Guardicore

Now part of **Akamai**

Case Study

> *"You should be getting every potential healthcare customer in front of your Centra 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 Akamai Guardicore Segmentation Customer

INDUSTRY

Healthcare

PRIMARY USE CASES

- Reducing Lateral Movement
- Protecting Crown Jewel Applications
- Securing Hybrid-Cloud Workloads
- Simplify and Accelerate Compliance

FEATURES USED

- Visibility
- Application Dependency Mapping
- Segmentation Policies

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

Customer Summary

As a large healthcare system, this Akamai Guardicore Segmentation customer is responsible for protecting their 6000+ workloads 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 where medical IoT devices had unmonitored access to the datacenter and significant BYOD use. This meant a possible breach could result in a significant 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 Guardicore Segmentation?

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

So, when the Akamai Guardicore Segmentation 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.

Results of Akamai Guardicore Segmentation

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 datacenter 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.

Want to learn more about Akamai Guardicore Segmentation? Visit www.akamai.com today.

Guardicore
Now part of Akamai