Akamai Customer Story

U.S. Healthcare Company Outsmarted 4,000 Cyberattacks in One Day

Network engineers used Layer 7 visibility and smart policies via microsegmentation to reduce cyber risks

Thwarted ransomware

Gained deep visibility

Improved policies

Connecting patients with essential healthcare

Imagine trying to protect a network that directly impacts patient lives — while staying ahead of increasingly sophisticated cyberattacks. That was the reality for a medium-sized healthcare company. Its network engineering team was facing growing ransomware threats and a need for greater visibility, so the team turned to Akamai Guardicore Segmentation to elevate the company's security posture.

Extending Zero Trust architecture

The organization had a bold vision: strengthen its IT environment with Zero Trust principles while meeting HIPAA and SOC 2 compliance requirements. Because the stakes were high, the network engineering team's goals included:

- Keeping critical applications online even during security incidents
- Reducing the impact of ransomware attacks by containing their spread
- Gaining detailed network visibility far beyond traditional firewalls

The organization needed a cost-effective, scalable microsegmentation solution that didn't require ripping and replacing existing IT infrastructure. Plus, it had to be simple enough for a lean team to manage — and scalable to grow with the company.

As one network engineer explained, "Ransomware targets healthcare. The faster we can isolate and eliminate these threats, the better."

Healthcare Company

Location

United States

Industry

Healthcare & Life Sciences

Solution

Akamai Guardicore Segmentation

Akamai

Finding the right microsegmentation solution

After quickly dismissing the option of a containerized approach, the company evaluated microsegmentation solutions. “We wanted the same capabilities we see in next-generation firewalls, namely visibility at the application layer,” explained the network engineer.

After evaluating many solutions, the organization found Akamai Guardicore Segmentation. A positive demo paired with hands-on support from Akamai’s engineers sealed the deal. The solution checked every box, including:

- **Deep visibility:** Layer 7 inspection and full network insights
- **Ease of deployment:** Software-based agents with no additional hardware
- **Resilience:** No single point of failure in the core network
- **Flexibility:** Support for diverse operating systems

According to the vice president of IT infrastructure and information security, Akamai Guardicore Segmentation delivers a huge advantage to lean teams. “Immediately after starting the deployment, we saw benefits around visibility and control.”

“We don’t need to purchase and manage multiple east-west firewalls — providing tremendous cost savings — and also get a level of visibility not possible via firewalls,” added the manager of IT infrastructure.

Stopping ransomware in its tracks

The results were immediate and impressive. By better ringfencing its apps and using Akamai Guardicore Segmentation’s out-of-the-box ransomware prevention policies, the team neutralized 4,000 cyberattacks on day one. The solution even tailored policies to fit the organization’s specific needs.

“For middle-ground policies, we used alert mode to flag incidents without causing downtime. It’s a great way to refine policies without disruptions,” shared the network engineer.

> “
>
> Akamai Guardicore Segmentation helped us do more than address our ransomware concerns — it elevated our approach to cybersecurity.
>
> – Network engineer

> "Climbing the 'Zero Trust mountain' is incredibly challenging. Akamai Guardicore Segmentation moved us rapidly up that mountain while reducing the challenges of expense and complexity."
>
> — Vice president of IT infrastructure and information security

Gaining unparalleled Layer 7 insight

According to the manager of IT infrastructure, Akamai Guardicore Segmentation provides valuable views into traffic flows between different apps. This unlocked a treasure trove of data for the team. The team could now inspect granular details beyond Layer 4 logs: user IDs, command-line inputs, and even service correlations.

"Our network team can look into traffic flow to troubleshoot issues, and provide our security team with the information needed to fully investigate incidents," noted the network engineer.

This visibility came in handy during an unexpected policy violation. A new employee connected a PC directly to its carrier's customer premises equipment (CPE) instead of to a LAN port shielded by a home-grade router. This was strictly no-go since the CPE assigned the PC a public IP, making it susceptible to public scans of the internet.

As the organization's network engineer explained, "Akamai Guardicore Segmentation detected the issue instantly, allowing us to isolate the PC and resolve the situation before it escalated. Moreover, this inspired us to create a policy aimed at preventing this type of incident from occurring in the future."

Smarter labeling, better policies

Thanks to intuitive labeling and policy creation, the network engineering team could easily map traffic and enforce security rules. According to the network engineer, "We could decide what works best for our environment. That capability impressed us far more than we were expecting, and helped us efficiently create policies."

For instance, the team limited access to print servers, allowing only trusted zones — a quick win that improved the organization's overall security posture. "That enabled us to address low-hanging fruit remediations right off the bat," the engineer continued.

Visibility that instills confidence

One unexpected benefit? A crystal-clear view of internal traffic flow and application behavior. This newfound visibility enabled better collaboration with application owners and streamlined maintenance windows. For instance, the team is empowered to show application owners whether their traffic is being blocked.

“In the past, troubleshooting and future-proofing were an issue. Now during cutovers, we could confidently confirm when traffic shifted from old servers to new ones. That allowed us to retire legacy systems with certainty,” the network engineer said.

The organization’s vice president of IT infrastructure and information security concluded, “Akamai Guardicore Segmentation has already made an impact and become an essential product in our security practice. I look forward to expanding its deployment across the organization.”

| Support | | Published 02/25