AKAMAI CUSTOMER STORY

Keeping Attacks (That Get Through Defenses) from Spreading

Research university strictly controls which servers can communicate with one another — on-premises and in the cloud — with Akamai Guardicore Segmentation

250+
Applications protected

Smaller blast radius for cyberattacks

Less effort for IT teams

Protecting university and personal data — on-premises and in the cloud

Even with multiple layers of defense, some attacks will sneak through to infect servers. Previously, this university IT team limited the spread of malware by painstakingly maintaining firewall rules to control which servers could communicate with one another. But the IP addresses of applications hosted in the cloud change constantly, making firewall rules almost impossible to keep up to date. Now the university controls the spread of threats more effectively and with less effort with Akamai Guardicore Segmentation.

What happens when a server attack evades defenses?

At this midwestern research university, a small team within the 100-person IT organization manages shared services including email, single sign-on, and administrative applications. “Security is always on our mind,” says an IT team member. “The university has 250 applications, so it’s a safe bet that a new exploit will affect at least one of them. Part of our job is to keep attacks that successfully breach one server from moving to other servers. It’s about limiting risk.”

The IT team uses a combination of security techniques to keep threats out, including regular patching, intrusion detection, and web application firewalls. If a threat makes it past all those protections, a technique called microsegmentation limits its spread. The goal is to only allow communications between servers when absolutely required — for example, when a web application connects to a database.

U.S.
Research University

Research university
United States

Industry
Higher education

Size
~20,000 students
4,400 faculty and staff

Solution
- Akamai Guardicore Segmentation

Akamai

The cloud makes segmentation more complicated

Previously, the IT team segmented the network by writing firewall rules. For example: Application A could accept traffic from applications B and C, blocking traffic from all other applications. That approach worked fine when all applications ran in campus data centers. But as the university began moving applications to the AWS and Azure clouds, firewall rules became more complicated and harder to manage.

Applications like Admissions, for example, connect to the AWS relational database service, which has dozens of IP addresses that continually change. The university IT team doesn't have time to constantly re-enter new IP addresses in the firewall rules, so they decided to look for a more effective and manageable segmentation solution.

Now, rules adjust automatically as cloud IP addresses change

The university found its solution in Akamai Guardicore Segmentation. The IT team installed the software on the university's on-premises and cloud servers. When the IP addresses behind a cloud service change, which is a frequent occurrence, Akamai immediately adjusts the rules to reflect the new IP addresses.

The university community experienced the benefits right away. In one example, the IT team had to update the configuration of all 250 servers as quickly as possible to correct a newly discovered security vulnerability. But the servers retrieve new configurations from a cloud repository that has many IP addresses, and these addresses had recently changed.

"If we were still using the firewall for segmentation, the servers would have remained vulnerable while we scrambled to update the rules with the new IP addresses," says an IT staff member. "Akamai reduced the window of vulnerability — and saved us a lot of work."

Stronger security — and a better experience for students and staff

Now, segmentation is not just easier to manage — it's also stronger. Where firewalls control inbound traffic to servers, Akamai Guardicore Segmentation can also control outbound traffic from servers — a protection called "egress blocking" — because it includes software that's installed right on the servers.

"Egress rules are a nightmare to figure out on firewalls, so before we just didn't do it," the IT staff member says. "With Akamai it's simple, and it's another way to keep infections from spreading."

The team also likes that Akamai helps them check that rules are working. With a glance at a visual map, they can see which connections are happening and which are blocked. Previously, they would have had to log into all 250 servers and look at firewall hit counters — which would've taken time they didn't have.

The IT team is getting kudos for improving the user experience while tightening security. Say a prospective student logs into the Admissions application at 8:00 PM to check application status and financial aid eligibility, and AWS had moved the underlying database to a different server at 7:59 PM. When communications between the application and database depended on firewall rules, the student might have seen a message to try again later. With Akamai Guardicore Segmentation, the student sees up-to-date information regardless of all that IP address shuffling in the cloud and gets a great first impression of the university.

> We knew Akamai would help limit the spread of threats between servers. The surprise is how simple the experience is. … It all adds up to stronger security — and a better experience for current students, prospective students, faculty and staff.

IT team member
U.S. university

Putting scarce time to better use

Now the IT team is adding more servers to the Akamai solution and has the process down to five minutes per server. With the time that Akamai Guardicore Segmentation saves, the team is learning new cloud technologies and paying down technical debt. They're also looking into using Akamai to reduce the blast radius of ransomware attacks.

Summing up, the IT staff member says, "We knew Akamai would limit the spread of threats between servers. The surprise is how simple the experience is. Especially the way Akamai Guardicore Segmentation adapts our rules to account for the constantly changing IP addresses behind our cloud services. It all adds up to stronger security — and a better experience for current students, prospective students, faculty, and staff."

> Egress rules are a nightmare to figure out on firewalls, so before we just didn't do it. With Akamai it's simple, and it's another way to keep infections from spreading.
>
> **IT team member**
> U.S. university