Guardicore

> *"Once we implemented Guardicore, we could identify traffic patterns that were not only unnecessary but also were previously unknown."*
>
> Edwin Blom,
> Chief Information Security Officer
> FCC Group

INDUSTRY

Environmental & Integral Water Management, Infrastructure Services and the Production of Associated Materials

ENVIRONMENT

- On-Premises Data Center
- Legacy Systems

PRIMARY USE CASES

- Preventing Lateral Movement
- East-West Traffic Visibility
- NIS Compliance
- Breach Mitigation

FEATURES USED

- Visibility
- Segmentation Policies
- Threat Detection and Response

CASE STUDY:

FCC Group

FCC Group Uses Guardicore To Improve Visibility and Prevent Lateral Movement

The Customer

With a presence in over 30 countries and 120 years of history, the FCC Group is a leading international operator in environmental, end-to-end water management, infrastructure construction and management services as well as associated materials production.

FCC's vision is to contribute to cities' development and progress, creating value for all citizens, customers, shareholders and partners. A century-old corporate culture and solid values enable FCC's businesses to grow based on long-lasting, transparent and mutually beneficial relationships with stakeholders who work with the Group.

The Challenges

Diverse Security and Compliance Requirements

The FCC Group prioritizes security in every engagement, ensuring measures are in place to protect client data whenever it begins a new project. With customers around the globe, it pays close attention to meeting evolving regulatory and certification requirements. These include the EU Network and Information Security (NIS) directive, which calls for segmentation and other protections for sensitive, critical information.

Coarse Data Center Segmentation

To accomplish the company's security and compliance goals, IT security leaders wanted to achieve segmentation granular enough to reduce the impact of breaches and prevent malware spread effectively. However, the organization determined that it could not easily or quickly accomplish this objective with its existing traditional firewall solution.

To address this challenge, the FCC Group began to search for a solution that would enable it to create and manage policies at the server level for its modern data center.

Selecting a Solution

The FCC Group evaluated several solutions, but Guardicore's software-based segmentation approach distinguished itself in several ways.

"Visibility and lateral movement detection were important when it came to the evaluation," commented Edwin Blom, Chief Information Security Officer at FCC Group. However, "The most critical capability was the ability to isolate a single asset, or group of assets, with the click of a button during a security incident."

Guardicore fulfilled these requirements, and, in addition, the platform was straightforward to use and could easily be extended to the organization's heterogeneous environment. This was critical since, though the business was primarily on-premises when the project began, cloud and container technology adoption was quickly ramping up and would need to be secured. Additionally, Guardicore would also enable the company to extend security to several legacy systems running critical workloads.

The Guardicore Centra Security Platform

The Guardicore Centra Platform's deployment was efficient, and the organization swiftly began to gain additional context into the network. This allowed the FCC Group to create informed segmentation policies to improve its security and compliance posture goals.

Comprehensive Visibility

Before, it was impossible to see and understand the context of traffic inside the organization's existing VLANs. "Once we implemented Guardicore, we could identify all traffic patterns that were not only unnecessary but also were previously unknown. With Guardicore, we can detect traffic, eliminate it or, if it's difficult to remove at the source, block it," explained Blom.

Additionally, the newfound visibility helped the security team better understand potential risks in the network and validate that the organization's servers, managed by a third party, are appropriately patched and that the latest antivirus version is installed.

More Effective Segmentation

FCC has successfully been able to meet its goals with Guardicore, separating traffic across business units and effectively isolating each one. The security team also applied additional segmentation policies to eliminate unnecessary communications between machines—significantly reducing the attack surface.

The team then further created a mechanism they refer to as the "red button", which uses Guardicore Centra's ability to create and enforce policies quickly. This policy template allows FCC Group responders to quickly isolate servers on the network if a breach or other security incident is suspected.

Detection and Deception

To further improve security, suspicious lateral movement is now tracked and can be addressed with Guardicore's deception capabilities. This allows the FCC Group to isolate any bad actors in a high-interaction deception environment, keeping them away from sensitive assets while recording their techniques for further analysis. Additionally, because FCC Group has integrated Guardicore with its SIEM solution, activity logs are available to help the team assess the possible impact of an attack and better respond to it.

Prepared for an Evolving Security and Regulatory Landscape

The organization plans to explore using Guardicore for container security and its enhanced Insight feature, which allows teams to collect real-time context from all endpoints and servers, use it to make informed decisions and create new rules to address additional compliance requirements at the workload level.

However, no matter what the future holds, the additional layer of security provided by Guardicore on top of the existing firewalls helps ensure the FCC Group is prepared for an evolving security and compliance landscape that increasingly calls for more granular segmentation.

Secure cloud migration with Guardicore Centra
www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.

Guardicore