Akamai

WHITE PAPER

Como obter a maturidade Zero Trust com a Akamai

Suporte aos recursos transversais da CISA para agências e departamentos federais

Introdução

A segurança Zero Trust tornou-se o padrão ouro para proteger dados confidenciais do governo, infraestrutura crítica e sistemas de segurança nacionais. Agências e departamentos federais não podem mais depender de modelos de segurança tradicionais baseados em perímetro para combater as ameaças modernas. À medida que os cibercriminosos se tornam mais sofisticados, usando táticas avançadas, como roubo de credenciais, ransomware e ataques internos, as organizações federais estão cada vez mais mudando sua postura de segurança para uma estrutura Zero Trust. No entanto, essa mudança foi fragmentada e mais precisa ser feito para proteger os sistemas federais.

O modelo de maturidade Zero Trust da CISA (Cybersecurity and Infrastructure Security Agency) ajuda agências e departamentos federais a implementar princípios de segurança que eliminem a confiança implícita e apliquem mecanismos de verificação rigorosos. O modelo é baseado em cinco pilares fundamentais: identidade, dispositivos, redes, aplicações e cargas de trabalho, e dados. Além disso, três recursos transversais (visibilidade e análise, automação e orquestração, e governança) garantem uma abordagem holística e consistente da cibersegurança.

Para atingir esses objetivos, a microssegmentação deve ser considerada um princípio básico da segurança Zero Trust, servindo como um componente fundamental da defesa da rede interna (ou seja, leste–oeste). Ao segmentar cargas de trabalho e restringir o movimento lateral, as organizações federais podem conter possíveis violações e aplicar políticas Zero Trust. Além disso, soluções abrangentes de segurança de API (Application Programming Interface, interface de programação de aplicações) devem ser implementadas para proteger as comunicações externas (ou seja, norte–sul), garantindo que somente entidades autorizadas acessem aplicações governamentais.

Este white paper explora as etapas essenciais para alcançar a maturidade Zero Trust, destacando como as soluções avançadas de segurança da Akamai, incluindo a Akamai Guardicore Segmentation, a API Security da Akamai e o Akamai Enterprise Application Access, capacitam agências e departamentos federais para atender às diretrizes da CISA e melhorar sua postura de cibersegurança.

A mudança da segurança baseada em perímetro para Zero Trust

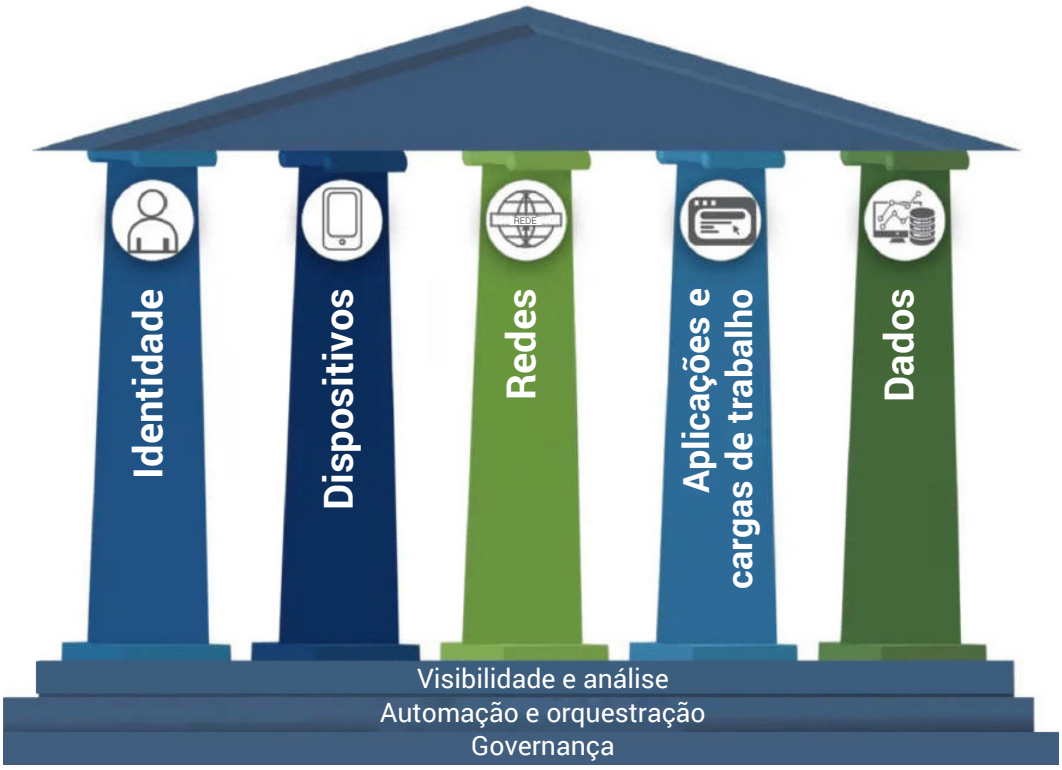
A cibersegurança tradicional dependia de defesas baseadas em perímetro, presumindo que, uma vez que uma entidade estivesse dentro da rede, ela seria confiável. No entanto, esse modelo falhou repetidamente diante de ciberameaças modernas. Os invasores exploram credenciais fracas e configurações de segurança mal definidas e usam técnicas de movimento lateral para contornar defesas tradicionais e obter acesso a informações confidenciais.

O Zero Trust elimina a confiança implícita exigindo a verificação contínua de usuários, dispositivos, aplicações e tráfego de rede. Cada solicitação de acesso é autenticada, autorizada e monitorada continuamente com base em avaliações de risco em tempo real. Essa abordagem reduz drasticamente a superfície de ataque e impede o acesso não autorizado, mesmo que um adversário viole parte da rede.

Modelo de maturidade Zero Trust da CISA

O modelo de maturidade Zero Trust da CISA fornece um roteiro para as agências e departamentos federais reforçarem progressivamente sua estrutura de segurança (Figura). O modelo é baseado em cinco pilares principais:

- **Identidade:** impor controles fortes de autenticação, autorização e acesso para garantir que somente usuários legítimos possam interagir com recursos confidenciais.
- **Dispositivos:** monitorar, proteger e validar dispositivos de ponto de extremidade para garantir que eles estejam em conformidade com as políticas de segurança antes de acessar redes governamentais.
- **Redes:** implementar microssegmentação e políticas avançadas de controle de acesso para evitar movimentos laterais não autorizados.
- **Aplicações e cargas de trabalho:** proteger aplicações e cargas de trabalho com políticas de acesso rígidas baseadas em identidade, segurança de tempo de execução e controles de segurança de APIs.
- **Dados:** garantir que os dados confidenciais do governo permaneçam criptografados, monitorados e protegidos contra acesso não autorizado e exfiltração.



Pilares do modelo de maturidade Zero Trust da CISA (fonte: CISA)

Além desses pilares, o modelo integra três recursos transversais críticos que se aplicam a todos os componentes Zero Trust:

- **Visibilidade e análise:** monitoramento contínuo, registro e detecção de anomalias para identificar e atenuar ameaças em tempo real.
- **Automação e orquestração:** automação de segurança orientada por IA para aplicar políticas, responder a ameaças e simplificar o controle de acesso.
- **Governança:** imposição centralizada de políticas para manter a conformidade com mandatos federais, como a FISMA (Federal Information Security Management Act) e a publicação especial 800-207 do NIST (National Institute of Standards and Technology).

A importância da microssegmentação e da segurança de APIs

Em modelos tradicionais de segurança das redes, elas geralmente são divididas em segmentos amplos usando firewalls baseados em rede. Embora essa abordagem forneça um determinado nível de segurança, ela não tem a granularidade necessária para proteger totalmente ambientes modernos e distribuídos. Em ambientes federais, a segmentação baseada em rede normalmente resulta em superprovisionamento, ou seja, usuários e aplicações têm acesso a mais recursos do que realmente precisam. Isso cria oportunidades indesejadas de movimento lateral. À medida que os invasores comprometem uma parte da rede, eles podem passar para áreas mais confidenciais com pouca resistência.

O conceito de microssegmentação aborda esse desafio, introduzindo um controle refinado sobre o tráfego leste–oeste dentro da rede. Em um ambiente microssegmentado, cada aplicação, carga de trabalho ou serviço é isolado de outros e o acesso é restrito com base em políticas específicas. Isso garante que usuários, dispositivos e aplicações só possam se comunicar com os recursos que estão explicitamente autorizados a acessar. Ao implementar a segmentação baseada em identidade e com reconhecimento de aplicações, a microssegmentação limita os possíveis danos causados por ataques cibernéticos, reduz a superfície de ataque e aplica o princípio de Zero Trust.

Quando se trata de tráfego de rede norte–sul, as redes federais dependem cada vez mais de APIs para facilitar a comunicação entre os sistemas. Como resultado, a proteção de pontos de extremidade de APIs se torna uma prioridade máxima. Os ataques à API, incluindo ataques de injeção, preenchimento de credenciais e acesso não autorizado a dados, aumentaram muito nos últimos anos. As agências e departamentos federais precisam de soluções abrangentes de segurança de APIs que forneçam proteção completa do ciclo de vida, permitindo que a equipe de segurança descubra, monitore e proteja seu tráfego de API em tempo real. A descoberta de API é especialmente importante: não é incomum ter APIs que ninguém conhece.

Soluções Zero Trust da Akamai em um piscar de olhos

Identidade

Akamai MFA é uma solução de identidade FIDO2 sem chave que protege as contas de funcionários contra phishing e outros ataques machine-in-the-middle. Ela garante que somente funcionários fortemente autenticados com base em identidade possam acessar as contas que possuem. Qualquer outro acesso é negado, impedindo a apropriação indevida da conta do funcionário.

Dispositivos

Akamai Guardicore Segmentation é uma solução de microssegmentação líder do setor, projetada para limitar a propagação leste–oeste de ransomware e outros malwares. Ao monitorar e aplicar continuamente políticas em dispositivos, a Akamai Guardicore Segmentation pode verificar as configurações do dispositivo, as instalações de software e as possíveis vulnerabilidades, garantindo que apenas dispositivos compatíveis possam acessar a rede. Além disso, a solução oferece suporte a uma abordagem sem agente para proteger dispositivos de Internet das coisas.

Akamai Enterprise Application Access é uma solução abrangente de acesso à rede Zero Trust que garante que somente usuários e dispositivos autenticados possam acessar as aplicações. Ao verificar a identidade e a postura dos dispositivos, o Enterprise Application Access complementa os recursos da Akamai Guardicore Segmentation. Se um dispositivo não for compatível ou representar um risco de segurança, o Enterprise Application Access poderá restringir seu acesso a aplicações confidenciais.

Redes

Akamai API Security oferece aos profissionais federais de segurança uma visibilidade total de todo o patrimônio de APIs por meio de descoberta contínua e análise em tempo real do tráfego norte–sul. A solução detecta APIs desconhecidas, identifica vulnerabilidades e analisa o comportamento de APIs para que as equipes de segurança possam detectar ataques e corrigir riscos nessa superfície em rápido crescimento.

Akamai App & API Protector reúne firewall de aplicações web, mitigação de bots, segurança de APIs e proteção DDoS (Negação de serviço distribuído) de Camada 7 em uma única solução. Ele identifica rapidamente as vulnerabilidades e atenua as ameaças nas propriedades de toda a rede e de APIs.

Akamai Secure Internet Access Enterprise é um DNS (Sistema de Nomes de Domínio) seguro baseado em nuvem que garante que os usuários e os dispositivos possam se conectar com segurança à Internet onde quer que estejam, sem a complexidade e as sobrecargas de gerenciamento associadas a outras soluções de segurança.

A **Akamai Guardicore Segmentation** oferece controle granular do tráfego de rede, permitindo apenas tráfego legítimo.

Soluções Zero Trust da Akamai em um piscar de olhos

Aplicações e cargas de trabalho

Akamai Enterprise Application Access fornece acesso Zero Trust a funcionários, terceirizados, parceiros e usuários de dispositivos móveis, independentemente da localização.

Akamai Guardicore Segmentation oferece visibilidade e compreensão de aplicações e cargas de trabalho.

Dados

Akamai Secure Internet Access Enterprise fornece acesso seguro a dados com recursos como filtragem de conteúdo, proteção avançada contra ameaças e prevenção contra perda de dados. Ele oferece suporte ao gerenciamento de inventário de dados, evitando acesso não autorizado e vazamentos de dados.

Akamai Guardicore Segmentation: a chave para a proteção leste–oeste

A Akamai Guardicore Segmentation é uma solução líder de microssegmentação projetada para ajudar as organizações, especialmente agências e departamentos federais, a implementar controles granulares de segurança em ambientes locais e em nuvem

Segmentação granular de cargas de trabalho e aplicações

Ao contrário da segmentação tradicional, que controla o acesso no nível da rede, a Akamai Guardicore Segmentation aplica políticas de segurança no nível da aplicação e da carga de trabalho. Isso garante que o acesso seja extremamente restrito. Por exemplo, em uma agência federal, uma aplicação de recursos humanos (RH) pode ser limitada à comunicação somente com seu banco de dados de RH designado, evitando que invasores se movam lateralmente se ocorrer uma violação.

Microssegmentação baseada em identidade

A Akamai Guardicore Segmentation aplica a segmentação com base na identidade do usuário e do dispositivo, em vez de apenas endereços IP. Isso garante que o acesso seja concedido dinamicamente com base na função, no nível de confiança e na verificação em tempo real. Por exemplo, terceirizados e parceiros externos podem ser restritos apenas aos sistemas de que precisam, reduzindo os riscos de acesso não autorizado.

Imposição de políticas dinâmicas

A Akamai Guardicore Segmentation ajusta constantemente as políticas de segurança com base em fatores em tempo real, como comportamento do usuário, integridade do dispositivo e atividade da rede. Se uma atividade suspeita for detectada, como um volume anormal de transferências de dados, a Akamai Guardicore Segmentation pode restringir automaticamente o acesso, bloquear o tráfego ou alertar as equipes de segurança. Essa abordagem proativa garante que as políticas de segurança evoluam para combater ameaças emergentes.

Ao integrar a microssegmentação da Akamai Guardicore Segmentation, as organizações podem fortalecer sua arquitetura Zero Trust, minimizar os riscos e manter um controle de acesso rigoroso sobre as próprias redes.

ESTUDO DE CASO

Akamai Guardicore Segmentation em um ambiente federal

Uma agência federal recentemente implementou a solução de microssegmentação da Akamai para proteger seus sistemas internos contra ataques de movimento lateral. Antes de adotar a Akamai Guardicore Segmentation, a agência dependia da segmentação tradicional baseada em rede, que fornecia granularidade limitada e permitia amplo acesso entre diferentes segmentos. Isso criava um risco significativo de movimento lateral se alguma parte da rede estivesse comprometida.

Com a Akamai Guardicore Segmentation, a equipe conseguiu:

- Implementar a segmentação granular: ao segmentar cargas de trabalho no nível da aplicação, a agência reduziu o risco de movimento lateral e garantiu que cada aplicação pudesse se comunicar apenas com os recursos necessários.
- Aumentar a visibilidade: as ferramentas de visualização da solução forneceram à agência uma visão detalhada do tráfego interno, permitindo que as equipes de segurança identificassem e atenuassem possíveis ameaças em tempo real.
- Aprimorar a segurança: ao integrar a Akamai Guardicore Segmentation com os sistemas existentes de gerenciamento de identidade e controle de acesso, a agência conseguiu impor a Zero Trust em toda a rede, garantindo que o acesso fosse constantemente monitorado e dinamicamente ajustado com base em avaliações de risco em tempo real.

Esse exemplo demonstra o poder da Akamai Guardicore Segmentation para melhorar a segurança da rede, reduzir o risco de movimento lateral e garantir que as permissões sejam mantidas no mínimo necessário o tempo todo.

API Security: protegendo o tráfego norte–sul

A Akamai oferece várias soluções para garantir a segurança de APIs. A plataforma de segurança de APIs da Akamai garante visibilidade abrangente das interações de API e detecta e atenua automaticamente as ameaças norte–sul em tempo real. Com a análise comportamental avançada, as agências e os departamentos federais podem:

- **Identificar APIs sombra** que podem ser exploradas por invasores.
- **Monitorar padrões de tráfego de APIs** para detectar tentativas de acesso não autorizado.
- **Implementar a limitação da taxa de API** para evitar abuso ou ataques de negação de serviço.
- **Identificar APIs esquecidas, negligenciadas ou desconhecidas** para descobrir possíveis caminhos de ataque.
- **Fazer o inventário de todas as APIs** independentemente da configuração ou do tipo, incluindo RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC.

O Akamai Secure Internet Access Enterprise é um firewall de DNS em nuvem desenvolvido para auxiliar as equipes de segurança a garantir que todos os usuários e dispositivos, estejam dentro ou fora da rede, acessem a Internet com segurança. Ele bloqueia proativamente solicitações de DNS mal-intencionadas, incluindo malware, ransomware, phishing e exfiltração de dados de DNS de baixa taxa de transferência. O Secure Internet Access Enterprise reduz a complexidade da segurança sem dispositivos para implantar, gerenciar e atualizar. A solução é simples e intuitiva de usar.

O Akamai App & API Protector descobre e atenua ameaças a APIs para aplicações e APIs em execução por meio da Akamai Cloud e pode bloquear qualquer tráfego que contenha possíveis ameaças não descobertas pelo API Security da Akamai. Quando implantadas juntas, as proteções de APIs da Akamai oferecem visibilidade abrangente e contínua das APIs e permitem à equipe de segurança descobrir, auditar, detectar e responder a preocupações relacionadas a segurança de APIs em todo o patrimônio de aplicações.

Como habilitar recursos transversais com Zero Trust

Um dos principais desafios das arquiteturas Zero Trust é o risco de criar silos de tecnologia. Cada silo geralmente opera de forma independente, levando à fragmentação nos controles de segurança, na imposição de políticas e na detecção de ameaças. Portanto, a importância da integração em todas as camadas de segurança é primordial.

Para agências e departamentos federais que gerenciam dados altamente confidenciais e infraestruturas complexas, essa abordagem fragmentada pode introduzir riscos de segurança significativos. Os invasores podem explorar a falta de visibilidade entre silos (ou pilares) ou capitalizar a imposição inconsistente de políticas em diferentes sistemas. Para atenuar esses riscos, as organizações federais devem adotar um modelo de segurança unificado que integre visibilidade, governança e automação em todos os pilares, garantindo a imposição consistente de políticas e reduzindo as lacunas que os adversários podem explorar.

Para alcançar um modelo de segurança unificado, a integração em vários pilares deve se concentrar nas três áreas transversais do modelo de maturidade Zero Trust da CISA: visibilidade e análise, automação e orquestração, e governança. Esses elementos são essenciais para habilitar uma arquitetura Zero Trust, em que o acesso e as permissões são ajustados dinamicamente em todos os pilares com base em avaliações de risco em tempo real.

Visibilidade e análise

A visibilidade é essencial para detectar ameaças, entender o comportamento do usuário e aplicar políticas de segurança dinâmicas em todos os pilares. Sem total visibilidade de como identidades, dispositivos, aplicações e dados interagem, as equipes de segurança ficam no escuro, dificultando a detecção de comportamentos anômalos ou tentativas de acesso não autorizado. As soluções da Akamai oferecem visibilidade abrangente e em vários pilares.

- A Akamai Guardicore Segmentation monitora o tráfego de rede entre cargas de trabalho segmentadas, oferecendo visibilidade do tráfego leste–oeste e detectando as tentativas de movimento lateral dentro da rede.
- O Enterprise Application Access fornece informações sobre padrões de acesso a aplicações, monitorando como os usuários interagem com aplicações confidenciais e garantindo que o acesso seja ajustado dinamicamente com base em dados contextuais.

Ao integrar esses recursos, as agências federais podem correlacionar dados em todos os pilares, permitindo uma visão unificada dos eventos de segurança. Quando um usuário solicita acesso a uma aplicação, as soluções da Akamai podem verificar não apenas sua identidade, mas também a segurança do dispositivo, a rede que ele está usando e o comportamento em tempo real da aplicação. Isso permite que as equipes de segurança detectem possíveis ameaças com mais rapidez, minimizem o risco de escalonamento de privilégios e garantam que as permissões sejam dinamicamente ajustadas em resposta a avaliações de risco em tempo real.

Automação e orquestração

Responder a incidentes e aplicar políticas em vários sistemas pode ser um processo lento e manual. Com Zero Trust, as políticas de segurança precisam ser aplicadas dinamicamente em todos os pilares, o que requer um alto nível de automação e orquestração. Isso garante que, à medida que os níveis de risco mudam, as permissões sejam imediatamente ajustadas ao nível mínimo necessário, reduzindo a chance de erro humano ou resposta atrasada. As soluções da Akamai oferecem fluxos de trabalho automatizados que abrangem segurança de identidade, rede e aplicação.

- A Akamai Guardicore Segmentation oferece microssegmentação automatizada, ajustando dinamicamente as políticas de segmentação de rede com base em padrões de tráfego em tempo real e anomalias detectadas. Isso garante que qualquer atividade suspeita dentro da rede seja rapidamente isolada, evitando movimentos laterais.
- O Enterprise Application Access automatiza o processo de proteção do acesso a aplicações, garantindo que os usuários só possam acessá-las por meio de um proxy seguro e que as permissões sejam continuamente atualizadas com base em fatores de risco variáveis.

Ao automatizar esses processos, as agências e os departamentos federais podem garantir que as políticas de segurança sejam aplicadas de forma consistente e rápida, reduzindo a janela de oportunidades para os invasores.

Governança

Governança é a base de qualquer estratégia de segurança, garantindo que as políticas sejam aplicadas de forma consistente e que os requisitos de conformidade sejam atendidos. Em um modelo de vários pilares, a governança deve garantir que todos os controles de segurança estejam alinhados aos princípios de Zero Trust. Com as soluções da Akamai, as agências podem implementar políticas de governança que abrangem todos os pilares.

- Governança de identidade: garantir que os controles de acesso baseados em identidades sejam aplicados de forma consistente em dispositivos, aplicações e redes, e que as permissões de acesso sejam revisadas e atualizadas periodicamente com base em avaliações de risco em tempo real.
- Governança de rede: aplicar políticas de segmentação de rede e monitoramento de tráfego entre ambientes, incluindo infraestruturas locais, em nuvem e híbridas; a Akamai Guardicore Segmentation permite que as agências definam políticas de segmentação de rede e garantam que elas sejam aplicadas de forma consistente em toda a infraestrutura.
- Governança de dados: proteger dados confidenciais garantindo que o acesso seja restrito com base no privilégio mínimo e que todas as transferências de dados sejam continuamente monitoradas quanto a acesso não autorizado ou atividade suspeita.

As tecnologias da Akamai são projetadas para funcionar perfeitamente em conjunto para oferecer às agências federais uma arquitetura de segurança totalmente integrada e em vários pilares que suporte Zero Trust.

ESTUDO DE CASO

Integração em vários pilares em uma agência federal

Uma grande agência federal enfrentou desafios importantes com políticas de segurança fragmentadas em suas camadas de identidade, rede e aplicação. Diferentes sistemas gerenciavam a verificação de identidade, o acesso a aplicações e a segmentação de rede, levando à imposição inconsistente de políticas de segurança e lacunas na visibilidade.

Ao adotar as soluções integradas da Akamai, a agência conseguiu:

- **Unificar identidade e segurança de aplicações:** o Enterprise Application Access, solução de ICAM (gerenciamento de identidade, credencial e acesso) da Akamai, foi integrado para garantir que o acesso à aplicação fosse sempre autenticado com base em dados de identidade em tempo real. Isso permitiu que a agência ajustasse dinamicamente as permissões da aplicação com base no comportamento do usuário e na integridade do dispositivo.
- **Aplicar segmentação de rede dinâmica:** a Akamai Guardicore Segmentation foi implantada para segmentar o tráfego de rede com base na identidade e no acesso a aplicações, impedindo o movimento lateral entre sistemas confidenciais e garantindo que as permissões fossem continuamente atualizadas com base em avaliações de risco em tempo real.
- **Melhorar a visibilidade e a automação:** a agência usou as ferramentas integradas de análise e automação da Akamai para obter total visibilidade de sua postura de segurança e automatizar a imposição de políticas em todos os pilares.

Como resultado, a agência reduziu sua superfície de ataque, melhorou os tempos de resposta a incidentes e obteve total conformidade com as normas de segurança federais. Esse caso demonstra o poder da integração em vários pilares para transformar uma arquitetura de segurança fragmentada em um modelo coeso e dinâmico que suporta Zero Trust.

Conclusão

A segurança Zero Trust não é mais opcional. É uma necessidade para proteger agências federais contra ciberameaças sofisticadas. Ao implementar a microssegmentação, a segurança de APIs e os fortes controles de identidade, as agências e os departamentos federais podem reduzir muito os riscos, mantendo a conformidade com os requisitos de cibersegurança federais.

A Akamai oferece um conjunto abrangente de soluções Zero Trust, incluindo Akamai Guardicore Segmentation, Akamai API Security e Akamai Secure Internet Access Enterprise, permitindo que as agências adotem uma postura de segurança proativa e adaptável. Ao envolver a experiência da Akamai, as organizações federais podem acelerar sua jornada Zero Trust e garantir sua resiliência de segurança no longo prazo.

Agora é a hora das agências federais agirem. Ao integrar as soluções de segurança da Akamai, elas podem alcançar a maturidade Zero Trust, atenuar os riscos cibernéticos e proteger os ativos digitais mais críticos do país.

Entre em contato com a Akamai hoje mesmo para saber mais sobre nossas soluções de segurança abrangentes.