# Quatro motivos pelos quais sua empresa precisa de segurança Zero Trust

# Índice

# Introdução

À medida que os invasores se tornam mais sofisticados, os grupos de ransomware proliferam e os avanços na tecnologia geram novas vulnerabilidades, as organizações estão optando por um modelo de segurança Zero Trust progressivamente. Fundamentalmente, essa abordagem elimina a confiança implícita atribuída a usuários, aplicativos e dispositivos, o que era o princípio central de abordagens de segurança anteriores. Em termos práticos, existem quatro cenários-chave em que uma organização se beneficiará de um modelo de segurança Zero Trust: um ataque de ransomware contra sua empresa, uma transição para o trabalho remoto, uma necessidade de proteger seu ambiente de nuvem ou uma auditoria futura.

Esses cenários são o resultado de tendências recentes: o aumento dos ataques de ransomware, a transição para uma força de trabalho híbrida, a migração para a computação em nuvem e o aumento das demandas de auditorias de segurança, que exigem uma abordagem de segurança baseada na verificação de identidade, independentemente da localização, e em que medidas proativas sejam tomadas ao lidar com violações. O Zero Trust é a única abordagem que requer que a identificação dos usuários seja feita de modo rigoroso para o acesso dos dados e que fornece mitigação proativa após um ataque.

A implementação de uma estratégia Zero Trust pode parecer um grande desafio para as equipes de segurança já sobrecarregadas, mas não precisa ser. Ao adotar uma abordagem em fases e se concentrar em ganhos rápidos, você pode diminuir parte da complexidade e dos riscos associados às soluções de segurança tradicionais e melhorar sua postura de segurança.

Você não precisa destruir e substituir sua tecnologia existente para começar. Comece alinhando seus investimentos no modelo Zero Trust às suas necessidades comerciais mais urgentes. Opte por um fornecedor de arquitetura Zero Trust confiável em vez de fornecedores que aprimoraram suas tecnologias da noite para o dia e passaram a promover sua antiga solução como uma solução Zero Trust. Considere seriamente um fornecedor que possa combinar vários elementos da segurança Zero Trust (Zero Trust Network Access, firewall de DNS, microssegmentação etc.) em uma única plataforma. Seja qual for o motivo para sua adoção, o Zero Trust permitirá que você tenha agilidade nos negócios, otimização de custos e consolidação de ferramentas, melhorando suas operações gerais.

## Os quatro principais motivos pelos quais as organizações optam pelo Zero Trust

O aumento dos ataques de ransomware

A força de trabalho híbrida

A adoção de recursos de computação em nuvem

Requisitos de conformidade rigorosos

01

# O aumento dos ataques de ransomware

## Aumente sua proteção contra ransomware

Nos últimos anos, os ataques de ransomware trouxeram problemas para organizações em todo o mundo, de hospitais e bancos a pipelines e outras infraestruturas críticas. Inclusive, a **Cybersecurity Ventures** prevê que o ransomware trará prejuízos de aproximadamente 265 bilhões de dólares por ano até 2031. Ela prevê que os criminosos de ransomware lançarão um novo ataque (em um consumidor ou empresa) a cada dois segundos à medida que refinam progressivamente suas cargas de malware e atividades de extorsão relacionadas.

Sem uma estratégia Zero Trust, os grupos de ransomware podem se aproveitar dos seguintes pontos fracos:

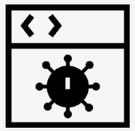
- Confiança implícita atribuída a usuários, aplicativos e redes, que permite a movimentação lateral e a disseminação de malware por invasores que conseguem violar a rede
- Políticas de acesso excessivamente permissivas, que possibilitam infecções e a subsequente injeção de ransomware
- Sistemas que confiam apenas em uma senha, o que oferece uma oportunidade de roubo de credenciais

## Como o modelo Zero Trust ajuda

As empresas que colocam em prática uma arquitetura Zero Trust, têm políticas de controle de acesso e usam a microssegmentação minimizam os danos que um ataque desse tipo pode causar. Em primeiro lugar, os invasores não só acham mais difícil violar o sistema como também são limitados em sua capacidade de expandir.

## Como a Akamai rompe a cadeia de destruição do ransomware

Um ataque de ransomware geralmente envolve uma infecção inicial, movimentação lateral e exfiltração e criptografia de dados. Com o Zero Trust, as organizações podem cuidar de cada etapa à medida que ela acontece — ou mesmo antes que aconteçam.



## Infecção inicial

A Plataforma Akamai Guardicore ajuda a impedir que um ataque se espalhe além do ponto inicial de entrada, enquanto o Akamai MFA protege os usuários contra o roubo e abuso de suas credenciais.

## Movimentação lateral

A Plataforma Akamai Guardicore reduz os caminhos de propagação e ajuda a impedir a movimentação lateral. O Akamai Guardicore Access limita a capacidade do invasor de se movimentar para infectar o aplicativo que planejava explorar. O Akamai Hunt detecta e mitiga ameaças avançadas evasivas em sua rede.

## Exfiltração e criptografia de dados

A Plataforma Akamai Guardicore limita o acesso a aplicativos críticos, impedindo que os invasores acessem dados confidenciais dentro de uma rede comprometida. O Akamai Secure Internet Access Enterprise bloqueia solicitações a websites de phishing e de comando e controle. Por fim, o Akamai Hunt detecta comportamentos irregulares, impedindo que os invasores criptografem dados valiosos que possam ser usados para fins de extorsão.

02

# A força de trabalho híbrida

## Proteja a nova força de trabalho híbrida

A proteção de uma nova força de trabalho híbrida que cresceu e se expandiu devido à pandemia de COVID-19 é mais desafiadora quando as organizações dependem de ferramentas de segurança obsoletas, como firewalls e VPNs. Quando as VPNs de acesso remoto começaram a ser usadas há cerca de 30 anos, tudo era diferente: a Internet estava nos primórdios, os aplicativos eram executados no data center e havia muito menos usuários se conectando de locais remotos. Quando a autenticação dos usuários e seu subsequente acesso a toda a rede continua sendo feita com uma VPN, a superfície de ataque aumenta, possibilitando muitas das vulnerabilidades de dia zero decorrentes de VPNs legadas. Qualquer usuário com as credenciais necessárias pode fazer logon em uma VPN corporativa e, uma vez dentro dela, pode mover-se lateralmente pela rede e acessar os recursos que a VPN foi criada para proteger.

# Como o modelo Zero Trust ajuda

Com base no princípio de acesso de privilégio mínimo, o Zero Trust pressupõe que nenhum usuário ou aplicativo seja inerentemente confiável. O Zero Trust Network Access (ZTNA) adota uma abordagem completamente diferente das VPNs para proteger o acesso de funcionários remotos. Em vez de arriscar toda a rede, os usuários são conectados diretamente apenas aos aplicativos e aos dados de que precisam, evitando a movimentação lateral de usuários mal-intencionados com acesso excessivamente permissivo a dados e recursos confidenciais. Em caso de violação, uma solução de microssegmentação Zero Trust eficaz pode segmentar a rede interna para que a violação não se espalhe e danifique outras partes da rede. De acordo com a **Gartner**, até 2025, pelo menos 70% das novas implantações de acesso remoto serão executadas principalmente pelo ZTNA e não por serviços de VPN, sendo que esse percentual era de menos de 10% em 2021.

# Como a Akamai facilita o trabalho híbrido e remoto

A abrangente plataforma Zero Trust da Akamai atende às necessidades de sua força de trabalho híbrida. Os benefícios incluem:

## Risco reduzido

A Akamai conecta diretamente o usuário certo ao aplicativo certo, reduzindo a superfície de ataque e limitando a movimentação lateral.

## Experiência do usuário aprimorada

Os usuários remotos desfrutam do acesso aos recursos independentemente do aplicativo, dispositivo ou localização, eliminando a necessidade de conexão e desconexão da VPN.

## Mais agilidade

Dado que a solução da Akamai é consumida como um serviço, as organizações não precisam implantar hardware nem se preocupar com o escalonamento à medida que as demandas aumentam, o que reduz os custos e a complexidade.

# 03

# A adoção de recursos de computação em nuvem

## Facilite a migração para a nuvem

As organizações estão migrando seus aplicativos para a nuvem a fim de obter flexibilidade e agilidade e modernizar sua infraestrutura. No entanto, esses ambientes de nuvem estão expandindo a superfície de ataque e gerando novos requisitos de segurança. As integrações entre diferentes nuvens e ambientes locais podem gerar falhas nos aplicativos e colocar a segurança em risco. Quando as organizações tentam migrar seus aplicativos para a nuvem usando estruturas de rede tradicionais — VPNs e firewalls —, elas muitas vezes enfrentam um risco maior de ameaças laterais, baixa escalabilidade e altos custos. Mesmo após a conclusão da migração, os ativos ainda precisam ser protegidos, e os usuários devem ser autenticados com base em permissões de função. Os usuários de infraestruturas de nuvem normalmente têm maior acesso a recursos, serviços e direitos de gerenciamento do que teriam com ambientes locais, o que gera riscos adicionais e o potencial de interrupção.

# Como o modelo Zero Trust ajuda

As estratégias de segurança Zero Trust facilitam a migração para a nuvem. O modelo Zero Trust elimina a confiança implícita inerente a muitos aplicativos baseados em nuvem, particularmente aplicativos de terceiros, que podem trazer vulnerabilidades. As soluções Zero Trust garantem que as organizações possam implantar mais facilmente seus aplicativos baseados em nuvem com proteções mais fortes. Alguns dos benefícios da implantação do modelo Zero Trust para a nuvem incluem:

- ☑ Melhor visibilidade dos ativos e riscos
- ☑ Superfície de ataque reduzida com segmentação Zero Trust e acesso de privilégio mínimo aos recursos de nuvem
- ☑ Infraestrutura de rede modernizada que oferece velocidade e agilidade
- ☑ Redução do custo operacional e da complexidade

# Como a Akamai melhora a migração para a nuvem

As soluções Zero Trust da Akamai podem ajudar você a migrar automaticamente seus ativos e as respectivas políticas. Não há tempo de inatividade e nenhuma interrupção nos negócios. A Akamai oferece:

## Maior visibilidade

Com melhor compreensão das dependências de apps, você pode criar políticas eficazes de segmentação de nuvem para reduzir a superfície de ataque e minimizar o risco.

## Zero Trust Network Access

Os usuários só podem se conectar aos aplicativos que estão autorizados a acessar com base em autenticação robusta.

## Busca por ameaças

A equipe dedicada de caçadores de ameaças da Akamai busca continuamente comportamentos de ataque atípicos em ambientes de nuvem e notifica os clientes da Akamai sobre qualquer risco para sua rede.

04

# Requisitos de conformidade rigorosos

## Simplifique a conformidade e reduza os riscos

Embora os líderes de segurança saibam que o cumprimento dos requisitos de conformidade não garante uma organização totalmente segura, as auditorias de segurança ainda são muito importantes para as equipes executivas. Elas sabem que a reprovação em auditorias pode levar a grandes interrupções nos negócios e afetar os resultados. Uma avaliação de conformidade é uma das atividades que mais consomem tempo e recursos das equipes de segurança. Além disso, a mudança para ambientes digitais sem perímetro e a prevalência do trabalho remoto tornaram isso ainda mais difícil. As organizações normalmente precisam isolar seus ambientes e delimitar seus ativos regulamentados para atender aos padrões de conformidade, como o PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act) e SWIFT (Society for Worldwide Interbank Financial Telecommunication).

As organizações também precisam acomodar usuários remotos, usuários corporativos no local, parceiros, fornecedores e mais, o que torna quase impossível definir o perímetro do ambiente de uma organização. À medida que as equipes de segurança se preparam para auditorias nas quais o controle do acesso é um grande fator de sucesso, elas devem abordar as seguintes perguntas:

- Como podemos restringir o acesso a informações confidenciais somente a usuários autorizados?
- Como podemos definir o escopo do ambiente de auditoria?
- Como podemos tornar o processo de auditoria mais simples e menos caótico?

## Como o modelo Zero Trust ajuda

Felizmente, uma abordagem Zero Trust pode ajudar a resolver todas essas perguntas e muito mais. Os dois principais pilares da segurança Zero Trust — a capacidade de verificar explicitamente e aplicar o princípio de acesso de privilégio mínimo — simplificam bastante o processo de conformidade. As organizações podem isolar seus ativos regulamentados de outras fontes de tráfego no data center ou na nuvem e permitir o acesso com base em identidades, independentemente do local. A visibilidade aprimorada mostra o que está entrando e saindo do ambiente regulamentado e ajuda a identificar o que está no escopo. Isso reduz bastante a complexidade e o custo da auditoria e facilita a vida do auditor.

# Como a Akamai facilita a conformidade

O abrangente portfólio Zero Trust da Akamai ajuda você a se preparar para todas as auditorias, sejam do PCI DSS, HIPAA, International Standards Organization (ISO), Sarbanes–Oxley (SOX) ou qualquer outra estrutura. O Akamai Enterprise Application Access controla o acesso de terceiros a informações pessoais confidenciais, atendendo aos requisitos do GDPR (General Data Protection Regulation). A Akamai Guardicore Segmentation melhora a compreensão dos ativos regulamentados sob o PCI DSS, isola as funções da câmara de compensação para lidar com a HIPAA, restringe o acesso à Internet e isola sistemas críticos para atender as normas da SWIFT. O Akamai MFA protege as informações de pacientes regulamentadas pela HIPAA contra invasores que obtiveram senhas de sistemas de saúde e reforça a conformidade com as normas da SWIFT ao impedir o comprometimento de credenciais.

# Banco global alcança conformidade com as normas da SWIFT em duas semanas

Autoridades reguladoras externas exigiram que um dos clientes da Akamai, um banco global, isolasse todos os seus aplicativos críticos para atender aos requisitos da SWIFT, garantindo a segurança de transferências monetárias entre instituições financeiras. Normalmente, um aplicativo como esse requer mais de 100 servidores implantados em locais diferentes, incluindo servidores bare-metal e virtuais. Em média, em um banco do porte desse cliente, o planejamento e a execução desse processo poderiam levar entre 8 e 12 meses, pois seria necessário criar uma VLAN (rede de área local virtual) para o segmento em vários locais. Descobrir as dependências do aplicativo da SWIFT e certificar-se de que o conjunto de regras estivesse correto e não teria falhas seria apenas um acréscimo à linha do tempo. Enquanto isso, o projeto também exigiria a compra de novos equipamentos de firewall. E, como o aplicativo da SWIFT é fundamental para os negócios bancários, o banco não poderia tolerar tempo de inatividade. No geral, imaginava-se que o projeto de segmentação exigiria um enorme esforço de muitas pessoas. Mas, com a Akamai, todo o processo precisou de aproximadamente duas semanas e apenas um engenheiro de segurança para ser concluído; ele não exigiu nenhuma alteração de rede, e o banco evitou alterações no aplicativo e tempo de inatividade.

# Simplifique e acelere a conformidade

## Banco global

- Necessidade de isolamento do aplicativo da SWIFT
- Ambiente complexo com servidores bare-metal, VMware e OpenStack

## Segmentação tradicional

- Dificuldade na definição de segmentos em uma infraestrutura complexa
- Ausência de visibilidade de aplicativos e dependências
- Exige tempo de inatividade
  Duração: 8–12 meses
  Pessoas envolvidas: pelo menos 5

## Akamai Guardicore Segmentation

- Mapeamento do aplicativo da SWIFT concluído em horas
- Políticas de segmentação automaticamente sugeridas e ajustadas
- Ausência da necessidade de comprar e implantar novo hardware e firewalls
- Não exige tempo de inatividade
  Duração: 2 semanas
  Pessoas envolvidas: 1 arquiteto

# Saiba mais sobre como atender às suas necessidades comerciais com o portfólio Zero Trust da Akamai

Saiba mais

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em **akamai.com** e **akamai.com/blog**, ou siga a Akamai Technologies no **X**, antigo Twitter, e **LinkedIn**. Publicado em 09/24.