FORTINET

Cinco erros comuns ao convergir segurança e rede

Índice

Visão geral executiva

Manter a aceleração digital de hoje leva tempo, esforço e escrutínio. A adição de novas ferramentas e investimentos aumenta a complexidade e a vulnerabilidade dos ambientes de segurança empresarial, expondo lacunas na comunicação e colaboração, criando sistemas em silos e diminuindo os tempos de resposta. Proteger a empresa contra o cenário de ameaças cada vez mais sofisticado de hoje exige uma arquitetura de plataforma de cibersegurança automatizada para eficiência operacional; uma arquitetura de segurança ampla o suficiente para reduzir o risco em toda a superfície de ataque digital, integrada para que as lacunas de segurança sejam fechadas e automatizadas para aumentar a eficiência e agilizar os tempos de resposta.

Introdução

A aceleração digital está impulsionando as organizações. Mas, para a maioria, também está testando as redes subjacentes devido ao aumento da complexidade resultante de uma rede em expansão e da rápida introdução de novos produtos e serviços pontuais. E à medida que sua rede se torna cada vez mais complexa, sua capacidade de gerenciá-la diminui.

Mas isso não é tudo. O aumento da complexidade não apenas dificulta sua capacidade de gerenciar a rede, mas também afeta seus recursos de detecção e resposta a ameaças, aumentando sua vulnerabilidade a ataques. A questão crítica é que, embora sua rede possa ser capaz de suportar novas iniciativas, se for como a maioria das redes, ela é composta por uma coleção de soluções individuais de rede e segurança em silos que nunca foram projetadas para funcionar juntas. E, dado o sofisticado ambiente de ameaças de hoje, a probabilidade de um ataque e violação de dados bem-sucedidos nunca foi tão alta.

Requisitos para consolidação

Abordar esses novos riscos e proteger esses vetores de ataque requer uma abordagem consolidada. Uma solução eficaz de cibersegurança projetada para fornecer proteção total e, ao mesmo tempo, reduzir a complexidade deve:

- Convergir soluções de rede e segurança de nível empresarial em um único dispositivo
- Proteger toda a superfície de ataque, não só agora, mas também à medida que se expande
- Gerenciar o ciclo de ataque completo, da detecção à resposta
- Suporta várias plataformas de nuvem e ambientes de nuvem híbrida com segurança nativa da nuvem que opera como uma extensão da postura de segurança no local
- Aproveita uma única fonte de inteligência de ameaças em todas as tecnologias de segurança implantadas
- Monitorar e gerenciar todas as soluções, permitindo que equipes de TI enxutas sejam dimensionadas para atender às necessidades de segurança da organização

E isso é apenas o começo. Reduzir a complexidade vai além de apenas implantar a tecnologia certa. Também diz respeito a como essas tecnologias funcionam juntas. E isso começa com a convergência da rede com sua infraestrutura de segurança. E continua com a adoção de uma abordagem de plataforma para reduzir o número de fornecedores diferentes necessários para compor a solução. O ambiente integrado resultante minimiza as lacunas de segurança e, ao mesmo tempo, fornece prevenções e respostas oportunas e coordenadas em todo o ciclo de vida do ataque.

Mas isso é mais difícil do que parece. Aqui estão cinco erros comuns que as organizações cometem ao consolidar suas soluções e estratégias de segurança e rede.

Erro nº 1: confiar demais

O modelo de segurança herdado e baseado em perímetro foi virado de cabeça para baixo, com dispositivos "confiáveis" implantados fora do perímetro da rede, enquanto os "não confiáveis" circulam livremente dentro dele. Usuários híbridos dentro e fora do local precisam de acesso gratuito à rede e seus recursos de qualquer lugar. Sem políticas mais rigorosas e controles consistentemente aplicados, o risco de uma violação bem-sucedida aumenta exponencialmente, especialmente à medida que usuários, aplicações e fluxos de trabalho se movem entre os vários segmentos de sua rede distribuída.

Um modelo de segurança Zero Trust significa que nenhum usuário ou dispositivo é confiável por padrão. Em vez disso, o acesso aos recursos é concedido ou negado com base na identidade do usuário, e as permissões são atribuídas com base nos deveres, responsabilidades e funções dos usuários e dispositivos. Os princípios do Zero Trust reduzem os riscos de dispositivos e usuários mal-intencionados ou vulneráveis, especialmente agora que o perímetro se expandiu e se fragmentou no mundo do trabalho remoto e os endpoints se multiplicaram exponencialmente.

Implementar e aplicar corretamente um modelo de segurança Zero Trust começa com uma segmentação de rede e um controle de acesso sólidos. Sua arquitetura de segurança deve ser capaz de identificar automaticamente os dispositivos que se conectam à rede, autenticar o usuário com segurança e fornecer ou negar acesso a recursos de rede com base nas permissões associadas à conta desse usuário.

A segmentação interna da rede limita o movimento lateral de invasores e malware, diminuindo o impacto de uma violação de dados. Quer as aplicações estejam no local ou na nuvem, os usuários e as aplicações podem ser geograficamente independentes e ainda criar conexões seguras e confiáveis para recursos críticos sem comprometer inadvertidamente o resto da rede.

O acesso a aplicações é outro componente crítico. O acesso à rede Zero Trust (ZTNA) é construído usando uma variedade de ferramentas — cliente, gateway de aplicações, mecanismo de política, autenticação, segurança — mas quando entregue por diferentes fornecedores usando diferentes sistemas operacionais e consoles de gerenciamento e configuração, estabelecer uma solução ZTNA bem-sucedida é quase impossível.

"A mudança da confiança implícita para o Zero Trust é uma resposta aos crescentes incidentes e custos do crime cibernético... Uma implementação robusta de soluções Zero Trust pode reduzir a probabilidade de ataque."[1]

Erro n.º 2: avaliar plataformas de nuvem e soluções de segurança em um silo

As organizações lutam para estabelecer e manter políticas de segurança e aplicação consistentes em ambientes híbridos multinuvem. Tentar implantar segurança em ambientes tão complexos apresenta desafios que muitas equipes de TI podem achar esmagadores, como manter controles de segurança consistentes, gerenciar e otimizar o acesso a aplicações e manter o desempenho geral. Isso é especialmente verdadeiro quando se usa várias soluções de diferentes fornecedores.

Os riscos mais significativos em implantações multinuvem são causados por expansão, segurança reforçada (não nativa) e configurações incorretas. As implantações na nuvem híbrida localizadas fora do perímetro da rede, mas acessíveis pela internet pública também podem resultar em problemas de acesso não autorizado.

Para capitalizar totalmente as promessas da nuvem, suas soluções de segurança devem suportar o uso eficaz de recursos de nuvem, como dimensionamento automático, ser conscientes do ambiente para fornecer a granularidade necessária, garantir recursos e aplicação consistentes em qualquer ambiente de nuvem e ser verdadeiramente nativas da nuvem em todas as principais plataformas de nuvem.

Ambientes multinuvem também exigem detecção e aplicação coordenadas em toda a superfície de ataque digital para permitir respostas rápidas às ameaças. Isso significa que as soluções de segurança que você implantou em diferentes plataformas não precisam apenas fornecer funcionalidade nativa da nuvem, mas também compartilhar inteligência de ameaças entre nuvens para fornecer segurança consistente e sensível ao contexto que possa avaliar e se ajustar automaticamente aos riscos. Isso também permite que as políticas de segurança sigam aplicações e fluxos de trabalho que abrangem nuvens, garantindo que as proteções sejam aplicadas de forma consistente de ponta a ponta.

A maioria das organizações (72%) está buscando uma estratégia híbrida ou multinuvem para integração de vários serviços, escalabilidade ou razões de continuidade dos negócios.[2]

Erro n.º 3: concentrar-se na prevenção em vez de no tempo para detecção

Os cibercriminosos usam cada vez mais ataques direcionados para explorar vulnerabilidades e configurações incorretas da rede. Suas campanhas bem orquestradas dão aos defensores cibernéticos uma janela limitada para interromper uma sequência de ataques. E a detecção e a resposta manuais simplesmente não conseguem acompanhar a automação, a escala da nuvem e a inteligência artificial (IA) usadas para lançar ataques sofisticados que visam perímetros distribuídos.

Para proteger sua organização contra os ataques de alta velocidade de hoje, incluindo malware polimórfico de mudança rápida, sua postura de segurança deve ser capaz de se "reprogramar" em tempo real para quebrar a sequência de ataque antes que seja bem-sucedida.

Para determinar se o seu sistema de segurança está à altura da tarefa, você precisa avaliar cinco coisas:

1. Sua capacidade de passar rapidamente da detecção de uma ameaça para o lançamento de uma defesa personalizada em seu ambiente distribuído.

2. A precisão e velocidade de suas capacidades de detecção.

3. Ele pode gerar novas prevenções em todo o ciclo de ataque, distribuí-las automaticamente entre as diferentes tecnologias e dispositivos e fortalecer os recursos de prevenção existentes.

4. Sua participação no compartilhamento de inteligência de ameaças globais e comunitárias para que você nunca seja um “segundo” Paciente Zero.

5. A qualidade de seus recursos de IA e aprendizado de máquina (ML) (se houver).

Uma cibersegurança robusta aproveita a escala de nuvem e IA avançada para fornecer proteção de usuário para aplicação automaticamente em tempo quase real em todo o ambiente. O uso estratégico de IA é essencial para coordenar prevenção, detecção e resposta em toda a superfície de ataque digital e ciclo de vida em bordas, nuvens, endpoints e usuários.

Os recursos de ML são igualmente cruciais. Um classificador de ML bem treinado pode diferenciar ameaças genuínas de falsos positivos, permitindo que as equipes de segurança concentrem as investigações e os esforços de remediação em ataques reais. As soluções em linha aproveitam o ML para detectar ameaças automaticamente com base em anomalias comportamentais e responder usando cartilhas predefinidas. O aprendizado de máquina também pode ajudar na coleta e análise de dados, fornecendo aos caçadores de ameaças e analistas do centro de operações de segurança (SOC) as informações necessárias para detectar e responder rapidamente a ataques avançados e rápidos.

Erro n.º 4: expandir a conectividade sem segurança convergida

As organizações estão acelerando seus planos digitais para que possam ser mais ágeis e adaptáveis. Mas, embora as redes de hoje sejam projetadas para serem altamente ágeis, a maioria das abordagens de segurança tradicionais não é. Quando as redes se adaptam às mudanças de requisitos, segmentos de rede inteiros podem ficar desprotegidos. Devido a essa necessidade de adaptabilidade e escalabilidade, a rede e sua infraestrutura de segurança subjacente não podem mais ser implantadas como entidades separadas em camadas umas sobre as outras. O que você precisa é de uma solução que combine as funções de segurança e rede em um sistema único e integrado que possa ser implantado em qualquer número de fatores de formato.

Infelizmente, para gerenciar seus vários ambientes de rede e a crescente variedade de dispositivos em suas redes — e ameaças cibernéticas associadas — muitas organizações implantaram uma grande variedade de produtos de segurança independentes que não estão integrados à infraestrutura existente e não interoperam. Isso os torna difíceis ou impossíveis de monitorar ou gerenciar e impossibilita a automação. Para agravar ainda mais esse problema, alguns até implantaram soluções de diferentes fornecedores para proteger seus vários casos de uso de hardware, software e nuvem.

A consolidação de produtos de cibersegurança está transformando a compra de segurança. De acordo com o Gartner, “75% das organizações buscaram ativamente a consolidação de fornecedores em 2022, em comparação com apenas 29% em 2020.”[3]

Erro n.º 5: não implementar um ecossistema completo

Nenhum fornecedor sozinho terá todas as tecnologias de que você precisa no momento em que precisar. Da mesma forma, ninguém pode abordar sozinho todos os requisitos para combater o cenário de ameaças atual. A resposta é escolher uma solução, geralmente uma plataforma, que possa se integrar facilmente ao restante do seu ecossistema de segurança, incluindo soluções de fornecedores terceirizados por meio de interfaces de programação de aplicações (APIs), conectores e ferramentas e scripts de automação DevOps. Isso permite que você crie uma frente unificada para prevenção, detecção e resposta para proteger sua superfície de ataque digital estendida.

Uma arquitetura de API aberta permite a comunicação e sincronização entre dispositivos de diferentes fornecedores. Conectores personalizados fornecem um nível ainda mais alto de integração e interoperabilidade, permitindo comunicações em tempo real e atualizações automáticas em todo o ecossistema. Uma biblioteca de ferramentas e scripts DevOps de finalidade específica permite implantação e gerenciamento rápidos e personalizáveis, dimensionando os recursos de equipes de segurança enxutas. Essa arquitetura de segurança integrada fornece de forma exclusiva proteção e conexões consistentes em todas as extremidades da rede, independentemente de onde residam.

Além da interoperabilidade, há a necessidade de coordenar e colaborar com parceiros de inteligência de ameaças, organizações de pesquisa e outros fornecedores de cibersegurança e redes. Organizações como o FortiGuard Labs colaboram com a comunidade global de inteligência para compartilhar as melhores práticas do setor e impedir a disseminação de ataques, protegendo as empresas contra milhões de eventos. Os próprios fornecedores precisam sair do seu interesse próprio e colaborar com a comunidade global de inteligência, compartilhando as melhores práticas e pesquisas de ameaças para impedir a disseminação de ataques. Trabalhar em conjunto expande a visibilidade e a detecção de ameaças e possibilita uma resposta coordenada, permitindo que as organizações concorram de forma eficaz e segura no mercado digital de hoje.

Conclusão

Sendo a mudança a única constante, especialmente tendo em conta o rápido consumo de inovações adicionadas aos ambientes existentes, a simplicidade e a adaptabilidade são vitais. À medida que sua rede se torna mais complexa e heterogênea, você precisa de uma plataforma consolidada de cibersegurança para simplificar e otimizar seus recursos de prevenção, detecção e resposta. Isso garante visibilidade unificada em toda a superfície de ataque digital, elimina lacunas de segurança e reduz a complexidade, ao mesmo tempo que acelera as operações e as respostas a incidentes.

A experiência digital otimizada requer a criação e manutenção de conexões confiáveis e de alto desempenho entre usuários, dispositivos e aplicações em ambientes diversos e globais, incluindo configurações de nuvem híbrida. Consolidar silos simplesmente não é suficiente para que isso funcione. Convergência de rede e segurança, consolidação de fornecedores e colaboração de parceiros são a resposta. Evitar esses cinco erros ao avaliar seu próximo investimento em segurança ajudará a fechar lacunas de segurança, unificar sistemas em silos, acelerar os tempos de resposta e garantir que sua segurança possa crescer e se adaptar ao seu negócio.

[1] Fortinet, O estado de Zero Trust, 10 de janeiro de 2022.

[2] Cybersecurity Insiders, 2022 Cloud Security Report, janeiro de 2023.

[3] Menghan Xiao, Security Week, "Security vendors report economic hit as they struggle to lure newer customers", 8 de março de 2023.

FORTINET

www.fortinet.com

outubro 26, 2023 11:05 AM

914666-B-0-PT