How Akamai Implemented a Zero Trust Security Model — Without a VPN

Background

As the public Internet and SaaS applications become more prevalent, and attack surfaces continue to shift, granting application access as a result of location is increasingly impractical. The demands for connectivity and a data-intensive reality also place an unprecedented amount of pressure on network infrastructure. Legacy solutions cannot possibly keep up, particularly as workers expect full mobility, as well as fast and reliable access to corporate applications — everywhere they go. Enterprises must evolve to meet the changing needs of today's IT and business environments.

Business Situation

Akamai IT believed that a network-centric approach to security and access was no longer sufficient to protect the company's assets. Traditional VPNs come with security drawbacks, including the increased risk of unauthorized remote access to sensitive data and access to all applications on the corporate network from any authenticated device. This approach to remote access creates unnecessary security risks; with VPN, each user can generally access the same applications that every other user can.

Akamai set out to adopt a Zero Trust security strategy that would eliminate the traditional corporate VPN and move away from a perimeter-based security model. The goal was to safeguard Akamai's corporate applications and data, and prevent lateral movement on the corporate network, while also providing improved user experience.

The goal was to safeguard Akamai's corporate applications and data, and prevent lateral movement on the corporate network, while improving the user experience.

As part of the Zero Trust transformation, Akamai settled on a core set of principles:

- *Transition to a perimeter-less environment where the Internet becomes the corporate network*
- *Every office must become a Wi-Fi hotspot*
- *Application access is dynamically and contextually granted based on identity; environmental factors, such as location and time of day; and device signals, such as client-side certificates or device compliance to corporate security policy*

Akamai IT also updated security guidelines to align with the tenets of Zero Trust; no machine or user would be trusted by default. This approach was based on finding cost-effective technologies that support mobility, enhanced security, flexible access, and virtualization — while also taking advantage of the simplicity of the cloud.

Pain Points

- ***Distributed workforce***
  Akamai's globally dispersed and diverse workforce — consisting of full-time employees, contractors, and partners — required high-functioning application access
- ***Mobile devices***
  A growing number of devices and device types needed access to corporate applications
- ***Acquisitions***
  The complexity and cost of providing newly acquired workforces with access to corporate applications was climbing
- ***Varied applications***
  Preventing business disruption and data loss from attacks was paramount, regardless of application type (on-premises, IaaS, and SaaS)
- ***Help desk tickets***
  Akamai's IT resources were increasingly sidelined by troubleshooting associated with remote, contractor, and partner access to internal applications
- ***Architecture management***
  The diversity of devices and increasing number and size of last-mile links were increasing network complexity and cost, driving up administrative requirements, and negatively impacting application performance
- ***Latency***
  Existing architectures and VPN connectivity resulted in slow and inconsistent application access

Solution

Akamai IT adopted Enterprise Application Access to transition from the VPN. This cloud-based access solution locks down the corporate network with dial-out only access to applications behind the firewall. With Akamai's technology, application access — regardless of where applications are hosted (on-premises, IaaS, SaaS) — is based solely on entitlement, identity, authentication, and authorization at a per-application level. By employing Enterprise Application Access for application-specific access and control, Akamai enables agility, simplicity, and a better user experience for the entire workforce, including IT and security teams.

Access is based solely on entitlement, identity, authentication, and authorization at a per-application level, regardless of where applications are hosted (on-premises, IaaS, SaaS).

For additional security, Akamai IT used Kona Site Defender — Akamai's web application firewall — in conjunction with Enterprise Application Access to protect internal applications against SQL injection attacks and other insider threats from formerly "trusted" hosts. This further reduced the risk and increased Akamai's overall security posture. Enterprise Application Access coupled with Ion — Akamai's performance optimization engine — helped Akamai IT deliver superior web application experiences for end users, regardless of their device, network, or geographic location.

Akamai's approach reduced the cost and complexities typically associated with securing access to applications. Instead of trying to control, or limit, various endpoints remotely accessing the corporate network, it made more sense for Akamai to adopt a solution that empowers IT to monitor and control access to only those applications users actually need. Moving everyone off of VPN and the corporate network — and using a Zero Trust approach to gain visibility and context for all traffic (across users, devices, locations, and applications) — not only reduced risk significantly, but also streamlined the corporate application deployment process.

Leveraging device posture for dynamic access decisions is another key component in completing Akamai's transition to a Zero Trust model. Device posture complements and enhances existing authentication, authorization, access control rules, and reporting capabilities by providing additional context and signal to drive dynamic application access decisions.

Akamai's Path to Zero Trust

2000s

Network and Application Controls

- *Client certificates for all*
- *Network dot1x – 2FA*
- *Federated authentication – SAML*
- *No internal wireless*
- *Bastion management hosts*
- *Default no outbound Internet*

2011

Utilization of Existing Akamai Solutions

- *Applications externally available via Akamai IT-created solution (inbound proxy)*
- Global Traffic Management *(intelligent traffic manager)*
- Site Shield *(restrict direct access to application origin)*

2016

Elimination of Most Passwords for Users

- *2FA evolves to certification and push MFA*
- *Passwords are largely eliminated from the environment*
- Enterprise Application Access *(third-party access)*

2017

Introduction of Akamai Enterprise Security Solutions

- *Enterprise Application Access removes homegrown Akamai IT solution*
- Enterprise Threat Protector *(DNS-based threat protection)*

NOW

Zero Trust

- *Enterprise Application Access and Enterprise Threat Protector clients deployed successfully to thousands of internal users*
- *Hundreds of applications enabled on Enterprise Application Access in conjunction with* Ion *(performance optimization)*
- *Device posture capability enabled with Enterprise Application Access*
- Kona Site Defender *(web application firewall)*
- Bot Manager *(bot protection)*

Business Benefits of Moving to a Zero Trust Security Posture

- *Minimize risk by providing access to only necessary applications — not full corporate network access*
- *Remove network complexity associated with legacy technologies, including backhauling VPN traffic to a central data center*
- *Improve productivity by enabling streamlined access for Akamai's workforce, as well as for third parties*
- *Reduce IT appliance and process overhead associated with providing access to employees from newly acquired companies*
- *Enable automation, orchestration, visibility, and analytics over workloads, networks, people, and devices to secure data*
- *Enhance user experience across devices, including mobile, with faster and more reliable application delivery*
- *Cut costs with more efficient allocation of IT resources; fewer hours spent updating, managing, and maintaining hardware and software means more time for strategic imperatives*
- *Reduce help desk requests associated with application access*

Visit **akamai.com/zerotrust** to learn more about transitioning your enterprise to a Zero Trust security model. Or **contact an Akamai specialist** to discuss a customized action plan for security transformation.

What Is Enterprise Defender?

Enterprise Defender leverages the Akamai Intelligent Edge Platform to secure all enterprise applications and users, delivering optimal security and reducing complexity without impacting performance. It enables you to ensure secure access to applications you control, while mitigating risks associated with your users accessing applications you don't control.

Enterprise Defender includes the following capabilities in an easy-to-consume per-user, per-month subscription service:

Malware Prevention: Akamai's secure Internet gateway (SIG) proactively identifies, blocks, and mitigates targeted threats such as malware, ransomware, phishing, DNS data exfiltration, and advanced zero-day attacks.

Secure Application Access: Akamai ensures that only authorized users and devices have access to the corporate applications they need — not the entire network.

Web Application Firewall: Akamai provides broad protection for critical web applications against the largest and most sophisticated DDoS and web application attacks.

Enterprise Defender combines malware prevention with adaptive application access, security, and acceleration in a simple-to-consume security service at the Edge.

Application Acceleration: Akamai enables enterprises to deliver applications that are fast, reliable, and secure in a cost-effective manner. Application delivery capabilities are placed at the Edge — close to users, the cloud, and on-premises workloads. Anywhere in the world.

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 07/19.