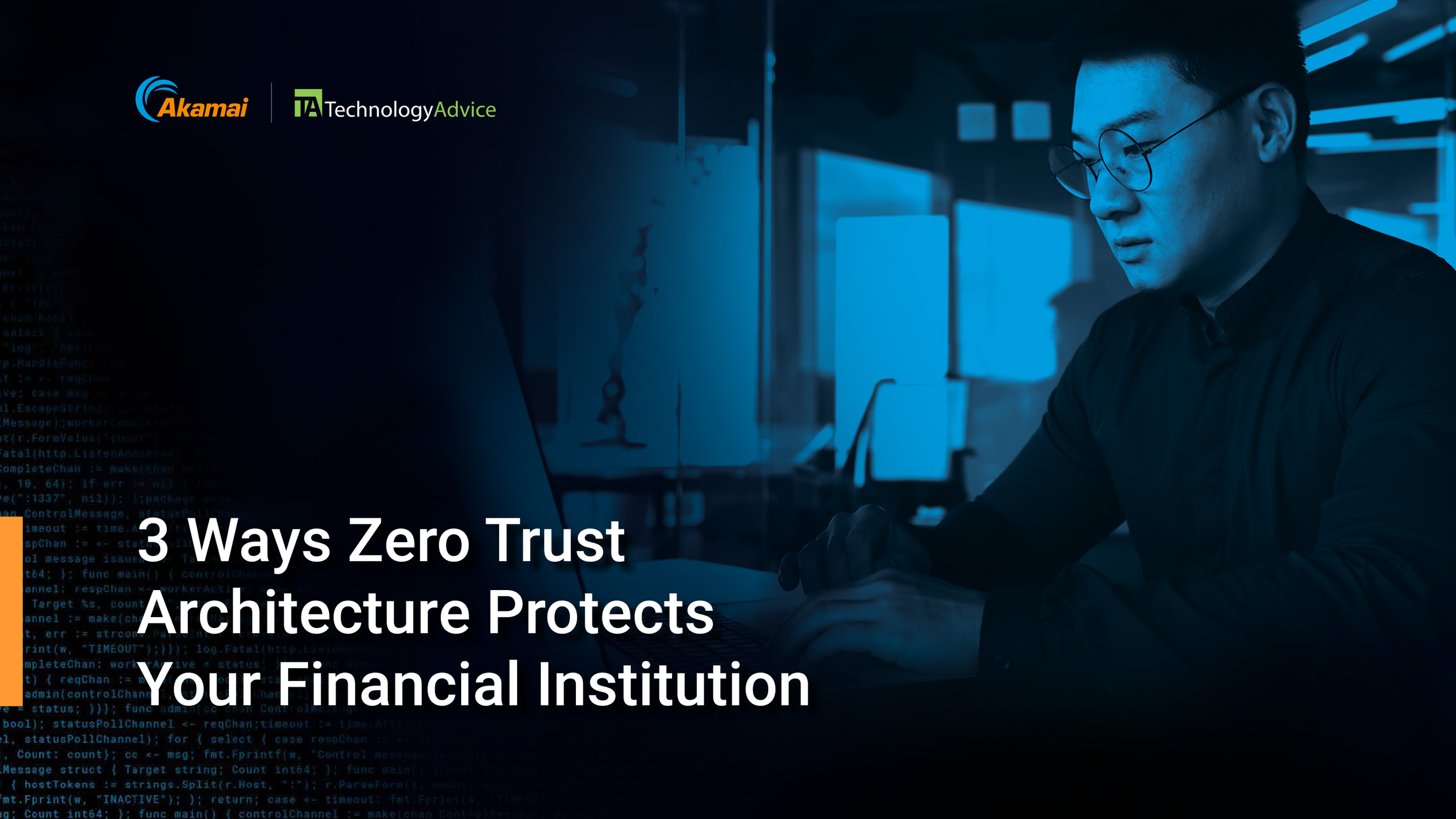
Akamai | TechnologyAdvice



3 Ways Zero Trust Architecture Protects Your Financial Institution

Financial institutions remain prime targets for threat actors, facing a 65% increase in web application and API attacks when comparing Q2 2022 with Q2 2023. This relentless assault of evolving cyberthreats not only drains resources but also diverts attention from essential core business functions.

Traditional firewall and endpoint solutions implicitly trust endpoints, devices, and users that pass the initial screening of a password and username combination, occasionally reinforced with multi-factor authentication (MFA). Applications, APIs, and system services within the network often operate without security screening beyond basic endpoint malware monitoring. To confront rising ransomware threats, strict compliance regulations, and the challenges of cloud migration, financial institutions are now adopting Zero Trust.

Zero Trust eliminates implicit trust and continuously verifies the access permissions for all applications, users, and devices based on the context of the request and permissions. Even if an attacker can compromise a device or credentials to access a network, access can be tightly restricted and damages highly reduced.

But how exactly does a Zero Trust framework protect your financial institution?

Comply with ever-changing regulations

Financial institutions must dedicate significant resources to proving compliance with diverse regulations, such as the well-established Payment Card Industry Data Security Standard (PCI DSS), or the looming Digital Operational Resilience Act (DORA), which is expected to be fully applied in January 2025. Audits regularly increase in complexity, cost, and time because of unclear, conflicting, and changing requirements, yet financial institutions must make the investment because failed audits can also lead to revenue loss, regulatory sanctions, fines, or penalties, as well as loss of reputation and potential legal liabilities.

Compliance reporting requires clear and accurate accounts of the systems that touch regulated data and demands proof that those systems are adequately protected. However, in a large financial institution, the IT environment is too large, too detailed, and too intricate to easily track assets and access.

Legacy firewalls and endpoint protection primarily track and protect traditional users and assets. Relying on this conventional approach to network segmentation poses challenges in scaling operations, hinders policy creation and enforcement, and limits agility.

To overcome the challenges of legacy environments with technology aligned with future strategy, financial institutions need granular visibility into east-west traffic and the ability to enforce segmentation policies in multicloud and container environments. With the growing need to manage multiple regions and IT infrastructure types, including container technology, financial institutions need the simplest, most straightforward path to microsegmentation with policy flexibility, DevOps integration, and automation.

Without regular identification, tracking, and securing of all resources, a financial institution cannot ensure that access to regulated data is fully controlled and protected. Overlooking or inadequately monitoring data, users, applications, or devices significantly increases the risks of a cyberattack and the potential failure of a compliance audit.

Zero Trust architecture denies access by default and all connections must be explicitly granted with context: the authorized user, on an authorized device, with authorized access to the requested data. Zero Trust defaults to least-privilege access, which disrupts forgotten or unknown legacy connections. Akamai's solution rapidly identifies rogue devices, legacy users (human, API, or application), and forgotten data sources that infest older branch offices or the legacy tech environments of acquired businesses.

Akamai's Zero Trust architecture applies regardless of the user's location, yet the context of location can be included in the decision process for access. Security teams gain the consolidated control and reporting needed to quickly analyze and fully manage access to resources in local networks, data centers, or the cloud.

Amid heightened regulatory pressure to safeguard critical applications and secure east-west traffic, financial institutions are focusing on enhancing the visibility and understanding of their environments. Through Zero Trust principles, they can now identify and segment noncompliant assets seamlessly, empowering application teams to autonomously manage segmentation policies. This ensures an efficient workflow and simplifies the reporting process.

Full context-rich visibility into east-west traffic facilitates effortless mapping and ringfencing of business-critical apps, without infrastructure or application changes. This capability enables institutions to restrict third-party access and bolster overall security.

Acquiring visibility streamlines secure migration to the cloud, while integrating segmentation into the DevOps cycle ensures immediate policy updates without substantial infrastructure modifications — a departure from previous VLAN practices. Additionally, Akamai enables and simplifies the uniform creation, enforcement, and reporting of compliance policies across multiple infrastructures. This is achieved through heightened visibility, application dependency mapping, automated segmentation policies, DevOps policy automation, and seamless change-management integration.

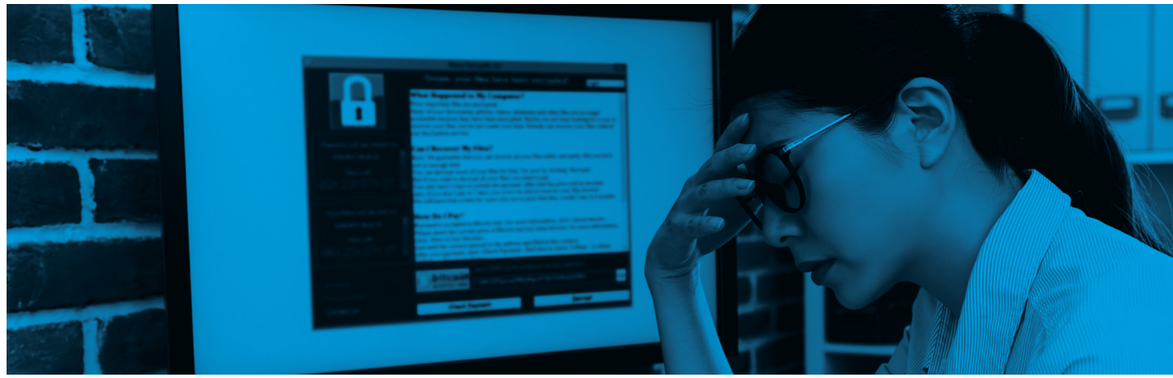
Prevent the spread of ransomware

From branch offices to global financial institutions, ransomware attacks make headlines and cause headaches worldwide. “Ransomware is expected to attack a business, consumer, or device every two seconds by 2031,” according to the 2022 Ransomware Market Report from Cybersecurity Ventures.

Because financial services institutions so often grow through mergers and acquisitions, they often lack visibility into their entire technology ecosystem, leaving backdoors open for attackers. Ransomware attackers exploit backdoors or use phishing attacks to either steal credentials or drop unknown malware on endpoints that evade endpoint protection.

Overly permissive user access policies and password-centric authentication enable attackers to bypass firewalls, evade endpoint detection, and gain unrestricted access to networks that implicitly trust traffic, users, and connected devices. Ransomware attackers, often operating in organized groups, such as CL0P, exploit compromised assets and then move laterally through the network to discover and exploit other vulnerable assets. Zero-day vulnerabilities, like the MOVEit SQL injection vulnerability, enable attackers to gain access and spread the attack quickly by using automated scripts to encrypt systems, steal data, and drop ransom requests.

Akamai’s Zero Trust solutions empower financial institutions to identify and isolate critical systems, and to restrict network access to and from these systems. This approach minimizes the likelihood of, impact of, and time required for remediating a ransomware attack. Initially, Akamai tracks and monitors malicious domains and IP addresses, implementing appropriate quarantine blocks to prevent many attacks from launching.



Subsequently, with near real-time visibility into network traffic, Akamai observes and controls traffic down to process and service levels. This depth of insight equips security operations center and network operations center teams to precisely identify and target the specific threats at hand.

Next, even a successful attack will be tightly limited in scope by the microsegmentation inherent in Akamai Guardicore Segmentation. Credentials and permissions will be continuously verified with every access request — and connections to applications protected by Akamai Enterprise Application Access will be denied.

Furthermore, applications, servers, and other resources not required by a user are automatically hidden from discovery, which prevents any lateral movement or extension of access for attackers. Finally, Akamai Hunt’s anomaly detection will flag unusual behavior to alert security teams to help identify attacks before data can be exfiltrated or encrypted.

Streamline digital transformation

To enable agility, scalability, and modernization, many financial institutions move apps to the cloud. However, such a move introduces a host of new challenges.

To start, financial institutions cannot migrate undetected and unknown resources and connections. Additionally, cloud migrations not only expand the attack surface, multicloud and local hybrid cloud integrations often break applications and introduce gaps into established security layers. Furthermore, software deployable infrastructure (containers, virtual machines, etc.) automatically deploys too quickly to secure or monitor effectively with the use of legacy solutions.

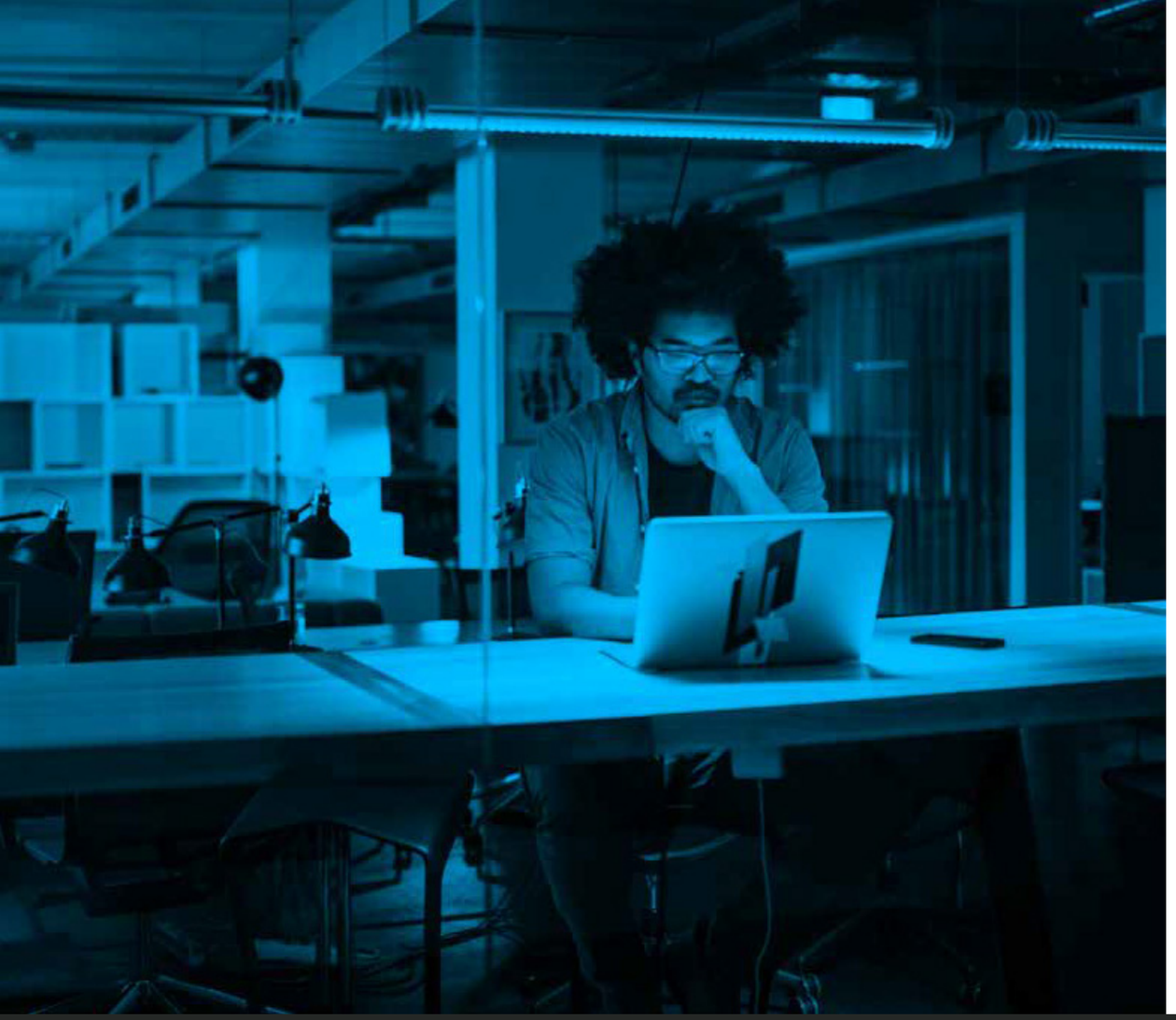
Zero Trust solutions ensure that financial institutions can more easily deploy their cloud-based applications with stronger protections and reduced operations overhead. Akamai's Zero Trust solutions track all data flows to quickly identify the potential attack surface and enforce policies without disrupting the business.

Once identified, security and operations teams can use Akamai's centralized control to segment and secure applications and monitor data flows. Akamai delivers granular control while simultaneously reducing operational cost and complexity. For security and operations teams within financial institutions, the application of universal policies ensures a swift and agile modernization of infrastructure. This is achieved via the robust security of least-privilege Zero Trust segmentation, which provides a powerful shield against evolving threats.

Financial institutions can't afford to ignore Zero Trust

Attacks on legacy technology can lead to major data breaches, cost millions in damages, and destroy customer and partner trust. Attacks are getting more sophisticated and faster, and without full visibility into the technical ecosystem, financial institutions may be leaving backdoors open.

Akamai provides greater visibility into the network, intelligently limits user access, continuously hunts threats, and flags any anomalies for security review. Learn more about meeting the needs of your financial institution with the Akamai Zero Trust Portfolio.



Learn more about securing your digital finance with Akamai

Learn more

TechnologyAdvice | Akamai

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.