Global Consulting Firm Secured 300,000 Endpoints in Record Time

A consulting firm protected endpoints and workloads worldwide in two weeks with microsegmentation that stopped lateral movement of ransomware

Fortifying business operations with unstoppable cybersecurity

As a global IT consulting and outsourcing leader, this firm supports 2,000 enterprise customers with a workforce of 300,000+ employees. But when a ransomware attack exposed vulnerabilities in its defenses, it had one mission: lock down security — fast. To safeguard its operations and prevent threats from spreading to customers, the company needed a highly scalable microsegmentation solution that could be deployed rapidly. By turning to Akamai Guardicore Segmentation, it launched one of the world's largest microsegmentation deployments to date.

Answering the ransomware wake-up call

With IT systems deeply intertwined with its customers' infrastructures, the company couldn't risk another attack. Firewalls alone weren't enough since ransomware had already slipped through.

Recognizing the urgency, the Board established a bold goal: Protect all business-critical servers and workloads worldwide within one year. The timeline wasn't the only ambitious goal — the solution had to scale across thousands of endpoints and workloads without disrupting operations.

Fast-tracking security with 100% coverage in two weeks

After a rigorous evaluation, the company selected Akamai Guardicore Segmentation for its:

- Granular visibility into east-west traffic
- Rapid deployment capability across diverse IT environments
- Powerful microsegmentation to stop lateral movement

Global Consulting Firm

Industry

Service Provider

Solution

Akamai Guardicore Segmentation

Key Impacts

- Protected 300,000 endpoints and workloads in 2 weeks
- Enforced 100% of policies in 8 days
- Reduced ransomware risk worldwide

To ensure airtight protection, Akamai worked with the company to implement both baseline and "rapid response" policies targeting commonly abused protocols. These rapid response policies, which are ready to deploy at a moment's notice, provide instant protection the moment an attack is detected.

Within two weeks, Akamai's agent-based microsegmentation solution was deployed in alert-only mode across all 300,000 workloads and endpoints across the globe. Eight days later, 100% were in enforcement mode, actively blocking threats.

Minimizing the attack surface and impacts

By layering in Zscaler's AI-powered access controls and Cortex XDR's attack detection, the company created a multilayered defense — and stopped ransomware attempts dead in their tracks. While Zscaler provided AI-powered analysis and real-time URL filtering, Cortex XDR indicated when a ransomware attack occurred. Akamai Guardicore Segmentation completed this defense-in-depth approach by quickly containing potential threats and minimizing the blast radius of real attacks.

In the event of a ransomware event, a single click instantly applied a quarantine policy, isolating potentially suspicious assets from the rest of the network. This approach enabled rapid response to potential ransomware attacks or any detected suspicious activity on servers and endpoints, significantly enhanced the company's security posture, and minimized risk.

Stronger, smarter, and ready for the future

With Akamai Guardicore Segmentation, this consulting giant gained full control over its traffic by limiting ransomware spread at scale. With the knowledge that there would be no more scrambling after an attack, the company's confidence in its cyber resilience soared.

With tighter segmentation between critical systems and IT environments, the consulting firm isolated threats before they spread. Going forward, it can use Akamai Guardicore Segmentation to create AI-driven risk-based policies that adapt dynamically, for even stronger protection.

By turning a security crisis into an opportunity for innovation, the company built a future-proof defense that ensured uninterrupted business operations and continued trust from its customers.