

RESPOSTA AO CRESCENTE DESAFIO DE CIBERSEGURANÇA COM O FORTINET SECURITY FABRIC



RESPOSTA AO CRESCENTE DESAFIO DE CIBERSEGURANÇA COM O FORTINET SECURITY FABRIC

A economia digital emergente promove o valor dos negócios usando a tecnologia para conectar usuários, dispositivos, dados, produtos e serviços. Para competir com sucesso, as organizações devem adotar novos modelos de conectividade e compartilhamento de dados, incluindo nuvens públicas e privadas e possibilitando a Internet das Coisas (IoT). Essas novas abordagens permitem que as organizações sejam mais ágeis e mais responsivas às necessidades dos clientes e às demandas do mercado, e que melhorem a diferenciação competitiva e expandam sua presença no mercado global.

A adoção de um modelo de negócio digital requer evolução rápida da rede, exigindo fluxo mais rápido de aplicativos, dados e serviços em um ambiente cada vez mais diversificado de usuários, domínios e dispositivos. Consequentemente, as redes atuais e sua segurança também estão cada vez mais sem fronteiras. Os aplicativos, serviços e a infraestrutura de IoT e nuvem forçam as organizações a se preocuparem com uma superfície de ataque que pode não ser visível ao pessoal de TI.

A ironia dessa evolução da rede é que, ao acelerarmos o fluxo de aplicativos, dados e serviços em um ambiente cada vez mais diversificado de usuários, dispositivos e domínios, estamos agravando a complexidade da proteção desse novo ambiente em um cenário de ameaças em constante mudança.

Hoje, vemos um grande volume de ciberameaças com ataques direcionados e muito sofisticados, viabilizados pela comercialização de um ecossistema de serviços de cibercrimes e recursos e serviços da cadeia de suprimentos.

Além de se protegerem contra essas ameaças, as organizações também devem documentar e mostrar as medidas que estão adotando para atender aos requisitos regulatórios e de conformidade sempre

em evolução. Como os riscos aumentam rapidamente, os órgãos de governança em todo o mundo estão exigindo processos de gerenciamento de riscos.

A adoção dessas medidas é uma tarefa árdua – a conformidade requer auditoria, monitoramento e aderência – e a complexidade desses processos se agrava à medida que a rede se torna cada vez mais distribuída.

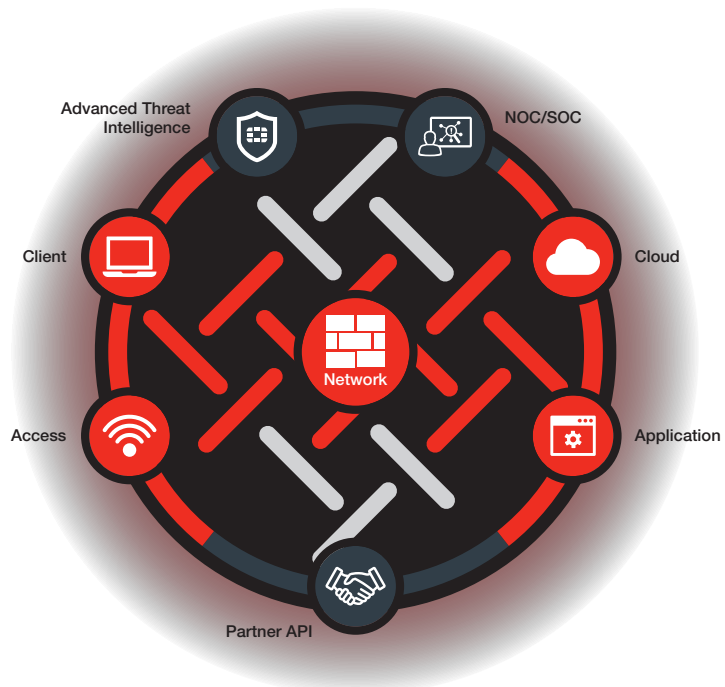
Até hoje, a abordagem mais comum tem sido adicionar novos dispositivos de segurança a um gabinete de segurança já sobrecarregado. Mas, conforme indica o aumento contínuo de ataques à rede, esta abordagem não está resolvendo o problema. O fato é que, enquanto compra e instala novos dispositivos para descobrir algumas novas ameaças com mais rapidez, os dados mostram que as ameaças comprometem as organizações de forma ainda mais rápida. Você tem que parar de usar essa abordagem.

Soluções de segurança em silos, com interfaces de gerenciamento separadas e sem uma maneira de coletar ou compartilhar informações sobre ameaças com outros dispositivos da rede, são pouco úteis.

UMA NOVA ABORDAGEM

Mas, e se os dados e os elementos de segurança dos vários ambientes de uma organização puderem ser bem integrados, coesos e correntes, como um fabric entrelaçado sem emendas? Essa abordagem permitiria às empresas ver, controlar, integrar e gerenciar a segurança de seus dados em toda a organização, até mesmo na nuvem, permitindo um modelo de negócio digital seguro.

Essa abordagem também permitiria que a segurança se expandisse e se adaptasse dinamicamente com a adição



de mais e mais cargas de trabalho e, ao mesmo tempo, seguiria e protegeria de forma transparente os dados, usuários e aplicativos em sua movimentação entre IoT e dispositivos inteligentes, redes sem fronteiras e ambientes na nuvem.

O FORTINET SECURITY FABRIC

O Fortinet Security Fabric fornece uma abordagem nova e inteligente de arquitetura de segurança que, pela primeira vez, permite que as empresas façam conectem todas as suas soluções de segurança separadas, formando apenas uma solução integrada. Esta abordagem do tipo *fabric* apresenta três características principais:



1. Ampla

O Security Fabric foi desenvolvido para proteger a superfície de ataque inteira. As soluções

de segurança instaladas na rede não podem operar separadamente, como dispositivos isolados. Para proteger as redes atuais, os administradores devem ter visibilidade de todo o ambiente, incluindo os dispositivos de usuários, pontos de acesso, elementos de rede, datacenter, o ambiente na nuvem e até os aplicativos e os próprios dados.

A visibilidade abrangente da empresa distribuída vincula dados, aplicativos, dispositivos e fluxos de trabalho para fornecer um nível de conhecimento e capacidade de resposta, gerenciado por meio de apenas um painel de vidro, nunca antes disponibilizado por outro provedor de solução de segurança. O conhecimento de cada elemento de rede, incluindo as soluções de outros fornecedores, e o fluxo de dados entre eles, permite que os administradores encontrem e respondam às ameaças mais sofisticadas.

Combinado à segmentação de rede dinâmica que separa logicamente dados e recursos, o Security Fabric pode ir fundo na rede para descobrir ameaças que se movem entre as zonas de uma rede. Essa amplitude e visibilidade detalhada ajudam na conformidade, no monitoramento do tráfego interno e dos dispositivos, impede o acesso não autorizado a dados e recursos restritos e controla a propagação de intrusos e malware.



2. Potente

Com os requisitos de desempenho exigidos pelas redes atualmente, a segurança deve ser

permeável e extremamente potente. As empresas digitais não podem favorecer o desempenho e se esquecer de proteger parte alguma da rede. Também não podem proteger-se de um vetor de ataque e deixar outros abertos, nem podem deixar um usuário ou aplicativo desprotegido.

Além disso, a mesma segurança forte deve ser implementada nos dispositivos de usuários e integrada à camada de acesso à rede com e sem fio, flexível para instalações de qualquer porte, em campus com fluxo complexo e intenso de dados e ambientes de datacenter, e ainda ser disponível virtualmente para proteger a nuvem privada, pública e híbrida.

As soluções de segurança da Fortinet usam as unidades de processamento de segurança (SPU) mais rápidas, desenvolvidas conforme a finalidade, para reduzir a carga na infraestrutura, além de versões de software otimizadas para fornecer segurança abrangente sem afetar o desempenho. No, Security Fabric, as tecnologias de segurança física e virtual podem ser entrelaçadas umas às outras para intensificar as políticas e sua aplicação em toda a rede distribuída, permitindo uma proteção mais eficaz do ambiente da rede em constante evolução e, ao mesmo tempo, resolvendo novos desafios das ameaças.



3. Automatizada

O Fortinet Security Fabric permite resposta rápida e coordenada às ameaças; assim, os elementos podem rapidamente

trocar inteligência sobre as ameaças e coordenar ações. Mas, como um ataque pode comprometer a rede em minutos, não basta ter só visibilidade. A rede também deve responder na mesma velocidade que o ataque. Por isso, as soluções de segurança não só precisam correlacionar a inteligência de ameaças para determinar o nível de risco, como também sincronizar automaticamente uma resposta coordenada. O Security Fabric

pode isolar dinamicamente os dispositivos afetados, segmentar partes da rede, atualizar regras, criar políticas e remover malware.

As soluções de segurança também devem se adaptar dinamicamente às configurações da rede em constante mudança e estabelecer e aplicar novas políticas conforme o ambiente a ser protegido se adapta às necessidades dos negócios. Medidas e contramedidas de segurança devem ser fornecidas automaticamente quando novos dispositivos, cargas de trabalho e serviços são incorporados em qualquer lugar, por ex., dispositivos remotos ou na nuvem.

UMA ABORDAGEM INTEGRADA E COLABORATIVA

O Fortinet Security Fabric conecta tecnologias fundamentais de segurança e rede – de firewalls até segurança de conteúdo e aplicativos para pontos de acesso seguros – para fornecer segurança sem emenda em toda a rede distribuída, local ou remota, física ou virtual, com ou sem fio, no seu domínio ou na nuvem.

Enterprise Firewalls – O Fortinet Security Fabric utiliza a solução Enterprise Firewalls da Fortinet – para instalação em escritórios remotos, campus, datacenter e segmentação interna – todos interligados por um sistema operacional unificado para implementação e controle simplificados e coordenados. Essa arquitetura de fato oferece os benefícios da padronização que muitos fornecedores de plataformas alegam oferecer.

Os recursos da solução Enterprise Firewalls podem ser expandidos para o campus todo e para o datacenter, fornecendo a defesa mais segura e eficiente contra ameaças conhecidas. Além disso, essa solução permite a segmentação dos elementos da rede, reforçando a separação de tráfego, dispositivos e dados para fornecer um controle mais forte. Além disso, à medida que novas ameaças se tornam conhecidas, todos os firewalls no ambiente podem ser atualizados dinamicamente para fornecer proteção contra eles.

Cloud Security – Com a expansão das redes corporativas, o Fortinet Security Fabric também pode proteger o ambiente na nuvem. Os firewalls virtuais podem ser instalados nos ambientes IaaS da nuvem privada e nuvem pública, para

microsegmentação norte-sul ou leste-oeste. A combinação da solução Cloud Security da Fortinet com sua instalação de firewall corporativo existente mantém sem emenda a mesma segurança potente em grande escala, bem como a mesma inteligência e mitigação de risco dinâmica para os aplicativos gerenciados localmente ou na nuvem.

Advanced Threat Protection – Detectar as ameaças conhecidas representa somente metade da batalha.

As soluções Advanced Threat Protection (ATP) podem detectar e mitigar ameaças já desconhecidas, compartilhando inteligência global e local entre os elementos de segurança do Security Fabric. Essas soluções são desenvolvidas para trabalharem juntas e entregarem dados de maneira automática e contínua entre os elementos da rede, para prevenir, detectar e mitigar ataques no ambiente e todos os vetores de ataque.

Segurança de aplicativos – O Fortinet Security Fabric garante a segurança e a disponibilidade dos aplicativos baseados na web que há muito tempo são alvos favoritos dos hackers, pois eles têm acesso a informações valiosas e são relativamente fáceis de explorar. Um ataque bem-sucedido pode causar uma série de consequências devastadoras, incluindo perda financeira, danos à reputação da marca e perda da confiança do cliente. A solução de segurança dos aplicativos da Fortinet é completa, de apenas um fornecedor, e fornece desempenho e eficácia comprovados, necessários para atender às crescentes demandas dos aplicativos atuais.

Secure Access – O Fortinet Security Fabric vai além da simples integração de soluções de segurança. Nossa solução Secure Access estende as políticas de segurança coordenadas até a borda da rede com e sem fio, que é o alvo da maioria das vulnerabilidades.

Operações de segurança – A visibilidade e o controle adaptativos de todo o Fortinet Security Fabric é um requisito para a equipe de operações de segurança encarregada de monitorar e responder a incidentes em toda a organização. Uma variedade de ferramentas está disponível para gerenciar, monitorar e relatar sobre os múltiplos componentes do fabric de um lugar, sejam eles múltiplas instâncias do mesmo produto Fortinet, vários produtos Fortinet ou vários produtos de diferentes fornecedores.

Parceiros certificados no Fortinet Security Fabric – Além das integrações nativas construídas entre as soluções de segurança da Fortinet, o Fortinet Security Fabric também oferece suporte a interfaces de programação de aplicativos (APIs) abertas, tecnologia de autenticação aberta e dados de telemetria padronizados. Isso permite a integração dos investimentos de segurança e de rede existentes no Fortinet Security Fabric. A Fortinet desenvolveu um ecossistema em expansão de Fabric-Ready Partners, cujas soluções foram certificadas para operar na estrutura do Fortinet Security Fabric.

RESUMO

A empresa em evolução e sua transição para um modelo de negócio digital é um dos aspectos mais desafiadores da segurança hoje. Como as tendências mais importantes na área de computação e redes continuam trazendo mudanças em infraestruturas, arquiteturas e práticas de negócios críticas, as organizações estão procurando soluções inovadoras de segurança de rede para ajudá-las nessa evolução.

O Fortinet Security Fabric é uma estrutura inteligente desenvolvida para fornecer segurança expansível e interconectada, combinada com conhecimento, inteligência de ameaças viável e padrões de API abertos para garantir flexibilidade e integração máximas para proteger até os ambientes empresariais mais exigentes. As tecnologias de segurança da Fortinet receberam as certificações mais independentes de eficácia e desempenho de segurança do setor. O Fortinet Security Fabric e seus componentes fecham lacunas deixadas por produtos e plataformas anteriores, fornecendo as proteções amplas, potentes e automatizadas que as organizações da atualidade exigem em seus ambientes físicos e virtuais, desde os dispositivos de usuários até os ambientes na nuvem.

Veja mais informações sobre o Fortinet Security Fabric em nosso [website](#).



SEDE GLOBAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

VENDAS EMEA
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

VENDAS APAC
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

VENDAS AMÉRICA LATINA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

MÉXICO
Paseo de la Reforma 412
Piso 16
Col. Juárez
06600 México D.F.
Tel: +52-(55) 5524-8428