O RISCO OCULTO NOS FIREWALLS MODERNOS

Saiba como evitar que seu firewall seja explorado em um ataque

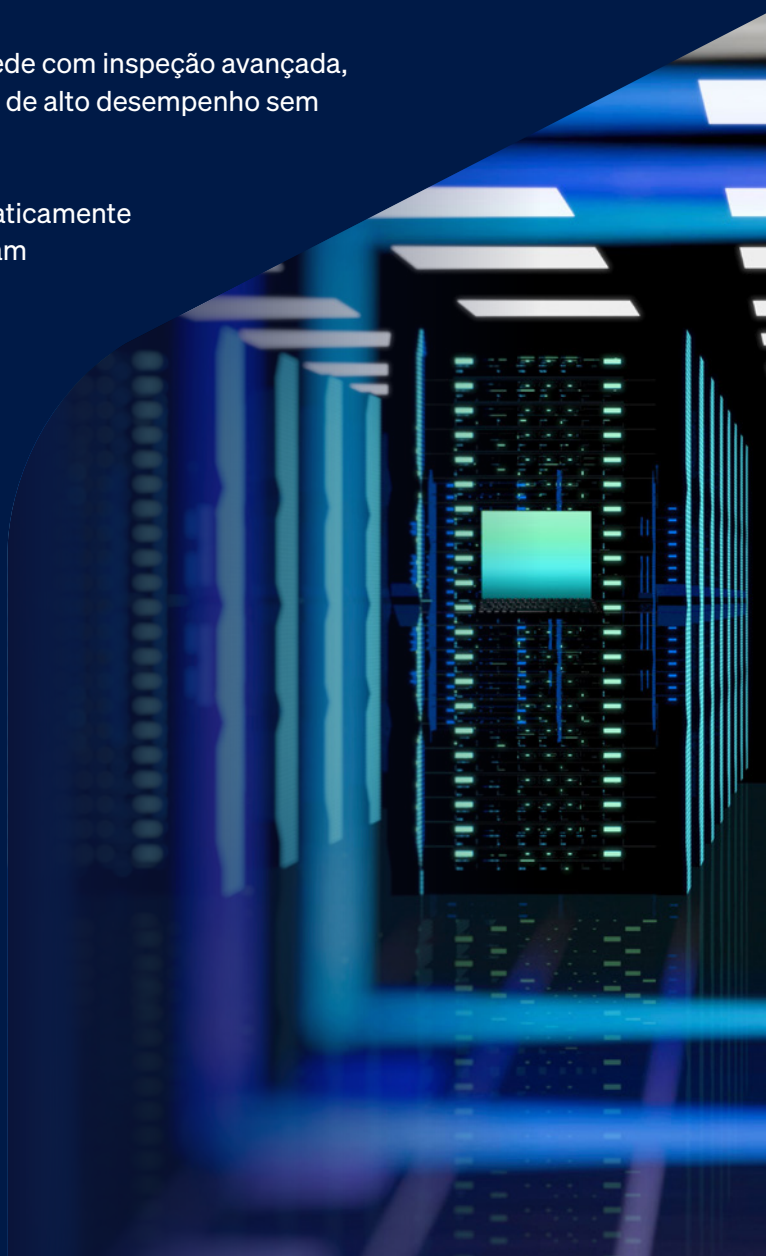
Sumário executivo

Firewalls de rede enfrentam um nível inédito de ataques direcionados. Quase todo dia há uma manchete relacionada a uma nova vulnerabilidade de firewall, revelando uma verdade preocupante: os firewalls — os mesmos sistemas projetados para proteger as redes — apresentam um risco significativo e se tornaram o alvo principal dos adversários mais sofisticados[1]. Esses ataques exploram não apenas vulnerabilidades no próprio software do firewall, mas também fraquezas fundamentais na forma como as organizações abordam a segurança da rede.

Este documento técnico apresenta uma estrutura fundamentada em três pilares para a segurança das redes modernas que aborda as ameaças antes, durante e depois de terem sido implantadas:

- **Fortalecimento.** Reduza sua superfície de ataque de forma proativa seguindo os princípios do Secure by Design, patches automatizados, auditoria de configuração e controles de acesso Zero Trust.
- **Proteção.** Bloqueie ameaças antes que cheguem à rede com inspeção avançada, detecção de ameaças alimentada por IA e segurança de alto desempenho sem comprometimento.
- **Detecção e Resposta.** Identifique e contenha automaticamente adversários ativos operando na rede antes que possam concluir um ataque.

A maioria das soluções de segurança de rede foca principalmente na proteção, deixando a infraestrutura vulnerável e incapaz de identificar e responder a um ataque ativo. Este documento oferece aos profissionais de segurança de rede e equipes de TI um roteiro prático para implementar esses três pilares com eficiência.



O cenário atual das ameaças

Firewalls estão sitiados

Os firewalls de rede estão posicionados na fronteira entre redes internas confiáveis e o mundo exterior hostil. Essa posição privilegiada os torna alvos excepcionais e de alto valor. Os noticiários documentam uma constante série de ataques a grandes fornecedores de firewalls, alguns explorando vulnerabilidades previamente divulgadas que permanecem sem correção em ambientes de produção, outros mirando configurações padrão pouco adequadas ou falhas de projeto que criam pontos fracos exploráveis[2].

A IA Fronteiriça colocou mais lenha na fogueira quando se trata de ataques cibernéticos impulsionados por IA Agêntica. O modelo Claude Mythos da Anthropic descobriu mais de 2.000 novas vulnerabilidades de dia zero em apenas algumas semanas, marcando uma mudança radical tanto para adversários quanto para defensores.

Enquanto as manchetes sobre a IA Fronteiriça focam na descoberta de vulnerabilidades em larga escala, a matéria mais importante é sobre como a IA comprime o tempo de resposta, reduzindo a janela entre a exposição à vulnerabilidade e o impacto no negócio. Isso permite que os invasores se movam mais rápido, em maior escala e com menos atrito do que antes.

As consequências vão muito além das organizações individuais. Quando os invasores comprometem um firewall, eles não apenas obtêm acesso direto à rede, mas potencialmente a credenciais, fornecedores e clientes da organização, obtendo, efetivamente, o controle geral.

Mais de 2.000

vulnerabilidades de dia zero descobertas pela Mythos em apenas sete semanas

Os três pilares da segurança de rede

A segurança eficaz da rede exige uma abordagem que englobe todo o ciclo de vida das ameaças: antes, durante e depois de serem implantadas. Isso cria três pilares de defesa distintos, porém interconectados:

FORTALECIMENTO

REDUZ A ÁREA DA SUPERFÍCIE DE ATAQUE

Projete, desenvolva e mantenha soluções para minimizar o risco, reduzir a exposição e reforçar a infraestrutura contra ataques

PROTEÇÃO

BLOQUEIA ATAQUES ANTES QUE ENTREM NA REDE

Implemente a melhor proteção possível para identificar e bloquear a entrada de invasores e exploits na rede

DETECÇÃO E RESPOSTA

INTERROMPE AS AMEAÇAS ATIVAS ANTES QUE CAUSEM DANOS

Utilize a detecção e a resposta para identificar e isolar um adversário ativo automaticamente

A lacuna crítica

A maioria dos firewalls de rede foca quase que exclusivamente na proteção em tempo real, como filtragem de tráfego, prevenção de ameaças e sistemas de prevenção de invasão. Embora essas funcionalidades sejam essenciais, concentrar-se exclusivamente na inspeção de tráfego em tempo real deixa as organizações vulneráveis.

As manchetes diárias demonstram que a maioria dos firewalls e equipes de TI está falhando em reforçar efetivamente seu ambiente, ou seja, em reduzir a área de ataque superficial. Os firewalls continuam vulneráveis, a fadiga de patches é generalizada, os produtos em fim de vida útil persistem em posições privilegiadas e a VPN de acesso remoto continua dominando, apesar de suas falhas de segurança. Enquanto isso, recursos de detecção e resposta para impedir ataques ativos antes que possam causar algum impacto muitas vezes estão totalmente ausentes na maioria das implantações de firewall.

Enfrentar esse desequilíbrio exige foco deliberado nos pilares negligenciados, especialmente o fortalecimento, que forma a base de uma postura de segurança resiliente.

Fortalecimento da infraestrutura de rede — Redução de riscos

O fortalecimento envolve reduzir proativamente a superfície de ataque, removendo fraquezas antes que os invasores possam descobri-las e explorá-las.

Estratégias essenciais de fortalecimento

1. **Minimizar a exposição.** Examine regularmente sistemas e infraestruturas expostos à internet e, consequentemente, reduza o número de possíveis pontos de entrada.

2. **Garantir que os sistemas sejam Secure by Design.** Selecione produtos desenvolvidos que tenham a segurança como princípio básico de design.

3. **Auditorar a configuração e manter software e firmware atualizados.** Mantenha a higiene de segurança por meio de monitoramento contínuo.

4. **Eliminar a identidade comprometida como vetor.** Bloqueie acesso e autenticação. Implante a autenticação multifator (MFA) universalmente e faça a transição de VPN para Zero Trust Network Access (ZTNA).

Minimizar a exposição

Examine regularmente sua infraestrutura de rede e avalie onde cada componente se encontra em seu ciclo de vida. Se alguma parte estiver chegando ao fim da vida, planeje substituí-la de forma proativa. O custo de atualizar tecnologias obsoletas é muito menor do que o potencial de impacto de um ataque de ransomware que explora sistemas sem suporte.

Essa também é uma oportunidade para simplificar e consolidar sua infraestrutura de rede. Se você depende de dispositivos separados para firewall, VPN, ZTNA, SD-WAN, DNS e filtragem da Web, considere reunir essas funcionalidades em uma única plataforma. Reduzir o número de dispositivos e soluções no seu ambiente pode diminuir a complexidade, melhorar a eficiência e reforçar a resiliência geral.

É igualmente importante manter sua infraestrutura atualizada. Atualizações de firmware e software frequentemente incluem patches críticos de segurança para vulnerabilidades que os invasores podem explorar. Embora sua aplicação tome tempo, é muito menos conturbado do que lidar com o impacto de um ataque de ransomware.

Garantir que os sistemas sejam Secure by Design

As empresas precisam de produtos seguros tanto quanto precisam de produtos de segurança.

A indústria da segurança cibernética deve abraçar uma verdade fundamental: as empresas precisam de produtos seguros tanto quanto precisam de produtos de segurança. Quando os adversários direcionam suas forças nas ferramentas criadas para defender as organizações, elas precisam de produtos de segurança que sejam protegidos e seguros. As organizações devem buscar fornecedores que demonstrem compromisso genuíno com a segurança e transparência, incluindo a divulgação transparente de violações, o que representa a abordagem correta, mesmo sendo desagradável.

Princípios-chave do Secure by Design incluem:

- MFA integrada por padrão a todos os sistemas.
- Eliminação das senhas e credenciais padrão.
- Implementação de patches de segurança automatizados que minimizam a interrupção.
- Processos rápidos e transparentes de divulgação de vulnerabilidades.
- Auditorias regulares de segurança e testes de penetração.
- Práticas seguras de ciclo de vida de desenvolvimento incorporadas à engenharia de produto.

Auditorar a configuração e manter os sistemas atualizados

Firewalls de rede são complexos, o que os torna propensos a parâmetros inadequados e configurações arriscadas que podem abrir portas não intencionais para os invasores. O desafio é saber o que está configurado de forma incorreta e onde as exposições se encontram. Às vezes o problema é óbvio, mas muito frequentemente as lacunas permanecem ocultas até serem exploradas. A maioria dos firewalls não dá nenhuma indicação sobre os parâmetros de configurações arriscadas. Escolha um que dê.

A fadiga de patches é real, mas não precisa ser assim. Processos tradicionais de patching geram uma carga operacional significativa. Vulnerabilidades de segurança podem ser descobertas a qualquer momento, e agora, com a IA, em um ritmo alarmante. A frequência das atualizações necessárias pode sobrecarregar as equipes administrativas. A maioria dos firewalls anuncia "atualizações automáticas", mas normalmente ainda exige que os administradores agendem o tempo de inatividade, apliquem firmwares e reiniciem dispositivos.

Uma pergunta simples que as organizações deveriam fazer: por que os patches não podem ser realmente automáticos? A resposta é que a maioria dos fornecedores não desenvolveu seu software para suportar atualizações de segurança em tempo real. No entanto, abordagens arquitetônicas modernas podem trabalhar com funcionalidades automatizadas de hotfix que:

- Apliquem patches de segurança automaticamente, sem intervenção do administrador.
- Não exijam tempo de inatividade do sistema nem reinicializações.
- Façam a ponte entre as versões principais de firmware.
- Reduzam a janela de vulnerabilidade de meses para horas ou dias.

A configuração inadequada representa outro ponto de entrada comum para invasores. Conjuntos complexos de regras de firewall, mudanças de política mal-documentadas e desvios de configuração ao longo do tempo podem, inadvertidamente, deixar pontos de acesso abertos que deveriam ser protegidos.

O desafio é a identificação: como os administradores sabem o que está configurado de forma inadequada? Firewalls tradicionais não fornecem informações sobre a segurança da configuração. Abordagens modernas incluem funcionalidades automatizadas do status de integridade que:

- Auditam continuamente a configuração do firewall com base nas melhores práticas estabelecidas e benchmarks de CIS.
- Fornecem visibilidade no painel sobre verificações aprovadas e reprovadas.
- Atribuam níveis de severidade a cada item avaliado.
- Permitam o detalhamento para ajustar rapidamente as configurações ou documentar exceções intencionais.

Essas funcionalidades proporcionam a visibilidade que os firewalls tradicionais não oferecem, garantindo que a postura de segurança permaneça ótima mesmo com as constantes mudanças em configurações.

Eliminar identidade comprometida como vetor de ataque

67% dos incidentes investigados pela Sophos em 2025 começaram com credenciais comprometidas[3], tornando a eliminação dos ataques baseados em identidade uma prioridade maior. Isso exige adotar os princípios Zero Trust: não confie em nada, confira tudo.

Organizações que ainda dependem de VPN de acesso remoto devem tratar a migração como uma alta prioridade. A ZTNA oferece uma alternativa moderna à VPN que se alinha com os princípios Zero Trust. Em vez de conceder acesso amplo à rede, a ZTNA oferece acesso granular a aplicativos e recursos específicos. Se um dispositivo for comprometido, a ZTNA pode limitar ou bloquear automaticamente o acesso até que o dispositivo seja remediado.

Mesmo que um invasor comprometa um dispositivo conectado via ZTNA, ele obterá acesso apenas aos aplicativos específicos que o usuário está autorizado a acessar, não à rede inteira. O perímetro de segurança se move para onde realmente é necessário: em torno de aplicativos e dados críticos.

67%

dos incidentes investigados pela Sophos em 2025 começaram com uma identidade comprometida

A ZTNA oferece seis vantagens principais sobre a VPN:

1. **Imposição de MFA.** A MFA é exigida em todo acesso, sem exceção, eliminando ataques de força bruta e credenciais comprometidas como vetores de ataque viáveis.

2. **Integridade do dispositivo como parte da política de acesso.** A conformidade e o status de verificação de integridade do dispositivo são continuamente avaliados como parte das decisões de acesso.

3. **Funciona em qualquer lugar.** A ZTNA funciona igualmente bem para os usuários na rede corporativa ou trabalhando remotamente, oferecendo segurança consistente independentemente da localização.

4. **Conectividade transparente.** Implementações modernas de ZTNA oferecem conexões transparentes e confiáveis, sem os problemas de conexão que frequentemente afligem as VPNs.

5. **Melhor visibilidade.** As organizações obtêm uma visibilidade clara sobre quais recursos os usuários estão acessando, dando suporte a um melhor planejamento de capacidade e gerenciamento de licenças.

6. **Administração mais fácil.** Adicionar e remover usuários, implantar novos aplicativos e gerenciar políticas de acesso são mais simples com a ZTNA do que com uma VPN tradicional.

As estratégias de fortalecimento devem incluir a eliminação da VPN de acesso remoto e a implantação de arquitetura Zero Trust com imposição universal de MFA.

Proteção: bloqueio de ameaças no gateway

Implante proteção abrangente para identificar e bloquear ameaças antes que cheguem à rede. Isso inclui inspeção avançada de TLS, detecção de ameaças de dia zero com IA e análise inteligente de tráfego que mantém um alto desempenho sem comprometer a segurança.

Requisitos modernos de proteção

- **Inspeção TLS 1.3 de alto desempenho.** A maior parte do tráfego da Web agora é criptografada, e os invasores escondem cada vez mais o tráfego de malware e de comando e controle dentro dos canais criptografados. Os firewalls devem descriptografar e inspecionar o tráfego TLS de forma inteligente, aplicando regras baseadas em políticas que equilibram os requisitos de segurança com considerações de privacidade e impacto no desempenho.

- **Aceleração de hardware.** Operações criptográficas e inspeção de tráfego são computacionalmente intensas. Arquiteturas modernas de firewall devem descarregar aplicativos confiáveis e operações criptográficas para caminhos de aceleração de hardware, liberando recursos para uma inspeção profunda de tráfego não confiável.

- **Proteção contra ameaças de dia zero alimentada por IA.** A detecção baseada em assinaturas continua valiosa, mas é insuficiente contra novas ameaças. A análise estática de arquivos alimentada por IA combinada com sandbox dinâmico em tempo de execução pode identificar e bloquear ameaças de dia zero antes que cheguem à rede — ameaças que sistemas tradicionais baseados em assinaturas deixariam passar completamente.

Funcionalidades de proteção E desempenho devem melhorar com o tempo, em vez de se degradar. Firewalls construídos sobre arquiteturas programáveis podem receber tanto melhorias de proteção quanto de desempenho por meio de atualizações de software, estendendo o ciclo de vida efetivo dos investimentos em hardware. Ao contrário dos firewalls tradicionais, que se tornam mais lentos à medida que novos recursos de segurança são adicionados, as arquiteturas modernas mantêm ou melhoram o desempenho por meio de otimização contínua.

Detecção e resposta: bloqueio de ataques ativos

Quando os adversários se infiltram com sucesso nas defesas, sua presença é detectada rapidamente e a ameaças é automaticamente contida. O NDR (Network Detection and Response), combinado com a coordenação entre produtos, pode identificar e isolar sistemas comprometidos antes que os invasores concretizem seus objetivos.

Network Detection and Response (NDR)

O sistema NDR de detecção e resposta de rede utiliza IA e análise comportamental para identificar adversários ativos já presentes na rede. Ao contrário das defesas perimetrais que analisam o tráfego de entrada, o NDR examina padrões internos de tráfego de rede em busca de indicadores de comprometimento:

- Movimento lateral incomum entre sistemas.
- Comunicações de comando e controle com hosts externos suspeitos.
- Padrões anômalos de acesso a dados.
- Tentativas de escalonamento de privilégio.
- Atividades de reconhecimento de varredura de recursos internos.

Tradicionalmente, o NDR tem sido um recurso de nível empresarial que exige produtos separados e investimentos significativos. Organizações visionárias agora estão integrando recursos de NDR diretamente a plataformas de firewall, tornando essa capacidade crítica acessível às organizações de médio porte.

Resposta automatizada

A detecção sem resposta apenas informa os administradores de que foram comprometidos — muitas vezes tarde demais para evitar danos. A capacidade de resposta automatizada permite a contenção imediata.

Quando uma ameaça é detectada em qualquer parte da infraestrutura de segurança — seja por firewall, proteção de endpoint, segurança de e-mail ou um analista de MDR — você precisa de uma solução de segurança que coordene uma resposta automatizada em todos os produtos de segurança integrados. Isso pode prevenir que um dispositivo comprometido se comunique com outros sistemas, bloquear o acesso a aplicativos e dados, e impedir que ele se mova lateralmente.

Essa resposta automatizada é especialmente valiosa fora do horário comercial, quando 88% dos ataques de ransomware são implantados[4]. Consideremos o cenário "Numa noite de sexta-feira": um invasor compromete um dispositivo tarde da noite em uma sexta-feira, quando a equipe de segurança não está disponível. Sem resposta automática, o invasor tem todo o fim de semana para mover-se lateralmente, escalonar privilégios e implantar ransomwares. A organização descobre a violação na manhã de segunda-feira, quando surgem arquivos criptografados e as exigências de resgate.

Com a resposta automatizada entre produtos, o comprometimento inicial dispara o isolamento imediato. O invasor se vê preso em um segmento de quarentena, incapaz de avançar ou se mover. Equipes de segurança retornam na manhã de segunda-feira e se deparam com um alerta ativo sobre uma ameaça contida, em vez de um incidente de ransomware de grande escala.

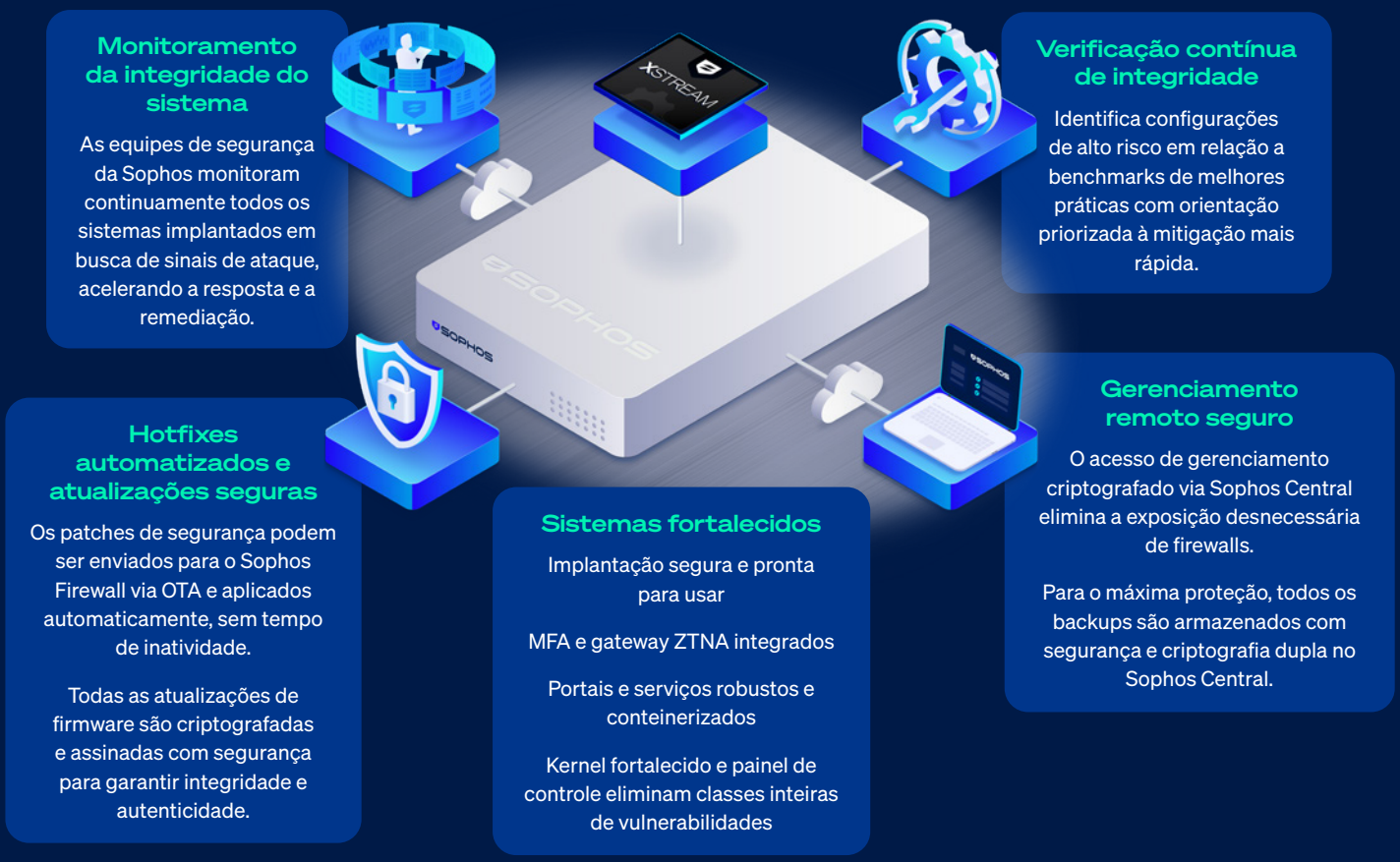
88%

dos ataques de ransomware são implantados fora do horário comercial

Sophos Firewall: uma solução completa

Embora a arquitetura de três pilares descrita represente as melhores práticas de segurança, implementá-la de forma eficaz exige escolher uma infraestrutura que apoie os três pilares.

O Sophos Firewall se destaca como uma das poucas soluções que fez um investimento significativo nessas três áreas, oferecendo muitas funcionalidades que os compradores não encontrarão em nenhum outro lugar.



Segurança no design

O Sophos Firewall aborda o pilar de fortalecimento por meio de uma abordagem abrangente do Secure by Design, que elimina o ônus normalmente associado à manutenção de uma infraestrutura segura.

Funcionalidade de hotfix automatizada: eliminar a fadiga de patches

A capacidade exclusiva de hotfix automatizado do Sophos Firewall muda fundamentalmente a janela de vulnerabilidades expostas:

- Os patches de segurança são enviados automaticamente por OTA assim que são desenvolvidos e valios pela Sophos.
- Os patches são aplicados sem nenhuma intervenção do administrador.
- Não é necessário tempo de inatividade ou reinicialização.
- Os hotfixes preenchem a lacuna entre as versões principais de firmware, garantindo proteção contínua.

Essa vantagem arquitetônica reduz a janela de vulnerabilidade de meses para horas ou dias. Quando o Sophos descobre e corrige uma vulnerabilidade, todos os clientes do Sophos Firewall são protegidos imediatamente, sem ter que esperar que os administradores encontrem tempo em suas agendas ou planejem janelas de manutenção.

Nenhum outro grande fornecedor de firewall oferece patches de segurança verdadeiramente automáticos e sem tempo de inatividade. Essa capacidade por si só representa uma melhoria transformadora no pilar de fortalecimento.

Status de integridade: auditoria contínua de configuração

O recurso de verificação de status de integridade que o Sophos Firewall oferece apresenta uma visibilidade de configuração sem igual:

- Audita continuamente dezenas de configurações de firewall com base em benchmarks de CIS e melhores práticas do setor.
- Apresenta as verificações aprovadas e reprovadas diretamente no painel central de controle.
- Atribui níveis de severidade a cada item avaliado (crítico, alto, médio, baixo).
- Permite o detalhamento para ajustar rapidamente as configurações ou documentar exceções intencionais.
- Atualiza automaticamente conforme as melhores práticas evoluem.

Esse monitoramento proativo da configuração garante que a postura de segurança permaneça ótima mesmo com a mudança das configurações ao longo do tempo. Os administradores recebem alertas imediatos sobre configurações potencialmente arriscadas antes que os invasores possam descobri-las e explorá-las.

Monitoramento remoto de integridade

A Sophos é única em monitorar toda a nossa base de instalações de Sophos Firewalls. Graças a um sensor Linux integrado Sophos Extended Detection and Response (XDR), podemos monitorar a integridade do sistema, incluindo:

- Alterações de configuração não autorizadas.
- Exportação de regras.
- Adulteração de arquivos.
- Tentativas de execução de programas maliciosos.

Esse sensor integrado permite que as equipes de segurança da Sophos monitorem proativamente toda a base de clientes instalada em busca de sinais de ataque — uma camada adicional de segurança que nenhum outro fornecedor de firewall atualmente oferece. Quando ameaças são detectadas, a Sophos pode responder imediatamente para ajudar os clientes a remediar a situação, enquanto simultaneamente promove hotfixes automáticos para proteger todos os outros clientes.

Autenticação multifator e Zero Trust Network Access integrados

O Sophos Firewall integra MFA a todos os pontos de acesso administrativos e inclui um gateway ZTNA integrado, facilitando a adoção e implantação de ZTNA, um upgrade ao acesso remoto por VPN vulnerável.

Proteção E desempenho poderosos

Embora muitos fornecedores ofereçam funcionalidades robustas de proteção, o Sophos Firewall oferece proteção de uma forma diferente, que garante uma segurança abrangente sem penalizar o desempenho, o que frequentemente força as organizações a desativarem recursos importantes de segurança.

Arquitetura Xstream FastPath

A arquitetura Xstream programável do Sophos Firewall gerencia o tráfego de forma inteligente para oferecer máxima segurança e máximo desempenho**.** Essa abordagem garante que habilitar recursos abrangentes de segurança, incluindo inspeção TLS, sandbox e IPS, não degrade o desempenho. O Sophos Firewall também integra proteção contra ameaças de dia zero com IA para identificar as ameaças mais recentes.

Melhorias contínuas de desempenho e proteção

Diferente dos firewalls tradicionais, que ficam mais lentos à medida que novos recursos de segurança são adicionados, a arquitetura programável do Sophos Firewall permite melhorias de desempenho **e** proteção por meio de atualizações de software. Os clientes recebem melhorias contínuas para seus investimentos em hardware sem precisar atualizar os equipamentos — proteção e desempenho que melhoram com o tempo, em vez de se degradarem.

Detecção e resposta sem igual

A maioria dos firewalls de rede oferece praticamente nenhuma capacidade de detecção e resposta. Uma vez que um invasor se infiltra nas defesas perimetrais, os firewalls tradicionais não conseguem identificar a invasão nem responder a ela. Isso representa uma lacuna crítica que deixa as organizações vulneráveis aos ataques mais sofisticados.

O Sophos Firewall é único, pois oferece funcionalidades automatizadas de detecção e resposta.

Network Detection and Response (NDR) integrado

Tradicionalmente, a detecção e resposta de rede de NDR tem sido um recurso apenas de grandes empresas que exige produtos separados e investimentos significativos. O Sophos Firewall inclui o NDR como um recurso padrão em sua assinatura de proteção convencional.

Isso leva a detecção de ameaças de nível empresarial para organizações de todos os tamanhos, assegurando que os adversários que se infiltram nas defesas perimetrais possam ser identificados antes que alcancem seus objetivos.

Segurança Sincronizada: resposta automatizada entre produtos

A detecção sem resposta apenas informa os administradores de que foram comprometidos — muitas vezes tarde demais para evitar danos. O Synchronized Security do Sophos Firewall oferece resposta automatizada e coordenada em toda a infraestrutura de segurança.

Quando um produto Sophos detecta uma ameaça, seja por firewall, proteção de endpoint, segurança de e-mail, proteção de espaço de trabalho ou um analista de MDR, o Synchronized Security automaticamente:

- Isola o dispositivo comprometido para evitar que se comunique com outros sistemas.
- Bloqueia o acesso a aplicativos e dados.
- Previne o movimento lateral pela rede.
- Contém a ameaça até que as equipes de segurança possam investigar e remediar.

O cenário "Numa noite de sexta-feira" ilustra o valor crítico da resposta automatizada:

Sem resposta automática. Um invasor compromete um dispositivo tarde da noite em uma sexta-feira, quando a equipe de segurança não está disponível. O invasor tem todo o fim de semana para mover-se lateralmente, escalonar privilégios e implantar ransomwares. A organização descobre a violação na manhã de segunda-feira, quando surgem arquivos criptografados e as exigências de resgate.

Com o Synchronized Security. O comprometimento inicial dispara o isolamento automático imediato. O invasor se vê preso em um segmento de quarentena, incapaz de avançar. Equipes de segurança retornam na manhã de segunda-feira e se deparam com um alerta ativo sobre uma ameaça contida, em vez de um incidente de ransomware de grande escala.

Essa capacidade de resposta automatizada é particularmente valiosa para organizações sem cobertura de operações de segurança 24h — precisamente as organizações de médio porte que os fornecedores tradicionais de NDR historicamente ignoraram.

Conclusão

Os firewalls de rede enfrentam uma pressão inédita de ataques. Os noticiários que expõem as vulnerabilidades dos grandes fornecedores revelam uma verdade desagradável: os sistemas projetados para proteger as redes tornaram-se os alvos principais dos adversários mais sofisticados.

A estrutura de três pilares apresentada neste documento técnico — fortalecimento, proteção, e detecção e resposta — proporciona uma abordagem de segurança de rede que engloba as ameaças antes, durante e depois de ocorrerem. Infelizmente, a maioria dos fornecedores de firewalls concentra-se quase que exclusivamente no pilar de Proteção, deixando lacunas críticas nos pilares de Fortalecimento e Detecção e resposta.

Implementar esse arcabouço de forma eficaz exige selecionar uma infraestrutura que invista igualmente em todos os três pilares. As organizações devem avaliar os fornecedores de firewalls com base em:

- **Compromisso com o Secure by Design** com evidências de implementação, não apenas palavras.
- **Funcionalidades automatizadas de patches** que eliminam o tempo de inatividade e a fadiga de patches.
- **Auditoria de configuração** que proporciona visão da postura de segurança.
- **Zero Trust Integrado**, incluindo recursos de MFA e ZTNA.
- **Detecção e resposta de rede** para identificar ameaças ativas.
- **Resposta automatizada** com funcionalidades que contenham as ameaças sem intervenção humana.

O custo de substituir uma infraestrutura obsoleta ou inadequada é drasticamente menor do que o custo de recuperação de um ataque de ransomware que explora vulnerabilidades conhecidas. O momento de agir é agora, antes que sua organização desponte na próxima manchete.

Segurança é uma responsabilidade compartilhada. Os fornecedores precisam construir produtos seguros. As organizações precisam implantá-los corretamente, zelar por eles e aposentá-los quando chegarem ao fim da vida útil. O cumprimento das responsabilidades por ambas as partes cria um ecossistema muito mais seguro.

A pergunta-chave que você precisa se fazer: **meu firewall está reduzindo o risco ou introduzindo-o?**

A resposta depende se a sua infraestrutura aborda os três pilares da segurança de redes modernas ou se deixa lacunas críticas que os invasores estão mais do que felizes em explorar.

Meu firewall está reduzindo o risco ou introduzindo-o?

1, 2, 3, 4 Relatório Sophos de Adversários Ativos 2026

SOPHOS

Para saber mais sobre o Sophos Firewall, acesse **sophos.com/firewall**

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

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