Government agency enhances cybersecurity.

State Department of Transportation identifies and shuts down attack paths in its complex Active Directory.

Department of Transportation

Country: **United States**

Employees: **2,500**

Industry: **Government**

Finding and mitigating attack paths is vital for security and compliance.

Like the private sector, government agencies are facing an onslaught of increasingly sophisticated cyberattacks. Unfortunately, the job of building an effective security strategy can be even more difficult, thanks to the complexity of long-standing legacy systems. The Department of Transportation (DoT) for one U.S. state faced an additional challenge: the loss of experienced IT professionals due to the Great Retirement in the wake of the pandemic. As a result, the IT team was acutely aware that they "didn't know what they didn't know" about the risks lurking in their IT environment.

For help, the DoT turned to longtime partner Quest and learned about attack path management using SpecterOps BloodHound Enterprise. With the solution, the agency has been able to uncover attack paths that could be used to compromise its Active Directory, pinpoint effective remediation measures, and — critically — provide clear visualizations proving the risk reduction to their business counterparts, which quickly resulted in their buy-in to the required changes.

About this case study

At one state Department of Transportation, the Great Retirement in the wake of the pandemic meant the loss of a number of experienced IT pros. The complexity of their long-established Activity Directory made one fact abundantly clear: The IT team didn't know what they didn't know — and those unknowns were putting security, business continuity and compliance at risk.

Solution

With SpecterOps BloodHound Enterprise, the IT quickly gained deep insight into the attack paths in its Active Directory that adversaries could exploit to gain access to its most valuable systems and data, or even total control of the domain. The clear visualizations of these attack paths made it easy to convince their business counterparts of the urgent need to remove certain permissions or otherwise restrict particular access. As a result, the DoT has been able to dramatically improve its cybersecurity and compliance posture.

Benefits

- Identified attack paths that adversaries could exploit to gain control of the IT environment
- Charted every relationship and connection to pinpoint effective remediation measures
- Clearly illustrated those attack paths to business stakeholders, gaining their buy-in for remediation
- Reduced stress on the IT team caused by loss of institutional knowledge due to retirements

Solutions at a glance

- Microsoft Platform Management

The IT team also relies on Quest Change Auditor to monitor attack paths that have not yet been mitigated, and Quest Recovery Manager for Active Directory to provide peace of mind that they can promptly revert unwanted changes to a particular AD object or restore an entire forest. As a result, the DoT has dramatically improved cyber resilience and strengthened its compliance posture.

Unknown vulnerabilities in Active Directory pose serious risk.

Active Directory is the epicenter of the DoT's operations, providing the critical authentication and authorization services that enable users to log on and access the resources they need to do their jobs. But like any identity management system, Active Directory is complex, so over the years, it can become quite convoluted.

As a result, users can end up with access rights they no longer require, stale objects can lie ripe for takeover by malicious actors, and the net effect of dozens or hundreds of Group Policy objects (GPOs) can be difficult to ascertain — especially when many experienced IT team members have retired and their replacements lack their deep knowledge of the evolution of both systems and processes.

What permissions does each user have now — and what access could they easily gain?

The IT team understood these risks and began implementing policies to enforce the least-privilege principle of granting each user exactly the access they need to do their job — no more, no less. "We make an Active Directory account for each new user," explains the information systems manager for the DoT. "Over their years working here, that person might have three or four different positions. A lot of times, their old permissions stay with them, even though they don't need them anymore. In addition, in the past, most users were granted local administrative rights on their machines, which introduced unnecessary risk. So our first goal was to strip away excessive permissions and enforce least privilege."

However, it's not enough to simply understand the permissions that each user currently has; it's also vital to understand what permissions they could gain by exploiting the ones they have. In other words, the complex vulnerabilities inherent in virtually any working Active Directory create opportunities — attack paths — for adversaries who compromise an ordinary user account to quickly escalate their privileges and seize control of Active Directory

> **Despite our earlier efforts to strip local administrative rights from all users, BloodHound Enterprise found a lot more people who were members of a group that was a member of the Administrators group of the local machine.**
>
> *Information Systems Manager, State Department of Transportation*

Least privilege is an elusive goal without the right tools.

The IT team at the DoT began using the Microsoft Security Assessment Tool (MSAT) to try to dive deeper into the security status of their IT infrastructure. However, they found that the tool did not provide useful insight and remediation guidance tailored to their specific environment. "The output of the Microsoft Security Assessment Tool was so vague and hard to understand that we often couldn't even be determine what changes were being proposed," notes the information systems manager at the DoT. "Moreover, when we did get a clear recommendation, we were worried about the impact that the change might have on our users and our business processes. You've got to be careful and understand exactly what you're doing to avoid causing serious issues."

> **You don't know what you don't know. Once you see the attack paths laid out by BloodHound Enterprise, it's like, holy crap, I didn't realize we're that vulnerable.**
>
> *Information Systems Manager, State Department of Transportation*

Then the IT team performed the Quest Active Directory Security Assessment featuring SpecterOps BloodHound Enterprise. Quite simply, they were amazed. "We didn't know how vulnerable we were until we did a trial with BloodHound," says the information systems manager. "BloodHound showed us security groups that were nested

down in our Active Directory. Wow — we didn't realize all those groups were members of other groups. In fact, despite our earlier efforts to strip local administrative rights from all users, BloodHound Enterprise found a lot more people who were members of a group that was a member of the Administrators group of the local machine."

Indeed, BloodHound Enterprise even discovered Tier Zero assets that the IT team had not previously known about. "I was surprised at the Tier Zero assets that were identified," recalls the information systems manager. "You don't know what you don't know. Once you see the attack paths laid out by BloodHound Enterprise, it's like, holy crap, I didn't realize we're that vulnerable. We've got a lot of good defenses and best practices in place, but there were still so many attack paths."

BloodHound Enterprise identifies the choke points for mitigating attack paths — and provides the clear insight required for buy-in from business users.

Moreover, unlike the MSAT, BloodHound Enterprise gave the IT team the practical insight they needed to take action to mitigate the attack paths in their Active Directory. "The hardest part of risk mitigation is actually communication — getting business users to understand why changes are necessary," the information systems manager explains. "We can't just start pulling permissions from them without a reason why. BloodHound Enterprise gives us a clear visualization of the attack paths in our Active Directory so business users can see for themselves the urgency of removing certain permissions."

As a result, the IT team was able to quickly get buy-in from the affected user groups, including application developers, CAD support teams and others. "The visualizations in BloodHound Enterprise saved us tons of time," says the information system manager. "Really they did, because if we didn't have those visuals to show the business users, there'd be too many questions and I would have to have schedule meeting after meeting."

In fact, the IT team was impressed with just how easy BloodHound Enterprise made the entire process. "We simply type a group name and we can see everything that it would touch in a visual map with all the attack paths, like a big spider web," says the information systems manager.

"Then we can simply click to drill down. That's invaluable — I show exactly how an attacker could gain access to critical assets. You can't argue with it; it's right there in front of you. And once the team sees the path and understands the risk, they're okay with the mitigation measures we need to take."

> **The hardest part of risk mitigation is actually communication — getting business users to understand why changes are necessary. BloodHound Enterprise gives us a clear visualization of the attack paths in our Active Directory so business users can see for themselves the urgency of removing certain permissions. That saved us tons of time.**
>
> *Information Systems Manager, State Department of Transportation*

Small changes — if they're the right ones — can have a profound impact.

The IT team understands that risk mitigation is a never-ending process, since IT ecosystems are constantly changing. But they rest easier knowing that each day, they have made significant, measurable progress toward stronger cybersecurity. "BloodHound Enterprise enables us to clearly see the choke points that cut off a whole set of attack paths at once," notes the information systems manager. "It's very exciting because after we make a change, we can see exactly the impact it made by reducing the number of attack paths in the visualization. We can keep track of what we've done in a quantifiable way and prove the value of the investment to the management team."

Those measurable improvements dramatically reduce the stress on the IT team members. "Before, we didn't know what we didn't know. Now, BloodHound gives us the knowledge we need," explains the information systems

manager. “It fills me with confidence that I can go home and say, ‘You know what? We made it better today. We choked off many more attack paths that could have been used to compromise our Tier Zero assets.’ I pride myself on my work, and when I go home, I can say we accomplished a great deal of good today.”

> **BloodHound Enterprise enables us to clearly see the choke points that cut off a whole set of attack paths at once.... We can keep track of what we’ve done in a quantifiable way and prove the value of the investment to the management team.**
>
> *Information Systems Manager, State Department of Transportation*

PRODUCTS

- Quest Active Directory Security Assessment
- SpecterOps BloodHound Enterprise
- Change Auditor
- Recovery Manager for Active Directory

Quest strengthens not just cybersecurity, but cyber resiliency.

The Department of Transportation understands that while identifying and mitigating attacks paths is vital, it is only one piece of a larger cyber resilience strategy. Accordingly, they rely on not just BloodHound Enterprise but additional Quest solutions as well. Quest Change Auditor delivers real-time threat monitoring and security tracking of all key user activity and administrator changes. In fact, Change Auditor can play a critical role in monitoring attack paths that organizations have identified but have yet to mitigate, and the IT team is eager to realize the full value of this powerful and flexible solution.

Of course, organizations also need to prepared in case disaster strikes. With Quest Recovery Manager for Active Directory in place, the IT team at the DoT has peace of mind that an AD disaster will not become a business disaster. The solution slashes AD forest recovery time from days or weeks to just hours.

These solutions complement BloodHound Enterprise beautifully, helping the DoT strengthen not just cybersecurity, but cyber resiliency.

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.