

DOCUMENTO TÉCNICO

Explicação da Segurança Sincronizada™

SOPHOS

Segurança sincronizada

A Segurança sincronizada™ está no centro do Sophos Fusion, o sistema de defesa e segurança cibernética nativo de IA líder do setor da Sophos. É o tecido conjuntivo que transforma informações sobre a ameaça em todos os pontos de controle conectados – Sophos e de terceiros – em uma resposta coordenada às ameaças.

Em sua Visão do Futuro da Tecnologia: Proteja a superfície de ataque global com um sistema autônomo de defesa cibernética.[1] A Gartner identificou que "as organizações precisam de uma sobreposição inteligente que conecte os diferentes elementos de seu conjunto de ferramentas de cibersegurança para responder de forma proativa e reativa a riscos e ameaças na velocidade das máquinas". A Segurança sincronizada é um elemento-chave na forma como isso é oferecido no Sophos Fusion.

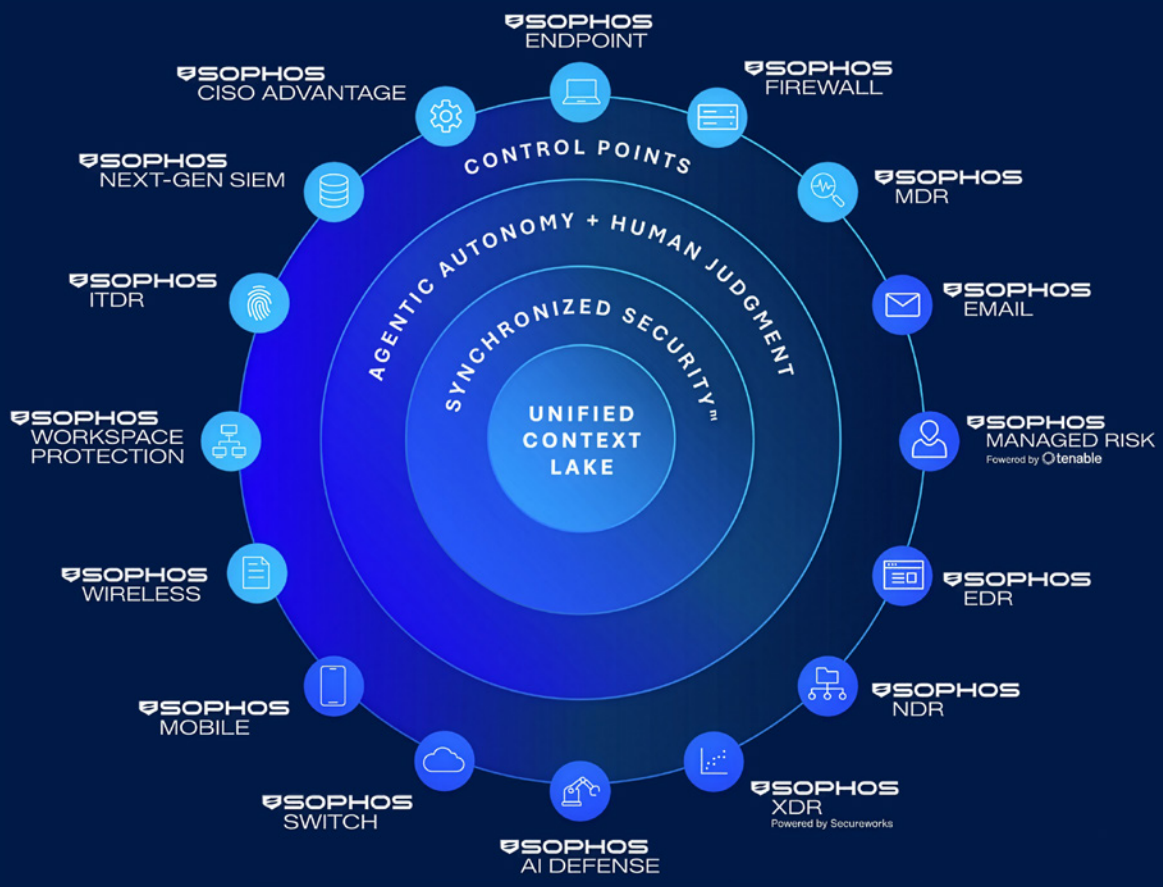
Este guia explica como funciona a Segurança sincronizada, os benefícios que ela oferece e como as organizações podem aproveitá-la.

1 Visão do Futuro da Tecnologia: 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 de suas afiliadas.



Resumo rápido

- A Segurança sincronizada é um elemento central do sistema de defesa Sophos Fusion e está incluída automaticamente – não é necessário comprar um módulo adicional ou licenciar componentes extras.
- Isso permite uma resposta coordenada a ameaças em diversos pontos de controle conectados. Para começar, é necessário que dois ou mais pontos de controle funcionem em conjunto dentro do Sophos Fusion.
- A Segurança sincronizada funciona tanto com pontos de controle da Sophos quanto com pontos de controle de terceiros. As ações de resposta em ambientes de clientes individuais dependem de quais controles estão conectados ao Sophos Fusion e do nível de ação de resposta autônoma que o cliente concede sobre cada ponto de controle.
- O Sophos XDR está no centro da Segurança sincronizada, correlacionando sinais de todo o ambiente do cliente em uma única cadeia de ataque e permitindo ações de resposta automatizadas ou conduzidas por humanos em todo o sistema de defesa.
- As soluções da Sophos também podem funcionar em conjunto sem o Sophos XDR, adicionando uma camada extra de segurança sincronizada.
- A segurança sincronizada baseia-se nas capacidades fundamentais comprovadas em combate que a Sophos lançou em 2015.



Por que a resposta coordenada é importante?

Historicamente, as ferramentas de segurança foram criadas para executar uma única tarefa com excelência. Um agente de endpoint protege o dispositivo em que é executado (por exemplo, desktop, laptop ou servidor). Um firewall monitora o que atravessa a rede. Um serviço de e-mail controla o que chega à caixa de entrada. Cada um é bom no seu trabalho e alheio a tudo o que está fora dele.

Os atacantes já sabiam disso há muito tempo. Uma intrusão moderna não é um evento isolado em um único local. Ele cruza identidade, e-mail, endpoint e rede por design, porque o espaço entre eles é exatamente onde estão as lacunas, e é aí que os atacantes as exploram.

A consequência é familiar para qualquer pessoa que já tenha gerenciado uma equipe de segurança. As soluções individuais enxergam apenas seu próprio domínio, identificando anomalias aparentemente díspares. Cada um, por si só, aparenta ser viável. Ninguém tem tempo nem contexto para reconhecer as anomalias como sendo o mesmo ataque até que o dano esteja feito.

A IA ampliou as lacunas. Os ataques agora são executados na velocidade das máquinas e em volumes nunca antes vistos na indústria. No entanto, a maioria das defesas ainda funciona em velocidade humana, com um analista se movendo entre consoles e correlacionando dados manualmente.

Adicionar mais um produto ao patrimônio não elimina essa lacuna. Em vez disso, as organizações devem considerar a possibilidade de conectar os produtos nos quais já investiram. É exatamente isso que a Segurança sincronizada faz dentro do Sophos Fusion.



O que a Segurança sincronizada oferece

A coordenação transforma a velocidade, a escala e o alcance da resposta à ameaça, alterando o resultado de um ataque. Quando endpoints, rede e outros controles atuam em conjunto, a contenção acontece em segundos — não depois que alguém percebe e reage. Um endpoint comprometido é isolado imediatamente antes que um adversário possa mover-se lateralmente, acessar dados sensíveis ou estabelecer persistência. Além disso, como a resposta é automatizada, funciona durante a noite e nos fins de semana, quando geralmente há menos pessoas disponíveis.

A coordenação também elimina as brechas que os atacantes exploram. Pontos de controle de terceiros que antes apenas geravam alertas passam a contribuir ativamente para a defesa. Os investimentos em segurança existentes deixam de ficar em isolamento e passam a fazer parte da resposta coordenada.

O impacto operacional em uma equipe de segurança é imediato. A contenção de rotina ocorre sem intervenção do analista. Quando é necessária uma investigação humana, o analista começa com o contexto entre as diferentes camadas já reunido, em vez de montá-lo manualmente em vários painéis.

Essa mesma coordenação facilita a comprovação da proteção. O contexto entre as diferentes camadas é preservado, e uma resposta coordenada deixa um registro consistente do que foi constatado e das medidas tomadas a respeito. Essa é a narrativa de controle que auditores, reguladores e seguradoras esperam. A arquitetura que aprimora a proteção também aprimora a capacidade do cliente de demonstrá-la.

A defesa também se fortalece à medida que cresce. Cada novo ponto de controle conectado ao Sophos Fusion envia um sinal adicional para o repositório de contexto unificado e abre mais um local de resposta – sem um aumento correspondente no esforço operacional. Mais cobertura não significa mais trabalho.

Para provedores de serviço gerenciado, a mesma coordenação ocorre de forma consistente em todos os ambientes de clientes, incluindo aqueles que combinam pontos de controle da Sophos e de terceiros. A contenção automatizada reduz a triagem manual e a sobrecarga de remediação.

Como funciona

A Segurança sincronizada começa com a telemetria. Cada ponto de controle conectado reporta o que observa para o repositório de contexto unificado em tempo real. Endpoint, firewalls, e-mail, nuvem, redes, identidade e ferramentas de produtividade alimentam o mesmo lago. Os pontos de controle de terceiros alimentam o sistema juntamente com os da Sophos. Nada fica em fila de espera para ser agregado, e não há um repositório de dados secundário para reconciliação posterior.

O Sophos XDR interpreta a imagem compartilhada e realiza o trabalho que um analista faria manualmente. Ele interliga eventos relacionados e os resolve em uma única cadeia de ataque, em vez de uma série de alertas separados. A correlação é o que importa, porque um ponto de controle só vê um fragmento.

As ações de resposta são então enviadas de volta aos pontos de controle. A Sophos XDR fornece a infraestrutura necessária: Automação SOAR, manuais de procedimentos, gerenciamento de caso e um amplo conjunto de ações de resposta. A maioria funciona automaticamente, sem intervenção humana. Quando for necessário julgamento, um analista interno pode acionar a mesma ação manualmente usando o Sophos XDR, assim como um analista do Sophos MDR.

A integração bidirecional com pontos de controle de terceiros significa que o Sophos Fusion pode enviar e receber dados por meio da integração. Por exemplo:

- Ele pode receber telemetria de um firewall que não seja da Sophos e enviar um Endereço IP para o firewall bloquear.
- A integração com o ServiceNow permite abrir, atualizar e fechar casos.
- A resposta a ameaças ativas no Sophos Firewall usa respostas acionadas por API a feeds de ameaças de terceiros para bloquear a conexão de um dispositivo comprometido ou não autorizado à rede.

De forma exclusiva, os pontos de controle da Sophos também atuam diretamente uns sobre os outros, sem qualquer envolvimento do Sophos XDR. O recurso Security Heartbeat integrado transmite a verificação de integridade de um dispositivo do Sophos Endpoint para os outros pontos de controle da Sophos – um status verde indica integridade, um status amarelo indica potencial comprometimento e um status vermelho indica comprometimento total.

Os demais pontos de controle da Sophos são projetados para atuar no estado de integridade do dispositivo. Uma vez que os pontos de controle estejam conectados à mesma conta Sophos Fusion, as respostas principais não precisam de configuração adicional. Funcionalidades que aproveitam o estado de integridade, como uma regra de firewall que restringe o acesso à internet ou uma política do Sophos Workspace Protection, são configuradas pelo cliente antes de entrarem em vigor.

Colete

Correlacione

Responder

O Sophos Fusion coleta telemetria, o Sophos XDR cria contexto e as ações de resposta automatizadas restabelecem a aplicação das regras aos pontos de controle.

Uma capacidade, múltiplas dimensões de coordenação

A segurança sincronizada foi lançada inicialmente em 2015, sendo uma inovação mundial na época, e expandiu seu escopo ao longo de mais de uma década. O nível de coordenação entre os pontos de controle varia de um ambiente de cliente para outro, dependendo da combinação exata de pontos de controle que eles têm implementados.

A coordenação é mais profunda entre os pontos de controle da Sophos, pois eles são projetados para funcionar em conjunto desde a sua concepção. Os pontos de controle de terceiros se integram por meio do Sophos Fusion, e as ações de resposta variam de acordo com o que o outro fornecedor expõe.

A profundidade da coordenação também depende do nível de controle que o cliente concede ao Sophos Fusion sobre cada ponto de controle. Essa escolha pertence ao cliente, e o fato de ela existir é o objetivo, e não uma falha. Pergunte à maioria das organizações se um endpoint infectado deve ser removido da rede sem que ninguém aprove, e a resposta é sim. Ao questionar se um sistema deve reescrever sua própria política de firewall para reduzir a exposição, a resposta varia.

Os firewalls são o exemplo que torna a tensão óbvia. No final das contas, bloquear um endpoint comprometido é uma simples alteração nas regras do firewall. Muitas organizações são cautelosas com alterações automatizadas na configuração do firewall, e seus processos de controle de mudanças existem por um bom motivo.

Os clientes podem criar suas próprias automações e playbooks e executá-los em conjunto com os fornecidos pela Sophos. Um cliente que utiliza o Sophos Endpoint decide por si próprio o que um dispositivo comprometido significa para o seu firewall Fortinet, abrangendo o comportamento desse firewall e sua configuração. Uma vez definidas, essas automações são executadas dentro do Sophos Fusion como qualquer outra resposta coordenada.



Segurança sincronizada em ação

A coordenação é mais fácil de reconhecer com exemplos. Os casos de uso abaixo mostram a mesma capacidade operando em diferentes profundidades, em vez de uma lista de recursos separados.

Coordenação entre produtos Sophos

Quando o Sophos Endpoint detecta uma ameaça em um endpoint ou servidor, ele define a verificação de integridade do Security Heartbeat desse dispositivo como vermelho. O novo status é compartilhado automaticamente com os outros pontos de controle Sophos conectados por meio do Security Heartbeat. Seguem-se várias respostas automáticas:

- O Sophos Endpoint tenta remediar a ameaça, o que pode incluir o bloqueio e a reversão da criptografia por ransomware ou a implementação de um nível mais elevado de controle para deter um adversário ativo.
- O Sophos Firewall limita o acesso do dispositivo à internet, cortando qualquer conexão com um servidor de comando e controle e impedindo que ele se conecte a dispositivos em funcionamento.
- O Sophos Wireless, os Sophos Switches e o Sophos Workspace Protection restringem o acesso do dispositivo aos recursos de rede, limitando ainda mais o impacto da violação.
- Os endpoints saudáveis são notificados sobre a verificação de integridade vermelha e rejeitarão solicitações de conexão de rede do dispositivo afetado.

O mesmo mecanismo detecta problemas que nunca se manifestam como uma infecção. Um Endpoint ou servidor que envia grandes volumes de e-mails de spam ou phishing é definido com a verificação de integridade vermelha. Em seguida, o Sophos Endpoint procura por usuários ou aplicativos maliciosos não identificados anteriormente, e o Sophos Email bloqueia as mensagens antes que elas cheguem à caixa de entrada.

Um Endpoint ou servidor pode permanecer na verificação de integridade vermelha por segundos ou até mesmo dias, dependendo da remediação necessária. Após a limpeza, a verificação de integridade do dispositivo retorna ao verde e o acesso é restaurado automaticamente em todo o sistema.

O valor se torna mais evidente quando ninguém está olhando. Um servidor comprometido no final da noite de sexta-feira é desconectado em segundos, em vez de dar ao adversário todo o fim de semana para se propagar pela rede.

CENÁRIO

O Sophos Endpoint detecta uma ameaça e define a verificação de integridade do Security Heartbeat como Vermelho. O novo status é compartilhado automaticamente com todos os pontos de controle Sophos conectados. Quando a ameaça ao endpoint é removida, o mesmo ciclo é seguido para restaurar o acesso.

SINAL

RESPOSTA COORDENADA

SOPHOS ENDPOINT

Detecta uma ameaça

SOPHOS FUSION

AI-Native Cybersecurity Defense System



SOPHOS FIREWALL

Remove a conectividade de rede e restringe o acesso à rede.

SOPHOS WIRELESS

SOPHOS SWITCH

SOPHOS WORKSPACE PROTECTION

Restrinja o acesso do dispositivo aos recursos de rede.

SOPHOS ENDPOINT

Endpoints saudáveis rejeitam a comunicação de rede.

Sophos Endpoint e um firewall de terceiros

A coordenação não se limita aos pontos de controle da Sophos. Um cliente que utiliza o Sophos Endpoint juntamente com um firewall Fortinet pode ter um dispositivo comprometido que acione uma resposta no firewall Fortinet. O cliente define qual será essa resposta e até que ponto ela irá, o que mantém a automação dentro dos limites de controle de mudanças definidos por ele. Os recursos de automação e playbook (SOAR) do Sophos XDR tornam isso possível, funcionando em conjunto com a integração do Fortinet no Sophos Fusion.



Tecnologia e telemetria da Microsoft

Quase todas as organizações utilizam tecnologia da Microsoft, e a identidade é o principal vetor de ataques de ransomware. Um token de sessão roubado ou uma conta comprometida oferece ao adversário uma forma legítima de acesso, e nenhuma contenção de endpoint será eficaz se a própria conta permanecer comprometida. A resposta deve abranger o ambiente da Microsoft para concluir a remediação.

O bloqueio da conta é o exemplo mais claro: O Sophos Fusion pode bloquear uma conta Microsoft comprometida para impedir o acesso do invasor e, em seguida, desbloqueá-la quando a conta estiver segura para uso novamente. A conta é tratada como um ponto de controle como qualquer outro – algo que o sistema pode ver e sobre o qual pode agir, e não algo que um administrador gerencie separadamente posteriormente.

A integração é bidirecional. A telemetria de diversas fontes da Microsoft alimenta o mesmo Context Lake unificado que os pontos de controle da Sophos, o Microsoft Entra ID e o Microsoft Graph Security, entre outros. Assim, um sinal da Microsoft pode gerar uma resposta em um ponto de controle da Sophos com a mesma facilidade que o inverso. Uma tentativa de login suspeita detectada pela Microsoft pode isolar um endpoint do Sophos, mesmo sem que nenhuma das partes esteja configurada para monitorar a outra.

A borda da rede, com fio e sem fio.

Switches e pontos de acesso raramente são considerados parte de uma defesa. Eles fazem parte da infraestrutura, adquirida para movimentar o tráfego e manter as pessoas conectadas, e a maioria das organizações os trata dessa forma. No entanto, eles estão localizados no ponto de encontro de todos os dispositivos com a rede, o que os torna um dos primeiros locais onde um dispositivo comprometido ou não autorizado pode ser bloqueado.

No Sophos Fusion, os Sophos Switches e os pontos de acesso Sophos Wireless funcionam como pontos de controle: eles contribuem com o que veem sobre os dispositivos conectados e podem agir com base no que o sistema em geral encontra. Os administradores podem identificar dispositivos novos ou não autorizados, clientes em uma SSID inesperada ou um dispositivo conectado à porta de switch errada.

A Resposta a Ameaças Ativas, um recurso de segurança sincronizada do Sophos Firewall, transforma esse contexto em ação. Ao utilizar a telemetria no Context Lake unificado, um dispositivo pode ser bloqueado na camada de acesso com fio ou sem fio antes de se propagar pela rede. Os clientes escolhem se desejam ativar a Resposta a Ameaças Ativas, mantendo em suas mãos a decisão de permitir o bloqueio automatizado na camada de acesso.

Dispositivos de rede de terceiros seguem o mesmo padrão do exemplo de firewall de terceiros acima.



A Sophos AI Defense revela o uso de Shadow AI.

A coordenação não se resume apenas a malware e intrusões. O Sophos AI Defense é um ponto de controle no Sophos Fusion que governa como a IA é usada em toda a organização. Ele interpreta a telemetria de atividade de IA de diversos produtos Sophos no contexto unificado, juntamente com todos os outros sinais visíveis para o Sophos EDR, Sophos XDR e Sophos MDR. O Sophos AI Defense foi projetado para revelar os detalhes minuciosos do uso de IA e, uma vez que essas informações estejam no Context Lake unificado, elas são processadas pela mesma funcionalidade de segurança sincronizada que os demais componentes.

Shadow AI demonstra por que isso é necessário. Um funcionário começa a usar uma ferramenta de IA desconhecida, colando nela código-fonte e registros de clientes. O navegador vê os dados colados, o endpoint vê o aplicativo e o firewall vê o tráfego para um serviço de IA proveniente de um dispositivo que pode nem mesmo ser gerenciado. Nenhum ponto de controle consegue enxergar o quadro completo, por isso a ferramenta passa despercebida.

O Sophos AI Defense reúne esses sinais e os avalia em contexto, fornecendo ao analista de segurança as evidências necessárias para entender o que aconteceu. Ele combina telemetria, como identidade, permissões, comportamento, exposição de dados e localização tanto do usuário quanto do modelo de IA, o que separa o uso aceitável da atividade não gerenciada, com privilégios excessivos ou contra a política.

A fiscalização é então executada nos pontos de controle:

- O Sophos Workspace Protection controla o navegador, incluindo copiar e colar, uploads, downloads e capturas de tela.
- O Sophos Endpoint restringe o acesso a aplicativos e sites de IA em diferentes grupos de usuários e tipos de dispositivo.
- O Sophos Firewall controla o tráfego de serviços de IA na camada de rede, incluindo dispositivos não gerenciados e atividades que não sejam do navegador.
- Os produtos da Sophos podem inspecionar solicitações, uploads e interações de IA em tempo real, mantendo o código-fonte, os registros de clientes e os dados financeiros dentro da empresa.
- Um administrador pode bloquear uma ferramenta de IA específica em todo o patrimônio a partir do Sophos Fusion.

A política não é o fim da questão. Uma violação ou comportamento não autorizado de um agente surge nos mesmos fluxos de trabalho do Sophos EDR, Sophos XDR e Sophos MDR que qualquer outra detecção, sendo tratado com a automação e os playbooks já utilizados para ameaças de identidade, endpoint e rede. O alcance da coordenação depende de quais pontos de controle estão conectados ao Sophos Fusion.

82%

82% das organizações descobriram ferramentas ou fluxos de trabalho de IA desconhecidos em seus ambientes.[2]

2 Cloud Security Alliance, O Problema do Agente Shadow AI em Ambientes Empresariais, 2025

Coordenação que vai além da resposta à ameaça

Entre os pontos de controle da Sophos, a coordenação vai além do compartilhamento de um veredito sobre ameaças. Um ponto de controle pode fazer uma pergunta direta a outro e agir de acordo com a resposta. Um endpoint ou servidor protegido pelo Sophos Endpoint já sabe a maior parte das informações que um Sophos Firewall não consegue fornecer sobre o tráfego de rede. Três exemplos mostram o que isso possibilita: identificar o aplicativo por trás do tráfego em uma porta, identificar o usuário por trás de uma sessão e decidir se um dispositivo está apto a receber acesso.

Controle Sincronizado de Aplicativo

Faça uma conexão não classificada em uma porta incomum. Um firewall que o inspeciona isoladamente vê um fluxo de pacotes e pouco mais. O Sophos Firewall pode consultar o Sophos Endpoint para saber qual aplicativo está enviando e recebendo dados nessa porta e obter uma resposta sobre qual aplicativo é o responsável. Os clientes podem então permitir ou bloquear o aplicativo com base nisso. Com o tempo, isso também constrói uma imagem precisa do que está sendo executado na rede, que geralmente é mais variado do que qualquer um espera.

Identidades, não endereços IP

A identidade do usuário funciona da mesma maneira. O Sophos Endpoint transmite informações de usuários autenticados para o Sophos Firewall, permitindo que as políticas sejam definidas com base em pessoas e suas identidades, em vez de usuários ou endereços IP que mudam. Isso elimina a necessidade de mapeamento manual, que os administradores teriam que realizar de outra forma e que tende a ficar desatualizado.

Somente dispositivos saudáveis se conectam.

As decisões de acesso também se beneficiam; uma VPN tradicional não tem como saber se um dispositivo está em um estado de integridade ou não, e admite o endpoint com base apenas em sua credencial. No entanto, o Sophos Workspace Protection verifica o estado de integridade do dispositivo com o Sophos Endpoint antes de conceder qualquer permissão, de modo que um endpoint comprometido nunca consiga acessar aplicativos ou dados da rede.

Trocas como essas não formam um conjunto fixo. Cada uma delas existe porque a Sophos a construiu, e a Sophos continua a expandir as suas funcionalidades ao longo do tempo. O que é compartilhado entre os pontos de controle da Sophos hoje é consideravelmente mais amplo do que o que era compartilhado entre eles há uma década.

Nada disso começa como resposta à ameaça, mas raramente permanece separado dela. Uma aplicação que ninguém consegue contabilizar, ou um usuário que iniciou sessão onde não tinha autorização, é um detalhe operacional normal até o momento em que deixa de ser. A visibilidade que facilita a gestão de uma rede também facilita a detecção de ameaças emergentes.

Uma resposta coordenada em um ambiente híbrido

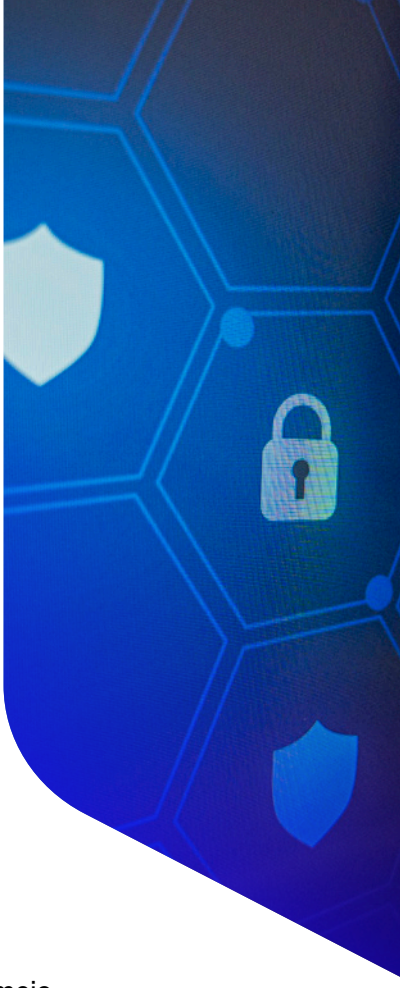
Este exemplo prático do Sophos MDR demonstra a segurança sincronizada em ação. A organização afetada era cliente do Sophos MDR e utilizava o Sophos Endpoint e o Sophos Email, juntamente com o Microsoft Entra ID, o Microsoft Graph Security e um firewall Fortinet. Eles também utilizavam um Sophos Firewall em uma rede separada. Cada um desses pontos de controle alimentava o mesmo lago de contexto unificado.

- O atacante iniciou o ataque com uma isca assistida por IA, usando uma página de phishing hospedada em um site legítimo. O usuário clicou e digitou sua senha.
- O kit roubou o token da sessão ativa em vez da credencial. Ao fazer isso, o atacante conseguiu contornar a autenticação multifatorial, tornando a redefinição de senha ineficaz.
- O adversário acessou a infraestrutura de um atacante conhecido e criou uma regra da caixa de entrada silenciosa, ocultando quaisquer e-mails de um fornecedor específico, o que configura um esquema de fraude eletrônica.
- Quatro pontos de controle registraram algo suspeito: o Sophos Endpoint, duas soluções da Microsoft e o firewall da Fortinet. Nenhum sinal isolado foi suficientemente forte para desencadear uma resposta.
- Uma detecção da Sophos desenvolvida especificamente para essa finalidade foi acionada e os sinais individuais foram resolvidos em uma única cadeia de ataque.
- O login foi bloqueado, as sessões foram revogadas e o Endpoint foi isolado com sucesso. Endereços IP maliciosos foram bloqueados no Sophos Firewall, usando telemetria fornecida pelo firewall da Fortinet.

Em seguida, um humano encerrou o caso. Um analista confirmou que a regra da caixa de entrada mencionava um fornecedor específico, o que permitiu identificá-la como uma preparação para fraude eletrônica.



Como os clientes habilitam a segurança sincronizada



Segurança sincronizada não é um produto, um SKU ou um complemento, e não há nada extra para licenciar. Os clientes obtêm esse benefício automaticamente quando dois ou mais pontos de controle funcionam juntos dentro do Sophos Fusion, independentemente de os pontos de controle serem da Sophos ou de terceiros.

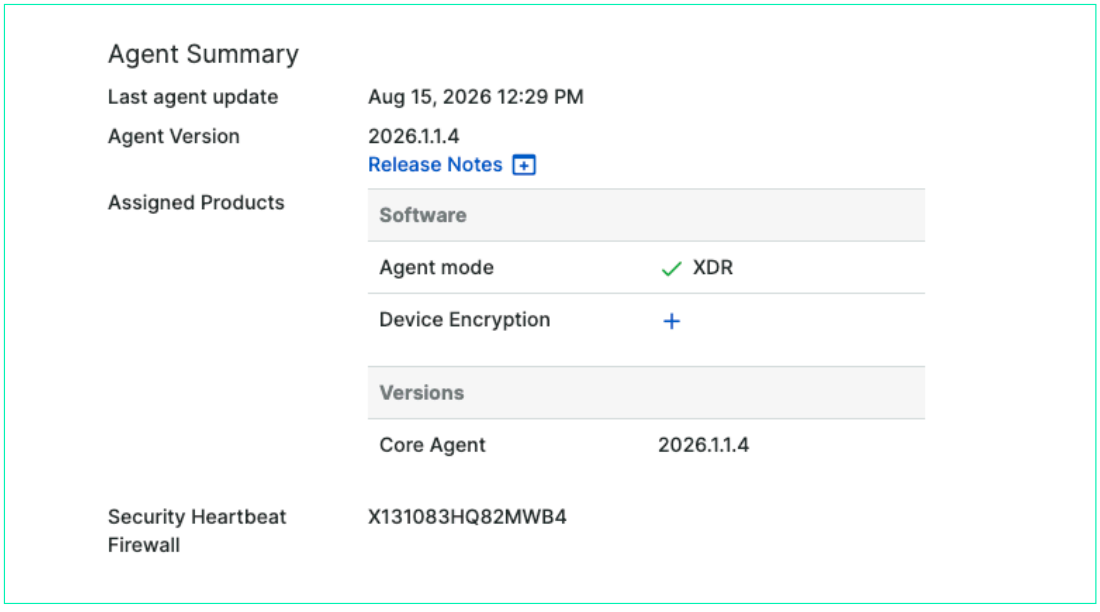
O Sophos Endpoint e o Sophos Firewall gerenciados através da mesma conta do Sophos Fusion são um ponto de partida comum. A coordenação entre eles é ativada assim que ambos se conectam à mesma conta, sem necessidade de configuração adicional. Os casos de uso que se baseiam no estado de integridade, como usar o estado de integridade como parte de regras de firewall ou políticas do Sophos Workspace Protection, são configurados pelo cliente.

A coordenação com pontos de controle de terceiros começa com a integração do ponto de controle no Sophos Fusion, que oferece suporte a integrações nativas da Sophos e a mais de 500 integrações de terceiros. No entanto, o nível de respostas automatizadas disponíveis varia de um ponto de controle para outro. Um exemplo é a Resposta Ativa a Ameaças nos pontos de controle da Sophos, habilitada pelo cliente e não por padrão.

A Sophos oferece automações e playbooks que são executados automaticamente por meio da segurança sincronizada, abrangendo uma ampla gama de casos de uso. Os clientes podem adicionar as suas próprias automações caso uma automação padrão não seja adequada ao seu ambiente, conforme descrito acima.

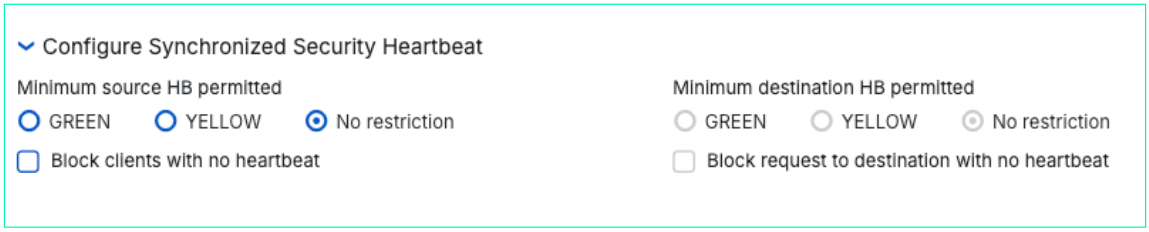
O Sophos Endpoint coordenando com o Sophos Firewall.

Para confirmar se o Sophos Endpoint está se coordenando com um firewall, abra o Resumo do computador no Sophos Fusion. Nele, você verá o número de série do Sophos Firewall que está recebendo o Security Heartbeat do endpoint.



Políticas do Sophos Firewall com segurança sincronizada

Uma regra de firewall pode, opcionalmente, exigir um estado de integridade "Verde" antes que um dispositivo tenha permissão para acessar a internet. Dispositivos desprotegidos (ou seja, aqueles que não executam o Sophos Endpoint) não conseguiriam se conectar, assim como qualquer dispositivo com um estado de integridade questionável.



Juntando tudo

O problema nunca foi a falta de ferramentas de segurança. O problema era que as ferramentas que uma organização já possui tendem a funcionar em isolamento, e os atacantes desenvolveram seus métodos para explorar as lacunas entre elas. A segurança sincronizada permite que suas ferramentas de segurança funcionem como uma defesa unificada e coordenada.

Se você utiliza dois ou mais pontos de controle no Sophos Fusion, a segurança sincronizada já está funcionando em seu nome. Conecte mais pontos de controle e o alcance será maior. As ferramentas que não são da Sophos, nas quais você já investiu, são integradas à resposta, em vez de ficarem apenas relatando os acontecimentos à margem.

A quantidade de execuções automáticas fica a seu critério. Uma coordenação que ignorasse seus processos de controle de mudanças não valeria a pena, portanto, o nível de automação é definido por você, ponto de controle por ponto de controle.

Esse é o valor prático do Sophos Cyber Defense System. Não se trata de uma lista mais longa de produtos, mas sim daqueles que você já utiliza, respondendo em conjunto na velocidade da máquina, mais rápido do que um ataque acelerado por IA conseguiria se mover entre eles.

Para saber mais, acesse www.sophos.com/synchronizedsecurity

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

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

© Copyright 2026. Sophos Ltd. Todos os direitos reservados.
Empresa registrada na Inglaterra e País de Gales sob o nº. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
Sophos é a marca registrada da Sophos Ltd. Todos os outros nomes de produtos e de empresas mencionados são marcas comerciais ou marcas registradas de seus respectivos proprietários.