Forcepoint

Datasheet

Forcepoint ONE Firewall

Proteja todo o seu tráfego de internet e proteja-se contra ataques projetados para explorar sites de filiais vulneráveis.

Principais benefícios

Entregue como um serviço

- Distribua, atualize e aplique novas políticas e assinaturas de segurança em tempo real.
- Implemente o dimensionamento automático (para cima ou para baixo) em uma arquitetura de nuvem moderna, impulsionada pelo uso real.
- Reduza os gastos e a mudança da infraestrutura de alta CapEx para a arquitetura de nuvem OpEX que economiza custos.

Aumente a segurança com os principais recursos de IPS

- Veja sinais de alerta precoce de possível atividade maliciosa, incluindo ameaças de dia zero e ransomware.
- Proteja-se contra ataques de negação de serviço (DoS). Identifique invasões conhecidas ou suspeitas, incluindo ataques de shellcode.
- Evite ataques de SSL projetados para explorar vulnerabilidades que visam vazar informações confidenciais.

Dashboards e relatórios

- Detecte rapidamente as ameaças com dashboards e relatórios personalizados, obtenha insights sobre os usuários ou grupos que enfrentam ataques com mais frequência.
- Reduza o risco identificando facilmente tendências e padrões de ameaças.
- Simplifique a investigação de incidentes visualizando eventos apenas associados a um incidente específico.

A transformação digital está aqui: os dados e aplicativos residem na nuvem e os usuários acessam recursos de qualquer lugar, usando dispositivos gerenciados e não gerenciados. No entanto, as organizações distribuídas ainda dependem de firewalls legados para proteger suas redes. Os cibercriminosos estão cientes disso e estão constantemente criando maneiras de atacar o elo mais fraco da cadeia, que geralmente está na filial.

Proteja sites de filiais e escritórios remotos com o Forcepoint ONE Firewall. Garanta visibilidade completa, segurança e controle sobre todo o tráfego de internet para eliminar os pontos cegos de rede. Mantenha a tranquilidade sabendo que sua rede está protegida com recursos de IPS de precisão de detecção e proteção contra evasão líderes do setor para proteger contra ameaças avançadas, incluindo ataques de dia zero.

Inspeção completa de tráfego

O Forcepoint ONE Firewall oferece capacidade de inspeção de tráfego para proteger contra os ataques que visam expor filiais vulneráveis e sites remotos que operam com firewalls legados. O Forcepoint ONE Firewall, juntamente com o Forcepoint ONE SWG, garante que todas as portas e protocolos sejam inspecionados. Proteja e controle todo o seu tráfego de internet para mitigar falhas de segurança e proteja-se contra os ataques não convencionais direcionados a portas.

Gerenciamento de políticas granulares

O Forcepoint ONE Firewall oferece aos administradores capacidades de gerenciamento de políticas granulares para aumentar a segurança geral. Os administradores podem especificar regras com base em usuários, grupos e serviços, o serviço que a regra de política rege e a ação a ser realizada quando a regra de política é acionada. Os administradores também podem reorganizar a prioridade das políticas de cima a baixo e atribuir uma política padrão para ser usada na ausência de outras políticas. Com o controle de políticas de cinco tuplas, os administradores podem definir facilmente regras com base no protocolo, endereços IP de origem e destino e portas de origem e destino, permitindo controle preciso sobre o tráfego e a segurança de rede. Esse nível de precisão permite que as organizações estabeleçam regras detalhadas que garantem que apenas comunicações autorizadas e seguras ocorram.

Implantação e gerenciamento de nuvem

Ao contrário dos firewalls de dispositivos físicos, pesados, caros e difíceis de manter — o Forcepoint ONE Firewall é "Entregue como um serviço". Essa solução baseada em SaaS permite que as organizações reduzam ou eliminem infraestrutura e despesas gerais associadas à aquisição, implantação e manutenção de firewalls físicos tradicionais em cada filial. Com o gerenciamento central, os administradores podem distribuir e aplicar rapidamente as atualizações e assinaturas de segurança mais recentes em tempo real, melhorando a segurança geral e reduzindo o risco de violações de dados.

Com base na tecnologia IPS confiável líder do setor

O Forcepoint ONE Firewall faz mais do que lidar com problemas de rede comuns; também identifica e mitiga rapidamente ameaças cibernéticas avançadas. Desde detectar ataques de negação de serviço (DoS) à visibilidade de ataques de SSL (como o Heartbleed), ela ajuda os administradores a proteger-se contra os ataques em servidores não corrigidos e infraestruturas não mantidas. Sinais de alerta precoce de uma violação de rede são fundamentais para mitigar a infiltração e evitar controle externo e não autorizado de recursos internos contra o vazamento de informações. É por isso que o Forcepoint ONE Firewall detecta botnet e tráfego anômalo, ambos indicadores iniciais de possível atividade maliciosa, incluindo ameaças de dia zero.

Fortes capacidades de relatórios para decisões informadas

O Forcepoint ONE Firewall fornece vários dashboards e recursos de relatórios para garantir que os administradores sejam informados com as informações fundamentais necessárias para tomar as decisões certas. Ele oferece gráficos de séries temporais para visualizar tendências e padrões de ameaças para que os administradores possam agir proativamente e evitar invasões repetidas. O Forcepoint ONE Firewall também fornece a capacidade de ver eventos relacionados no registro para simplificar a investigação de incidentes visualizando apenas eventos associados a um incidente escolhido. Os administradores podem gerar relatórios detalhados com base em ameaças identificadas, incluindo ameaças conhecidas e de dia zero detectadas em downloads ou uploads, juntamente com insights sobre os usuários ou grupos que se depararam com elas com mais frequência.

PLATAFORMAS	
Administração centralizada	Sistema de administração centralizada de nível empresarial com recursos de análise de registros, monitoramento e geração de relatórios. Consulte o datasheet do Forcepoint Security Management Center para ter detalhes
RECURSOS DE SEGURANÇA DE REDE	
Controle de políticas de 5 tuplas	Crie políticas com base em usuários/grupos, sites de origem ou listas de endereços IP, domínios de destino ou listas de endereços IP, portas de origem e destino e protocolos
Serviços e protocolos de rede pré-configurados	Centenas de protocolos predefinidos e agentes de protocolo
Protocolos definidos pelo usuário	Crie protocolos definidos pelo usuário para regular o comportamento interno do aplicativo
INSPEÇÃO DE TRÁFEGO	
Integração com o Forcepoint ONE SWG	Integração com o Forcepoint ONE SWG para proteção da web.
DNS	Prevenção de ameaças de DNS, aplicação de protocolo para evitar ataques maliciosos por meio de consultas de DNS.
IPS E CAPACIDADES DE PREVENÇÃO DE AMEAÇAS	
Inspeção profunda de pacotes	Inspecione metadados de pacotes e o comportamento do protocolo para verificar se há padrões de assinatura de tráfego suspeito.
Extenso catálogo de situações de ameaças	Proteja-se contra dezenas de milhares de situações de ameaças continuamente atualizadas por meio da nuvem
Proteção contra ameaças baseada em categoria	Aprimore a detecção de ameaças e simplifique o gerenciamento de configuração
Detecção baseada em anomalia	Forneça sinais de alerta precoce de possível atividade maliciosa, incluindo ameaças de dia zero, observando o tráfego antes e após os ataques
Detecção baseada em assinatura	Identificação de aplicativo/protocolo/serviço a partir de impressão digital
Proteção DoS	Proteja a rede identificando ataques de negação de serviço, detecte ameaças que tentam travar servidores não corrigidos e proteja infraestruturas não mantidas
Ataques de divulgação	Obtenha visibilidade sobre os ataques de ameaças de SSL (como o Heartbleed) projetados para explorar vulnerabilidades em servidores que podem vazar informações confidenciais, incluindo senhas, chaves de criptografia, nomes de usuários, código fonte, diretório, configuração e conteúdo de arquivos
Proteção de botnet	Detecte o tráfego de botnet — um indicador de que a rede foi comprometida — e evite o controle externo e não autorizado de recursos internos a partir da exfiltração de dados
Malware / antivírus	Detecte e evite ameaças de serviços conhecidos por demonstrar comportamento malicioso ou indesejável, incluindo spyware, adware e malware
Violações do protocolo	Aplica a conformidade estrita para uma variedade de protocolos, incluindo TCP, HTTP, DNS e outros
Sondas	Impede a atividade de verificação projetada para reunir inteligência e identificar vulnerabilidades
Roteamento malicioso	Ataques que tentam usar indevidamente protocolos de rede para evitar ou contornar filtros de segurança