Os 10 melhores provedores NGFW (próxima geração do firewall) em 2025

Data: 2025-09-18 20:07:10

Autor: Inteligência Against Invaders

Proteger a infraestrutura digital é fundamental em 2025, como Ameaças cibernéticas Escala em complexidade e diversidade.

Os firewalls da próxima geração (NGFWs) tornaram -se a pedra angular da segurança corporativa, oferecendo não apenas a filtragem robusta do tráfego, mas também a inspeção profunda de pacotes, a inteligência avançada de ameaças e a integração sem costura da defesa contra ameaças persistentes e evolutivas de hoje.

Por que os 10 melhores fornecedores de firewall da próxima geração (NGFW) de 2025

Os operadores corporativos, SMB e nuvem precisam de NGFWs para proteger os ativos contra riscos de ransomware, malware, phishing e insider.

Esses principais fornecedores oferecem detecção de ameaças a IA, escalabilidade modular, gerenciamento centralizado e conectividade a Arquiteturas híbridas Garantir a segurança à prova de futuro que se adapte às demandas regulatórias e ao crescimento dos negócios.

Tabela de comparação: os 10 melhores fornecedores de firewall da próxima geração (NGFW) de 2025

1. Sophos

Por que escolhemos

Sophos Firewall aproveita AI movida a nuvemaprendizado profundo e recursos anti-malware de dia zero para proteção hiper-eficaz e de baixa latência.

O gerenciamento centralizado da nuvem e o compartilhamento automatizado de ameaças maximizam a eficiência operacional, tornando a Sophos uma das organizações com redes distribuídas e forças de trabalho remotas.

Especificações

A Sophos Appliances suporta implantações em nuvem, SD-WAN e no local, alimentadas pela arquitetura Xstream para acelerar SaaS e o desempenho crítico do aplicativo.

A gerência é unificada nos pontos de extremidade e na nuvem com análises e proteção em tempo

real.

Características

NDR baseado em nuvem, prevenção de malware orientada pela IA, bloqueio instantâneo de URLs de risco, integração flexível do ZTNA, orquestração SD-WAN e controles de política granular.

Razão para comprar

A Sophos oferece proteção poderosa e focada em valor, com altas classificações de satisfação do cliente para usabilidade, integração e resposta automatizada de ameaças em diversas infra-estruturas.

Prós

- Análise abrangente de IA
- Gerenciamento de nuvem simplificado
- Alta satisfação do usuário

Contras

- Alguns recursos avançados requerem conectividade em nuvem
- Atrasos ocasionais de apoio

? Melhor para: SMBs acionadas pela nuvem, empresas distribuídas, forças de trabalho remotas.

`? Try Sophos here ?` Sophos Official Website

2. Forpoint

Por que escolhemos

O NGFW forcepoint combina proteção de inteligência premiada com SD-WAN, SASE Security e Centralized Management para grandes empresas.

Sua arquitetura suporta agrupamentos de alta disponibilidade, controles granulares de privacidade e caixa de areia anti-malware.

Resposta rápida e configuração de políticas centralizadas se destacam para gerenciar redes grandes e distribuídas.

Especificações

A ForePoint oferece oito séries de eletrodomésticos para atender a todos os tamanhos organizacionais, suportando implantações físicas, virtuais e em nuvem.

O servidor SMC gerencia milhares de dispositivos de um único painel, com alta disponibilidade e arquitetura escalável.

Características

Conectividade SD-WAN, IPS embutido, sandboxing, integração em nuvem, gerenciamento centralizado, defesa anti-Evasion, inteligência proativa de ameaças e inclusão perfeita de SASE.

Razão para comprar

O fácil gerenciamento de políticas, alta disponibilidade e postura de segurança premiada da Forcepoint o torna adequado para grandes empresas, especialmente aquelas que exigem forte conformidade e coesão multi-ambiente.

Prós

- Fácil gerenciamento de políticas
- SD-WAN integrado
- Alta disponibilidade

Contras

- Algumas integrações são demoradas
- Questões de renovação de licença relatadas

? Melhor para: grandes empresas, organizações orientadas a conformidade, arquitetura distribuída.

`? Try Forcepoint here ? Forcepoint Official Website`

3. Cisco

Por que escolhemos

O Cisco Secure Firewall oferece integração perfeita com a pilha de rede da Cisco, defesa avançada de malware via AMP e poderosa visibilidade da rede posicionando -a bem para empresas que aproveitam Infraestrutura da Cisco.

Com regras exclusivas do NGIPS e integração fácil de dispositivos AD/ISE/AMP, a Cisco simplifica a aplicação da política e reduz a sobrecarga administrativa.

A Inteligência Global de Ameaças da Cisco (Talos) impulsiona atualizações rápidas e proteção de dias zero.

Especificações

Os aparelhos da Cisco suportam a implantação flexível (no local, nuvem, remota), regras de IPS

personalizáveis ??e opções avançadas de VPN, todas gerenciadas por meio de uma GUI unificada.

A plataforma combina o DPI, a análise de tráfego criptografada e a descoberta de rede para visibilidade superior.

Características

NGIPs personalizáveis, inteligência de ameaças profundas, fácil integração de dispositivos, suporte em nuvem e remoto, GUI simplificada para gerenciamento de políticas, atualizações de segurança contínuas.

Razão para comprar

Mais adequado às redes corporativas alinhadas pela Cisco, oferecendo integração perfeita e eficiente, resposta rápida de ameaças e conectividade abrangente do ponto de extremidade.

Prós

- Confiável e eficaz
- Serviço eficiente
- Poderosas opções de integração

Contras

- Custos mais altos de hardware e licença
- A configuração inicial pode ser complexa

? Melhor para: empresas usando infraestrutura da Cisco, organizações em vários sites.

`? Try Cisco Systems here ?` [Cisco Systems Official Website]

4. Redes Palo Alto

Por que escolhemos

A Palo Alto Networks lidera a inovação da NGFW com detecção de ameaças orientada pela IA e arquitetura de segurança unificada, protegendo empresas em ambientes de nuvem, data center e escritório remoto.

Sua profunda visibilidade e controles simplificados de confiança zero permitem às organizações defesas flexíveis, porém poderosas. Com o melhor suporte do setor para implantações híbridas e SASE, ele é escalado de escritórios de filiais para data centers de escala de hiperescência.

A plataforma oferece prevenção consistente e em tempo real contra ataques conhecidos e de dia zero, mesmo em tráfego criptografado. O controle avançado de aplicativos e a segurança contextual oferecem precisão e adaptabilidade.

O Gartner classifica Palo Alto como um líder de quadrante mágico, destacando seu compromisso com a rápida inovação.

Especificações

Os aparelhos Palo Alto Networks variam de modelos compactos para escritórios de filiais a chassi modular para data centers em larga escala, todos acionados por uma arquitetura de passagem única e processamento específico da função.

Eles suportam vários modos de implantação, incluindo nuvem, virtual e local, e são projetados para oferecer desempenho e escalabilidade previsíveis.

Características

Prevenção de ameaças integradas, conscientização robusta de aplicativos, análise avançada de malware, sd-wan sem costura e análises de aprendizado profundo são suportadas, com orquestração simplificada entre ambientes.

A segurança proativa com os recursos de IA/ML permite uma proteção adaptativa rápida.

Razão para comprar

Confiados pelas empresas da Fortune 10, a Palo Alto NGFWS reduz a complexidade operacional, maximiza a visibilidade da segurança e garante a conformidade com organizações com necessidades de segurança rigorosas.

A confiabilidade e a melhoria contínua de sua plataforma tornam a principal opção para empresas que priorizam a segurança dinâmica e escalável.

Prós

- Aprimoramento do desempenho
- Confiável e escalável
- Melhorando continuamente o produto

Contras

- Alto custo em comparação com a concorrência
- Pode exigir experiência avançada para configuração

? Melhor para: grandes empresas, data centers, ambientes de várias nuvens.

? Try Palo Alto Networks here ? Palo Alto Networks Official Website

5. Huawei

Por que escolhemos

A Huawei NGFWS oferece proteção de alto desempenho e custo-eficiente, com prevenção avançada, controle de aplicativos e gerenciamento de segurança centralizado.

Projetado para escalabilidade global e implantação flexível, a Huawei é uma forte escolha para organizações sensíveis a custos e para aqueles que operam em ambientes híbridos.

Especificações

A Huawei suporta virtualização e integração em nuvem, com implantações modulares para empresas de todos os tamanhos.

A arquitetura oferece inspeção profunda de pacotes, avançada inteligência de ameaçase prevenção confiável de intrusões sem sacrificar a velocidade.

Características

Controle de aplicativos, prevenção avançada de ameaças, inteligência de ameaças profunda, gestão centralizada, opções de implantação flexíveis, alta disponibilidade, programação de políticas automatizadas.

Razão para comprar

Melhor para organizações com infraestrutura da Huawei ou com o orçamento priorizando, o Huawei NGFWS se destaca em proteção escalável e adaptativa, mantendo os custos operacionais baixos.

Prós

- Econômico
- Gestão intuitiva
- Desempenho consistente

Contras

- Suporte técnico pode ser lento
- Algumas integrações avançadas menos robustas

? Melhor para: empresas sensíveis a custos, implantações híbridas, infraestrutura da Huawei.

`? Try Huawei here ? Huawei Official Website`

6. Barracuda

Por que escolhemos

O Firewall do Barracuda Cloudgen se destaca em proteção econômica e integrada à nuvem, com defesa de várias camadas contra ransomware, DDoS e explorações da Web.

Seus recursos de acesso remoto e gerenciamento centralizado são adaptados para MSPs e organizações com equipes distribuídas. A proteção de ameaças adaptativas de Barracuda oferece uma rápida resposta e acionabilidade.

Especificações

Os firewalls de Barracuda são altamente personalizáveis, suportando implantações em nuvem (Azure, AWS, GCP) e local.

Relatórios históricos e em tempo real, acesso remoto unificado e interfaces simples do painel facilitam a administração.

Características

Proteção avançada de ameaças, arquitetura pronta para a nuvem, gerenciamento de segurança unificado, análise comportamental e de sandbox, opções robustas de VPN, holos de DNS e criação de políticas simplificadas.

Razão para comprar

Ideal para organizações que precisam de resiliência de várias nuvens, resposta rápida de ameaças e segurança escalável e econômica para ambientes de email, Web e rede.

Prós

- Fácil personalização
- Forte integração em nuvem
- Gestão simples

Contras

- Análise avançada limitada
- Alguns recursos requerem configuração detalhada

? Melhor para: empresas de várias nuvens, MSPs, empresas conscientes de custos.

`? Try Barracuda Networks here ?` Barracuda Networks Official Website

7. Fortigate

Por que escolhemos

O FortiGate NGFWS da Fortinet combina inteligência de ameaças a IA, aceleração baseada na

ASIC e um tecido de segurança forte e unificado, criando um líder de desempenho para custo no mercado.

Conhecidos por suas ferramentas robustas de integração SD-WAN e gerenciamento universal, o Fortinet se destaca em alto rendimento e Arquiteturas híbridas.

A plataforma aborda o aumento de redes distribuídas e migração em nuvem, oferecendo segurança consistente e eficiência operacional.

O reconhecimento da indústria é reforçado por sua posição no quadrante mágico do Gartner.

Especificações

Os aparelhos FortiGate utilizam processadores de segurança patenteados para aceleração escalável e gerenciamento de ameaças unificadas, atendendo a ambientes de todos os tamanhos de pequenas e médias empresas a empresas de escala hiperescária.

Múltiplos fatores de forma suportam implantações de malha híbrida, integração em nuvem e segmentação dinâmica.

Características

Inteligência de ameaças centrada na IA, SD-WAN integrada, ZTNA, implantação pronta para a nuvem, proteção em tempo real contra ameaças em evolução, interface de gerenciamento unificada intuitiva e processamento de segurança rápida são os principais recursos.

Razão para comprar

As organizações se beneficiam de segurança de rede confiável e de alto desempenho, com implantação flexível e licenciamento econômico, tornando o Fortinet ideal para dimensionar empresas e equipes distribuídas.

Automação e visibilidade profunda reduzem a sobrecarga e o risco operacionais.

Prós

- Taxa de transferência de alta segurança
- Gestão intuitiva
- Operação econômica

Contras

- Configuração inicial complexa
- Recursos avançados podem precisar de experiência

? Melhor para: SMBs, empresas híbridas, redes distribuídas.

? Try Fortinet here ? Fortinet Official Website

8. Watchguard

Por que escolhemos

O WatchGuard é um NGFW rico em recursos, fácil de usar, com um portfólio abrangente de serviços de segurança para pequenas e médias empresas e MSPs.

Seu portfólio integrado inclui controle de aplicativos, sandboxing anti-malware, Wi-Fi seguro, autenticação de vários fatores e poderoso gerenciamento centralizado.

Especificações

Os aparelhos de WatchGuard vêm em vários fatores de forma, apoiando a integração fácil da nuvem e o gerenciamento centralizado em vários dispositivos e locais.

Sua plataforma de fogueira é elogiada por confiabilidade econômica e facilidade de implantação.

Características

Prevenção de intrusões integradas, antivírus do gateway, filtragem de URL, controle de aplicativos, inteligência de ameaças em tempo real, proteção de terminais, acesso remoto seguro e expansível por meio de serviços em nuvem.

Razão para comprar

O WatchGuard se destaca em usabilidade, gerenciamento eficiente e forte suporte ao cliente, tornando-a uma das principais opções para o crescimento de empresas que precisam de segurança escalável e amigável.

Prós

- Fácil de usar
- Serviço eficiente
- Forte suporte ao cliente

Contras

- Custo dos recursos avançados
- Confusão de renovação da licença

? Melhor para: pequenas e médias empresas, MSPs, organizações focadas no usuário.

? Try WatchGuard here ? WatchGuard Official Website

9. Redes de Juniper

Por que escolhemos

A Juniper Networks NGFWS fornece uma proteção robusta de várias camadas com alto desempenho, escalabilidade e análise profunda.

Aproveitar a inteligência avançada de ameaças, a conscientização sobre aplicativos e as interfaces fáceis de usar, a série SRX da Juniper e as integrações em nuvem servem a empresas que precisam de defesas flexíveis e de alta disponibilidade.

Especificações

Os eletrodomésticos da Juniper escalam de implantações para pequenas empresas a grandes ambientes de data centers, oferecendo inspeção no nível do aplicativo, análise em tempo real e relatórios abrangentes.

Inspeção profunda de pacotes e balanceamento de carga garantem a segurança e o tempo de atividade.

Características

Inteligência de ameaças em tempo real, gerenciamento dinâmico de políticas, sem costura Integração da nuvemSuporte de conformidade automatizada, controle de aplicativos, alta disponibilidade e interface de gerenciamento intuitiva.

Razão para comprar

O Juniper oferece tecnologia à prova de futuro adaptada a casos de uso específicos do setor, fornecendo controle granular e proteção confiável em ambientes híbridos e virtualizados.

Prós

- Alta escalabilidade
- Inteligência avançada de ameaças
- Interface amigável

Contras

- Integrações limitadas para feeds de terceiros
- Requer habilidade especializada para configuração avançada

? Melhor para: empresas orientadas pelo desempenho, requisitos de segurança específicos do setor.

? Try Juniper Networks here ? Juniper Networks Official Website

10. Ponto de verificação

Por que escolhemos

O ponto de verificação é comemorado para a melhor prevenção da categoria, gerenciamento integrado e escalabilidade modular.

Sua arquitetura de maestro e interface do smartconsole suportam o gerenciamento de políticas ultra eficientes e a prontidão de conformidade.

Confiável em todo o mundo, o Check Point se concentra na inteligência de ameaças em tempo real, fácil expansão da licença e precisão operacional, estabelecendo altos padrões para indústrias regulamentadas e arquiteturas de várias camadas.

Especificações

O Check Point oferece plataformas escaláveis ??com taxa de transferência de até 1 TBPS, interfaces modulares e políticas unificadas para implantações no local e na nuvem.

Seus firewalls incluem defesa de ataque de dia zero, licenciamento flexível e integração com SoCs de terceiros.

Características

Inteligência automática de ameaças em tempo real, prevenção de ameaças profunda, suporte de hiperescala, integração baseada na API para automação, extração abrangente e taxas mais baixas positivas mais baixas são recursos notáveis.

Razão para comprar

A inovação consistente e a maturidade robusta da segurança tornam o ponto de verificação ideal para empresas focadas na conformidade e na eficiência operacional.

A plataforma deles lida com ambientes regulamentados de várias nuvens com facilidade.

Prós

- Prevenção de ameaças profunda
- Escalabilidade modular
- Gerenciamento de políticas integradas

Contras

- Preços premium
- Configuração avançada complexa

? Melhor para: indústrias fortemente regulamentadas, empresas de várias nuvens.

? Try Check Point here ? Check Point Official Website

Conclusão

Selecionar o provedor de firewall da próxima geração da próxima geração é fundamental para Segurança de rede robustaeficiência operacional e crescimento escalável em 2025.

Cada uma dessas dez principais soluções NGFW oferece uma mistura distinta de proteção de ameaças, recursos de gerenciamento, opções de integração e desempenho que podem atender às necessidades de empresas, pequenas e médias empresas e organizações orientadas a nuvem.

Pesquisas detalhadas sobre especificações, recursos, profissionais e contras garantem que as decisões sejam alinhadas com requisitos de negócios específicos e planos de infraestrutura futuros.