Large Healthcare System Chooses Akamai to Improve Compliance Posture and Enable Move to Cloud

Comprehensive network visibility

Segmentation across IT infrastructures

Secure adoption of new technologies

Customer summary

As a large healthcare system, this Akamai customer is responsible for protecting their 6,000+ assets and patient data from potential threats.

Business challenges/requirements

Though the organization planned to migrate several of its critical workloads to Microsoft Azure, its IT stakeholders found themselves facing several roadblocks to successful cloud adoption.

Their current environment had several existing security risks, including a relatively flat network in which Internet of Medical Things devices had unmonitored access to the data center and a well-used bring your own device policy. This meant a possible breach could result in substantial lateral spread that could compromise patient and payment data in other business-critical applications. With little isolation, it also made proving compliance to auditors a manual task of combing through exhaustive security logs.

Equally frustrating was a lack of visibility into traffic and application dependencies that were undermining attempts to move workloads to Azure.

Why Akamai?

Remediating the organization's current visibility and security challenges using VLANs or firewalls would have meant coordination and significant effort among several already maxed-out teams to execute required network changes.

So when the Akamai team was able to demonstrate a software-defined segmentation approach that could granularly map out their diverse environment and consistently apply segmentation policies to workloads across on-premises and cloud, stakeholders secured the budget, and IT leadership moved forward with a purchase decision.

Large Healthcare System

Industry
Healthcare

Solution
Akamai Guardicore Segmentation

Key impacts
- Prevents unauthorized lateral movement
- Protects critical applications
- Simplifies and accelerates compliance
- Enables secure migration to the cloud

Results of Akamai Guardicore Segmentation

Simplifying and accelerating microsegmentation

Because Akamai Guardicore Segmentation uses a software overlay approach independent of the underlying infrastructure, the customer's security team was able to accelerate the segmentation project independently, limiting the impact on other groups in IT.

With the new platform, the organization was able to ringfence critical applications quickly and tightly restrict device access to the data center with no downtime or need for any application or network changes. Using the new visibility into real-time and historical data, the organization can also now easily prove to auditors that all regulated assets are effectively isolated. Today, the company manages its data center security with only two employees.

Finally, by mapping application dependencies and creating the necessary policies, the healthcare system was successfully able to achieve its cloud adoption goals while also ensuring that any future workload migrations to the cloud remain just as secure.

Please visit akamai.com/guardicore for more information.

"

You should be getting every potential healthcare customer in front of your [Akamai] solution so they can see their entire data center traffic from a single view and how easy it is to create and apply security policies in hybrid cloud environments.

— IT Security Leader at
Large Healthcare System