AKAMAI SOLUTION BRIEF

Simplify and Secure with End-to-End Zero Trust

Zero Trust is a strategic approach to cybersecurity that secures an organization by removing implicit trust across users, devices, networks, data, and applications. Instead of assuming everything behind the corporate firewall is safe, the Zero Trust approach assumes breach at any moment and applies least-privileged access to every request, regardless of where it originates.

Why Zero Trust matters now

Zero Trust has become top of mind for organizations that need to more effectively adapt to the ever-changing modern environment. These organizations are looking for a new security model that embraces the hybrid workforce and protects users, devices, and apps wherever they are located.

Principles of modern Zero Trust architecture

- Verify explicitly, always in context
- Enforce least privilege explicitly
- Monitor continuously

Consolidation is essential

Integrated end-to-end approach

A holistic approach to Zero Trust should extend to all the organization's entities, including identities, network, and apps. Zero Trust serves as an end-to-end strategy, which is why it requires integration across all the elements. Going with multiple, loosely integrated point solutions does not align with this strategic approach.

Akamai has assembled a holistic, robust portfolio to deliver all the Zero Trust solutions critical for the modern organization. Instead of installing, running, and fixing multiple security products, organizations can rely on a single vendor to deliver all the technologies required and enjoy reduced costs and improved operational efficiencies.

Signal sharing between solutions

Akamai has worked built-in automation across its Zero Trust portfolio, greatly reducing complexity and customization. This way, the portfolio products can share threat knowledge across all its products, making each product more secure.
If one product identifies a threat, another product can be alerted to mitigate it.

Benefits

- **Distributed workforce**
  Allow users to work more securely from anywhere, anytime, on any device
- **Cloud migration**
  Provide secure access control across cloud and hybrid cloud environments
- **Risk mitigation**
  Stop threats and minimize lateral movement of ransomware and other types of malware
- **Compliance**
  Support compliance with micro-perimeters around sensitive data

Akamai

A holistic end-to-end portfolio: users, applications, and network

Secure the workload

Akamai Guardicore Segmentation: Zero Trust for applications

Akamai Segmentation provides the industry-leading microsegmentation solution, designed to limit the spread of ransomware and other malware. The product provides visibility and understanding into the workloads, processes, and applications, as well as enforcement of access policies.

Secure the network

Enterprise Application Access: Zero Trust network access

Akamai's Zero Trust Network Access technology was designed to replace the traditional VPN technology for strong user identity. Instead of risking the entire network, Enterprise Application Access allows users access based on the specific app the user needs to access to perform a role. Enterprise Application Access provides visibility into users identity and strong enforcement of identification and authentication.

Secure the user

Secure Internet Access: Zero Trust internet access

Secure Internet Access is a cloud-based secure web gateway solution. Secure Internet Access inspects every web request that users make and applies real-time threat intelligence and advanced malware analysis techniques to ensure that only safe content is delivered. Malicious requests and content are proactively blocked.

Multi-factor authentication: strong Zero Trust identity

Akamai MFA protects employee accounts from phishing and other machine-in-the-middle attacks. This ensures that only strongly authenticated employees can access the accounts they own, other access is denied, and employee account takeover is prevented.

Track and monitor

Hunt: security services

By adopting an "always assume a state of breach" approach, Akamai's elite team of threat hunters continuously hunts for anomalous attack behavior and advanced threats, which often escape standard security solutions. Our threat hunters immediately notify you of any critical incident detected in your network and then work closely with your team to remediate the situation.

The Akamai advantage

Akamai provides a few advantages that set it apart from other Zero Trust vendors. We offer the broadest coverage: legacy and modern, Windows and Linux, on-premises and virtualized, containers, and more. Because of our unmatched visibility capabilities, users are able to know what each workload is doing with full context. And our in-house elite threat-hunting services extend any security team's capabilities and allows your organization to stay ahead of threats.

To learn more about Zero Trust and how to get started, visit akamai.com.

| Support | Published 06/22