Guardicore technology reinforces security at Mater Dei hospital through network visibility and monitoring

Centra Platform ensures network microsegmentation for critical environment protection operating 24 x 7 x 365

Created in 1980 and located in the metropolitan region of the capital of Minas Gerais, Mater Dei Hospital has 1,081 hospital beds distributed in three units and 96 health centers. The institution is among the 10 best hospitals in Brazil, and is ranked one of the best in the world.

VISIBILITY: THE FIRST BIG CHALLENGE

You can't protect what you can't see

With a heterogeneous network connecting servers, medical equipment and workstations, Mater Dei Hospital sought greater visibility of the environment and the flow of applications. They needed information to be accessed uninterruptedly by the medical team, and were concerned about availability and security of applications.

The hospital environment is extremely critical as it must operate 24 hours a day, 7 days a week, 365 days a year without interruptions and without failures. The different areas of the hospital request access to applications at all times. Availability must be immediate for patient care. The security and privacy of data is also crucial, because any failure compromises the work of doctors and the treatment of patients.

Ianno Soares, CISO of Mater Dei Hospital, sums it up: "In addition to network transparency, we needed secure processes that worked all the time. Our big challenge was to see everything that goes through the network, while protecting our entire environment."

SOLUTION: THE GUARDICORE CENTRA PLATFORM

Microsegmentation prevents lateral movements in the network

Taking into account the aspects of network transparency and security, the hospital opted for the implementation of Guardicore's Centra platform, which, through microsegmentation, offers total visibility of network traffic, shielding both new and legacy applications through Zero Trust security.

"You can't protect what you don't know. The Guardicore platform shows all the network devices, pointing their location and the connection paths between servers and between them and other equipment," explains Ianno Soares, CIO of Mater Dei Hospital.

Thus, the security team visualizes traffic across the network, showing "who's talking to whom" - that is, all connections between servers - to securely deliver the resources needed by medical teams. It is this visibility that allows the flow between certain paths to be released only when that communication is predicted and legitimized by the security policies in place.

MaterDei
Rede de Saúde

INDUSTRY
Healthcare

HQ COUNTRY
Brasil

CHALLENGES

Increased visibility into network traffic composed by servers, medical equipment and workstations in order to increase system availability and security

Operating in an environment that does not allow failures, such as a hospital, the Guardicore system works in layers, staggering the monitoring and the connection path between servers. The system offers a "map" indicating the layers to be monitored through careful planning of stages that, in the hospital environment, are extremely critical: "you cannot stop an examination or robotic surgery", explains Ianno Soares.

ANTI-RANSOMWARE TECHNOLOGY

It's easier to isolate machines than people

Instead of trying to fight malware, Guardicore technology focuses on understanding and controlling the environment and applications. It uses micro-segmentation to minimize security gaps and prevent the attack from spreading in lateral movements. If a machine or application is compromised, it can be quickly isolated, preventing it from infecting other equipment.

That's the way ransomware is avoided, because ransomware happens exactly when the attack spreads from a single point, allowing the theft of access privileges to reach strategic information, which then becomes the object of the ransom demand.

TEAM INTEGRATION

Infrastructure, development, business and security all come together

"Today we can see everything that goes through the network, from the simplest to the most critical equipment," says Ianno Soares. Among the benefits this provides, he highlights the ability to better plan processing and security strategies for the most critical assets - which implies greater synergy between the security, infrastructure, development, and business teams.

By showing, for example, the processes and TCP/UDP ports that are being used, the Centra platform also reveals those that are free for the use of new developments, which allows security to stop being a limitation and, most of all, to become an ally of the other IT teams.

In addition to network transparency, we needed secure processes that went live on time. Our big challenge was to see everything that goes through the network while protecting our entire environment.

You can't protect what you don't know. The Guardicore platform shows all devices on the network, pointing out their location and the connection paths between servers and between them and other equipment."

Ianno Soares, CIO of Mater Dei Hospital

FEATURES USED

- Guardicore Centra

RESULTS

- Full visibility into network traffic at the process level
- Protection against the spread of malware
- Ransomware protection
- Better process planning
- Greater integration between the various technology teams
- Development of secure applications

Guardicore

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.