Guardicore

Case Study

> *"Nano-segmentation is about monitoring the access context in order to allow only authorized users to access each server and each communication channel between machines. This is the kind of control we must have today."*
>
> Alex Amorim, Information Security Manager

INDUSTRY

Education

ENVIRONMENT

- On-Premises Data Center
- Multi - and Hybrid-Cloud

MAIN USE CASES

- Data Center Migration
- Secure Cloud Adoption
- Simplifying and Accelerating Compliance
- Realizing the Zero Trust Framework
- Faster Innovation

FEATURES USED

- Visibility
- Application Dependency Mapping
- Segmentation Policies

cogna EDUCAÇÃO

Cogna Group Migrates Data Center in Two Weeks With Guardicore

The Customer
A Leader in the Education Business

Founded in 1966, Cogna Group is a leader in the Brazilian education business. Operating under four brands – Kroton, Platos, Saber, and Vasta/Somos – the company offers primary, secondary, and higher education services to both B2B and B2C markets.

Aiming to improve peoples' lives through education, Cogna serves more than 2.4 million students across Brazil with its direct programs and partner institutions.

The Challenge
Securely Migrate a Data Center in Less Than 30 Days

When Cogna Group acquired Somos, the plan was to consolidate all of the new company's infrastructure, applications, and data into Cogna's existing datacenter. This would enable teams to manage on-premises equipment from a single location. It would also unify the parent organization's private cloud.

However, it quickly came to light that there was a short timeline for the project. By the time the company finalized the acquisition, the data center hosting Somos' assets only had one month of services remaining on its contract. This left Cogna's telecom and IT teams with less than 30 days to perform the migration. Such a tight deadline raised concerns over completing the move on time, in a way that would not compromise security.

Cogna needed to mitigate risk and preserve the organization's reputation. Therefore, it committed to creating and upholding a security framework based on the principles of confidentiality, integrity, and availability.

Additionally, Cogna had to keep its current information secure both during and after the migration. The range of products and services offered by Cogna was extensive. As a result, the company required the continued security of a tremendous amount of information related to students, proprietary materials, teaching systems, services, and application microservices.

Prior to working at Cogna, Alex Amorim had worked on sanitizing firewall rules for a large telecommunications company in Brazil. After six months compiling firewall rules, the project still had not been completed. As such, he was well aware of the challenges Cogna was facing.

Best-Practice Security
Embracing Zero Trust and Granular Segmentation

Amorim notes that, with the rise of new technologies, the market is evolving towards a new Zero Trust concept. Security solutions that were useful in the past are no longer effective today. In a corporate environment with direct connections between machines, you need to have visibility into communication flows and dependencies. This capability is key to ensuring the success of segmentation projects and threat hunting.

IT security leaders are adopting a new paradigm, moving away from traditional models and towards those that provide more flexibility.

They are seeking total protection against known and unknown threats in each of the network's segments and the equipment connected to them. Protection has to be as granular as possible, because risks come from every corner.

> **According to Amorim,**
> *"I can't trust anything nowadays. I can't trust my device, which is capable of stealing what is inside my network; I can't trust a third-party, who comes with a notebook and connects it to my network; I can't trust the notebook that an employee takes home; and so on. The context is Zero Trust."*

Firewalls on the edge of the network still have their uses. However, in the server environment, companies need to view and protect direct connections to VLANs and VPCs. Firewalls do not offer visibility into what happens within the server environment, who communicates with whom, and how tools communicate with one another Moreover, firewalls do not segment the environment - a key part of preventing threats from spreading.

The Solution
Simplifying and Accelerating Segmentation with Guardicore

With a rapidly approaching deadline and a desire to continue embracing the Zero Trust model, Amorim and his team considered their next steps.

Luckily, the solution to the migration challenge was close at hand. Cogna Group had recently deployed the Guardicore Centra Security Platform to improve security at its primary data center. This was the very data center into which the Somos assets needed to be migrated before the old data center contract expired.

Amorim knew how easy and fast it was to create and enforce segmentation policies with Cogna's existing Centra installation. He therefore immediately contacted the Brazilian Guardicore team to help him meet his swiftly approaching deadline. The team quickly mobilized and provided the assistance and speed Cogna required.

By partnering, Guardicore and Cogna Group found an efficient solution: install Centra into Somos' environment before the migration. That way, Cogna could safely make the move they needed, with the ability to control and view all interactions.

> **Amorim commented how well the migration went, saying,**
> *"The entire segmenting of the Somos infrastructure, applications, and data had been completed when we entered the new environment – where the machines were already protected by Guardicore technology. "*

Amorim continued, "Imagine the risk if we were to migrate to the new data center with machines without the proper protection, subjecting the whole group to Internet threats for lack of segmentation."

He also pointed out that Cogna could count on the excellent services provided by Guardicore support, which helped with the small adjustments needed on some machines. With both teams working together, the migration was successfully and securely completed in just under two weeks.

Looking to the Future
The Need for Multi-Cloud Security

In addition to maintaining a private cloud, the Cogna Group also uses multiple public cloud platforms such as AWS, Google, and Azure. Management of the environment is shifting from the responsibility of the company that provides colocation services to a new service provider.

Cogna plans to take this opportunity to improve its security posture and comply with the requirements of the upcoming Brazilian General Personal Data Protection Act.

> **Amorim explained,**
> *"Nano-segmentation is about monitoring the access context to allow only authorized users to access each server and each communication channel between machines. This is the kind of control we must have today."*

The future goal is to create centralized access through a password safe using the jump server concept. With the Centra platform overseeing the entire environment and all of Cogna Group's assets, it will be possible to make the vault the only access point.

Users, even if they are IT professionals, will not access the servers outside the password vault. In addition, they will not be able to move from one server to another without returning to the jump server, thus avoiding the lateral spread.

This approach will protect Cogna's assets from lateral attack movement, no matter where they are located, today or in the future.

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

About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security for any application, in any IT environment. www.guardicore.com