WHITE PAPER

Guia de uso:

Transformação da segurança com Zero Trust

Akamai

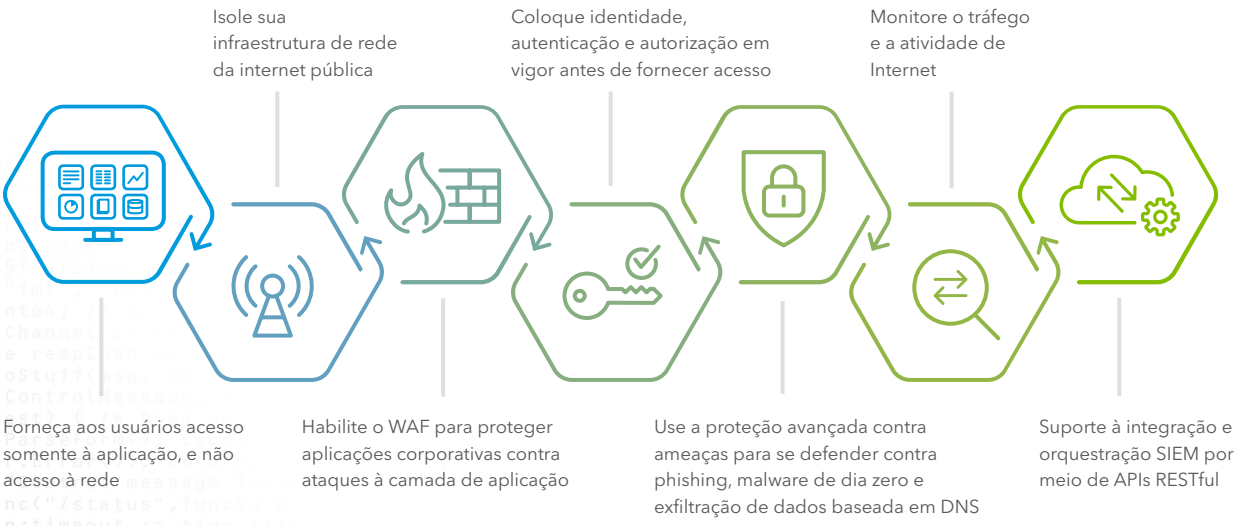
Resumo executivo

A noção de perímetro de rede, em que todos fora da zona de controle da empresa são mal-intencionados e todos dentro dela são honestos e bem-intencionados, já não pode mais ser confiável no atual cenário de negócios. A ampla adoção de aplicações SaaS, a migração para arquiteturas baseadas em nuvem, um número cada vez maior de usuários remotos e um fluxo de dispositivos BYOD tornaram irrelevante a segurança baseada em perímetro. Além disso, uma defesa centrada no perímetro exige o gerenciamento de políticas de segurança e de aplicações, além de upgrades frequentes de softwares, causando complexidade operacional e sobrecarregando equipes de TI que já estão bastante atribuladas. À medida que a superfície de ataque se expande e os recursos de TI limitados lutam para controlar a arquitetura de rede cada vez mais complexa, os criminosos virtuais tornam-se cada vez mais eficientes, sofisticados e incentivados a burlar medidas de segurança. É necessária uma estrutura de segurança estratégica que lide com esses desafios distintos.

O que é segurança Zero Trust e por que ela é importante?

O modelo Zero Trust substitui a arquitetura de segurança centrada no perímetro. Esse método aplica decisões de segurança e de acesso de forma dinâmica, com base na identidade, no dispositivo e no contexto do usuário. Uma estrutura de segurança Zero Trust também estabelece que somente usuários e dispositivos autenticados e autorizados podem acessar aplicações e dados. Ao mesmo tempo, ela protege essas aplicações e os usuários contra ameaças avançadas na Internet.

Para progredir na sua jornada rumo ao modelo Zero Trust e proteger usuários e aplicações, bem como o futuro da sua empresa, sugerimos que você:



Forneça aos usuários acesso somente à aplicação, e não acesso à rede

As tecnologias de acesso remoto legadas, como redes privadas virtuais (VPNs), não são capazes de atender às crescentes demandas das atuais empresas digitais sem perímetro. A VPN tradicional coloca uma ameaça à segurança empresarial, pois ela basicamente abre uma brecha no firewall, fornecendo assim acesso irrestrito à rede. Assim que um invasor adentra, ele está livre para mover-se lateralmente para acessar e explorar qualquer sistema ou aplicação dentro da rede. As VPNs tradicionais não só expõem a empresa a riscos de segurança, mas também são soluções complexas que exigem recursos de TI consideráveis para o gerenciamento de hardware e software, tornando-se custosas para manter e escalonar.

A segmentação de rede, às vezes vista como uma contramedida ao acesso integral, provou ser cara, difícil de implementar e complicada para gerenciar. E, em última análise, ela não reduz o risco: a "permissão de qualquer" acesso ainda permite a movimentação lateral dentro da rede. Embora ele compartimentalize o tráfego leste-oeste dentro de uma sub-rede, não pode impedir a navegação horizontal dentro da mesma sub-rede.

Para proteger sua empresa e permitir o modelo Zero Trust, conceda aos usuários acesso apenas às aplicações necessárias para sua função. Baseie o acesso em privilégios, identidade de usuário, postura do dispositivo, autenticação e autorização. Essas práticas recomendadas reduzirão os ataques laterais, limitando a exposição da rede. A eliminação de VPNs tradicionais melhorará a experiência do usuário, aumentará a produtividade da força de trabalho e reduzirá os tíquetes de suporte técnico. E sair da dependência de firewalls, hardware e software significa reduzir os custos de manutenção de TI. Além disso, as permissões somente para aplicações melhoram a governança, proporcionando visibilidade e insight sobre quem está acessando as aplicações, para onde os dados estão indo e como estão sendo acessados.

Conceda acesso aos usuários somente às aplicações de que precisam, e baseie esse acesso em privilégios, identidade do usuário, postura do dispositivo, autenticação e autorização.

Isole sua infraestrutura de rede da internet pública

Expor aplicações internas e infraestrutura de acesso à Internet as torna vulneráveis a ataques DDoS, injeção de SQL e outros ataques à camada de aplicação. Os criminosos virtuais estão se tornando cada vez mais astutos. Eles usam técnicas em constante evolução para verificar as configurações de rede corporativa e descobrir aplicações vulneráveis e dados valiosos. Dessa forma, as empresas devem isolar a arquitetura de aplicações e de acesso da Internet pública, de modo que não possa ser visada por agentes mal-intencionados que usam portas de escuta abertas. Se os criminosos virtuais não conseguirem encontrar a rede ou determinar quais aplicações e serviços o dispositivo de destino está rodando, eles não poderão atacá-lo.

Ative o Web Application Firewall (WAF) para proteger aplicações corporativas

Os ataques virtuais modernos são hiperdirecionados. Agentes mal-intencionados aproveitam a engenharia social (e-mails, redes sociais, mensagens instantâneas, SMS, entre outros) para enganar indivíduos usando iscas relevantes e personalizadas. Os criminosos virtuais procuram usuários específicos com níveis de experiência, habilidades e acesso desejáveis e, então, iniciam ataques em aplicações direcionados às permissões desses usuários.

Se a máquina de um usuário torna-se comprometida, ela é empregada como dispositivo zumbi e, sem conhecimento do proprietário, executa ataques a aplicações corporativas que supostamente estão seguras por trás do firewall. Embora a maioria das organizações use um firewall de aplicação web (WAF) para proteger suas aplicações com acesso externo contra tais ataques, muitas não estenderam essa proteção às aplicações corporativas dentro da rede. O WAF pode proteger aplicações internas e os dados por trás delas contra ataques de injeção e à camada de aplicação, como injeção de SQL, execução de arquivos mal-intencionados, falsificação de solicitação entre websites (CSRF) e execução de scripts entre websites.

Os criminosos virtuais atacam um dispositivo, o transformam em máquina zumbi e o usam para atacar aplicações consideradas seguras por trás de um firewall.

Coloque identidade, autenticação e autorização em vigor antes de fornecer acesso

Os sistemas digitais concedem acesso a qualquer pessoa que insira a senha correta, sem verificar a identidade da pessoa. Credenciais fracas e reutilização de senhas aumentam significativamente a superfície de ataque e o risco de uma empresa. No atual cenário de ameaças, confiar na autenticação de um só fator, como nome de usuário e senha, não é mais suficiente. A autenticação multifator (MFA) fornece nível extra de verificação e segurança; ela garante que somente usuários validados obtenham acesso a aplicações críticas para os negócios.

A autenticação multifator é essencial. Credenciais fracas e a reutilização de nomes de usuário e senhas entre aplicações, aumentam significativamente a superfície de ataque de uma empresa.

Depois que o usuário é autenticado e autorizado por meio da MFA, o login único (SSO) permite que os usuários façam login em todas as aplicações com um conjunto de credenciais. Isso aumenta a produtividade; não há necessidade de reconfirmar a identidade a cada aplicação e não há problemas de sincronização entre as aplicações. Tomar decisões contínuas de acesso em uma variedade de sinais, incluindo MFA e SSO em aplicações IaaS, locais e SaaS, proporciona maior proteção aos negócios e, ao mesmo tempo, oferece conveniência para os usuários finais.

Use a proteção avançada contra ameaças para se defender contra phishing, malware de dia zero e exfiltração de dados baseada em DNS

Apesar da ampla adoção corporativa da segurança em camadas, agentes mal-intencionados continuam a obter acesso às empresas ao explorar as fraquezas de segurança. Mesmo com firewalls, gateways seguros da Web, sandboxes, sistemas de prevenção de invasões e antivírus de endpoints implantados, as empresas são expostas e tornam-se vítimas de phishing, malware de dia zero e exfiltração de dados baseada em DNS. Então, o que as empresas estão deixando passar?

O DNS é um vetor frequentemente negligenciado. E os criminosos virtuais desenvolveram malware especificamente adaptado para explorar essa lacuna de segurança, evitando camadas de segurança existentes para se infiltrar na rede e extrair dados. Adicionar uma camada de segurança que reforce o protocolo DNS é essencial; ao utilizar essa fase de consulta inicial como ponto de controle de segurança, uma solução de segurança de DNS pode detectar e interromper ataques virtuais no início da cadeia de destruição, protegendo proativamente a empresa.

As empresas devem aproveitar o protocolo DNS como um ponto de controle de segurança, para ajudar a detectar e interromper ataques virtuais no início da cadeia de destruição.

Monitore o tráfego e a atividade de Internet

As empresas devem assumir que o ambiente é hostil. Este é o princípio básico do Zero Trust. Dessa forma, as organizações precisam garantir a auditoria e a confirmação de todas as atividades, em vez de permiti-las sem critérios. Para isso, as empresas devem ter visibilidade do que está acontecendo em suas redes, com amplo tráfego e inteligência para fazer comparações relevantes.

As empresas devem monitorar e verificar todas as solicitações de DNS de dispositivos dentro e fora da rede corporativa, sejam provenientes de notebooks, telefones celulares, desktops, tablets, Wi-Fi para visitantes ou dispositivos de IoT, para garantir que as consultas não sejam direcionadas a websites mal-intencionados ou não aceitáveis. As organizações também devem examinar o comportamento do tráfego em busca de sinais de atividades suspeitas, como a comunicação com um servidor de comando e controle (CnC) ou exfiltração de dados, e alertar imediatamente a TI sobre qualquer problema. Uma visão do volume de tráfego global e das tendências de ameaças facilita para a TI a identificação de padrões irregulares ou perigosos.

Integração de suporte com gerenciamento de evento e informação de segurança (SIEM) e orquestração por APIs RESTful

As empresas podem ter centenas, ou até milhares, de aplicações. Elas demandam configuração via API para implantar rapidamente aplicações em massa, além de definir controles de política para acesso. Essa é uma funcionalidade essencial para qualquer ambiente de aplicação em grande escala que busca migrar rapidamente do tradicional acesso por VPN para o acesso específico por aplicações. A adoção de APIs continua a aumentar à medida que as empresas adotam o DevSecOps e procuram tarefas de monitoramento e configuração disponíveis por API RESTful. Elas também precisam de plug-ins para incorporar dados de ameaças e eventos ao SIEM, para fins de investigação e correlação. Um sistema escalonável também deve se integrar a plataformas de automação de fluxo de trabalho e neutralização de ameaças sinalizando em soluções de detecção e resposta de endpoints de terceiros.

Conclusão

A transformação digital é uma realidade e as empresas devem adotar um modelo de segurança Zero Trust para desenvolver com sucesso os negócios, permitindo inovação e agilidade, sem comprometer a segurança. Proteção avançada contra ameaças, aceleração de aplicações, MFA e SSO em todas as aplicações, SaaS, local e IaaS, são alguns dos principais benefícios de operar em um ambiente Zero Trust. E um modelo de segurança Zero Trust permite a orquestração por meio de API, bem como a integração com SIEM e plataformas de automação de fluxo de trabalho, fornecendo visibilidade dos usuários e aplicações, ao tempo em que facilita implantações de larga escala em menor tempo.

A Akamai pode ajudar a orientar a evolução de sua rede e de sua segurança. Responda a uma Avaliação Zero Trust, de sete perguntas, para entender o nível de adequação de sua empresa a uma estrutura de segurança Zero Trust. Você receberá as etapas seguintes personalizadas para a transformação da rede. Ou, para obter recursos para iniciar sua transição, visite akamai.com/3waystozerotrust.