WHITE PAPER

Transforme a conformidade em uma vantagem competitiva com as soluções de segurança da Akamai

Uma abordagem de quatro pilares para aumentar a segurança e garantir a preparação para auditorias

Concentre-se em quatro pilares de segurança para abrir caminho para a conformidade

Hoje, organizações de todo o mundo enfrentam um cenário cada vez mais desafiador de normas, da GDPR e HIPAA ao PCI DSS e uma crescente variedade de exigências regionais. Mas estar em dia com as normas de conformidade não se resume apenas às exigências de autoridades reguladoras — é essencial manter a confiança de clientes e partes interessadas internas, como líderes seniores e conselhos administrativos.

Na verdade, as implicações das falhas de conformidade vão muito além das penalidades regulatórias diretas. Os custos dessas falhas incluem a interrupção nos negócios durante as etapas de investigação e remediação, danos à reputação e maior exposição legal. Se uma organização descumprir as normas de conformidade, isso poderá resultar em perda de receita devido à rotatividade de clientes e aos custos operacionais significativos, uma vez que os recursos são desviados para fins de remediação em vez de inovação. Em 2024, as 35 maiores violações globais acumularam US$ 3 bilhões em multas, e 23 estavam relacionadas às regras da General Data Protection Regulation (GDPR) da União Europeia como a causa, de acordo com a Forrester.

No passado, as equipes de segurança abordavam amplamente a conformidade à medida que as regulamentações surgiam. Mas agora, com a tecnologia avançando rapidamente e os ataques crescendo cada vez mais, a conformidade precisa entrar em pauta nos processos de avaliação de ferramentas e modelos de maturidade. As equipes precisam se perguntar: "Como as minhas escolhas de segurança atuais me ajudarão a atender aos requisitos de conformidade agora e no futuro?"

Na Akamai, ajudamos os clientes a responder a essa pergunta através de quatro pilares de segurança que também promovem naturalmente áreas essenciais da preparação para a conformidade. Esses pilares são:

- Obter visibilidade de todo o patrimônio de TI
- Evitar o movimento lateral (entre redes, aplicações e APIs)
- Impedir o acesso não autorizado
- Proteger dados confidenciais de clientes e informações de contas

O resultado gera uma clara vantagem competitiva. As organizações não ficam apenas mais seguras; elas ficam mais bem preparadas para eliminar os obstáculos regulatórios. Ao garantirem a segurança e a conformidade, elas também têm mais chances de ganhar a confiança dos clientes e de líderes internos.

Pilar 1

Obter visibilidade de todo o patrimônio de TI

A base da preparação para a conformidade começa com uma visibilidade abrangente de todos os ativos digitais. As organizações não podem proteger o que não podem ver, e cada vez mais as autoridades reguladoras precisam de evidências de inventários completos de ativos, monitoramento contínuo e conscientização sobre ameaças.

Não é tão fácil. Um estudo recente da Forrester descobriu que mais da metade (52%) das empresas financeiras concordam/concordam plenamente que não têm visibilidade total de seu patrimônio de TI. Infelizmente, os riscos da falta de conformidade são altos para qualquer setor. O número de organizações que pagam mais de US$ 100 mil em multas regulatórias aumentou quase 20% entre 2023 e 2024.

Para muitas organizações, o desafio da visibilidade reside no monitoramento do tráfego de redes e de APIs. Estas são algumas das normas e padrões que exigem uma visão clara dos riscos:

- O PCI DSS (Payment Card Industry Data Security Standard) contém orientações para confirmar que o software de uma empresa usa com segurança as funções de componentes externos, como APIs que transmitem dados de pagamento de um aplicativo móvel para o sistema de um banco.
- Normas como a ISO (International Organization for Standardization) IEC 27001 exigem o isolamento de dados e de recursos de processamento de dados no caso da invasão de uma rede.
- A Lei de Segurança de Dados da República Popular da China exige controles de segurança robustos para proteger o acesso às informações pessoais dos clientes por meio de tecnologias que trocam dados confidenciais entre diferentes sistemas de TI.

Muitas empresas têm ferramentas ou processos que podem atender a alguns desses requisitos. No entanto, à medida que eles se expandem para ambientes de computação híbrida e entre regiões geográficas, o monitoramento se torna muito mais difícil. Isso se aplica especialmente às APIs. De acordo com uma pesquisa da Akamai, apenas 27% dos profissionais de segurança que possuem inventários completos de APIs realmente sabem quais de suas APIs retornam dados confidenciais — uma queda em relação aos já preocupantes 40% registrados em 2023.

Em última análise, as organizações precisam saber onde estão seus dados confidenciais e o que os está acessando para saber onde concentrar seus esforços de segurança. Isso exige visibilidade sobre:

- Quais ativos estão se comunicando com a rede (com visualizações históricas e em tempo real), incluindo processos da camada 7 e tráfego de edge, em ambientes de nuvem híbrida e locais
- Inventários de APIs, incluindo APIs sombra e zumbi, mostrando onde elas se integram com fontes de tráfego e código
- JavaScript do lado do cliente — o que é particularmente importante para os requisitos mais recentes do PCI DSS

O portfólio da Akamai pode ajudar as equipes de segurança a ganhar a visibilidade de que precisam.

A **Akamai Guardicore Segmentation** pode identificar e visualizar os ativos que se comunicam dentro da rede em toda a infraestrutura de TI, incluindo detalhes de processos da camada 7, hash e linha de comando. Além disso, ela oferece visibilidade histórica para a certificação durante auditorias de conformidade, com o objetivo de comprovar que os ativos em questão não foram comprometidos. As visualizações de tráfego norte-sul e leste-oeste também mostram onde o acesso está acontecendo.

O **API Security** fornece um inventário em tempo real de APIs que as organizações exigem para fins de conformidade e pode ajudar a identificar onde e quando dados não criptografados podem estar fluindo por APIs.

O **App & API Protector** oferece visibilidade no nível das aplicações, incluindo inventários de APIs, detecção da exposição de dados confidenciais e análise de tráfego em tempo real.

O **Client-Side Protection & Compliance** fornece a visibilidade de scripts do lado do cliente exigida pelo PCI DSS v4.

Uma organização de saúde implementou a Akamai Guardicore Segmentation para atender aos requisitos de conformidade da HIPAA e do SOC 2. Ele proporcionou informações valiosas sobre os fluxos de tráfego entre diferentes aplicações. A equipe de segurança pode inspecionar detalhes granulares além dos logs da camada 4: IDs de usuários, entradas de linhas de comando e até mesmo correlações de serviços.

Pilar 2

Evitar o movimento lateral

Assim como as equipes de segurança, muitas autoridades reguladoras sabem que, mesmo com uma forte postura de segurança, uma violação pode acontecer, e buscam garantias de que as empresas podem limitar os danos causados. Por exemplo:

- O Artigo 32 da GDPR exige "a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de processamento" e "a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais em tempo hábil no caso de um incidente físico ou técnico".
- O PCI DSS v4 exige igualmente que as organizações "Implementem firewalls para proteger os dados do titular do cartão de crédito e garantir que os firewalls estejam configurados para restringir conexões entre redes confiáveis e não confiáveis."
- A **Organização Internacional de Normalização/Comissão Eletrotécnica Internacional (**ISO**/IEC) 27001** exige a segregação das instalações de processamento de informações e dados para proteger a confidencialidade, integridade e disponibilidade das informações.

Embora a maioria das organizações tenha alguma forma de firewall, limitar o movimento lateral quando um agente mal-intencionado está dentro da rede requer um nível maior de controle. Isso torna a microssegmentação, de preferência definida por software, uma ferramenta-chave para alcançar a conformidade. A Akamai está bem posicionada para lidar com as preocupações dos auditores em relação ao movimento lateral.

A **Akamai Guardicore Segmentation** fornece os limites de movimento lateral de que as organizações precisam para manter a conformidade. Os modelos de política prontos para uso facilitam a aplicação rápida de iniciativas relacionadas à conformidade com controles granulares da camada 7. E, como é definida por software, ela pode fornecer o mesmo nível de proteção granular, independentemente de onde os ativos residam. Além disso, sua capacidade de identificar aplicações que se comunicam dentro da rede e tentativas de comunicação entre zonas segmentadas proporciona aos auditores outro nível de confiança em sua capacidade de atenuar ameaças.

Os invasores estão encontrando novas oportunidades de movimento lateral devido à proliferação de APIs, especialmente pontos de extremidade de APIs que são vulneráveis a ataques de Autorização Interrompida em Nível de Objeto (BOLA). Os invasores podem manipular IDs de objetos em solicitações de APIs para permitir a movimentação lateral na rede. Uma vez dentro, os agentes maliciosos podem burlar a autorização, elevar privilégios e obter acesso aos dados dos clientes.

O **Akamai API Security** pode sinalizar APIs que expõem dados confidenciais sem a autenticação adequada e identificar APIs com controles de acesso fracos ou mal configurados que podem levar a acesso não autorizado a dados e movimentação lateral. A integração com o firewall de aplicações web (WAF) da Akamai também permite que o API Security bloqueie ameaças maliciosas em tempo real.

Um cliente da Akamai, uma organização global de serviços financeiros, implementou o API Security porque estava tendo dificuldades com APIs desconhecidas em seu ambiente. A implementação reduziu drasticamente a proliferação de APIs e melhorou a conformidade, já que o Akamai API Security classifica dados confidenciais para ajudar a atender regulamentações como GDPR, HIPAA e outras. Durante auditorias regulatórias, essas implementações servem como evidência direta de que a empresa tomou as medidas técnicas apropriadas.

As ameaças de IA atuais são os obstáculos regulatórios do futuro

Hoje, qualquer análise das defesas de cibersegurança de uma organização deve abordar o espectro da IA. O rápido surgimento de aplicações impulsionadas por IA, modelos de linguagem grandes (LLMs) e APIs gerativas ligadas à IA trouxe novas vulnerabilidades que muitas organizações ainda não conhecem. Exemplos desses tipos de aplicações incluem chatbots com inteligência artificial, mecanismos de recomendação de varejo, ferramentas de diagnóstico de integridade e mecanismos de decisão de risco. Enquanto isso, os agentes de ameaça estão aproveitando a IA para lançar ataques mais sofisticados.

E em qualquer lugar que surjam ameaças às operações comerciais e ao público, é provável que as regulamentações entrem em ação.

As organizações que buscam proteger seus investimentos em IA, seus dados e seus clientes estão buscando ajuda da Akamai. Como um provedor de segurança com um sólido histórico de atender aos requisitos de visibilidade, movimento lateral e controle de acesso atuais, a Akamai investiu proativamente em atender aos requisitos de IA do futuro. A Akamai desenvolveu recursos avançados de IA para fortalecer suas soluções de segurança e agora implementou uma solução para ajudar as organizações a proteger seus próprios investimentos em IA.

O **Akamai Firewall for AI** oferece segurança abrangente para aplicações orientadas por IA, identificando e mitigando ameaças e ataques específicos de IA que as ferramentas de segurança tradicionais não foram projetadas para enfrentar. As proteções específicas do Firewall for AI incluem:

- **Defesa contra injeções de prompt**: protege contra invasores que manipulam modelos de IA por meio de entradas enganosas
- **DLP (prevenção contra perda de dados)**: detecta e bloqueia vazamentos de dados confidenciais em respostas geradas por IA, além de proteger contra o recebimento de dados confidenciais nas solicitações
- **Filtragem de conteúdo tóxico e prejudicial**: sinaliza discurso de ódio, informações falsas e conteúdo ofensivo antes da entrega
- **Segurança de IA contra adversários**: protege contra execução remota de código, backdoors de modelos e ataques de envenenamento de dados
- **Mitigação de negação de serviço**: mitiga ataques de DoS por IA controlando o uso excessivo de consultas e a sobrecarga de modelos

Além disso, o Firewall for AI pode ajudar as organizações a cumprir com as diretrizes existentes de privacidade, segurança e proteção. Ao impor políticas de segurança específicas de IA, as empresas podem mitigar os riscos relacionados a regulamentos de proteção de dados, uso ético de IA e exigências de governança corporativa.

Pilar 3

Impedir o acesso não autorizado

Controlar o acesso a sistemas e dados confidenciais representa uma base de conformidade em praticamente todas as estruturas regulatórias. As organizações devem entender sua postura de segurança de aplicações e APIs e impedir o acesso não autorizado e as violações. Isso exige autenticar os usuários adequadamente, autorizar o acesso com base na necessidade e manter registros detalhados de todas as atividades de acesso.

Para um controle de acesso completo que atenda aos requisitos normativos, as organizações devem lidar com três desafios principais. O portfólio de segurança da Akamai pode ajudar a oferecer defesas profundas que abordam cada um deles:

1. **Obter uma compreensão abrangente da postura de segurança de aplicações e APIs**

O App & API Protector da Akamai permite que as organizações apliquem políticas de tráfego em todos os ambientes em que estão em execução, enquanto o Akamai API Security pode alertar uma organização sobre qualquer atividade incomum, acesso não autorizado a dados ou configurações incorretas, todos fatores importantes para os auditores. Enquanto isso, a Akamai Guardicore Segmentation pode rastrear todas as aplicações que se comunicam dentro da rede e estabelecer uma linha de base para a atividade.

2. **Monitorar o comportamento dos usuários e limitar o acesso a informações confidenciais**

A Akamai Guardicore Segmentation limita o acesso dentro da rede com base na identidade do usuário, enquanto o **App & API Protector** aplica políticas de tráfego com detecção de ameaças alimentada por IA para evitar violações. Por fim, o **Client-Side Protection & Compliance** monitora o comportamento da execução do JavaScript para mitigar ataques do lado do cliente.

3. **Detectar e limitar atividades fraudulentas**

O API Security pode ajudar a detectar o comportamento anormal de APIs e controles de autenticação configurados incorretamente para bloquear ataques de alto risco. A Akamai Guardicore Segmentation protege a rede, sinalizando e bloqueando conexões suspeitas que possam indicar atividade fraudulenta. O App & API Protector detecta e atenua ameaças identificadas pelo OWASP para reduzir ainda mais o risco de fraude.

NIS2 e proteção do acesso

A atualização da Network and Information Security Directive (NIS2) foi projetada para criar um nível comum de cibersegurança entre os membros da UE. Entre as recentes adições à NIS2 está a exigência de que as empresas criem um sistema de gerenciamento de segurança de informações que avalie pessoas, políticas e tecnologias para proteger dados confidenciais e garantir a resiliência operacional. A NIS2 também tem uma ênfase maior na proteção das cadeias de suprimentos de TI e das relações com fornecedores terceirizados.

Pilar 4

Proteger dados confidenciais de clientes e informações de contas

O último pilar de uma abordagem de prontidão regulamentar abrangente exige que as organizações tenham planos em vigor para dados confidenciais. Proteger os dados de clientes, pacientes, parceiros e muito mais está no centro da maioria das regulamentações com foco em segurança.

Por exemplo, a Lei Japonesa de Proteção de Informações Pessoais exige avaliações de impactos na proteção de dados que possam identificar e mitigar riscos em tecnologias que processam grandes volumes de dados pessoais ou envolvem atividades de processamento de dados de alto risco.

Para instituições financeiras dos EUA, o Federal Financial Institutions Examination Council (FFIEC) exige controles que garantam que as APIs só permitam o acesso a dados específicos por usuários autorizados por meio de segurança em camadas, por exemplo, monitoramento, registro e relatórios.

A abordagem desse pilar começa com a detecção de ameaças. O **App & API Protector**, a solução da Akamai de proteção de aplicações web e APIs, oferece a primeira camada de defesa, enquanto a **Akamai Guardicore Segmentation** monitora e segmenta o tráfego norte-sul e leste-oeste. O **portfólio da Akamai de soluções de proteção contra bots e violações** garante uma camada extra de segurança contra ameaças automatizadas e ataques humanos.

No entanto, para identificar adequadamente as ameaças, as organizações também precisam entender o comportamento normal da rede. Veja como os recursos das soluções de segurança da Akamai podem fornecer essas informações essenciais:

- O Akamai API Security e a Akamai Guardicore Segmentation, respectivamente, fornecem o entendimento básico de APIs e aplicações que se comunicam dentro da rede para sinalizar qualquer comportamento anormal.
- O Adaptive Security Engine, tecnologia central do App & API Protector, aprende padrões de ataque usando dados locais e globais para fazer ajustes específicos para cada cliente nas proteções, ao mesmo tempo em que se adapta a ameaças futuras.
- O Akamai Hunt, um serviço gerenciado de busca de ameaças que utiliza informações da equipe de pesquisa especializada da Akamai, permite que as empresas usem uma abordagem de defesa mais proativa.

A DORA e a segurança de dados

A Digital Operational Resiliency Act (DORA) foi criada para ajudar organizações de serviços financeiros nos estados-membros da UE a enfrentar e superar ciberataques. Com a DORA, o setor passa a contar com um quadro vinculativo e abrangente de gestão de riscos para tecnologia da informação e comunicação (TIC). O Artigo 3 da DORA exige que as organizações utilizem soluções e processos de TIC que:

- Minimizem os riscos, o acesso não autorizado e as falhas técnicas relacionados a dados
- Evitem a indisponibilidade de dados, a perda de dados e violações de integridade e confidencialidade
- Garantam a segurança da transferência de dados

Do isolamento da conformidade à vantagem competitiva

Programas de conformidade eficazes devem demonstrar impacto nos negócios além de simplesmente "cumprir formalidades" das exigências regulatórias. As organizações que implementam as soluções de segurança da Akamai focadas na conformidade relataram melhorias mensuráveis em três dimensões principais.

Redução de custos de conformidade

Organizações com programas de conformidade maduros normalmente gastam menos em atividades de conformidade do que aquelas com abordagens ad-hoc. A automatização da coleta de evidências por meio de plataformas de segurança integradas pode reduzir significativamente o tempo de preparação para auditorias, assim como a consolidação de soluções pontuais em uma plataforma abrangente.

Melhoria da postura de risco

Além da redução de custos, as melhorias de conformidade devem oferecer redução de riscos mensurável. As organizações que implementam as soluções de segmentação da Akamai podem restringir os caminhos de movimento lateral vulneráveis, atendendo diretamente aos principais requisitos de conformidade e, ao mesmo tempo, reduzindo o risco organizacional.

Recursos de monitoramento abrangentes melhoram a visibilidade, o que se traduz diretamente na redução de riscos, eliminando pontos cegos onde violações de conformidade podem passar despercebidas.

Eficiência operacional

O terceiro aspecto do impacto da conformidade envolve melhorias na eficiência operacional. Controles pré-aprovados e padrões de segurança consistentes podem significar aprovações de segurança significativamente mais rápidas para novas aplicações. Isso melhora a satisfação dos desenvolvedores ao reduzir o atrito nos processos de análise de segurança e acelerar o tempo de lançamento no mercado de novos aplicações.

Ajustes de conformidade

À medida que os requisitos normativos continuam evoluindo e as organizações crescem, elas precisam de uma abordagem de conformidade que se adapte. O portfólio de segurança integrada da Akamai fornece a base para uma estratégia de conformidade que antecipa as tendências regulatórias e se adapta ao crescimento da organização.

- As estruturas de políticas configuráveis podem se adaptar a novos requisitos sem rearquitetura significativa, enquanto os recursos de geração de relatórios extensíveis podem acomodar requisitos de evidências emergentes à medida que as normas evoluem.
- A implantação automatizada de políticas para novos ativos garante que a cobertura de conformidade se estenda automaticamente à medida que a empresa se expande.
- Os recursos de gerenciamento centralizado mantêm a visibilidade abrangente independentemente da escala, enquanto o suporte abrangente de APIs permite a automação de processos de conformidade para gerenciar a complexidade crescente.

Além disso, as organizações precisam ser proativas ao estabelecer uma rotina regular para revisar regulamentos e atualizar seus controles de conformidade de acordo. A Akamai fornece atualizações regulares de nossas soluções de segurança, especificamente projetadas para atender aos requisitos de conformidade em evolução, garantindo que os clientes mantenham a conformidade contínua, independentemente das alterações regulatórias.

Conclusão: a conformidade como um diferencial competitivo

A conformidade efetiva não se trata mais apenas de satisfazer os requisitos normativos — ela representa um imperativo estratégico de negócios que afeta diretamente o desempenho organizacional, a confiança do cliente e o posicionamento competitivo. Independentemente do seu setor ou região, uma abordagem proativa em relação à conformidade garante uma postura de segurança forte e ágil.

Ao implementar uma abordagem integrada de segurança nos quatro pilares da prontidão para conformidade (visibilidade em todo o ambiente de TI, prevenção de movimentação lateral, prevenção de acesso não autorizado e proteção de dados sensíveis dos clientes e informações de contas), as organizações podem estabelecer uma base sustentável de conformidade que gera valor comercial mensurável além do cumprimento regulatório.

As organizações que estão alcançando o maior sucesso são aquelas que transformaram a conformidade: de um custo comercial necessário, ela é agora uma vantagem estratégica que permite a transformação digital, protegendo o que é mais importante — a confiança do cliente, a integridade dos dados e a reputação da empresa.

Entre em contato conosco para saber como a Akamai pode ajudar sua organização.

Entre em contato conosco

| Publicado em 07/25