CUSTOMER CASE

Global bank ensures security, cyber resilience and compliance

The Canada-based bank relies an integrated suite of Quest solutions — and its partnership with the world's top Active Directory experts.

In industries like banking, Active Directory security and availability is especially vital

No business wants to suffer a security breach or service downtime, but for highly regulated and critical sectors like finance, such events can be especially devastating. That's why a large Canada-based bank with a presence in North America, the Caribbean, Europe and Asia-Pac has long relied on a suite of solutions from Quest Software to secure, monitor and ensure swift recovery of its hybrid IT ecosystem.

The bank has a single production Active Directory (AD) forest with seven domains and one production Entra ID tenant. Keeping them secure and available is a top priority. "When retailers, social media companies and many other service providers experience an outage, customers may get angry and some of them may even take their business to another vendor," explains a senior infrastructure engineer from the bank. "But banking is super sensitive because that is where your money is. If our operations were to shut down for any length of time, there will be loss of revenue, and there would also be regulatory impact because we have to comply with mandates from multiple regions, including not just Canada but the US, the EU and more. But even

Region: Canada

Employees: 60,000

Industry: Finance

Challenges

A large international bank must ensure the security and cyber resilience of its large hybrid IT ecosystem, as well as maintain and prove compliance with a growing set of increasingly stringent regulations across the many regions it serves.

Solution

For nearly two decades, the bank has relied on solutions and expertise from Quest Software. As it migrated workloads to the cloud, Quest Software was ready with integrated solutions that deliver unified visibility and control over the entire IT environment. Moreover, the Quest professional services team provides in-depth consulting and knowledge transfer, empowering the bank to proactively optimize security, cyber resilience and compliance.

Benefits

- Stronger security through robust auditing and change control
- Enhanced cyber resilience with reliable backup and fast recovery of the hybrid environment
- Ability to ensure and prove compliance with regulations
- Peace of mind that comes from a long-term relationship with a trusted partner and advisor

more important would be the serious and lasting damage to the bank's reputation. As a result, Active Directory security and cyber resilience are critical for our business."

The bank has relied on AD security and recovery solutions from Quest Software for nearly two decades

The bank has been partnering with Quest Software for nearly two decades. "We started with Recovery Manager for Active Directory, followed by InTrust and Active Roles, and we quickly saw the value add," says the senior infrastructure engineer. "When Change Auditor came along, we saw the benefits it offered, so we brought it in. Although we have kept a close eye on the market over the years, we have never found another vendor that offers products with such wide range of features — and that also coexist and integrate amongst each other, which greatly enhances the value add of the whole solution."

Moreover, as technologies advanced and business realities changed, the bank found that Quest products kept evolving to keep up. "Almost everything we are doing on premises is getting extended into the Entra ID space," he adds. "Quest Software has been ready with SaaS solutions that give us visibility and control over the entire hybrid environment, and those tools have been rapidly joining our portfolio. We found the value we get from our Quest solution set is much more attractive to us compared to other tools on the market."

Robust auditing and change management deliver strong security

Today, cybersecurity experts recommend that organizations adopt an assume-breach mindset. That makes it vital to implement comprehensive auditing and analysis of activity across the environment. With Quest solutions, the bank's IT team has the visibility and control they need to prevent costly breaches and downtime.

"We used to do auditing with native tools, and we found it quite painful because it was difficult to interpret the cryptic logs and identify threats," the senior infrastructure engineer recalls. "Change Auditor provides highly enriched logging that is truly beneficial for us. We easily customized some of the built-in reports and now our InfoSec teams can accurately spot

and investigate out-of-band activity. We even have the reports generated automatically on the schedule we choose and sent to a designated mailbox."

The bank team also relies on Change Auditor to detect drift in Active Directory configurations that could open security gaps or compromise service availability. "Over the years, any Active Directory tends to accumulate excess access rights, stale identities and other issues, and ours was no exception," notes the senior infrastructure engineer. "With Change Auditor, we were able to collaborate with the InfoSec team and clean up the directory to make it more secure and easier to manage."

An additional benefit of Change Auditor is its ability to block changes to powerful security groups, critical Group Policy objects and more. "Using Change Auditor, we have put many Active Directory objects and attributes into protection policies, which prevents them from being changed, whether accidentally or maliciously," the senior infrastructure engineer explains. "That approach has withstood extensive testing: We perform regular red team exercises to attempt to breach the environment, and Change Auditor has been there to prevent the breach from occurring."

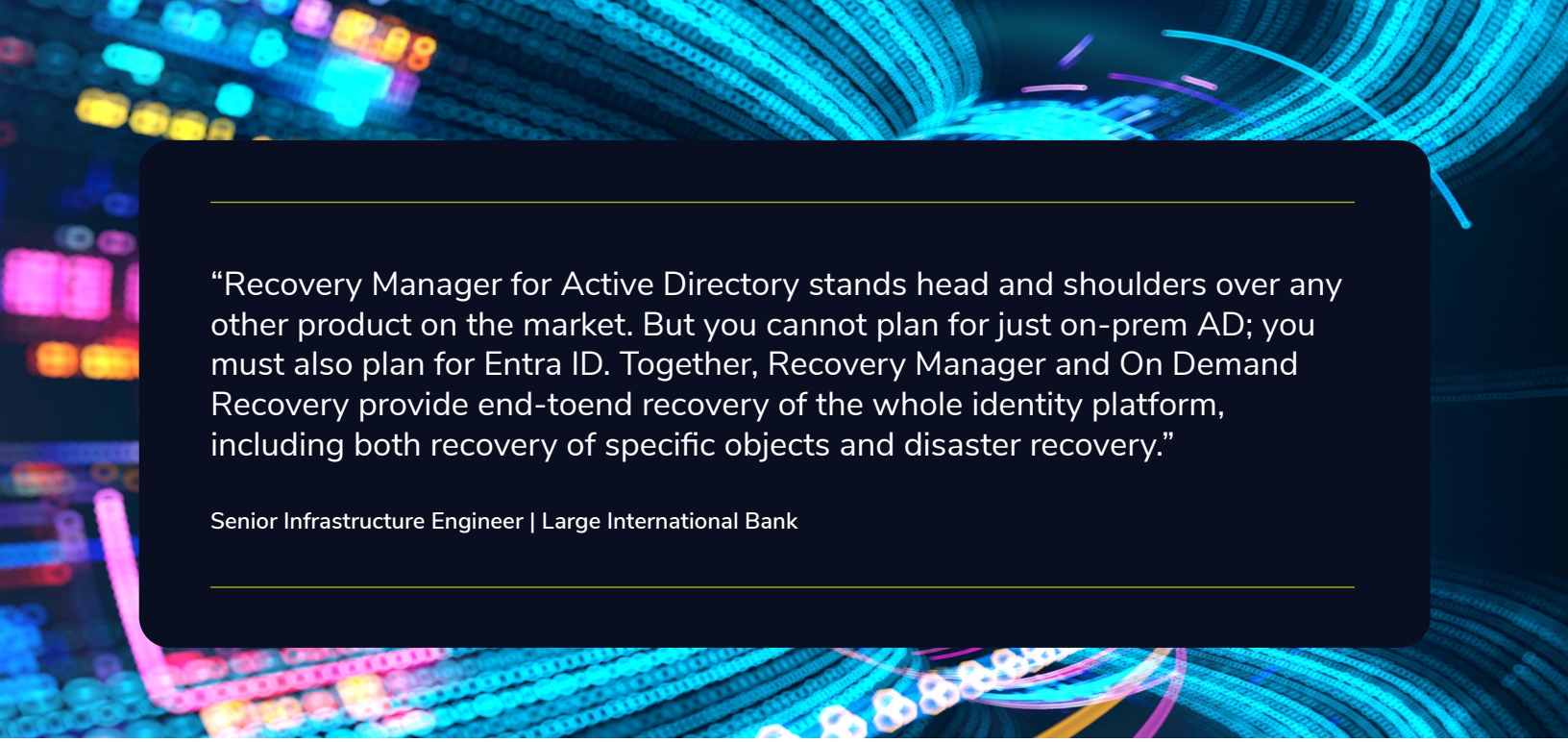
Moreover, with its Quest portfolio, the bank has visibility and control across the entire hybrid environment. "Because Change Auditor is integrated with On Demand Audit, we have consolidated reporting," says the senior infrastructure engineer. "Being able to track changes both on premises and in Entra ID is a tremendous value add for us. For example, when a team requests privileged access to certain

data or applications, we can thoroughly review their previous activity. We can show them what changes they have made over a long period of time and demonstrate that they don't actually need any standing privileged access. As a result, we can minimize our attack surface area."

Speedy and reliable disaster recovery delivers cyber resilience

The bank recognizes that even the most comprehensive identity threat detection and response strategy cannot prevent all adverse events. Accordingly, they have built a robust disaster recovery strategy using Recovery Manager for Active Directory integrated with On Demand Recovery.

> "Although we have kept a close eye on the market over the years, we have never found another vendor that offers products with such wide range of features — and that also coexist and integrate amongst each other, which greatly enhances the value add of the whole solution."
>
> Senior Infrastructure Engineer | Large International Bank



> "Recovery Manager for Active Directory stands head and shoulders over any other product on the market. But you cannot plan for just on-prem AD; you must also plan for Entra ID. Together, Recovery Manager and On Demand Recovery provide end-toend recovery of the whole identity platform, including both recovery of specific objects and disaster recovery."
>
> Senior Infrastructure Engineer | Large International Bank

Indeed, the bank's senior leadership understands how critical the Active Directory and Entra ID identity platforms are for the business. The senior infrastructure engineer recalls that they attended a presentation about the infamous NotPetya attack. While the primary target was Ukraine, companies around the world suffered staggering damage. For instance, shipping giant Maersk had no backups of its Active Directory, so it had to painstakingly shuttle a domain controller that luckily had been offline during the attack from Ghana to the UK; Maersk estimated that recovery cost $250–$300 million, though other insiders suspect the total was actually much higher. Even more compelling for the executives at the presentation may have been the fact that it took just 45 seconds for NotPetya to bring down the network of a large bank. "We didn't have to sell the importance of our identity platforms to our CEO," says the senior infrastructure engineer. "He grasped it very quickly. AD and Entra ID disaster recovery was aligned with the risk known to the business."

With the Quest solutions, the bank has implemented a comprehensive disaster recovery strategy that includes a pair of synched Recovery Manager servers in each data center. "Each server has a full immutable backup of the entire environment, so we don't need all four to survive a disaster, we need just one. In addition, we have two Recovery Manager servers in Azure with their own immutable backups, which provides additional redundancy."

The bank tests its disaster recovery plan regularly, and the results speak for themselves. "If we were to have a cybersecurity incident that destroys our entire forest, we know we could restore the forest well within four hours," the senior infrastructure engineer reports. "Recovery Manager removes the definitions of the 70+ domain controllers we have in production and brings up a pristine new forest using one of our immutable backups. Plus, thanks to the integration with On Demand Recovery, we can recover not just AD but also Entra ID."

Security and cyber resilience are essential for regulatory compliance

Financial institutions are subject to strict regulatory requirements and oversight, and banks with an international presence have to comply with mandates from multiple jurisdictions. Quest solutions can dramatically ease this compliance burden.

"Change Auditor automatically generates the reports we need and sends them to appropriate teams," explains the senior infrastructure engineer. "At the same time, Recovery Manager and On Demand Recovery enable us to comply with the most stringent disaster recovery requirements. In fact, given the depth of reporting and the capability of the tooling we have, we have no issues whatsoever in meeting the regulations we are subject to. Moreover, we are well-positioned to address any new requirements that come our way."

An integrated suite of solutions is critical for today's hybrid IT ecosystems

A collection of disparate point solutions is not an effective approach to cybersecurity and cyber resilience today; organizations need integrated solutions that enable a unified approach across the hybrid environment. Indeed, the senior infrastructure engineer argues that this is a defining value of the bank's investment in Quest solutions.

"When you look at the extensive portfolio of Quest solutions and how they integrate seamlessly with each other and complement one another, that's where the value add is," he says. "For example, Recovery Manager for Active Directory stands head and shoulders over any other product on the market. But you cannot plan for just on-prem AD; you must also plan for Entra ID. Together, Recovery Manager and On Demand Recovery provide end-to-end recovery of the whole identity platform, including both recovery of specific objects and disaster recovery."

An experienced and trusted partner is as important as any software product

As much as the bank values the Quest solutions it replies upon, the senior infrastructure engineer is quick to point out that the relationship with the vendor is just as crucial. "There are very few vendors with the maturity and capability that Quest Software has," he notes. "We particularly appreciate the depth of experience and knowledge of Quest professional services. Our internal teams very much take a hands-on-keyboard approach, and we rely on the Quest experts to advise us about optimizing our processes. They help us understand best practices and use the Quest products most effectively in our environment."

The support team is equally experienced and helpful. "We actually have not had many support engagements over the years because the solutions work so well," notes the senior infrastructure engineer. "But when we have reached out, the support team is quite responsive and usually resolves the problem quickly. And if we happen upon a product bug, the issue gets escalated into the sight of relevant executives, which we appreciate."

In fact, the bank is interested in expanding its portfolio of Quest solutions. In particular, they are actively looking at protecting their Tier Zero assets with Security Guardian and SpecterOps BloodHound Enterprise.

"There are very few vendors with the maturity and capability that Quest Software has. We particularly appreciate the depth of experience and knowledge of Quest professional services. Our internal teams very much take a hands-on-keyboard approach, and we rely on the Quest experts to advise us about optimizing our processes. They help us understand best practices and use the Quest products most effectively in our environment."

Senior Infrastructure Engineer | Large International Bank

"We used to do auditing with native tools, and we found it quite painful because it was difficult to interpret the cryptic logs and identify threats. Change Auditor provides highly enriched logging that is truly beneficial for us. We easily customized some of the built-in reports and now our InfoSec teams can accurately spot and investigate out-of-band activity."

Senior Infrastructure Engineer | Large International Bank

Products

- Change Auditor
- Enterprise Reporter Suite
- GPOADmin
- InTrust
- On Demand Audit
- On Demand Migration
- On Demand Recovery
- Recovery Manager for Active Directory Disaster Recovery Edition
- One Identity Active Roles

Solutions

- Microsoft Platform Management

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 Software 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.

Explore our solutions →

Quest