Quest Software automates and optimizes identity lifecycle management with Active Roles

Country: **California, USA**

Employees: **3,600**

Industry: **IT Solutions and Management Provider**

Website: **quest.com**

Does a two-decade use of One Identity solutions like Active Roles make a difference in an organization's cybersecurity? It does for Quest Software.

Cybersecurity and software solutions companies like Quest have always known it's important to be proactive about their defenses. Being proactive with their identity security, instead of reactive, was of grave importance.

"Reactive organizations are not going to put this tool in until they either fail an audit or they're breached," said Eric Weintraub, Quest Software IT Manager.

"This tool" is Active Roles from One Identity, and with it, Quest was ahead of the identity security game. "We've been using Active Roles for almost two decades," said Weintraub. And while they currently have a hybrid environment utilizing both Active Directory and Entra ID, they benefit daily from the benefits of Active Roles in their directory security.

Challenges

Governing identities in an organization from start to finish was always a manual effort for Quest Software, done directly through Active Directory. Provisioning and deprovisioning were ticket-based tasks that bogged down the service desk and exposed the company to risk from human error.

Solutions

Active Roles allowed Quest to automate identity lifecycle management securely and efficiently, minimizing human error, saving time and offering nearly unlimited flexibility.

Benefits

- User-operated self-service enablement
- Risk reduction by removing the need for more security permissions
- Access templates for effectively delegated administration
- Streamlined logging for optimized audits and compliance adherence
- Integrated automation with custom scripts and HR provisioning for more efficient workflows and minimized risk of human error
- Ability to craft dynamic groups and rules for maximum flexibility
- Virtual attributes

Heavily reduced risk

“The reality is,” said Weintraub, “everybody has these issues.” That is very true. Every organization, particularly the growing number of businesses that rely on digital assets, faces risk in their digital environment. But using Active Roles enabled Quest to minimize their risk profile.

Human error – minimized

Weintraub and his team at Quest know that one of the greatest security risks to a company is human error. And that Active Directory is one of the biggest targets for threat actors to attack.

Before implementing Active Roles and other One Identity solutions, Quest was using native Active Directory tools to manage and protect their data. It was manual, laborious work, and was prone to human error. With Tier 0 assets at stake, access management was critical, and privilege management that reduced the possibility of human error couldn’t be more important.

> Admin credentials that are used by humans can only be accessed for a few hours at a time before their passwords are reset by Safeguard

said Weintraub, emphasizing the benefit of integrating Active Roles with privileged access management tools for air-tight security.

The security of groups within AD was a deciding factor for using Active Roles at Quest. Active Directory allowed them to reduce human error by automating security policies for each and every group. “They kind of self-manage themselves,” said Weintraub. “It’s an important thing to do, not just from a governance perspective but from a security point of view as well, because if you don’t do that, then inevitably one of these groups, inadvertently and due to human error, will end up being a problem. Too many rights and a hacker will find their way into that group and make it to the top.”

Manual tasks - automated

Automation goes beyond group policy for Quest when using Active Roles. Weintraub commented on the efficiency and accuracy of the tool through its automations, particularly when dealing with both provisioning and deprovisioning. “What happens when somebody leaves the company, and their password isn’t turned off and they are not happy about being terminated? They can do all sorts of horrible things.”

Quest no longer has to worry about this problem – Active Roles automates permissions management for a smooth transition both coming into an organization and going out. “All of our permissions delegation is done within Active Roles. Delegated administration leads to better security, better auditing and tighter security control.”

Jon Hillis, Quest Software Systems Engineering Senior Advisor, adds that a huge benefit of Active Roles “is the dynamic groups and the rules that you can craft.” These rules and groups, while editable, have set-it-and-forget-it policies that are automatically policed and enforced.

Risk reduction has become a quantifiable factor for Quest thanks to automation that minimizes human error. “The automation of account management removes human error,” Weintraub said, “and removes the need for more security permissions.”

Easily met compliance standards

“You know, we get audited dozens of times a year,” Weintraub said, “ad nauseam, to be honest.”

Active Roles helps them face those audits with confidence, empowered by the knowledge that they are fully compliant with industry standards. They attribute this confidence to the identity lifecycle automation that Active Roles provides. Weintraub, for that matter, is convinced that without this automation, Quest wouldn’t pass some of the more stringent audits.

Between effectively delegated administration thanks to access templates, and the fact that Quest drives all Active Directory changes through Active Roles, the team can reach full visibility for incredibly easy compliance adherence through activity trails and tracking.

“If you’re in a healthy environment and you’re an IT person doing what they’re supposed to do, you have all this governance and compliance stuff these days,” said Weintraub, adding “I don’t see how you can actually achieve any of it without a tool like Active Roles.”

Immensely enhanced efficiency

It's common knowledge that service desks are perpetually backlogged and are rarely ever afforded the resources needed for real-time resolution. And while Quest strives for a good quality service desk, deadlines are still measured in days, not hours. "So, if somebody new needs to be hired and then the service desk needs to provision their accounts, there can be time delays," Weintraub said, adding that quality issues consistently arise from a rushed IT team. This makes lifecycle management automation crucial for Quest and makes Active Roles invaluable to their workflow.

Active Roles enables self-service experiences for Quest, without compromising security for groups and objects, and automates access during provisioning and deprovisioning to ensure high-level security for more valuable assets.

This not only reduces risk but also saves the IT team tremendous amounts of time. According to Weintraub, "The unified self-service experience is a huge time and data savings since we don't have to record all that data when it's deprovisioned or reach out to the user. To make resources go further, we empower our users to do more. Increasingly more."

Hillis said the amount of time to locate data and craft queries has gone from 15 minutes or more to milliseconds as a result of deploying Active Roles.

"Active Roles does all the heavy lifting for us," said Weintraub. "There's no way a human being could provide an SLA like that. And it's done correctly and accurately every time."

Ultimate flexibility

The ease of deployment is one of the most endearing features of Active Roles for Weintraub. Its flexibility extends beyond what it can do into the realm of how fast one can master it.

"Anyone that actually knows how to use Active Directory in basic Windows Server management should be able to take it and run with it," said Weintraub.

That said, it can be used for all sorts of things, from password management to self-service attribute changes and more. "It's a testament to the product's flexibility that it's capable of taking something so complex and automating it," Weintraub said. "We literally bend and flex [Active Roles] to our needs in really wonderful ways."

Conclusion

The role of directory administration and management can be rife with challenges and complexity, time constraints and regulations to comply with. According to Eric Weintraub, IT Manager at the decades-long Active Roles user Quest Software, "[Active Roles] really does make you look like a rock star."

Active Roles empowers an organization to reduce risk through automation, reducing human error and saving valuable time. Its flexible features streamline security while simultaneously optimizing user experience and minimizing human error.

To Quest, said Weintraub, "Once you enable [Active Roles features], you will look like a very competent IT organization."

About One Identity

One Identity helps organizations strengthen cybersecurity, boost efficiency and control costs through the One Identity Fabric, a holistic approach to identity and access management (IAM). By unifying IAM tools, including identity governance and administration (IGA), access management (AM), privileged access management (PAM), and Active Directory management (AD Mgmt), it ensures optimal functionality and efficiency. This cohesive structure reduces identity sprawl and extends governance to the farthest endpoints of your IAM ecosystem. Proven and trusted on a global scale, One Identity manages more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY