



220 + Service centers



10.000 +**Employees** 

## **History**

A **healthcare** giant that processes 75 million clinical exams per year.

# **Situation**

Complex infrastructure

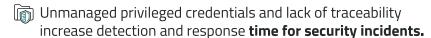
- **\* 2.000** unmanaged devices
- \* 1.500 critical servers
- **\* 500** databases
- **1.500** local domain credentials unmanaged and unprotected.

Configuration files and code contained hardcoded unprotected credentials.

## **Problem**



**Ransomware attacks** causes data loss and downtime, which affects its operation and business continuity.



Client was victim of a ransomware attack, which affected its systems and stopped exam delivery for seven days.

No visibility of actions performed through **privileged credentials.** 



#### **Solution**

- 500 people use **senhasegura** in the organization to perform privileged access on critical assets.
- senhasegura was implemented in only 3 days on a 3-node High Availability/Disaster Recovery architecture using a Cloud deployment architecture.
- senhasegura's best-in-class Discovery feature allowed the scan, discovery and onboard of devices in less than 6 hours
  1.500 servers 100 network assets and workstations
- **User Behavior** is used to stop any access from unknown origin.
- Integration with SIEM for real time alert sending.

#### Results

- 100% privileged credentials are now managed through senhasegura, allowing full traceability of actions performed in the environment.
- All privileged access is blocked from outside of the PAM solution and is allowed only through **senhasegura**.
- MFA, segregation of access and tiered environment delivers maximum level of security.
- Minimum recovery time of the environment