10 melhores soluções de filtragem de conteúdo da web 2025 - Against Inva

Data: 2025-08-24 17:57:59

Autor: Inteligência Against Invaders

No cenário digital moderno, a filtragem de conteúdo da Web é um componente fundamental da

segurança cibernética e do gerenciamento de rede.

Uma solução de filtragem de conteúdo da Web é uma tecnologia que controla e monitora as páginas da web, URLs e Endereços IP que os usuários podem acessar.

Essas ferramentas protegem as organizações, impedindo o acesso a sites maliciosos, bloqueando conteúdo inadequado e aplicando políticas de uso aceitáveis.

Um filtro robusto é a primeira linha de defesa contra phishing, ransomware e outras ameaças baseadas na Web, além de ajudar as empresas a melhorar a produtividade e a manter a conformidade regulatória.

Nossa metodologia orientada por Eeat para escolher as melhores soluções de filtragem de conteúdo da web?

Nosso processo de seleção para essas soluções de filtragem de conteúdo da Web de primeira linha é guiado pelos princípios principais do EEAT: experiência, experiência, autoridade e confiabilidade.

Avaliamos meticulosamente cada produto para garantir que nossas recomendações sejam abrangentes e confiáveis.

- **Experiência e funcionalidade:** Avaliamos o desempenho do mundo real de cada solução, avaliando sua capacidade de lidar Filtragem DNSanálise de URL em tempo real e tráfego seguro sem latência significativa.
- **Especialização e público -alvo:** Categorizamos cada ferramenta com base em seu caso de uso de melhor ajuste, seja para uma pequena empresa, uma grande empresa com uma força de trabalho híbrida ou um provedor de serviços gerenciados (MSP). Isso garante que nossas recomendações sejam adaptadas às necessidades específicas do usuário.
- **Autoridade e implantação:** Consideramos a posição da indústria de cada fornecedor, observando seu reconhecimento por empresas de pesquisa líder. Por exemplo, a inclusão de um fornecedor em um **Gartner Magic Quadrant** O relatório é um forte indicador de sua autoridade da indústria.
- **Confiabilidade e forças -chave:** Nossa análise destaca forças e desvantagens exclusivas, baseando -se em críticas independentes e feedback verificado para fornecer uma visão geral honesta e imparcial.

Tabela de comparação

Solução	Foco primário	Principais recursos	Melhor para
PORCOPOINT ONE Security	Serviço de segurança nativo da nuvem Edge (SSE)	SWG integrado, CASB, ZTNA e RBI	Empresas adotando uma estrutura de confiança zero
Guarda -chuva da Cisco	Segurança da camada DNS e gateway da web segura	Filtragem DNS, Gateway Web Secure, Firewall entregue na nuvem	SMBs e empresas que precisam de implantação simples e rápida
Acesso à Internet do ZScaler	Confiança zero nativa em nuvem	SWG, DLP, Sandbox, Firewall da nuvem	Grandes empresas distribuídas globalmente
Filtragem de URL da Fortinet FortiGuard	Segurança de firewall integrada	Filtragem de URL, inspeção SSL, antivírus, DLP	Empresas com infraestrutura de Fortinet existente
Dnsfilter	Filtragem DNS movida a IA	Proteção de ameaças a IA, fácil implantação, Ferramentas MSP	MSPs e SMBs buscando uma solução fácil de usar
Webtitan	Filtragem na Web local e nuvem	Controles de política granular, relatórios avançados, recursos do MSP	Empresas que precisam de implantação e controle flexíveis
Gateway de segurança na web barracuda	Appliance de segurança integrado	Segurança da Web, inspeção SSL, relatórios, bloqueio de spyware	Organizações que precisam de uma solução de hardware/software tudo-em-um
Palo Alto Networks PRISMA Acesso	Secure Access Service Edge (SASE)	SWG, ZTNA, Firewall como um serviço, DLP	Grandes empresas com ambientes complexos de nuvem e híbridos
Sophos Web Security	Endpoint e gerenciamento de ameaças unificadas (UTM)	Filtragem na web, inspeção SSL, inteligência de ameaças	SMBs usando o ecossistema Sophos mais amplo
Netskope Secure Web Gateway	Segurança nativa em nuvem e DLP	SWG centrado em dados, DLP em tempo real, CASB	Empresas que priorizam a proteção e visibilidade dos dados

1. Forpoint One Web Security

Especificações:

O Forcepoint One é uma plataforma Native Security Service Edge (SSE). Ele consolida Gateway Web Secure (SWG), CASB de segurança em nuvem de acesso à nuvem e CASB e Acesso à rede de confiança zero (ZTNA) em uma solução única e unificada.

Esta plataforma foi projetada para fornecer segurança abrangente e centrada em dados para a força de trabalho híbrida moderna.

Motivo para comprar:

O Forcepoint One é uma escolha ideal para grandes organizações totalmente comprometidas com uma arquitetura de confiança zero.

Sua abordagem integrada simplifica a segurança, fornecendo aplicação consistente de políticas para todos os usuários, independentemente da localização ou dispositivo.

Características:

SWG integrado, CASB, ZTNA, Prevenção de perda de dados (DLP)Isolamento do navegador remoto (RBI).

Prós: Console de gerenciamento unificado; forte foco na segurança centrada em dados; Conjunto abrangente de recursos.

Contras: Pode ser complexo para organizações menores; pode ter uma curva de ensino superior.

? Melhor para: Empresas adotando a Modelo de segurança de confiança zero e buscando uma plataforma consolidada e nativa em nuvem para segurança da Web e dados.

Site oficial: Forcepoint um

2. Cisco guarda -chuva

Especificações:

Uma plataforma de segurança líder entregue em nuvem que fornece a primeira linha de defesa contra ameaças da Internet.

A Cisco Umbrella opera na camada DNS, que permite bloquear domínios maliciosos e indesejados antes mesmo de uma conexão ser estabelecida.

Também oferece um Gateway da web segura e firewall entregues em nuvem para uma proteção mais avançada.

Motivo para comprar:

A segurança da camada DNS da Umbrella torna incrivelmente rápida e fácil de implantar, oferecendo proteção imediata para todos os usuários, dentro ou fora da rede corporativa.

É um componente fundamental de uma sólida estratégia de segurança cibernética.

Características:

Segurança da camada DNS, Gateway Web Secure (SWG), firewall entregue em nuvem, inteligência de ameaças alimentada pela Cisco Talos.

Prós: Implantação extremamente rápida e simples; altamente confiável com mais de uma década de tempo de atividade verificado; inteligência proativa de ameaças.

Contras: Controle de políticas menos granulares em comparação com os gateways da web seguros de alguns concorrentes.

? Melhor para:

SMBs e empresas que precisam de uma solução fácil de implantar e altamente eficazes para bloquear ameaças no início da cadeia de mortes.

Site oficial: Guarda -chuva da Cisco

3. Acesso à Internet do ZScaler

Especificações:

O ZSCaler Internet Access (ZIA) é um gateway da Web Secure Native (SWG) nativo da nuvem e parte da plataforma ZSCALER Zero Trust Exchange.

Ele direciona todo o tráfego do usuário para a nuvem do ZSCaler, onde é inspecionada quanto a ameaças e filtrada de acordo com a política.

Zia fornece um conjunto abrangente de serviços de segurança, incluindo DLP, Firewall em nuvem e sandboxing.

Motivo para comprar:

O ZSCaler foi pioneiro no mercado de Edge Secure Service (SSE) e é uma solução líder para grandes empresas distribuídas globalmente.

Sua arquitetura nativa em nuvem garante segurança e desempenho consistentes para todos os usuários, eliminando a necessidade de aparelhos tradicionais no local.

Características:

Gateway Web Secure (SWG), Prevenção de Perda de Dados (DLP), Firewall da nuvemSandbox em nuvem, inspeção SSL.

Prós: Arquitetura nativa em nuvem para alta escalabilidade; pilha de segurança abrangente; Reconhecido como líder no Gartner Magic Quadrant for Security Service Edge. .

Contras: Pode ser caro para empresas menores; requer planejamento significativo para implantação em larga escala.

? Melhor para: Grandes empresas com presença global e uma força de trabalho remota que requerem segurança na Web escalável e de alto desempenho.

Site oficial: Acesso à Internet do ZScaler

4. Filtragem de URL da Fortinet FortiGuard

Especificações:

A filtragem de URL da FortiGuard é um componente essencial dos firewalls de próxima geração do FortiGet da Fortinet (NGFWs) e é integrado ao seu tecido de segurança mais amplo.

Ele fornece filtragem robusta e em tempo real com mais de 100 categorias de URL, oferecendo controle granular sobre o acesso ao usuário.

Motivo para comprar:

Para organizações já investidas no ecossistema Fortinet, a filtragem de URL da FortiGuard é uma adição perfeita e econômica.

Sua integração com os aparelhos FortiGate fornece gerenciamento centralizado e uma postura de segurança unificada.

Características:

Filtragem de URL em tempo real, inspeção SSL, Antivírus da WebControle de aplicativos, prevenção de perda de dados.

Prós: Integração rígida com outros produtos da Fortinet; alto desempenho com hardware dedicado; Opções de implantação flexíveis.

Contras: Principalmente uma solução local; Menos adequado para organizações em nuvem sem um aparelho.

? Melhor para: Empresas que possuem uma infraestrutura de rede Fortinet pré-existente e desejam uma solução de segurança da Web totalmente integrada.

Site oficial: Fortinet FortiGuard

5. Dnsfilter

Especificações:

O DNSFilter é uma solução de filtragem DNS moderna e movida a IA que oferece implantação rápida e gerenciamento fácil.

Ele usa o aprendizado de máquina para categorizar novos domínios em tempo real, fornecendo proteção superior contra ameaças de dia zero e sites maliciosos recém-criados.

Motivo para comprar:

Esta solução é perfeita para MSPs e SMBs que precisam de uma ferramenta simples, mas eficaz, para proteger seus usuários.

Seu painel intuitivo e automatizado inteligência de ameaças Torne-o uma solução “Configure-It-Itget-It” para equipes de TI ocupadas.

Características:

Detecção de ameaças a IA, rede global de anycast, relatórios de ameaças, integração do Active Directory.

Prós: Extremamente fácil de implantar e gerenciar; resolução rápida do DNS; Detecção precisa de ameaças em tempo real.

Contras: Menos abrangente do que as soluções de gateway Web Seguro completo; Falta alguns recursos avançados, como a inspeção completa do SSL.

? Melhor para: Provedores de serviços gerenciados (MSPs) e empresas pequenas a médicas que procuram uma solução de filtragem DNS direta e altamente eficaz.

Site oficial: Dnsfilter

6. Webtitan

Especificações:

O WebTitan é uma solução de filtragem de conteúdo da Web altamente flexível disponível como um serviço baseado em nuvem, um dispositivo virtual ou um gateway de hardware.

Ele fornece controle de políticas granulares, relatórios avançados e recursos com vários inquilinos, tornando-o um dos favoritos entre os MSPs.

Motivo para comprar:

A flexibilidade da Webtitan permite que as empresas escolham o modelo de implantação que melhor se encaixa em sua infraestrutura.

Suas opções detalhadas de relatórios e personalização dão aos administradores um alto grau de controle sobre as políticas de acesso à Internet.

Características:

Emprega em nuvem ou local, controle de políticas granulares, relatórios avançados, rotulagem branca para MSPs.

Prós: Implantação flexível (nuvem, virtual, hardware); Excelentes relatórios e análises; forte suporte multi-inquilino para MSPs.

Contras: A solução local requer gerenciamento e manutenção de hardware.

? Melhor para: Empresas e MSPs que requerem opções de implantação flexíveis e um alto nível de personalização para suas políticas de filtragem na Web.

Site oficial: Webtitan

7. Gateway de segurança na web Barracuda

Especificações:

O Barracuda Web Security Gateway é um dispositivo integrado ou solução virtual que fornece

segurança abrangente da Web.

É um Gateway da Web Secure Tradicional (SWG) que combina filtragem na web com proteção avançada de ameaças, bloqueio de spyware e relatórios.

Motivo para comprar:

Esta solução é uma opção sólida para organizações que preferem um aparelho local para segurança.

Oferece um pacote completo e all-in-one para filtragem e segurança da Web sem depender de um modelo somente em nuvem.

Características:

Filtragem de conteúdo da Web, bloqueio de spyware, inspeção SSL, relatórios avançados, mecanismo de política.

Prós: O APLACIONE ALL-IN-ONE simplifica a implantação; eficaz para inspeção profunda de conteúdo; Recursos de relatórios fortes.

Contras: Menos adequado para forças de trabalho remotas e híbridas; Manutenção de hardware necessária.

? Melhor para: As organizações que preferem um dispositivo de hardware dedicado e local para sua segurança na Web e têm uma arquitetura de rede tradicional.

Site oficial: Gateway de segurança na web barracuda

8. Palo Alto Networks PRISMA Acesso

Especificações:

O Palo Alto Networks PRISMA Access é uma plataforma Secure Access Service Edge (SASE) que fornece segurança e rede unificadas a partir de um único serviço nativo em nuvem.

Inclui um gateway da Web Secure (SWG), o Access Zero Trust Network (ZTNA) e o firewall entregues em nuvem para proteger uma força de trabalho híbrida.

Motivo para comprar:

O Prisma Access é construído para proteger redes modernas e é líder no mercado da SASE.

Ele fornece segurança consistente e de alto desempenho para todos os usuários, estejam eles no escritório, no local da filial ou em casa.

Características:

SWG, ZTNA, Firewall como serviço, prevenção de ameaças, DLP.

Prós: Plataforma SASE unificada; Aproveita a inteligência de ameaças de Palo Alto; alto desempenho e escalabilidade.

Contras: Alto custo e complexidade; muitas vezes exageram para organizações menores.

? Melhor para: Grandes empresas com ambientes complexos em nuvem e híbridos que precisam fazer a transição para um modelo de segurança moderno baseado em SASE.

Site oficial: Palo Alto Networks PRISMA Acesso

9. Sophos Web Security

Especificações:

A Sophos Web Security é um recurso fundamental da plataforma de segurança unificada da Sophos, que inclui os aparelhos de proteção de pontos de extremidade e gerenciamento de ameaças unificadas (UTM).

Ele fornece filtragem granular da Web, controle de aplicativos e inteligência de ameaças para proteger os usuários de conteúdo malicioso.

Motivo para comprar:

Sophos é uma ótima opção para empresas que desejam uma plataforma de segurança centralizada.

Se você já está usando os produtos de extremidade Sophos ou Firewall, a adição de segurança da Web fornece um console unificado para o gerenciamento, simplificando a administração e melhorando a visibilidade em suas camadas de segurança.

Características:

Filtragem na Web, Controle de Aplicativos, Inspeção SSL, Gerenciamento Centralizado, Inteligência de Ameaças.

Prós: Integra perfeitamente com outros produtos da Sophos; gerenciamento centralizado fácil de usar; Proteção abrangente.

Contras: O desempenho pode ser impactado ao executar com outros recursos de segurança da Sophos; pode não ter alguns dos recursos avançados dos provedores dedicados ao SWG.

? Melhor para: SMBs e organizações que já fazem parte do ecossistema Sophos e desejam consolidar seu gerenciamento de segurança.

Site oficial: Sophos Web Security

10. Netskope Secure Web Gateway

Especificações:

O gateway Web Netskope Secure é uma parte essencial da nuvem de segurança Netskope.

É um SWG centrado na nuvem e centrado em dados que fornece visibilidade granular e controle sobre o tráfego da Web, com uma forte ênfase na proteção de dados confidenciais.

Motivo para comprar:

O Netskope é uma excelente opção para organizações com um alto volume de uso de aplicativos em nuvem que estão particularmente preocupados com a perda de dados.

Sua abordagem “Data-primeiro” garante que informações confidenciais sejam protegidas em tempo real, seja se movendo pela Web ou dentro de um aplicativo em nuvem.

Características: Gateway Secure Web (SWG), Prevenção de Perda de Dados em tempo real (DLP), Broker de Segurança de Acesso à Cloud (CASB), Proteção Avançada de Ameaças.

Prós: Fortes recursos de DLP e proteção de dados; Arquitetura em nuvem altamente escalável; Excelente visibilidade no uso de aplicativos em nuvem.

Contras: Pode ser caro e complexo para implementar para equipes menores.

? Melhor para: Empresas priorizando a proteção de dados e procurando uma solução SWG nativa em nuvem que é profundamente integrada a um CASB.

Site oficial: Netskope Secure Web Gateway

Padrões da indústria e práticas recomendadas

Para tomar uma decisão informada e construir uma postura de segurança verdadeiramente resiliente, é crucial alinhar seu **Estratégia de filtragem de conteúdo da Web** com padrões estabelecidos da indústria.

NIST (Instituto Nacional de Padrões e Tecnologia):

O NIST SP 800-41, diretrizes sobre firewalls e políticas de firewall, fornece uma estrutura abrangente para a segurança da rede.

Embora focados nos firewalls, seus princípios no estabelecimento de uma política clara, filtragem de tráfego e monitoramento contínuo são altamente relevantes para a filtragem de conteúdo da Web.

CISA (Agência de Segurança de Infraestrutura e segurança cibernética):

A orientação da CISA sobre a filtragem e a segurança do DNS destaca a importância de bloquear ameaças no nível DNS.

Essa estratégia é uma maneira altamente eficaz de impedir que os usuários acessem domínios maliciosos, mesmo antes que uma página da web completa seja carregada.

Gartner:

A análise do Gartner dos mercados Seguro Gateway e Security Service Edge (SSE) fornece um contexto valioso sobre recursos de fornecedores e tendências de mercado.

Suas pesquisas, como os relatórios do quadrante mágico, ajudam os líderes de TI a identificar fornecedores com uma forte visão e capacidade de executar.