Akamai Customer Story

Manufacturing Company Protects Against Lateral Movement Attack

Learn how a leading manufacturing company improved security with Akamai Guardicore Segmentation, boosting visibility and halting lateral attacks

Prevented lateral movement

East-west traffic visibility

Endpoint segmentation and visibility

The Challenge

Protecting a global enterprise

The IT security team of this manufacturing firm is responsible for multiple sites around the globe, most of which are mixed-use office and manufacturing facilities. To ensure a strong security posture, the team needed to standardize security controls throughout the organization and provide consistent protection across the distributed geographies.

“We wanted to move from an open, flat network to a best-practice segmented architecture,” explained the infrastructure architect leading the segmentation project.

Like many companies, this manufacturing firm initially turned to firewalls. However, managing a multitude of infrastructure-based rules and workstation-level changes and upgrades across the network quickly became time-consuming, even at a single site. Additionally, though visibility improved, it remained restricted to specific zones, making it difficult to get a full, centralized view of network activity and the dependencies between assets.

Stopping unauthorized lateral movement

While firewalls offered some coarse segmentation controls, they failed to address another key concern of the security team — unmanaged peer-to-peer communications. Therefore, it was essential to extend protection and visibility to that specific area. Not addressing it would leave the organization vulnerable to pass-the-hash attacks, ransomware, and other threats that rely on **lateral movement** among endpoints to propagate.

Manufacturing Company

Location
USA

Industry
Commerce

Solution
Akamai Guardicore Segmentation

Akamai

The Solution

After several unwieldy firewall control deployments, the team learned about Akamai Guardicore Segmentation and began internal discussions about the benefits and possibilities of a next-generation segmentation platform.

Comprehensive research must be performed for all new solutions that the company implements, so the team also evaluated several alternatives. After a thorough vetting process, the team ultimately moved forward with Akamai. “None of them gave us the whole solution like [Akamai], with traffic monitoring, flexible labeling, and rich application-level visibility through only a single agent footprint on a client,” said the infrastructure architect.

New insights and segmentation in action

For the first phase of the project, the company was able to quickly deploy the agent on approximately 2,000 workstations. The IT security team discovered a new level of visibility into the network and its communication flows as soon as the solution was in place.

“With the [Akamai] traffic maps, our visibility is 1,000% better now and includes PC-to-PC communications,” said the infrastructure architect.

The ability to drill down to the activity of an individual computer, while also understanding overall application-level activity, has helped the organization make more informed security decisions. For example, some users have installed applications for their home printers on their company laptops. It was discovered that many of these applications would continually scan the corporate network for supported devices. Based on this new insight from Akamai visibility, the team was able to stop the scans.

Threat remediation with microsegmentation

This new understanding of network activity has also helped the company stop external threat actors. For example, soon after the platform was deployed, the additional managed threat hunting service detected an asset communicating with a file with characteristics of a known piece of malware called GoldenSpy. Akamai analysts notified the company’s IT security team about the detected threat. The customer was also provided with an analysis of the infection scope, potential risks (matching findings with MITRE’s information about GoldenSpy), forensics (leveraging host-level insights gleaned from the platform), and recommendations for internal investigation and mitigation. The company then used granular policy controls to quarantine the infected system and stop the malware from moving laterally to new machines.

With a single agent on a machine, we’ve solved the problem of an endpoint attack by lateral movement for good.

Infrastructure Architect, Manufacturing Company

The Results

This company can now also create and manage policies centrally, including a central global workstation policy, and they have the flexibility to create one-off exceptions when a use case requires it. This ensures consistent enforcement anywhere there is an Akamai Zero Trust agent and reduces the risk of configuration mistakes and delays.

Additionally, time to policy has also improved dramatically at the organization. For example, making a change to firewall controls used to be a process that could take days. Using the pre-built policy templates as an initial guide, the IT security team can now create security controls for even the most complex use cases in less than an hour and apply them to the entire installed base in seconds.

The future with Akamai

While the project's initial focus was on standardizing the security controls for endpoint segmentation and access, there are plans to tackle additional use cases with Akamai Guardicore Segmentation. Stakeholders are now discussing an expansion of protection to include servers and critical applications such as the organization's ERP system.

No matter what tomorrow's plans include, the original project is already considered a success at the manufacturing firm and has dramatically reduced the attack surface and risk for the company's workstations. The team is now more confident in the organization's security posture against attacks that move laterally from endpoint to endpoint. As the project leader explained, "Now, with a single agent on a machine, we've solved the problem of an endpoint attack by lateral movement for good and can now go from a workstation with no policies to the full implementation of security controls in 30 seconds."

| Published 04/26