente aos produtos Sophos e a mais de 500 tecnologias de terceiros, de modo que os investimentos que você já fez passam a fazer parte de uma defesa coordenada, em vez de ficarem isolados.

Ela também inclui a integração de segurança Microsoft mais completa do mercado em todos os planos da Microsoft e não apenas nos mais caros, permitindo que as organizações com licenças básicas da Microsoft fortaleçam suas defesas com essa mesma telemetria.

## Uma visão compartilhada, em tempo real

Toda a telemetria de cada ponto de controle flui em tempo real para o Context Lake unificado, uma camada de dados compartilhada. Não há atraso na agregação nem armazenamento separado de dados nos pontos de controle individualmente. Imagine isso como um sistema nervoso compartilhado: cada ponto de controle percebe o que todos os outros pontos de controle percebem, no momento exato em que acontece. É esse entendimento mútuo que torna a coordenação possível.

## Resposta coordenada em todas as camadas: Synchronized Security™

O Synchronized Security™ é o tecido conjuntivo que transforma o entendimento compartilhado em ação coordenada na plataforma Sophos Fusion. Isso permite que pontos de controle da Sophos e de terceiros respondam automaticamente às ameaças em conjunto.

Uma detecção no endpoint pode disparar uma resposta no firewall. Uma identidade comprometida pode bloquear o acesso em todo o ambiente. Um e-mail suspeito pode levar a um maior escrutínio em todas as outras camadas. Quanto mais soluções Sophos você implantar, mais benefícios obterá do Synchronized Security™.

Pense no sistema de incêndio em prédios modernos: o sensor em uma sala não apenas dispara o alarme, mas também fecha as portas corta-fogo, redireciona o fluxo de ar e aciona os chuveiros de água nos andares próximos. O Sophos Fusion funciona da mesma maneira: como um todo e de forma coordenada. Isso é possível porque os dados já estão unificados. Nenhuma configuração ou ação adicional é necessária.

## IA agêntica com responsabilidade humana

O Sophos Fusion detecta, investiga e responde na velocidade da máquina, mas nunca sem supervisão humana. Cada ação permanece dentro dos limites definidos e continuamente ajustados por peritos. É isso que a torna uma IA agêntica: inteligência artificial capaz de raciocinar sobre novas situações, não apenas seguir roteiros predefinidos.

Uma boa analogia é o piloto automático na aviação. O sistema pode pilotar o avião, mas o piloto define os parâmetros, monitora os instrumentos e assume o controle quando a situação é desconhecida ou de alto risco.

No Sophos Fusion, essa capacidade agêntica é entregue pelo Fusion AI, a IA agêntica nativa da Sophos. A Sophos possui mais de 50 modelos de IA integrados a suas defesas, todos continuamente aprimorados com inteligência de ameaças em tempo real. Por exemplo, o Sophos Email utiliza mais de 20 modelos, incluindo modelos proprietários de processamento de linguagem natural (NLP) que analisam o texto, o tom, o contexto e a estrutura dos e-mails para identificar ataques de phishing e comprometimento de e-mail corporativo.

O Sophos MDR, um serviço disponível 24 horas por dia, 7 dias por semana, no qual especialistas da Sophos monitoram e respondem em seu nome, opera o maior centro agêntico de operações de segurança do mundo utilizando o Sophos Cyber Defense System. Trata-se da maior operação de detecção e resposta gerenciadas do setor, protegendo mais de 40.000 organizações. A solução resolve 52% dos incidentes de ponta a ponta com IA, com uma média de 89 segundos entre o alerta e a resposta automatizada, enquanto os especialistas humanos permanecem responsáveis pelas decisões que acarretam risco organizacional.

## Inteligência composta

O Sophos Cyber Defense System aprende com todos os ataques, não apenas os ataques direcionados à sua organização. Todas as ameaças encontradas nas mais de 625.000 organizações protegidas pela Sophos retroalimentam o Sophos Fusion, assim como todos os casos atípicos resolvidos por um analista e todos os novos ambientes que entram em operação. O Sophos X-Ops aprimora isso com sua própria expertise aprofundada e inteligência de ameaças em tempo real, posteriormente distribuídas automaticamente para todos os produtos Sophos e todos os clientes para melhorar suas defesas.

Funciona de forma muito semelhante a um sistema imunológico biológico. Cada ameaça que o corpo enfrenta torna-se parte da memória permanente, catalogada, compreendida e pronta para a próxima vez que surgir. O Sophos Fusion funciona da mesma maneira. Um novo cliente está protegido desde o primeiro dia contra ameaças nunca enfrentadas nem mesmo observadas, isso porque o sistema já as conhece.

Por isso o número 625.000 é importante: ele reflete a amplitude da experiência que permite a composição entre proteção e inteligência. Quanto mais o sistema vê, melhor ele pode defender os que estão dentro dele.

## Sophos Fusion: a morada do seu sistema de defesa cibernética

O Sophos AI-Native Cybersecurity Defense System é a arquitetura. O Sophos Fusion é onde você vivencia isso. Um só local para gerenciar seus pontos de controle Sophos, visualizar o panorama completo de cada ponto de controle conectado e tomar as medidas necessárias.

Isso significa que não há nada extra para comprar ou ativar nem necessidade de mudar a forma como você trabalha hoje. Cada ponto de controle da Sophos já é parte integral do Sophos Fusion, portanto, no momento exato em que o implanta, você passa a integrar essa arquitetura. E à medida que você adiciona mais pontos de controle da Sophos ou de terceiros, mais partes do sistema ganham vida, proporcionando uma visão compartilhada mais rica e criando mais valor em tudo o que você já utiliza.

## O ataque visto da perspectiva do Sophos Fusion

Vamos voltar ao ataque em vários estágios que vimos anteriormente. Um e-mail infectado, uma credencial roubada, um login incomum, uma regra de encaminhamento de caixa de correio e movimentos laterais em direção a dados sensíveis. No Sophos Fusion, a telemetria do Sophos Email e do ambiente Microsoft do cliente flui em conjunto para o Context Lake unificado. Em seguida, o Sophos XDR correlaciona esses sinais à medida que chegam, reconhecendo a sequência como um único ataque conectado, em vez de cinco alertas não relacionados.

A partir daí, o Synchronized Security™ coordena a resposta em e-mail, identidade, endpoint e rede. A IA agêntica age na velocidade da máquina, enquanto os analistas do Sophos MDR tomam medidas diretas e assumem as decisões de alto risco. O ataque que poderia passar despercebido em produtos isolados é detectado por um sistema que tem uma visão completa da situação.

# O que o Sophos Fusion significa para a sua organização

O Sophos Fusion oferece resiliência cibernética para a era da IA agêntica em quatro áreas importantes para os negócios.

- **Proteção contra ameaças aceleradas por IA que se movem mais rapidamente do que a capacidade de resposta da defesa.** Ataques em vários estágios são detectados e contidos precocemente, mesmo com a aceleração e o aumento da escala dos ataques realizados por IA, porque cada ponto de controle compartilha o contexto e responde em conjunto, em vez de agir individualmente.

- **Maior impacto de suas pessoas e investimentos.** A IA agêntica absorve o trabalho rotineiro e ruidoso de triagem e resposta, permitindo que sua equipe existente e seus pontos de controle alcancem mais resultados sem a necessidade de aumentar o número de funcionários ou a complexidade do processo. Todas as ferramentas conectadas, Sophos ou não, contribuem para o resultado.

- **Postura elevada em conformidade e seguro de proteção digital.** Cobertura 24 horas, contexto intercamada preservado e resposta coordenada fornecem as evidências que auditores, reguladores e seguradoras esperam a partir de um único registro pesquisável, em vez de logs exportados manualmente. A mesma arquitetura que aprimora a proteção também aprimora a sua capacidade de demonstrá-la.

- **Estratégia de segurança cibernética alinhada ao seu negócio.** Ao conectar e coordenar suas defesas, o Sophos Fusion permite que você passe do gerenciamento de painéis táticos para a confiança operacional, com visibilidade clara de onde estão suas lacunas e maiores riscos, e se seus investimentos estão dando resultado. Assim, organizações de qualquer porte, com ou sem CISO, podem finalmente implementar a estratégia que sempre desejaram.

Todos os clientes Sophos são parte do Sophos Fusion, o sistema de defesa da Sophos. Um upgrade automático e transparente que protege os clientes contra as ameaças da era da IA.

# Introdução ao Sophos Fusion

Todas as soluções Sophos são parte do Sophos Fusion, transformando cada uma delas em um ponto de entrada em vez de uma ferramenta independente. Começar é tão simples quanto implantar um produto ou serviço Sophos: o Sophos MDR, Sophos XDR, Sophos Endpoint, Sophos Firewall e Sophos Email são todos pontos de partida comuns. Quanto mais soluções você adicionar, mais da arquitetura você desbloqueará.

Não há necessidade de alterar pontos de controle de terceiros atuais em que você confia. Integre-os ao Sophos Fusion para fornecer inteligência de ameaças em tempo real e executar ações de resposta. Comece onde o risco é maior e expanda no seu próprio ritmo.

Pronto para começar? Fale com um especialista da Sophos para definir o ponto de partida ideal para o seu ambiente ou saiba mais em sophos.com/fusion.

# Conclusão

Durante anos, a resposta padrão a cada nova ameaça era adicionar mais um produto, e esse hábito criou a fragmentação que os adversários agora exploram. A IA só agravou o problema, estendendo a diferença entre a velocidade de movimento de um ataque e a rapidez com que a resposta painel a painel consegue acompanhar. Mais produtos não vão diminuir essa diferença. Um sistema de defesa cibernética sim.

Um sistema de defesa cibernética muda o foco da defesa, passando de produtos individuais para a arquitetura que os conecta:

- Uma visão compartilhada
- Resposta coordenada em todas as camadas
- Inteligência artificial integrada para agir na velocidade da máquina
- Especialistas humanos mantêm o julgamento e a responsabilidade em seus devidos lugares

Garantir a segurança na era da IA significa fazer com que tudo o que você já possui funcione como uma unidade. O Sophos Fusion, o Sophos AI-Native Cybersecurity Defense System, é a forma de colocar esse modelo em prática sem substituir o que você já possui hoje.

SOPHOS

# Pronto para discutir suas necessidades de defesa cibernética na era da IA?

Fale com um especialista da Sophos ainda hoje.

**Vendas na América Latina**
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com