Hybrid Active Directory cyber resilience

Protect your hybrid AD environment and mitigate risk with the NIST Framework

Active Directory (AD) security sits as your organization's cornerstone, but it's also every cyber villain's favorite target. After all, if they can control your AD, then they can control your entire enterprise. But, the constantly changing and complex nature of AD environments makes AD security difficult. Ransomware, insider threats, misconfigurations – one misstep, and adversaries have a foot in the door.

In 2021, 25 billion attacks on Azure AD accounts were reported. Without a top-to-bottom AD cyber-resiliency framework in place, your organization is going to be exploited by a very real threat.

To combat today's advanced and evolving threats, you need a layered defense that protects you against every phase of an attack lifecycle. At Quest, we offer an approach that tackles defense in depth at every layer of the NIST Framework, so you can mitigate risk before, during and after an attack.

The solutions in our hybrid AD cyber resiliency suite work hand-in-hand and build on each other to give you the ability to:

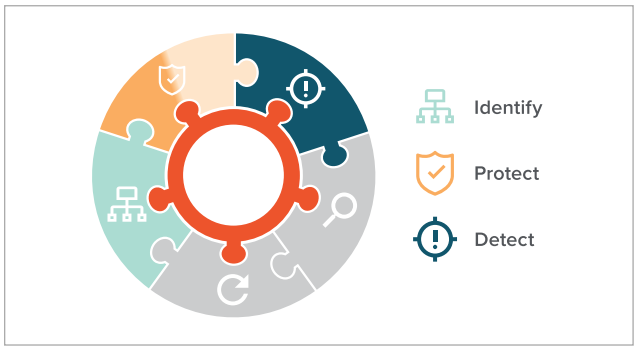
- **Identify** indicators of exposure (IOEs) and prioritize the attack paths an adversary could take to own your environment.
- **Protect** your environment so attackers can't make changes to critical groups, GPO settings or exfiltrate your AD database to steal credentials.
- **Detect** indicators of compromise (IOCs) with real-time auditing, anomaly detection and alerting.
- **Respond** to threats and rapidly gather information to speed investigations.
- **Recover** AD from any attack, big or small, and restore business operations, data integrity and customer data in minutes instead of days, weeks or even months.

How Quest can help

The Quest difference is that we provide a complete and continuous AD cyber resilience lifecycle that offers defense in depth across many layers that map to the NIST Cybersecurity Framework.

Quest AD Risk Assessment Suite

Products included: SpecterOps BloodHound Enterprise, Quest Change Auditor and On Demand Audit



- Assess and prioritize the attack paths in your environments so you can eliminate the ones with the most exposure that pose the greatest risk.
- Audit all AD security changes and detect threats early, including unauthorized domain replication, offline databased extraction, and GPO linking.
- Block attackers from making changes to critical groups or GPOs, or exfiltrating your AD database.

Quest AD Risk Protection Suite

Products included: AD Risk Assessment Suite + Quest GPOADmin

- Ensure changes adhere to change management best practices prior to deployment.
- Continually validate GPOs through automated attestation.
- Improve GPO auditing and verify setting consistency with side-by-side GPO version comparisons.
- Quickly revert back to a working GPO in the event that a GPO change has an undesired effect.

Quest Hybrid AD Cyber Resiliency Suite

Products included:AD Risk Protection Suite + Quest Recovery Manager Disaster Recovery Edition, and On Demand Recovery

- Automate every step of the manual AD forest recovery process.
- Protect AD backups from compromise and eliminate the risk of malware reinfection.
- Restore cloud-only objects not synced by Azure AD Connect.

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 Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.