Publicly Traded Manufacturing Company Standardizes Security Controls and Saves Time with Guardicore Centra

A leading manufacturing firm that is traded publicly on the NYSE and serves markets around the world.

The Challenges

Protecting a global enterprise

The IT security group 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 for the project. 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 between endpoints to propagate.

Selecting a Solution

After several unwieldy firewall control deployments, the team learned about the Guardicore Centra Security Platform and began internal discussions about the benefits and possibilities of next-generation segmentation.

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 the Guardicore Centra Security Platform. **"None of them gave us the whole solution like Guardicore, with traffic monitoring, flexible labeling and rich application-level visibility through only a single agent footprint on a client,"** said the infrastructure architect.

INDUSTRY
Manufacturing

HQ COUNTRY
USA

ENVIRONMENT
Windows workstations

The Guardicore Centra Security Platform

For the first phase of the project, the company deployed Guardicore Centra to approximately 2,000 workstations. The IT security team immediately discovered a new level of visibility into the network and its communication flows once the solution was in place.

New insights and segmentation in action

"With the Guardicore traffic maps, our visibility is 1000% 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 Guardicore's visibility, the team was able to stop the scans.

Guardicore's Hunt service, leveraging Centra for threat detection

This new understanding of network activity has also helped the company stop external bad actors. For example, soon after the platform was deployed, the Guardicore Hunt service detected an asset communicating with a file with characteristics of a known piece of malware called GoldenSpy. The Hunt team 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 Guardicore Insight) and recommendations for internal investigation and mitigation. The company then used Guardicore 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

Standardizing and saving time

This company can now also create and manage policies centrally, including a central global workstation policy and the flexibility to create one-off exceptions when a use case requires it. This ensures consistent enforcement anywhere there is a Guardicore 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 before the new platform was a process that could take days. Using Guardicore's new policy templates as an initial guide, the IT security team can create security controls for even the most complex use cases in under an hour and apply them to the entire installed base in seconds.

The future with Guardicore

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 Guardicore. 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 manufacturer and has dramatically reduced attack surface and risk for the company's workstations. The team is now much 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 that problem for good and can now go from a workstation with no policies to the full implementation of security controls in 30 seconds."**

PRIMARY USE CASES

- Preventing lateral movement
- East-west traffic visibility
- Endpoint segmentation and visibility

FEATURES USED

- Process-level visibility
- Endpoint segmentation

Guardicore
Now part of Akamai

About Guardicore

Guardicore delivers easy-to-use Zero Trust network segmentation to security practitioners across the globe. Our mission is to minimize the effects of high-impact breaches, like ransomware, while protecting the critical assets at the heart of your network. We shut down adversarial lateral movement, fast. From bare metal to virtual machines and containers, Guardicore has you covered across your endpoints, data centers and the cloud. Our software-based platform helps you become more secure to enable your organization's digital transformation.