Large telecom boosts cybersecurity and cyber resilience

Bell Canada strengthens cybersecurity and ensures quick AD recovery with solutions from Quest.

Country: **Canada**

Employees: **50,000+**

Industry: **Telecommunications**

Website: **https://www.bell.ca/**

Founded in Montréal in 1880, Bell is now the largest communications company in Canada. The company provides advanced broadband wireless, internet, TV, media and business communications services. Bell is wholly owned by BCE Inc.

Bell is committed to ensuring strong cybersecurity and cyber resilience. Its IT environment is mainly on premises. Its primary Active Directory domain includes 105,000 user accounts, and the IT team is in the process of consolidating some 30 additional domains into the primary domain.

Active Directory is too critical to trust to manual tools.

Bell recognizes that Active Directory is more than just infrastructure — it runs their identity services, which are critical for Bell to operate as a business.

Challenges

As the largest communications company in Canada, Bell knows the importance of strong cybersecurity. The IT team recognized that native solutions and manual processes were insufficient to monitor the organization's large IT ecosystem with more than 100,000 user accounts and ensure quick recovery of its forest in the event of a cyberattack or other disaster. Accordingly, they sought out top-of-the-line Active Directory cyber resilience solutions.

Solution

With Quest® Change Auditor and Quest® Change Auditor for Logon Activity, the IT team now has deep visibility into modifications and other events throughout the IT ecosystem. They are able to promptly spot suspicious activity, quickly investigate it and take action to prevent security incidents. Meanwhile, the Quest Active Directory forest recovery solution provides peace of mind that the team could restore operations quickly in case of a disaster.

Results or Benefits

- Improves security by enabling the identification and elimination of outdated, risky protocols like NTLM v1 and RC4
- Reduces the attack surface area by identifying important vulnerabilities like unneeded Group Policy objects (GPOs)
- Enhances cyber resilience by ensuring quick recovery of the Active Directory forest in case of disaster
- Speeds troubleshooting with deep insight into changes across the hybrid IT ecosystem

As a result, the company wanted to move on from native tools and manual processes for AD auditing and recovery. Simply put, trying to parse cryptic logs and correlate disparate events is not an effective way to spot suspicious activity in the IT ecosystem and respond to threats to AD security. Even worse, restoring just one domain controller (DC) requires meticulous coordination of numerous steps across multiple phases, and recovering an entire forest is an even more complex, time-consuming and error-prone process.

Accordingly, Bell wanted not just a tool vendor,but a cybersecurity partner. Quest fit the bill, thanks to its unmatched expertise in Active Directory, comprehensive and integrated portfolio, and top-notch support teams. The company now relies on Quest solutions for both AD disaster recovery and change management.

Reliable AD forest recovery is a vital insurance policy.

Bell's partnership with Quest began with disaster recovery. "The evaluation team said that the Quest Active Directory recovery solution was far superior to the other tools they researched," reports Phillip Palha, Senior Manager for Active Directory Delivery at Bell. "The Quest AD recovery solution gives us the peace of mind that we can recover back to a specific point in time if there is a catastrophic failure in Active Directory — that's huge. We know that if anything ever goes down, we can quickly bring everything right back to normal, because of this tool."

By automating many of the manual tasks in the process, the Quest AD recovery solution speeds recovery dramatically — while ensuring that steps are completed in the correct order and without errors. In fact, a Forrester Consulting Total Economic Impact Study commissioned by Quest found that the solution consistently reduced AD recovery time to just 1–4 hours for those interviewed. Without an AD recovery tool, recovery time was almost 100 times longer! Plus, the Quest solution can significantly reduce the risk of malware reinfection during the recovery process with the option to restore to a clean operating system.

Phil also lauds the Quest solution for simplifying the personnel requirements for AD recovery. "Bell enforces proper separation of duties as a business best practice," he notes. "As a result, with our old manual approach, multiple teams needed to be involved in recovery, which slowed the process significantly. With the Quest solution, we no longer have to reach out to the various storage and utility teams within Bell; my team can handle the entire recovery ourselves without outside assistance."

Thankfully, Bell has not actually needed to use the Quest solution to restore its AD forest. As Phil puts it, "The Quest AD recovery solution is more of a valuable insurance policy... We hope to never have to use it, but it's there if we need it.'" However, the IT team has used the Quest tool a few times to recover specific domain controllers.

Tracking change and logon activity empowers Bell to identify and close security gaps.

The Bell IT team is always eager to learn about tools that help strengthen cybersecurity. When Quest presented Quest Change Auditor, they were quickly saw that it would be a valuable addition to their security tool portfolio.

"With Change Auditor, we can easily see exactly what changes were made, who made each change, where the change came from, and the previous and new values. Moreover, it enables us to quickly revert unwanted changes, and even to protect critical objects from being modified in the first place," explains Phil. "It is a fantastic tool that we've leveraged quite a bit already. It has enabled us to identify and mitigate a lot of vulnerabilities that we might not have uncovered without it."

Phil recalls several occasions when the corporate security team noticed unusual activity and asked his team to investigate. "With Change Auditor, we were able to quickly check for any suspicious changes made during the timeframe indicated by the security team," he says. "For example, Change Auditor enabled us to identify GPOs that were no longer needed and delete them to reduce our attack surface area."

The Logon Activity module of Quest Change Auditor has also proven invaluable to Bell. "The tool has allowed us to track and eliminate antiquated protocols that are logging into our Active Directory systems," Phil reports. "In particular, we leveraged it to identify use of the NTLM v1 authentication protocol, which is far less secure than NTLM v2. As a result, we were able to strengthen security by eliminating use of the weaker protocol across our IT infrastructure. We also use it to track use of the insecure RC4 protocol and TLM and TLS connections."

A true cybersecurity partner, Quest offers unmatched support, regular product updates and a comprehensive portfolio.

Bell values its partnership with Quest for a range of reasons beyond the effectiveness of the solutions the company currently uses. "The support has been fantastic, including detailed information about product functionality," notes Phil. "Moreover, unlike other vendors, Quest is constantly improving its solutions; they are not stagnant."

Plus, Quest offers a comprehensive portfolio of solutions that enable customers to keep strengthening their security. improvement to it. "Quest has a number of additional products that we can leverage in the future," Phil says. "Right now, we're especially interested in SpecterOps BloodHound Enterprise for its ability to map out attack paths in Active Directory and pinpoint the choke points to mitigate to shut them down."

Bell heartily recommends all the Quest solutions it relies on.

"I would definitely recommend all of the Quest products we use," states Phil. "They are easy to learn and simple to use, and they provide all the functionality that they promise."

In fact, Bell is frequently approached by other vendors, so Phil has had lots of opportunities to compare other tools with the Quest solutions. "When you're the largest telecom in Canada, everybody knocks on your door," he says. "But no other vendor has been able to offer us anything nearly as good as what we already have with Quest products. When other vendors claim they could serve us better, we just chuckle and think, 'yeah, good luck with that.'"

> **"When you're the largest telecom in Canada, everybody knocks on your door. But no other vendor has been able to offer us anything nearly as good as what we already have with Quest products. When other vendors claim they could serve us better, we just chuckle and think, 'yeah, good luck with that.'"**
>
> *Phillip Palha,*
> *Senior Manager for Active Directory Delivery at Bell*

PRODUCTS AND SERVICES

Products

- Quest Change Auditor
- Quest Change Auditor for Logon Activity
- Quest Recovery Manager for Active Directory

Solutions

- Microsoft Platform Management
- Enterprise Backup and Recovery

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

Quest