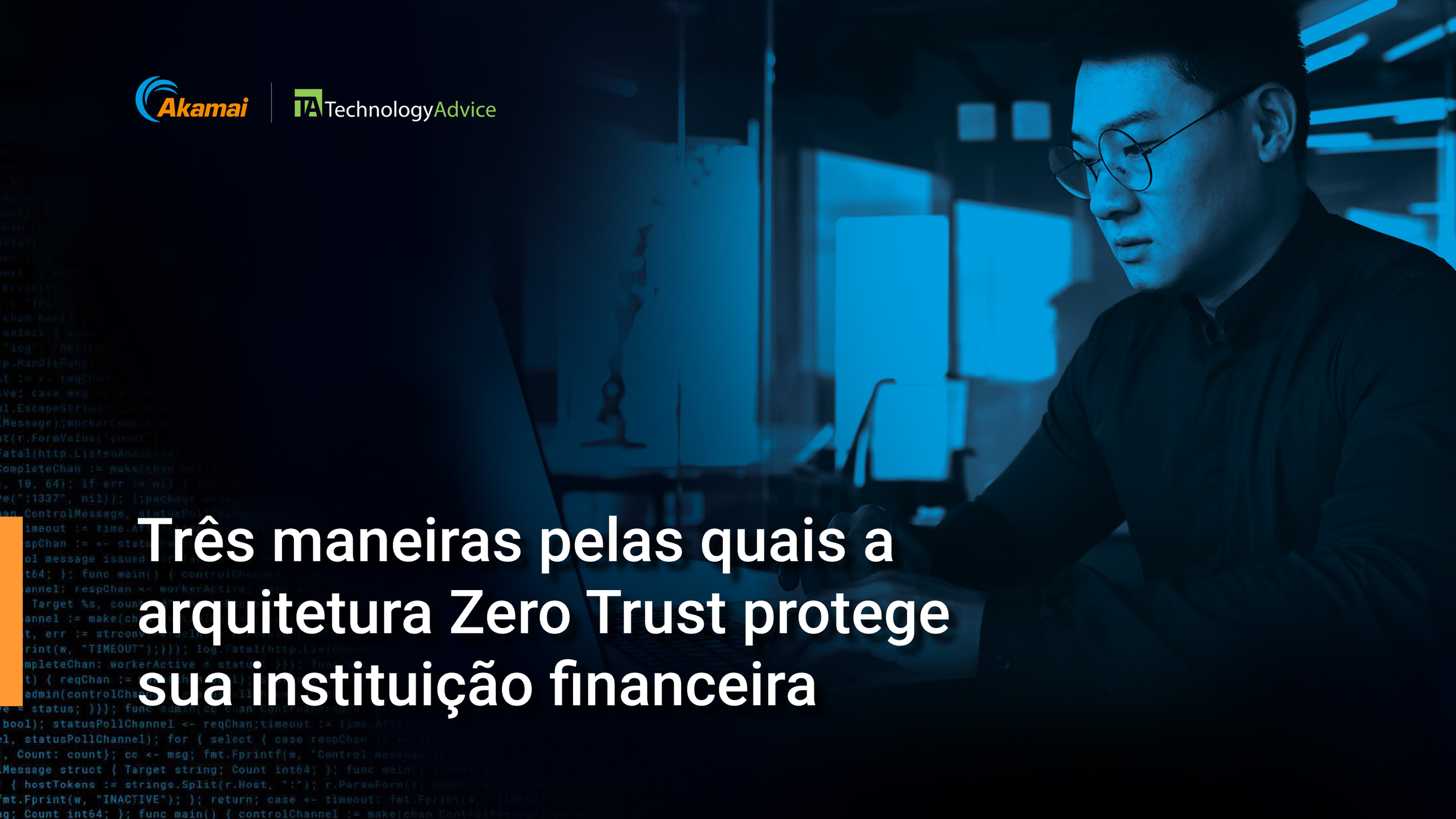
Akamai | TechnologyAdvice



Três maneiras pelas quais a arquitetura Zero Trust protege sua instituição financeira

As instituições financeiras continuam sendo grandes alvos dos agentes de ameaças, com um aumento de 65% em ataques a aplicações da Web e APIs ao comparar o segundo trimestre de 2022 com o segundo trimestre de 2023. Além de esgotar recursos, esta onda implacável e crescente de ciberameaças também desvia o foco que deveria estar em funções comerciais essenciais.

As soluções tradicionais de firewall e ponto de extremidade confiam implicitamente em pontos de extremidade, dispositivos e usuários que passam pela triagem inicial de uma combinação de senha e nome de usuário, ocasionalmente reforçada com a autenticação multifator (MFA). Aplicações, APIs e serviços de sistema na rede geralmente operam sem triagem de segurança além do monitoramento básico de malware em pontos de extremidade. Para enfrentar as crescentes ameaças de ransomware, as rigorosas regulamentações de conformidade e os desafios da migração para a nuvem, as instituições financeiras agora estão adotando o Zero Trust.

O Zero Trust elimina a confiança implícita e verifica continuamente as permissões de acesso de todos os usuários, dispositivos e aplicações com base no contexto da solicitação e das permissões. Mesmo que um invasor consiga comprometer um dispositivo ou credenciais para acessar uma rede, o acesso pode ser rigorosamente restrito e os danos altamente reduzidos.

Mas como exatamente a estrutura Zero Trust protege sua instituição financeira?

Cumprir os regulamentos em constante mudança

As instituições financeiras devem dedicar recursos significativos para provar a conformidade com diversas regulamentações, como o bem estabelecido Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS), ou a iminente Lei de Resiliência Operacional Digital (DORA), que deverá ser totalmente aplicada em janeiro de 2025. As auditorias aumentam regularmente em termos de complexidade, custo e tempo devido a requisitos pouco claros, conflituantes e mutáveis. Entretanto, as instituições financeiras precisam fazer os investimentos necessários, pois os resultados negativos em auditorias também podem levar à perda de receita, sanções regulamentares, multas ou penalidades, bem como perda de reputação e possíveis responsabilidades legais.

Os relatórios de conformidade exigem registros claros e precisos dos sistemas que lidam com dados regulamentados, além de solicitar provas de que esses sistemas estão adequadamente protegidos. No entanto, em uma grande instituição financeira, o ambiente de TI é grande, detalhado e complexo demais para rastrear facilmente os ativos e o acesso.

Os firewalls herdados e a proteção de pontos de extremidade rastreiam e protegem principalmente usuários e ativos tradicionais. Confiar nessa abordagem convencional de segmentação de rede coloca desafios no dimensionamento das operações, dificulta a criação e aplicação de políticas e limita a agilidade.

Para superar os desafios de ambientes herdados com tecnologias alinhadas a estratégias futuras, as instituições financeiras precisam de visibilidade granular do tráfego leste-oeste e da capacidade de aplicar políticas de segmentação em ambientes multinuvem e de contêineres. Com a crescente necessidade de gerenciar múltiplas regiões e tipos de infraestrutura de TI, incluindo tecnologia de contêineres, as instituições financeiras precisam do caminho mais simples e direto para a microssegmentação com flexibilidade de políticas, integração de DevOps e automação.

Sem identificação, rastreio e segurança regulares de todos os recursos, uma instituição financeira não pode garantir que o acesso aos dados regulamentados seja totalmente controlado e protegido. Ignorar ou monitorar inadequadamente dados, usuários, aplicações ou dispositivos aumenta consideravelmente os riscos de um ataque cibernético e a possibilidade de reprovação em uma auditoria de conformidade.

A arquitetura Zero Trust nega o acesso por padrão, e todas as conexões devem ser explicitamente aprovadas de acordo com o contexto: o usuário autorizado, em um dispositivo autorizado, com acesso autorizado aos dados solicitados. O Zero Trust tem como padrão o acesso com privilégios mínimos, o que interfere em conexões herdadas esquecidas ou desconhecidas. A solução da Akamai identifica rapidamente dispositivos não autorizados, usuários herdados (humano, API ou aplicação) e fontes de dados esquecidas que infestam filiais mais antigas ou ambientes tecnológicos herdados de empresas adquiridas.

A arquitetura Zero Trust da Akamai aplica-se independentemente da localização do usuário, mas o contexto da localização pode ser incluído no processo de decisão de acesso. As equipes de segurança obtêm o controle e os relatórios consolidados necessários para analisar rapidamente e gerenciar totalmente o acesso aos recursos em redes locais, data centers ou na nuvem.

No meio da crescente pressão regulamentar para proteger aplicações críticas e o tráfego leste-oeste, as instituições financeiras estão se concentrando em melhorar a visibilidade e a compreensão dos seus ambientes. Com os princípios Zero Trust, elas agora podem identificar e segmentar de forma integrada ativos que não estão em conformidade, capacitando as equipes de aplicações a gerenciar as políticas de segmentação de forma autônoma. Isso garante um fluxo de trabalho eficiente e simplifica o processo de geração de relatórios.

A visibilidade completa e rica em contexto do tráfego leste-oeste facilita o mapeamento e a delimitação sem esforço de aplicações essenciais aos negócios, sem alterações na infraestrutura ou nas aplicações. Esse recurso permite que as instituições restrinjam o acesso de terceiros e reforcem a segurança geral.

A aquisição de visibilidade agiliza a migração segura para a nuvem, enquanto a integração da segmentação no ciclo DevOps garante atualizações imediatas de políticas sem modificações substanciais na infraestrutura, o que contrasta com as práticas anteriores de VLANs. Além disso, a Akamai permite e simplifica a criação, aplicação e geração de relatórios de políticas de conformidade em diversas infraestruturas de maneira uniforme. Isso é alcançado por meio de maior visibilidade, mapeamento de dependências de aplicações, políticas de segmentação automatizadas, automação de políticas de DevOps e integração perfeita de gerenciamento de mudanças.

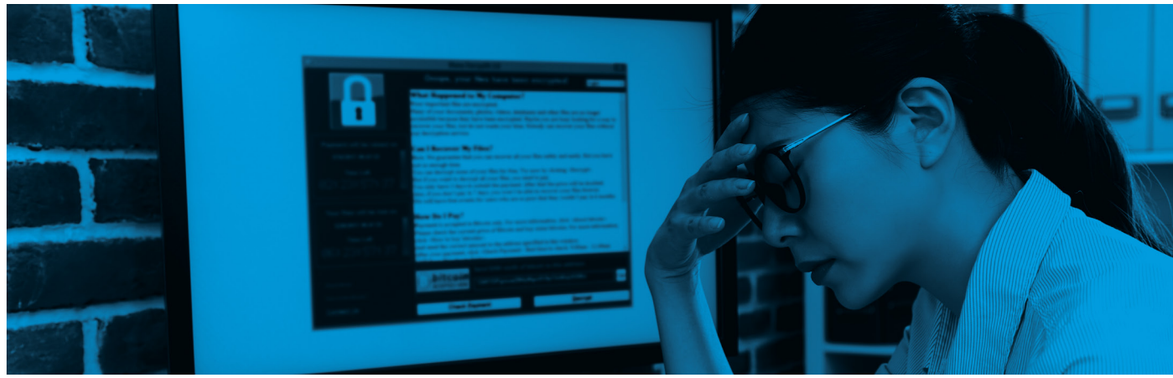
Impedir a propagação de ransomware

Desde filiais até instituições financeiras globais, os ataques de ransomware chegam às manchetes e causam dores de cabeça em todo o mundo. "Espera-se que ataques de ransomware atinjam uma empresa, um consumidor ou um dispositivo a cada dois segundos até 2031", de acordo com o 2022 Ransomware Market Report (Relatório de mercado sobre ransomware de 2022) da Cybersecurity Ventures.

Como as instituições de serviços financeiros crescem frequentemente por meio de fusões e aquisições, elas muitas vezes não têm visibilidade de todo o seu ecossistema tecnológico, deixando brechas para os invasores. Os agentes de ransomware exploram essas brechas ou usam ataques de phishing para roubar credenciais ou lançar malware desconhecido em pontos de extremidade que escapam da respectiva proteção.

As políticas de acesso de usuários excessivamente permissivas e a autenticação centrada em senhas permitem que os invasores burlem firewalls, evitem a detecção em pontos de extremidade e obtenham acesso irrestrito a redes que confiam implicitamente no tráfego, nos usuários e nos dispositivos conectados. Os agentes de ransomware, muitas vezes operando em grupos organizados, como o CL0P, exploram ativos comprometidos e depois movem-se lateralmente pela rede para descobrir e explorar outros ativos vulneráveis. Vulnerabilidades de dia zero, como a vulnerabilidade de injeção de SQL do MOVEit, permitem que os invasores obtenham acesso e espalhem o ataque rapidamente usando scripts automatizados para criptografar sistemas, roubar dados e lançar solicitações de resgate.

As soluções Zero Trust da Akamai capacitam as instituições financeiras a identificar e isolar sistemas críticos e a restringir o acesso à rede de e para esses sistemas. Essa abordagem minimiza a probabilidade, o impacto e o tempo necessário para remediar um ataque de ransomware. Inicialmente, a Akamai rastreia e monitora domínios e endereços IP maliciosos, implementando blocos de quarentena apropriados para evitar o lançamento de diversos ataques.



Em seguida, com visibilidade quase em tempo real do tráfego de rede, a Akamai observa e controla o tráfego até os níveis de processo e serviço. Essa visibilidade aprofundada capacita as equipes do centro de operações de segurança e do centro de operações de rede para identificar e atingir com precisão as ameaças específicas em questão.

Além disso, mesmo um ataque bem-sucedido terá seu escopo fortemente limitado pela microssegmentação inerente à Akamai Guardicore Segmentation. As credenciais e permissões serão verificadas continuamente a cada solicitação de acesso, e as conexões com aplicações protegidas pelo Akamai Enterprise Application Access serão negadas.

Além disso, aplicações, servidores e outros recursos não exigidos por um usuário são automaticamente ocultados da descoberta, o que impede qualquer movimento lateral ou extensão de acesso para invasores. Por fim, a detecção de anomalias do Akamai Hunt sinalizará comportamentos incomuns para alertar as equipes de segurança para ajudar a identificar ataques antes que os dados possam ser exfiltrados ou criptografados.

Agilizar a transformação digital

Para permitir agilidade, escalabilidade e modernização, muitas instituições financeiras movem aplicações para a nuvem. No entanto, tal medida traz uma série de novos desafios.

Para começar, as instituições financeiras não podem migrar recursos e conexões não detectados e desconhecidos. Além disso, não apenas as migrações para a nuvem expandem a superfície de ataque, mas as integrações multinuvem e de nuvem híbrida local geralmente invalidam as aplicações e introduzem lacunas nas camadas de segurança estabelecidas. Além disso, a infraestrutura implantável de software (contêineres, máquinas virtuais etc.) é implantada automaticamente com muita rapidez para proteger ou monitorar de forma eficaz com o uso de soluções herdadas.

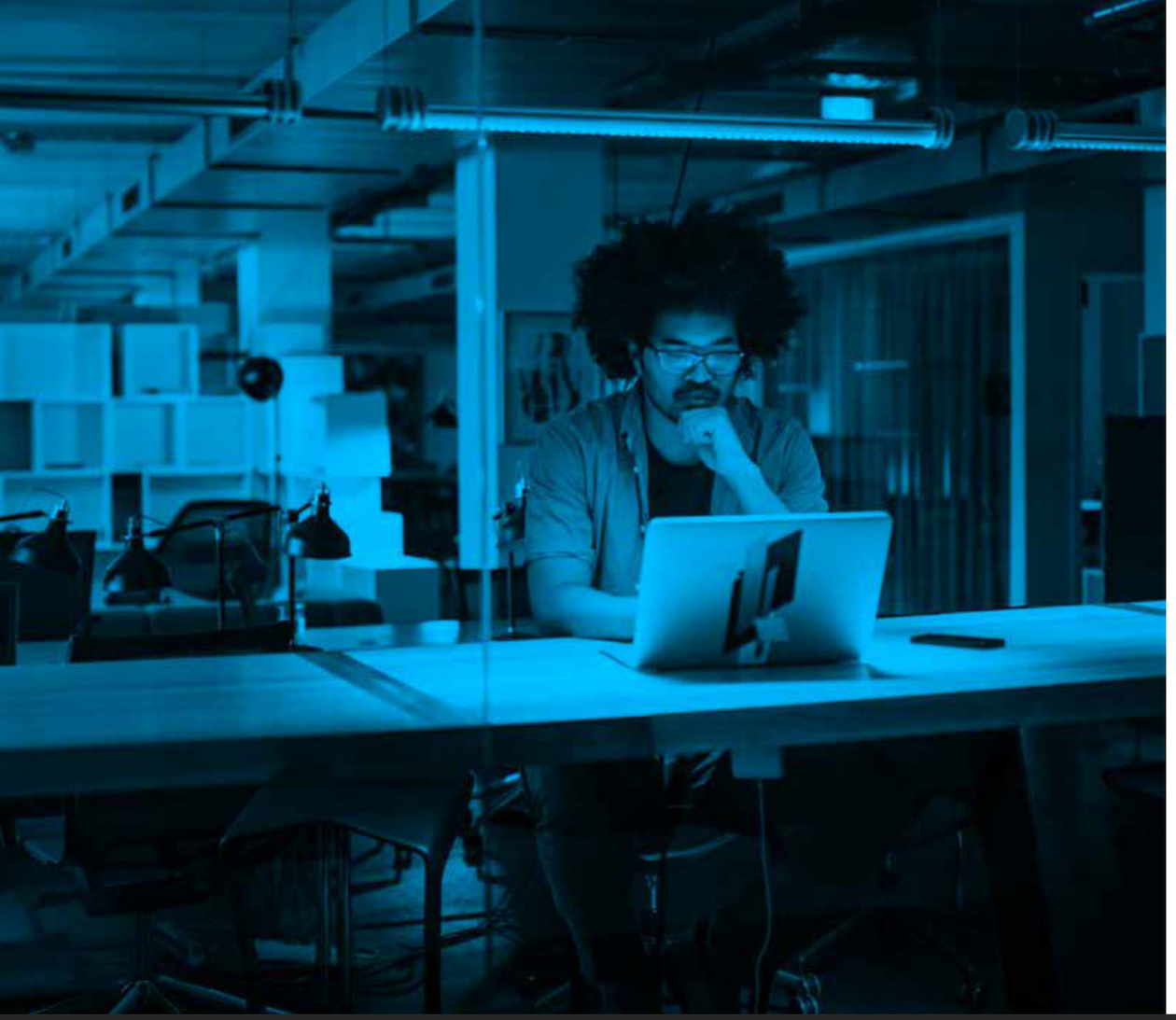
As soluções Zero Trust garantem que as instituições financeiras possam implementar mais facilmente suas aplicações baseadas na nuvem, com proteções mais fortes e despesas operacionais reduzidas. As soluções Zero Trust da Akamai rastreiam todos os fluxos de dados para identificar rapidamente a superfície de ataque em potencial e aplicar políticas sem interromper os negócios.

Uma vez identificada, as equipes de segurança e operações podem usar o controle centralizado da Akamai para segmentar e proteger aplicações e monitorar fluxos de dados. A Akamai oferece controle granular e, ao mesmo tempo, reduz custos operacionais e a complexidade. Para as equipes de segurança e operações das instituições financeiras, a aplicação de políticas universais garante uma modernização ágil da infraestrutura. Isto acontece graças à segurança robusta da segmentação Zero Trust com privilégios mínimos, que fornece um escudo poderoso contra ameaças em evolução.

As instituições financeiras não podem se dar ao luxo de ignorar o Zero Trust

Os ataques a tecnologias herdadas podem levar a grandes violações de dados, causar danos muitos caros e destruir a confiança de clientes e parceiros. Os ataques estão se tornando mais sofisticados e rápidos e, sem visibilidade total do ecossistema técnico, as instituições financeiras podem estar deixando lacunas abertas.

A Akamai oferece maior visibilidade de rede, limita de forma inteligente o acesso dos usuários, caça ameaças continuamente e sinaliza quaisquer anomalias para análise de segurança. Saiba mais sobre como atender às necessidades da sua instituição financeira com o portfólio Zero Trust da Akamai.



Saiba mais sobre como proteger seus fundos digitais com a Akamai

Saiba mais

TechnologyAdvice | Akamai

A Akamai protege a experiência dos seus clientes, sua força de trabalho, seus sistemas e seus dados ajudando a integrar a segurança a tudo o que você cria, em qualquer lugar que você cria e entrega. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para alcançar o Zero Trust, interromper ransomware, proteger apps e APIs e combater ataques de DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. 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.