CUSTOMER CASE

Leading steel producer reduces risk while saving millions in disaster preparation with Quest

A multinational steel producer with 30,000 employees modernized its IT infrastructure with Quest. By implementing Recovery Manager, Change Auditor, and Active Roles, the company enhanced security by restricting AD access, automated disaster recovery processes, and improved governance with proactive monitoring. These innovations support efficiency, resilience, and global compliance.

From towering skyscrapers to heavy-duty machinery, steel forms the backbone of everyday life. A global leader in steel production that operates across the Americas delivers these essential materials that shape industries and communities. To support such critical operations, the company's IT infrastructure must be as strong and resilient as the steel it produces.

With more than 30,000 employees in Brazil, Argentina, Mexico, Canada, and the United States, the steel producer relies on Microsoft Active Directory (AD) to power its identity management, access provisioning, and security protocols. But managing an extensive network that spans 70 domains across a single forest brings unique challenges, from maintaining clear and secure access policies to ensuring rapid recovery in the rare event of

Country: Brazil

Employees: 30,000

Industry: Manufacturing

Challenges

With 70+ domain controllers in a single consolidated AD forest, the company struggled with slow, complex, manual processes to maintain security, manage access, and prepare for potential attacks. To strengthen internal controls, increase efficiency, and solidify disaster preparedness, they turned to Quest Software.

Solution

The company implemented Quest Software's Recovery Manager for Active Directory Disaster Recovery Edition and Change Auditor along with One Identity Safeguard.

Benefits

- Accelerated disaster recovery from 10 hours to 65 minutes
- Saved equivalent of $14.18M USD by reducing disaster recovery time
- Reduced risk of unauthorized access by enhancing security protocols

disruptions.

By partnering with Quest, the company has begun transforming its IT landscape. Tools like Recovery Manager for Active Directory Disaster Recovery Edition, Change Auditor, and One Identity Safeguard have enabled the automation of critical workflows, stronger security controls, and a more robust disaster recovery framework. These solutions ensure the company's IT infrastructure is prepared for today's challenges and the opportunities of tomorrow.

Reduced risk of unauthorized access by enhancing security protocols

Enhancing security and readiness across a complex environment

Managing IT at a global steel production company means navigating the demands of a multinational organization whose operations rely heavily on technology. With over 70 domain controllers housed within a single consolidated AD forest, the company struggled with complex processes to maintain security, manage access, and prepare for potential attacks.

"We've been fortunate not to experience downtime from cyberattacks or major outages, but our reliance on manual processes left us exposed to risks," explains an information security specialist at the organization. "As a company operating at our scale, we didn't want to wait for an incident to happen before improving our systems."

However, users and analysts had broad access permissions to the AD console, creating potential vulnerabilities, while a lack of automation in workflows slowed processes down. Recovery strategies depended on manual intervention, making them time-consuming and difficult to execute with precision in high-pressure situations.

To stay ahead of regulatory mandates, the company recognized that its multinational footprint meant it should be ready to provide evidence of disaster recovery protocols when needed. Above all, the company's leadership set a clear goal to strengthen internal controls, improve operational efficiency, and solidify disaster preparedness to ensure they could meet future challenges with confidence.

A unified solution for security, access, and recovery

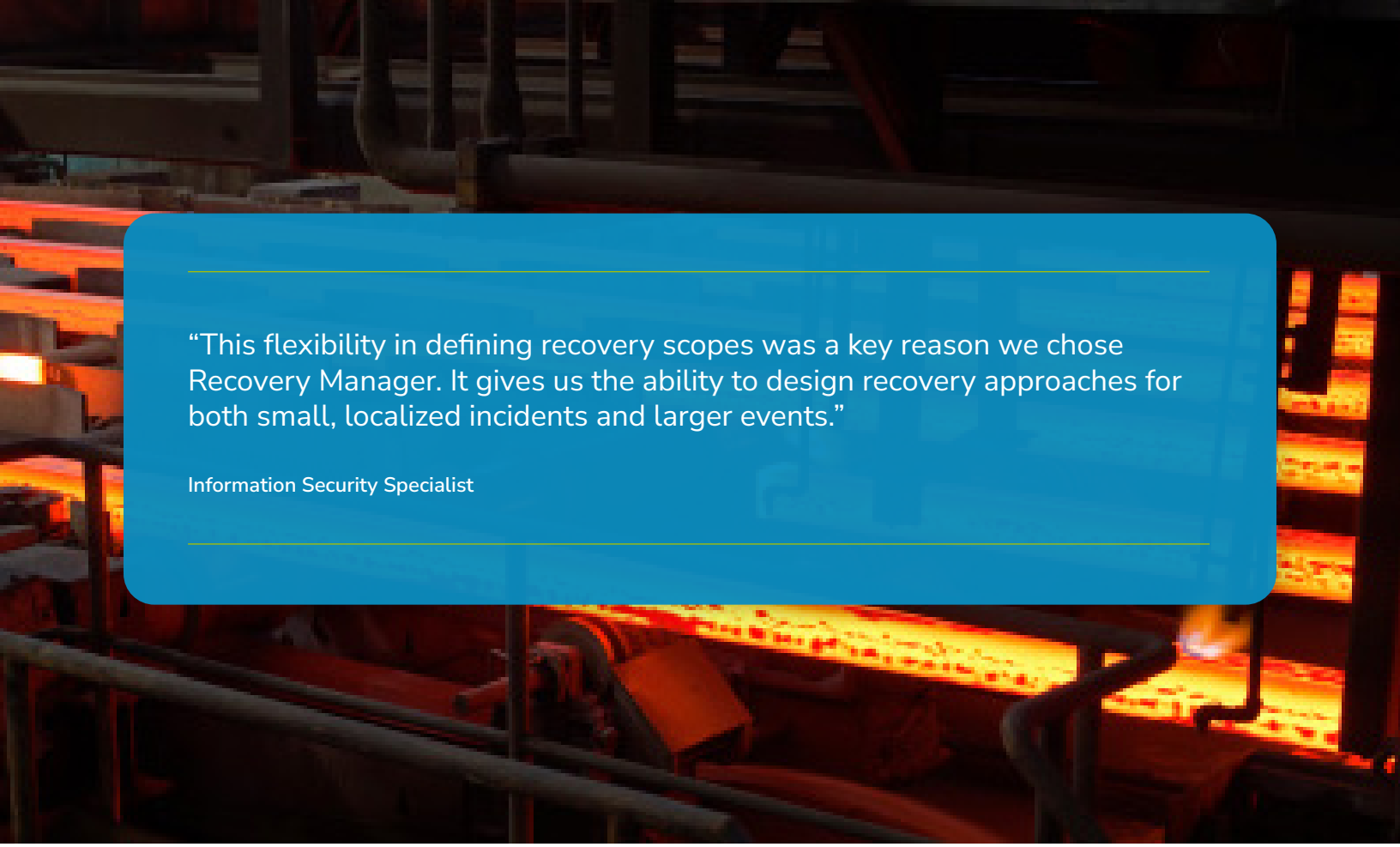
To address its growing infrastructure needs, the steel producer turned to Quest, implementing a suite of solutions designed to enhance security, automate workflows, and simplify disaster recovery. The adoption of Quest's Active Directory security and resilience solutions allowed the company to modernize its IT environment while supporting the company's global operations.

One of its first priorities was to improve access security by eliminating direct connections to the AD console. With Safeguard, the team created strict controls around privileged access, ensuring that administrative activities could only be performed following a structured approval process. No user or IT analyst could directly access critical AD infrastructure, which reduced the risk of accidental changes or vulnerabilities caused by human error.

Accelerated disaster recovery time from 10 hours to 65 minutes by automating processes

"We've been fortunate not to experience downtime from cyberattacks or major outages, but our reliance on manual processes left us exposed to risks. As a company operating at our scale, we didn't want to wait for an incident to happen before improving our systems."

Information Security Specialist



> “This flexibility in defining recovery scopes was a key reason we chose Recovery Manager. It gives us the ability to design recovery approaches for both small, localized incidents and larger events.”
>
> Information Security Specialist

“These changes brought greater consistency and control to our workflows,” the company says. “With Quest, we can govern AD access more effectively, while still maintaining operational flexibility.”

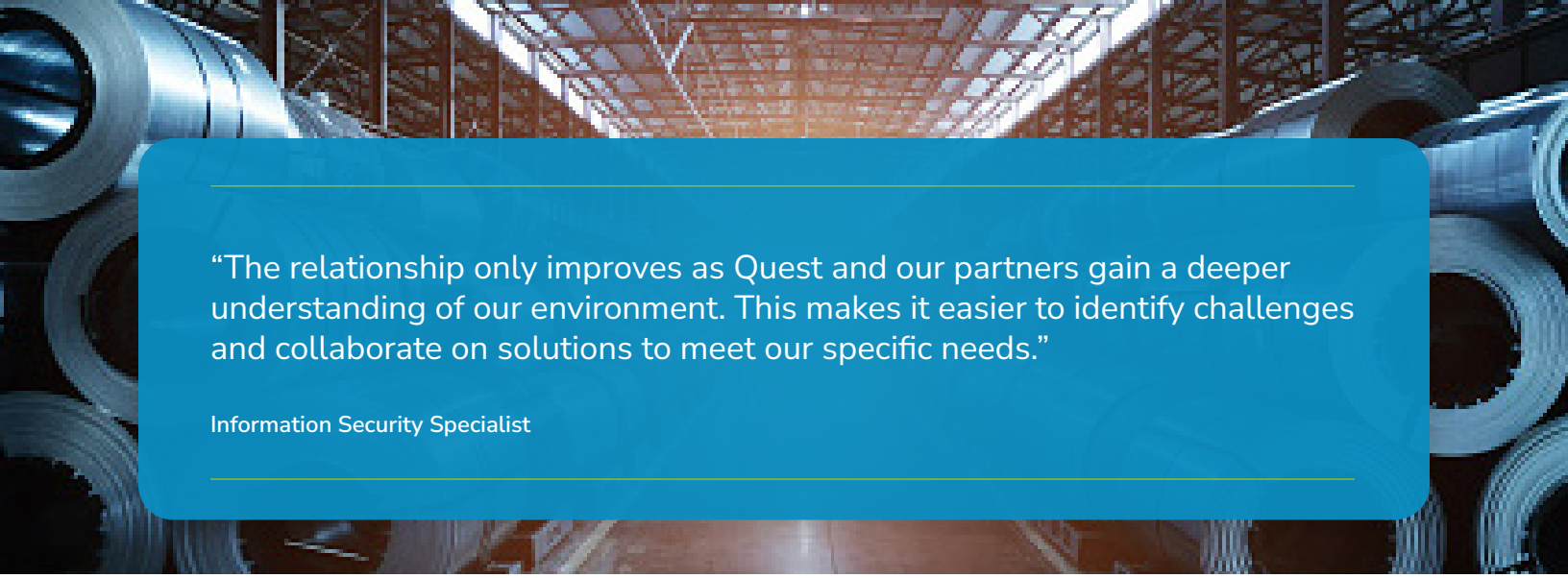
The team also implemented Recovery Manager for Active Directory Disaster Recovery Edition to simplify and accelerate disaster recovery processes. By enabling the creation of recovery projects tailored to specific scenarios, Recovery Manager allows the company’s IT team to recover individual services or even their entire AD environment quickly and automatically in case of disruptions.

“This flexibility in defining recovery scopes was a key reason we chose Recovery Manager,” a representative explains. “It gives us the ability to design recovery approaches for both small, localized incidents and larger events.”

Although still in the early stages of testing the solution within a new Oracle Cloud Infrastructure (OCI) environment, the company is already developing updated disaster recovery plans that reflect the enhanced capabilities of Recovery Manager. These plans will allow automated recovery processes to replace manual intervention, speeding up recovery times and adding operational resilience.

To further optimize AD management, the team uses Change Auditor, which provides detailed visibility and monitoring of changes to AD objects and configurations. This solution allows the IT team to identify potential issues or misconfigurations before they escalate, ensuring a more proactive approach to infrastructure management.

Saved equivalent of $14.18M USD by reducing disaster recovery time



> “The relationship only improves as Quest and our partners gain a deeper understanding of our environment. This makes it easier to identify challenges and collaborate on solutions to meet our specific needs.”
>
> Information Security Specialist

Accelerating disaster recovery to save $14.18M USD

By implementing Quest’s solutions, the company has significantly improved security, operational efficiency, and disaster preparedness. With Recovery Manager, the team reduced disaster recovery time from 10 hours to 65 minutes, representing savings equivalent to $14.18M USD. The company now has a scalable and future-ready framework for managing access, infrastructure, and recovery.

In addition to day-to-day improvements, streamlined governance processes have made it easier to demonstrate compliance with multinational regulatory requirements. Whether internally driven or prompted by external audits, the company’s updated workflows ensure the team can provide proof of disaster recovery protocols and security practices with ease.

The steel producer is currently finalizing and testing its disaster recovery plans in its new OCI environment. Once operational, these plans will allow the team to run annual recovery tests with speed and precision, offering a new level of confidence in their ability to respond to potential disruptions.

As the company continues to refine its processes, the flexibility of Quest solutions provides the adaptability needed for a business of this scale. This foundation ensures the company remains resilient as new technological and operational needs arise.

Beyond security and recovery, the company values the strong partnership it has developed with Quest and its implementation partners. “The relationship only improves as Quest and our partners gain a deeper understanding of our environment,” the team says. “This makes it easier to identify challenges and collaborate on solutions to meet our specific needs.”

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on

CaseStudy-Anonymous-KA-101624

Explore our solutions →

Quest