Customer Success

Orizon

Ensures Healthcare Record Confidentiality for 13 Million Patients

Overview

Orizon is a health technology company, responsible for handling procedure authorization for 43 healthcare insurance companies throughout Brazil. The company manages more than 150 million transactions annually across their payment and authorization systems for medical visits, exams, hospitalizations and claims for 13 million patients.

Challenge

About 1,100 users require regular access to over 40 systems where sensitive and confidential information for 13 million people are hosted. Orizon needed to ensure comprehensive management of the identities accessing the applications and personal records in compliance with audit requirements and in preparation for the Data Protection General Law (LGPD) which will go into effect in Brazil in August 2020.

Solution

Orizon adopted SailPoint to ensure governance of these records. The project ensured governance for more than 50 applications through an individualized, documented, controlled and monitored process to provide greater information security across the enterprise.

In markets advancing their legal framework in governance and data protection, it is now critical to define who accesses what, under what circumstances, and for how long. This is particularly the case in organizations where data is sensitive and confidential, which is common in the healthcare industry.

Ricardo Zeviani, Information Security Superintendent at Orizon, lives this challenge. He experienced firsthand what the complexity of managing access from an increasing user base along with an increased number of accessed systems means. On a small scale this may appear simple – such as administrative access to a workstation, password reset, new access requests and their respective levels of approval, registration, change of function and deactivation of users. This was the stage that Orizon was at in 2018. As the company started growing and expanding its strategic mission, they realized the need for stronger governance. The pending rigorous requirements of the Data Protection General Act, which will be in force in Brazil in August 2020, made this even more pressing.

With more than 10 years of experience, Orizon is the leader for back office management in Brazil. They have 43 clients for which they perform the authorization processing of plans, exam requests, and billing of the associated transactions. Orizon also offers services to turn a myriad of hard copy documents into digital records. On another front, it operates a benefit program for medications, which provides discounts on medicines sold in accredited pharmacies.

The company has a relationship with 140,000 service providers and over 11,000 pharmacies. In total, it processes 150 million transactions annually in its authorization systems and platform, which results in a significant database. Orizon uses this database to suggest more efficient administrative processes to reduce the waste or duplicity rate in exam and procedures.

This is where Zeviani's responsibility lies. The superintendent is responsible for the access of about 1,100 employees to more than 40 systems, with differentiated levels of access. In December 2017, they decided database access security should be centralized, individualized, rigorously documented, as well as automated where possible. Even more important was that the tool managing all of this required straightforward connectivity with legacy systems, and third-party validation including the Gartner Magic Quadrant. "Previously, access security was split between IT, the governance team, and the service desk," he describes. The creation of identities was ad hoc and did not follow a standard process. Basically, new users inherited the very same access permission as their colleagues in the same position and function, without further scrutiny.

The need for stronger information security, combined with the pressure posed by the new data protection legal framework, drove the deadline to implement an identity governance system within eight months. In this period, the connector of 23 main legacy systems should interact with the identity management tool. In turn, Orizon's goal for 2019 would be to extend the identity management to 43 systems, and simultaneously, implement a governance policy across all of them.

Following a bid including three other solutions, SailPoint gained the superintendent's preference for the program. All of the company's requirements were addressed with the solution. The strategy for a quick implementation was based on hiring two partners. The technology consulting company, Cherokee, performed a thorough analysis of Orizon to know which systems and programs to understand their current identity management framework. Another partner, Netbr, developed connectors with the legacy systems. "In parallel, we were assembling the solution's infrastructure: databases, servers, and deployment. With this, we were able to achieve all our implementation goals in the first year," shared Zeviani.

The project covered the entire lifecycle and system access of identities, according to each profile and function, as well as the follow up of the identities' useful life. It also took into account the automation of people and system provisioning and deprovisioning processes.

> **"We did not have a full picture of access, let alone who accessed what.**
>
> **Ricardo Zeviani,**
> Information Security Superintendent,
> Orizon

In a few months, Orizon achieved its initial goal, and today, it can automatically create new users for employees in its systems. "This reduced the service desk calls by 10%. We believe that, once the entire solution is implemented, this reduction will reach as much as 30%," the executive calculates. While before it would take about one week for an employee to be granted access to all of the systems he or she needed, today they can access what they need in less than one hour. Zeviani also touts the 80% fall in the recorded operating errors related to identity management. "Before SailPoint was implemented, the information fields gave room for mistaken or inaccurate information due to the manual entry of data", he added.

And just as important as guaranteeing better quality of data, SailPoint was to be able to centralize access across several systems from a single point. "In the past, each area was responsible for its team's access," he explains.

In Zeviani's opinion, the top management's engagement with the identity governance program was critical for its success. "Granting and removing access to the company's systems affects people's power inside the organization," he points out. "Users now only access what their positions and functions require, and everything is documented."

Zeviani is looking forward to the full implementation of the solution, when the life cycle of a user in the company is fully contemplated in the tool: hires, promotions, change of areas and dismissals, with their respective access permission and exclusion control mechanisms.

SailPoint®

About SailPoint
SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.