Guardicore

Case Study

"A firewall management system can't compete with Guardicore."

University project leader

INDUSTRY

- Education

MAIN USE CASES

- Preventing Lateral Movement
- Application Ringfencing

FEATURES USED

- Visibility
- Segmentation Policies
- Threat Detection and Response

State University Selects Guardicore to Protect Critical Building Operating Technology Across 24 Campuses

The Customer
Large State University

This large state university serves the higher education needs of more than 100,000 students, with more than 17,000 faculty and staff across its 24 campuses.

The Challenge
Centralizing the Network Infrastructure of 600+ Buildings

A prominent state university wanted to incorporate building automation systems securely into a statewide smart campus initiative. The team responsible for the university's physical plant and OT systems was concerned about a lack of segmentation protecting these devices and applications. They were also concerned about the university's IT network if it was removed from its existing air-gap state. As a result, the team responsible undertook an ambitious effort to centralize its building automation systems and improve security.

The university's project leader explained, "Up until about two years ago, all the campuses were pretty much on their own. We were hosting the main application server, but the individual campus controllers were sitting on IT networks, and not always segmented on separate VLANs from the rest of the campus traffic."

This meant a successful attack on a single building's control systems could easily spread to a campus's IT network or vice versa.

There was an additional economic reason for the project as well. "The university wanted to do energy management and see where we could cut costs," the project leader explained, "but we weren't getting any data from the campuses because they were all standalone systems."

"So we needed to connect them, but we needed to do it securely. With the connections coming from those remote campuses into our data center, they could create a backdoor into our network for a potential attack."

The ambitious project to bring everything onto a shared network infrastructure covered more than 600 buildings across 24 campuses in its scope. The department's Facilities Automation team was selected to execute the project.

However, the sheer complexity of the university's automation systems and the number of vendors involved presented another enormous challenge.

"We're managing elevator systems, HVAC, vibration analysis, lighting, electrical distribution, and electrical metering. Then we have all our main utilities, including steam generation, electrical distribution, and wastewater treatment. We deal with roughly 260+ contractors who work on these systems across all the various companies."

All those vendors needed access to the network – without introducing risk or interfering with each other's control systems.

Selecting a Solution

Wanted: East-West Traffic Visibility and Centralized Policies

Tempered Networks, a security provider focused on smart control systems and Internet of Things (IoT) networks was used to address the north-south connections between the remote campuses and the university's primary data center. With that challenge under control, the university still faced the problem of protecting more than 300 servers running within the data center from breaches.

"We were looking at solutions that supposedly handled east-west traffic, but none were as clean and simple as we wanted," the university's project leader recalled.

> *"We needed to find something easy to manage with a single pane of glass and a way to create rule sets based on application type. That's when Guardicore came into the picture."*

The team first discovered Guardicore when they came across Guardicore's free Infection Monkey breach and attack simulation (BAS) tool. Infection Monkey helps data center operators assess the resilience of their environments to post-breach attacks and lateral movement.

After the team downloaded the tool and started using it, they realized Guardicore Centra could solve the issues Infection Monkey uncovered.

The Guardicore Centra Security Platform is one of the few solutions on the market today focused primarily on micro-segmentation. It makes it easy for operators to define, create, and deploy security policies to govern communications between individual or logically grouped applications.

In the very first presentation with the university, the Guardicore team demonstrated the platform's unique visualization capabilities. Using Centra, data center operators can see all of the applications running in their environment and graphically map dependencies among them.

"That did it instantly for us. We knew this was exactly what we needed."

The Guardicore Centra Security Platform

A Distributed and Integrated Platform That Simplifies Security

Guardicore Versus Internal Firewalls

"Some people are dead set on firewalling and think it will solve everything," the project leader observed.

> *"A firewall management system can't compete with Guardicore."*

"With central firewall management, you still have to set up the rules for each firewall individually. With Guardicore, we can create an application group and say, "We want these systems to talk only to each other.""

Firewalls also present cost, resource, and manageability issues. "The management of all those firewalls would just be a nightmare. We'd probably need half a dozen people just to get the system deployed and make sure there are no issues, then at least two dedicated people just to manage it."

Moreover, firewalls lack the flexibility to set and modify policies at the application level. "With Guardicore, we can listen for a while and understand what's happening between systems and why they may need to communicate. With firewalls, it's all-or-nothing. A firewall is just going to block port-to-port, and that's it."

Micro-Segmentation with Centralized, Easy Management

The speed and ease with which team members can create and deploy rules was cited as another significant benefit.

"The first day we fired it up, we installed it on a couple of boxes, and then tried creating a policy to block one vendor from being able to see another. And just like that, it locked the first vendor out. That proved to me that this product was what we've been looking for," the project leader noted.

Guardicore's micro-segmentation tools and methodology don't require an expert. "Having something simple enough that anybody on our team can take advantage of it was a big seller for me."

> *"As soon as we got it installed, the team was able to get in, deploy it, and put some protection rules in place, and they were sold on it."*

Beyond Micro-Segmentation: Detection and Response

The visibility gained with Guardicore had the added benefit of surfacing operational anomalies within the data center. "We found a print spool service connecting to a network that wasn't ours," the project leader recounted. "When we finally tracked it down, it was somebody's remote desktop session that disconnected but never terminated, and it was continuously trying to talk back to the print server on their PC. If that PC got compromised, it could potentially be an avenue back to the application server."

Now that the team is actively using Guardicore, the university is already envisioning further security enhancements and efficiencies the solution makes possible.

"A future project is automating a lot of the functionality of the network if an incident happens. For example, if we detected a rogue MAC address or access point from a building, used Guardicore Centra to send a command to the Tempered Network solution to lock down that building, then sent an alert to an operator to remediate it and figure out what happened. Until now, we have not had that detection capability."

The Guardicore platform enabled the university's Facilities Automation team to reach its desired security state more quickly and easily than ever anticipated. "We've never really had a proactive tool like this that is constantly monitoring everything," the project leader explained.

Because Guardicore is monitoring east-west data center traffic, the team doesn't have to. "I want our team to be able to concentrate on our job, which is to help the university save energy and save money. We can't focus on that if we have to worry about what's going on in the data center."

The university's team set out to find a simple micro-segmentation solution. With Guardicore, they found that and more.

> *"We wanted something very easy to maintain over a long period, and by far, Guardicore exceeded our expectations."*

"It does what it says it does."

Want to learn more about Guardicore Centra? Visit www.guardicore.com today.