Energy company improves Active Directory security and cyber resilience.

Edison slashes risk with attack path management and auditing tools from Quest.

Country: **Italy**

Employees: **5,800**

Industry: **Energy**

Website: **http://www.edison.it/**

Founded in 1884, Edison S.p.A is one of the leading energy companies in Italy. In addition to the production, distribution and sale of electricity from a variety of gas-fired, hydroelectric, wind and solar power plants, the company provides innovative energy and environmental services. Moreover, Edison is accelerating Italy's path towards decarbonization and sustainable energy through a research and investment plan aligned with the United Nations' Sustainable Development Goals.

Keeping Active Directory functional and secure is vital to cyber resilience.

Edison takes a similarly proactive approach to the cyber resilience of its hybrid IT ecosystem. Years ago, they launched a program to regularly analyze and classify their applications according to business

Challenges

Edison S.p.A has been serving Italy through responsible energy production for over 135 years. A consequence of this long history, however, was an Active Directory (AD) infrastructure that had grown in both size and complexity over the years. The IT team recognized that AD was one of the most vital technologies in use, so they used a variety of Microsoft, open-source and custom tools to try to uncover its vulnerabilities and monitor changes and other activity. However, they were all too aware that those tools were not providing the deep visibility they needed to ensure cyber resilience.

Solutions

Working with partner Microsys and using solutions from Quest, Edison dramatically expanded its ability to thwart adversaries by both identifying attack paths in AD and seeing exactly how to remediate them. Moreover, the IT team can promptly spot and respond to threats in progress by efficiently auditing and alerting on activity across their entire hybrid AD environment.

Benefits

- Identified attack paths in Active Directory that other tools missed
- Clearly visualized those attack paths, facilitating communication among IT teams
- Provided clear remediation strategies
- Delivered comprehensive monitoring of the hybrid environment from a single dashboard
- Improved threat investigation and response with actionable, customizable alerts

impact so they can be protected appropriately. Applications that are absolutely essential to the company's continued operations are categorized as "vital."

One of those vital technologies is Active Directory, which provides the authentication and authorization services required for users to do their jobs and most business processes to run. As Giampaolo Tacchini, CISO of Edison, put it, "Since the beginning of our cyber resilience project, Active Directory has been classified as one of our vital applications. If we are not able to deliver this application, the company would be in serious trouble to survive."

Getting a complete understanding of Tier Zero assets was challenging.

With that classification of AD in mind, Edison began working with its trusted partner Microsys to analyze, consolidate and restructure its AD environment using migration solutions from Quest. One key goal was to identify all the company's most valuable, or Tier Zero, assets. Tier Zero includes critical servers like domain controllers (DCs) and all highly privileged accounts — as well as all accounts that could gain elevated privileges through a series of steps known as an attack path, which abuses factors like concealed permissions, nested group membership and inherent security gaps in AD architecture.

Using a variety of tools, Edison and Microsys gained some valuable information about the company's Tier Zero assets, but they were keenly aware that the insight was not comprehensive enough, nor did it account for the dynamic nature of Active Directory. Moreover, the team was simply not getting the actionable information they needed to address issues that were uncovered.

"We used a custom tool, a Microsoft tool, the open-source version of BloodHound and an internal tool developed in collaboration with a specialized third party," recalls Tacchini. "They helped us understand that we had serious problems with our Active Directory — but not how to solve them. For instance, the internal tool supplies only basic information about AD and not details like nested groups that can be part of attack paths, and the Microsoft tool provides only a static picture of the situation. As a result, we lacked proper visibility into how the changes made day by day could influence the availability and security of our Active Directory."

Lack of insight into Active Directory means business risk.

The team was acutely aware that lack of comprehensive insight into Active Directory put the company at risk. "We needed to improve the resilience of our Active Directory to warranty the availability of the entire information system of the company," Tacchini explains. "But the tools we had did not allow us to have the proper level of control over the system. We were not confident in our ability to determine if we were exposed to a serious security threat."

The risk to security and cyber resilience was increasingly serious. As Tacchini put it, "We had identified more than 20,000 issues within our Active Directory — and we were aware that the situation was worsening."

Quest offers a suite of solutions to improve Active Directory security and resilience.

To address the problem, Edison and Microsys considered solutions from Quest, Semperis and Tenable. After careful evaluation, they chose SpecterOps BloodHound Enterprise for advanced attack path management, and Change Auditor and On Demand Audit for auditing and change management across the hybrid IT ecosystem. Key factors in the decision included Quest's strong reputation for service and expertise, the quality of the solutions, and the thorough coverage of Edison's use cases.

"We were not looking only for a monitoring tool — our project is named 'Active Directory resilience'," says Tacchini. "Not fully understanding the potential risks to which our Active Directory was exposed and not grasping how the changes being made affected its posture was a serious problem. Quest offers a complete portfolio that enabled us to improve cyber resilience by strengthening Active Directory security."

> Not fully understanding the potential risks to which our Active Directory was exposed and not grasping how the changes being made affected its posture was a serious problem. Quest offers a complete portfolio that enabled us to improve cyber resilience by strengthening Active Directory security.

Giampaolo Tacchini, CISO at Edison

In particular, the Quest solutions deliver the powerful combination of attack path management and attack path monitoring. "We were already using BloodHound in red teaming activities and we knew that it was the right choice from an offensive point of view," says Francesco Contardi, project manager of the Active Directory resilience program at Edison. "So, the Quest integration with BloodHound was another big advantage — BloodHound Enterprise enables us to visualize attack paths and understand the choke points, and the Quest auditing tools allow us to continuously monitor all attack paths we have not yet addressed."

> BloodHound Enterprise enables us to visualize attack paths and understand the choke points, and the Quest auditing tools allow us to continuously monitor all attack paths we have not yet addressed.

Francesco Contardi, Project Manager at Edison

BloodHound Enterprise provides insight into attack paths, choke points and Tier Zero assets.

SpecterOps BloodHound Enterprise provided far deeper insight into attack path management than Edison and Microsys had been able to glean with their previous tools. While the team had already identified some weaknesses in AD, they were surprised at the number and types of issues that were posing a risk. "BloodHound Enterprise highlighted a wide variety of vulnerabilities in our Active Directory," reports Contardi. "In addition, it has helped us further map out our Tier Zero assets to inform our AD restructuring initiative. It is very helpful indeed."

Moreover, SpecterOps BloodHound Enterprise delivers visibility not only into the security weaknesses in AD, but how to remediate them. "The graph analysis in BloodHound Enterprise is extremely valuable because it highlights the choke points where we can intervene to reduce the risk most efficiently," Contardi explains. "From a technical point of view, it was quite complex because we had to communicate the misconfiguration or other issue to all the different teams and get them all on board to fix the problem. Having better visibility enabled us to do it easier and faster."

Still, Active Directory is a complex system, so remediation efforts need to proceed with caution. "BloodHound Enterprise provided practical remediation guidance that we could easily apply from a technical perspective, and we have been able to address a number of choke points," Contardi continues. "But from an organic point of view, remediation is complicated because of possible impacts on the teams, applications, teams and other factors involved. We need to be sure that any change that we apply does not fix one problem only to generate two new ones."

Change Auditor and On Demand Audit provide attack path monitoring as part of broader activity auditing and change management.

With Change Auditor and On Demand Audit, Edison can effectively monitor the attack paths they have identified but have not yet been able to mitigate.

More broadly, these integrated solutions pinpoint suspicious activity across the hybrid IT ecosystem and provide advanced alerting and search capabilities to speed investigation and informed response.

"The Quest hybrid auditing suite enables us to promptly detect risky activity, both in our on-premises environment and on the Microsoft 365 platform," says Contardi. "We are particularly happy that we can now monitor for possible indicators of compromise (IOCs) related to identity attacks, such as DC replication and Golden Ticket creation. And the automated email alerts are also really helpful because they enable faster response with a higher level of certainty. Real-time alerts have been especially valuable for spotting suspicious logon activity from Azure. In addition, the improved AD auditing allows us to troubleshoot technical problems faster and improve our security level."

> **"The Quest hybrid auditing suite enables us to promptly detect risky activity, both in our on-premises environment and on the Microsoft 365 platform. We are particularly happy that we can now monitor for possible indicators of compromise (IOCs) related to identity attacks, such as DC replication and Golden Ticket creation."**
>
> *Francesco Contardi, Project Manager at Edison*

Another key benefit of the integrated Quest auditing solution was improving the accountability of third parties charged with managing Edison's systems. "With On Demand Audit in place, we began to see actions in our cloud platform being performed by our outsourcers that didn't respect our policies," recalls Contardi. "For example, we spotted usage of service accounts by human operators and other improper activity designed to cut corners and complete their day-to-day tasks faster or more easily. With the information from the Quest tool, I was to be able to ask them to stop doing those things and to monitor the situation to ensure they complied with our policies."

The right partners make all the difference.

Edison praises both Quest and Microsys for their vital roles in the success of their Active Directory security and cyber resilience project. "Over the past decade, Microsys has helped us complete several projects using Quest solutions, including migrating workloads to Microsoft 365," says Tacchini. "As we have collaborated with them to implement a strong AD security model based on Tier Zero, the Quest tools have been quite valuable, especially the visualizations of attack paths and prioritization of mitigation strategies."

"Microsys has been really helpful throughout our projects and solved many problems, such as setting up custom rules," adds Contardi. "But the real value comes from their deep knowledge of Active Directory. We have a really complex environment with more than 20 years of history, and their expertise has made it possible to migrate our systems without disrupting vital applications and operations, as well as to complete projects much faster."

Edison is continuing to expand its Active Directory resilience project and will be considering several additional Quest solutions. In particular, GPOADmin improves attack path management by securing Group Policy objects (GPOs), in addition to delivering other critical Group Policy management capabilities like automated attestation and the ability to quickly revert unwanted changes. And adding On Demand Recovery will ensure reliable backup of the hybrid Active Directory environment and quick recovery from any mistakes, corruption or disaster.

PRODUCTS AND SERVICES

Products

- On Demand Audit by Quest
- Change Auditor for Active Directory by Quest
- SpecterOps BloodHound Enterprise

Solutions

- Microsoft Platform Management
- Cybersecurity Risk Management for Active Directory

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 X (formerly Twitter) and LinkedIn.