Akamai

WHITE PAPER

Mapa estratégico para uma postura de segurança de classe mundial

Tenha um plano de transformação personalizado com base em Zero Trust

Para garantir que a Akamai não se acomode e permaneça protegida em um ambiente de segurança em constante evolução, recentemente avaliamos nosso desempenho de segurança com base no Modelo de Maturidade Zero Trust, ou ZTMM (Zero Trust Maturity Model). Aqui, compartilhamos como é possível aplicar esse processo em sua própria organização e identificar áreas críticas de melhoria, a fim de desenvolver um claro plano estratégico rumo a uma postura de segurança de classe mundial.

Simplifique a jornada rumo ao Zero Trust

O acesso e a segurança de uma empresa são complexos e estão em constante mudança. Nesse cenário, pode ser desafiador saber onde concentrar os esforços ao adotar uma postura de segurança Zero Trust.

Por isso, recomendamos o uso do ZTMM como ferramenta para avaliar e visualizar sua postura de segurança atual. Usamos essa solução para avaliar nossa própria postura de segurança corporativa na Akamai, bem como as posturas de segurança de vários clientes. No final do processo, você terá um mapa estratégico de ações que o deixarão mais perto de uma arquitetura Zero Trust. (Consulte o Apêndice A para mais informações sobre o conceito Zero Trust.)

Por que o Zero Trust Maturity Model faz sentido

Para nós, o passo inicial rumo à implementação de uma postura de segurança mais robusta é o mais importante. No entanto, quando se trata do tópico complexo e em constante mudança da cibersegurança, começar é mais difícil do que parece. Observamos que muitas organizações enfrentam desafios ao decidir o que implementar, em que medida e em qual ordem para alcançar o Zero Trust.

É aqui que o ZTMM entra em ação. O ZTMM cria uma estrutura em torno do Zero Trust, proporcionando uma sensação de linearidade que facilita a implementação. O ZTMM ajuda as organizações a criar um plano de mudança e um orçamento para atualizações. O ZTMM também explica os conceitos de Zero Trust para os responsáveis pela tomada de decisões que não são especialistas em TI, ajudando equipes de TI a obter a adesão necessária.

O ZTMM é testado e aprovado. O ZTMM foi desenvolvido pela CISA (Agência de Segurança de Infraestrutura e Cibersegurança) dos EUA e tem sido amplamente adotado nas agências federais dos EUA.

Os cinco pilares e três recursos do Zero Trust Maturity Model

O ZTMM consiste em um gradiente de implementação em cinco pilares distintos, de modo que pequenos avanços possam ser feitos ao longo do tempo. Os pilares envolvem considerações sobre Identidade, Dispositivos, Redes, Aplicativos e Cargas de trabalho, e Dados (Figura 1).
O ZTMM também inclui considerações sobre três recursos que perpassam os cinco pilares:

- Visibilidade e análise
- Automação e orquestração
- Governança

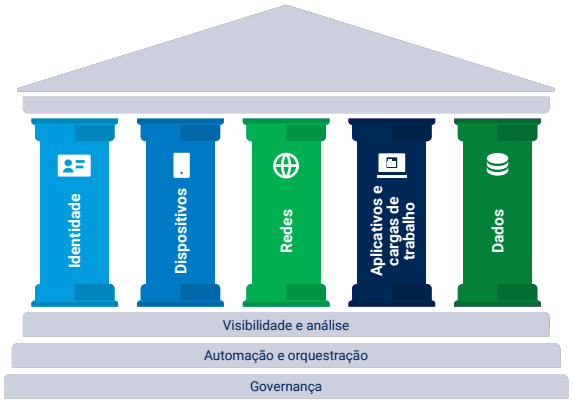


Fig. 1: O ZTMM da CISA é um dos muitos caminhos de apoio à transição para Zero Trust (Fonte: CISA)

Cada uma dessas áreas recebe um status de maturidade descrevendo a proximidade de uma organização para alcançar uma abordagem Zero Trust. Os quatro estágios de maturidade (Tradicional, Inicial, Avançado e Ideal) descrevem a jornada da configuração manual e VPNs para uma configuração ideal de "segurança sem limites" (Figura 2). Na maturidade Ideal, organizações concedem privilégios mínimos aos aplicativos, negam autenticação e acesso a dispositivos vulneráveis, impedem que as ameaças internas se espalhem e detectam e respondem imediatamente a incidentes de segurança. (Consulte o Apêndice B para uma descrição mais detalhada da estrutura ZTMM.)

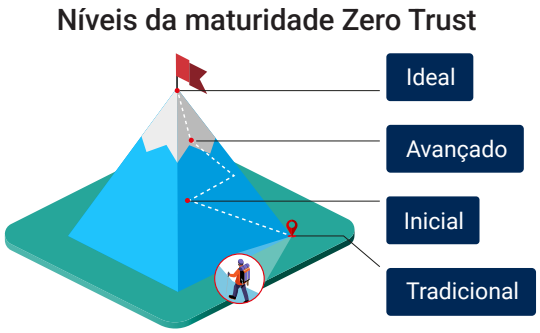


Fig. 2: Os níveis da maturidade Zero Trust (fonte: CISA)

Ao destacar áreas em que a maturidade é mais baixa, o ZTMM ajuda as organizações a desenvolver um ambiente de segurança mais equilibrado. O conjunto de soluções de segurança líder do setor da Akamai, combinado com nossa experiência, está facilitando como nunca a jornada rumo a uma postura de segurança madura.

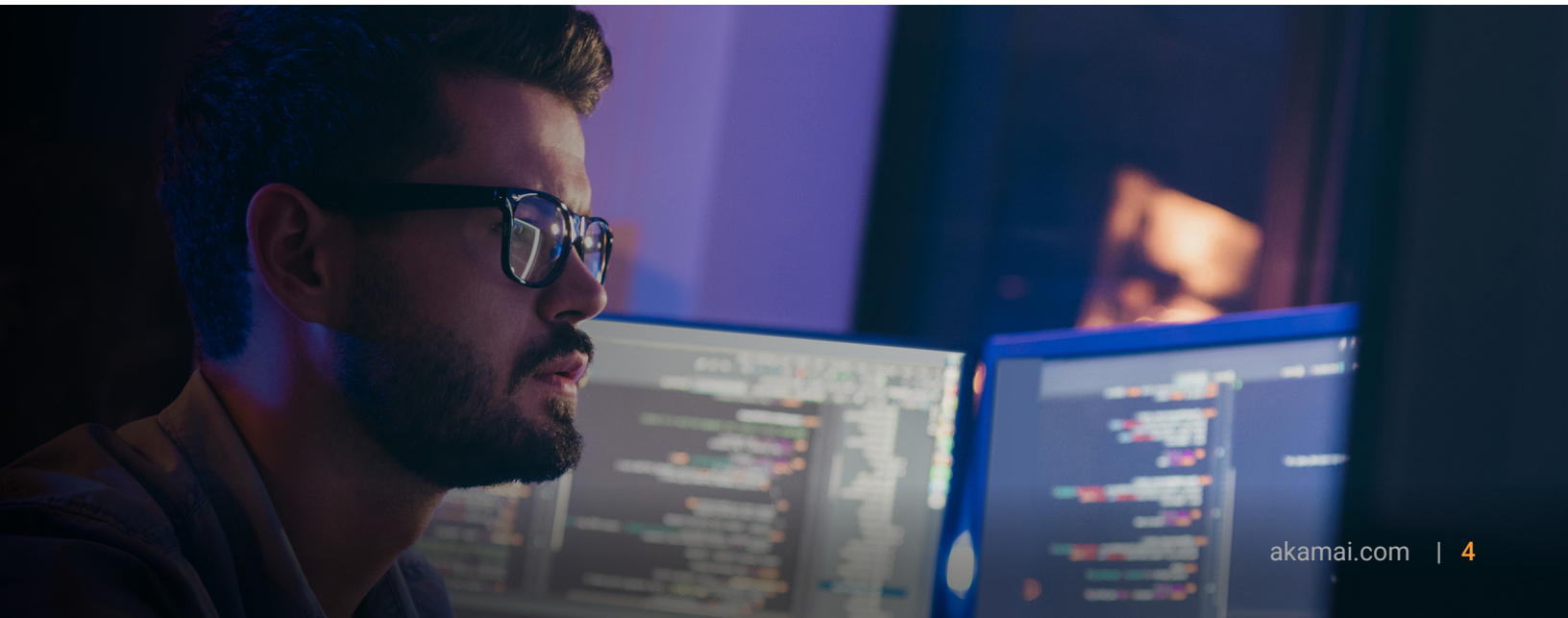
Suas equipes estão com dificuldade para implementar o Zero Trust? Não é só você.

A responsabilidade de criar uma arquitetura Zero Trust não é de apenas um departamento. É algo que requer adesão, flexibilidade e aprovação de uma série de partes interessadas em todos os níveis de uma organização.

A Akamai é a empresa de cibersegurança e computação em nuvem que potencializa e protege negócios online. Nossas soluções de segurança, inteligência avançada contra ameaças e equipe de operações globais, todas líderes no mercado, protegem dados e aplicativos essenciais em todos os pontos de contato, em todo o mundo. Essa visão abrangente significa que compreendemos os desafios mais comuns quando se trata de adotar uma postura de segurança Zero Trust, e podemos ajudar você a encontrar soluções.

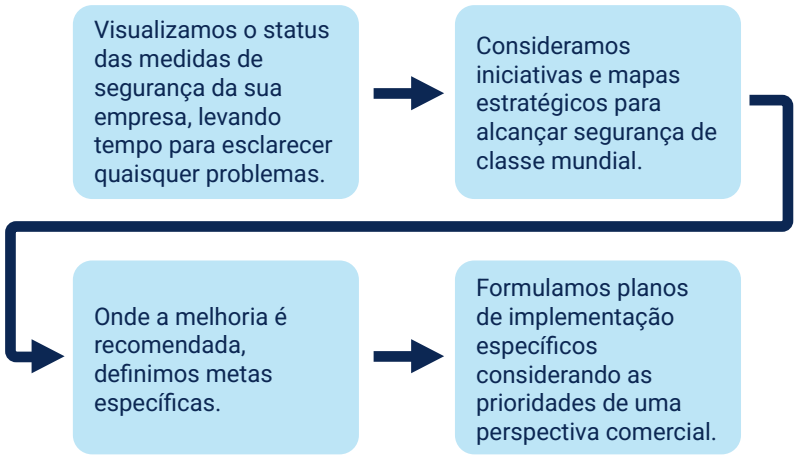
Três desafios Zero Trust comuns

1. **Saber onde começar.** Normalmente, recomendamos começar com a visibilidade da carga de trabalho e reduzir a superfície de ataque para reforçar a resiliência cibernética. Contudo, isso depende, é claro, da postura de segurança atual da organização.
2. **Alcançar o sucesso com rapidez.** Alcançar o Zero Trust pode parecer uma tarefa tão complexa que fica difícil para as equipes se concentrar em algo específico ou comemorar os pequenos passos dados em direção ao objetivo.
3. **Demonstrar o ROI.** Projetos Zero Trust não são baratos, e geralmente exigem mudanças culturais e tecnológicas dentro de uma organização. A capacidade de demonstrar o retorno do investimento – seja uma superfície de ataque reduzida, uma violação mitigada, uma vulnerabilidade protegida ou uma vitória financeira – é fundamental, especialmente para os decisores e líderes de segurança.



Tudo pronto para começar a jornada Zero Trust e visualizar sua postura de segurança?

Como fizemos na Akamai, você pode usar o ZTMM para visualizar o status de maturidade das medidas de segurança atuais de sua organização. Isso ajudará a destacar como você pode trazer mais equilíbrio para o seu processo e o que precisa mudar para alcançar uma arquitetura Zero Trust.



Como a Akamai pode guiar você em direção a uma postura de segurança Zero Trust

Uma arquitetura Zero Trust bem-sucedida usa uma variedade de controles e princípios para lidar com os desafios de segurança.

Consideraremos iniciativas e mapas estratégicos para ajudar você a criar um plano de implementação que leve toda a sua empresa e seus objetivos em consideração, para alcançar segurança de nível mundial. Essa abordagem nos permite trabalhar juntos para criar sistemas e processos de segurança que sejam eficazes e sustentáveis a longo prazo.

Juntamente com a Akamai Cloud, nosso conjunto de produtos de segurança (incluindo uma solução ZTNA distribuída avançada, microssegmentação líder do setor, MFA (autenticação multifator) à prova de phishing e um firewall DNS proativo) levará sua postura de segurança até o nível Ideal da escala de maturidade Zero Trust. Além disso, todo o sistema pode ser executado por apenas um agente, usando apenas um console (Figura 3).

Fig. 3: O conjunto de produtos de segurança da Akamai pode ser executado por apenas um agente, usando apenas um console

Estudo de caso

Visualização da postura de segurança de e-commerce de um varejista multinacional usando o Zero Trust Maturity Model

Recentemente, analisamos a postura de segurança de e-commerce de um varejista multinacional, visualizando seu status de segurança e apresentando um mapa estratégico correspondente para aproximá-lo de uma postura de segurança de classe mundial. Nossa equipe de especialistas identificou áreas de melhoria em todo o ZTMM, que classificamos em importância de alta para baixa. Aqui, compartilhamos os resultados.

Um sistema desequilibrado com variação na implementação

Em cada pilar, descobrimos que algumas funções foram implementadas no nível mais alto (Ideal) de maturidade, como o gerenciamento de dispositivos móveis e a automação da implantação de aplicativos. No entanto, algumas funções em cada pilar permaneciam no nível Tradicional, o que apresentava sérios riscos.

Em particular, funções importantes nos pilares Identidade e Rede, que são a base de uma arquitetura Zero Trust, não foram reforçadas. Essas funções incluíam MFA, gerenciamento integrado de infraestrutura de identidade, controle de acesso baseado em contexto e microssegmentação.

Infraestrutura de ID arriscada

Nossos analistas descobriram que a autenticação de ID e senha era o padrão do varejista, e o uso da MFA estava limitado a alguns sistemas. Isso criava um alto risco de abuso das informações de autenticação. Além disso, havia várias infraestruturas de ID, como o Microsoft Entra ID, AD (Active Directory) local e LDAP (Lightweight Directory Access Protocol). Como o gerenciamento do varejista não foi integrado, havia um risco de violação a partir de uma infraestrutura de ID com medidas de segurança mais fracas, como o LDAP.

Controles de autorização não integrados

Controles de autorização não haviam sido integrados, por isso cada aplicativo estava sendo tratado individualmente. Não era possível bloquear o acesso de dispositivos vulneráveis ou acesso suspeito: se o PC de um funcionário ou parceiro com acesso à rede da empresa estivesse infectado por malware, havia um alto risco de acesso não autorizado a sistemas e recursos por movimento lateral.

Segmentação inadequada

Descobrimos que as medidas de segurança do varejista estavam fortemente voltadas para ameaças externas, ignorando os riscos de invasores que já houvessem violado a rede. Sem uma segmentação interna robusta, a invasão pela rede Wi-Fi de um depósito ou por vulnerabilidades na VPN poderia levar a movimentos laterais não controlados. Essa falta de barreiras internas aumentou de forma significativa o risco de comprometimento generalizado do sistema, vazamento de dados e interrupções operacionais, pois o ataque poderia se mover livremente pela rede, sem medidas de contenção.

Insuficiência de gerenciamento e resposta a vulnerabilidades

O varejista não tinha um sistema de gerenciamento que vinculasse uma lista de materiais de software, ou SBOM (Software Bill Of Materials), a informações de vulnerabilidade. Assim, não seria possível identificar e responder rapidamente a vulnerabilidades de aplicativos, o que representava um alto risco.

Nossas recomendações

Recomendamos que o varejista seguisse estas cinco etapas para fortalecer sua postura de segurança:

1. Tomar medidas proativas para reduzir o risco de intrusão não autorizada e movimento lateral existente na configuração atual
2. Continuar a integrar a infraestrutura de identidade à pilha de tecnologia existente
3. Desenvolver um plano para expandir os recursos de autenticação e autorização, em conjunto com um acesso Zero Trust à rede
4. Decidir sobre a maneira mais eficaz de implementar uma carga de trabalho granular e uma proteção de aplicativos
5. Criar um sistema de resposta e um processo para ameaças futuras desconhecidas, desenvolver um sistema e um processo para fortalecer o gerenciamento e a resposta a vulnerabilidades e formular um plano

Se tiver interesse em embarcar na jornada Zero Trust, fale conosco para ter uma avaliação de segurança gratuita.

Apêndice A: Uma visão geral do conceito Zero Trust

Zero Trust é uma filosofia de segurança baseada na ideia de que nenhum usuário, dispositivo ou sistema, dentro ou fora do perímetro de rede de uma organização deve ser confiável.

Em vez disso, processos de verificação e monitoramento são usados para minimizar o risco. Isso inclui abordagens como impor políticas rígidas de gerenciamento de identidade e acesso, ou IAM (Identity and Access Management); usar autenticação multifator, ou MFA (Multi-Factor Authentication); e priorizar o controle de acesso baseado em função, ou RBAC (Prioritizing Role-Based Access Control).

O conceito Zero Trust já existe há 15 anos, mas se tornou mais importante durante a pandemia de COVID-19, quando organizações enfrentaram um aumento nos requisitos de acesso remoto. Muitas empresas perceberam que suas medidas de segurança existentes não funcionavam quando usuários e dispositivos estavam dispersos em vez de centralizados.

Hoje, há muitas implementações de princípios Zero Trust, incluindo a arquitetura Zero Trust, o ZTNA (Zero Trust Network Access), o Zero Trust SWG (Secure Web Gateway) e a microssegmentação.

Leia mais sobre Zero Trust

Apêndice B: A estrutura ZTMM 2.0

Os cinco pilares

Cada pilar pode progredir no seu próprio ritmo e progredir mais depressa do que outros, até que seja necessária uma coordenação entre pilares.

Pilar	Descrição
Identidade	Um atributo ou conjunto de atributos que descreve exclusivamente um usuário ou entidade da agência, incluindo entidades não pessoais
Dispositivos	Qualquer ativo que possa se conectar a uma rede, incluindo servidores, computadores desktop e laptop, impressoras, telefones celulares, dispositivos de IoT (Internet das coisas), equipamentos de rede e muito mais
Redes	Um meio de comunicação aberto, incluindo canais típicos, como redes internas de agências, redes sem fio e a Internet, bem como outros canais potenciais usados para transportar mensagens
Aplicativos e cargas de trabalho	Sistemas de agência, programas de computador e serviços que são rodados no local, em dispositivos móveis e em ambientes de nuvem
Dados	Arquivos e fragmentos estruturados e não estruturados que residem ou residiram em sistemas, dispositivos, redes, aplicativos, bancos de dados, infraestrutura e backups, bem como os metadados associados

Recursos entre pilares

Esses três recursos suportam toda a estrutura Zero Trust, garantindo que as medidas de segurança sejam integradas, responsivas e consistentes.

Recursos	Descrição
Visibilidade e análise	Organizações devem ter uma visão clara e em tempo real de todas as atividades do usuário, estados do dispositivo e interações de rede. Ameaças são detectadas e respondidas rapidamente, reduzindo os riscos. Organizações tomam decisões de segurança informadas e proativas
Automação e orquestração	Erro humano é uma causa comum de problemas de segurança. Quando a automação e a orquestração são otimizadas, as chances de erro humano são minimizadas. A automação simplifica tarefas de rotina, enquanto a orquestração organiza ações de segurança em diferentes sistemas. Isso cria as condições certas para respostas mais rápidas e coordenadas às ameaças
Governança	Uma boa governança de segurança cria responsabilidade, garantindo que todos sigam as mesmas práticas e normas de segurança. Isso constrói uma base sólida para operações seguras. Além disso, define diretrizes claras de Zero Trust e ajuda as organizações a atender aos padrões de conformidade

O aspecto de maturidade do Zero Trust Maturity Model

O ZTMM 2.0 define quatro níveis de maturidade para cada função. O objetivo é determinar o nível de maturidade atual dos cinco pilares e dos três recursos e, em seguida, criar um plano para mover cada um até o nível de maturidade mais alto.

Nível de maturidade	Descrição
Tradicional	Configuração, resposta e mitigação manuais; políticas e soluções estáticas e isoladas
Inicial	Início da automação; soluções iniciais entre pilares; algumas alterações responsivas ao menor privilégio; visibilidade agregada para sistemas internos
Avançado	Controles automatizados quando apropriados; aplicação de políticas entre pilares; alterações de privilégio mínimo com base em risco/postura; resposta a atenuações predefinidas
Ideal	Controles automatizados quando apropriados; aplicação de políticas entre pilares; alterações de privilégio mínimo com base em risco/postura; resposta a atenuações predefinidas