Quest

5 key risk factors for identity systems and how to reduce them

Active Directory can impact every aspect of your business.

When identity services are unavailable or compromised, your business halts, your public reputation suffers and costs quickly mount. Active Directory (AD) and Azure AD (now Microsoft Entra ID) have been the backbone of identity for decades, and that's why bad actors design their methods and ransomware specifically for them, sparing no industry. For example, AD attacks have recently resulted in disruptions that cut across industry functions such as:

- Global shipping and supply chains
- Airline ticketing and flight information
- Oil pipelines
- Financial transactions
- Healthcare delivery

Accordingly, control frameworks and risk registers detail specific AD competencies that must be satisfied for business continuity, security and compliance. While these requirements might seem like a burden, well-implemented controls get you out of firefighting mode, remove friction from processes and services, and put you ahead of both competitors and bad actors.

> **Executives should understand that at least 90% of their organization is dependent on Active Directory to function, and 90% to 100% of their authentication is dependent on Active Directory to be available.**
>
> *Vice President of Enterprise Services, Managed Service Provider*

Five key factors that put AD at risk

While AD and Azure AD are critical for your organization's identity service to run and business policies to be enforced, they are also a major source of risk. Specifically, it's vital to understand the following five risk factors, preferably through a recent security assessment:

- **M&A projects —** Mergers, acquisitions and divestitures are a vital business strategy. But each project requires integrating and/or consolidating two or more IT environments. That usually means taking on another organization's old, complicated and misconfigured AD, which might well include stale user and service accounts ripe for takeover by attackers, as well as accounts with excessive access due to poor provisioning processes.
- **Technical debt and complexity —** As your identity services sprawl and AD starts to show its age, a wide range of security controls become more difficult. In particular, AD adaptations, customizations and sprawl hinder the speed and reliability of threat detection, troubleshooting and response, and disaster recovery. As a result, more vulnerabilities are introduced and more go undetected.
- **An expanding attack surface —** Chains of abusable privileges and misconfigurations across hybrid AD form thousands of attack paths that enable lateral movement and privilege escalation, resulting in unknown vulnerabilities and intolerable risk. And it takes just one exploited attack path for the organization to suffer a serious security incident.
- **Short-staffed IT and security teams —** Your vital identity and access controls are in the hands of a small group of highly skilled professionals. Every time someone retires or finds a more attractive pursuit, it increases the chance that some critical knowledge will leave with them or that some vital tasks will be left undone moving forward.

- **Regulations and SCRM —** Implementing the widening set of required controls, from data privacy to supply chain risk management to credit card processing, can easily divert attention and budget from core business goals. But to treat them as a burden is short sighted. Instead, a comprehensive set of controls can be used to measure yourself internally and against other organizations in your supply chain, providing an opportunity for leadership and added safety.

Quantifying identity and Active Directory risk

Active Directory is so critical to business operations and even business survival that it cannot be relegated merely to the technical realm. Today, AD also needs to be viewed through the lens of business risk.

The risk factors below manifest themselves in different ways for each organization, but it's useful to show a partial example of a risk register for an AD environment (see Figure 1) that includes how likely a risk is to occur and how severely it might impact an organization.

Reducing risk with Quest

Organizations need to be able to uncover, assess and prioritize their AD-related risks, and reduce them effectively by partnering with trusted advisors that deliver a broad and reliable set of M&A integration, migration and cybersecurity risk management solutions.

When it comes to minimizing identity system risks, Quest is the AD and Azure AD authority, boasting a portfolio with defense in depth and decades of reliability. In fact, Gartner lists Quest as an example vendor more than double any other vendor in its 2022 IAM Best Practices for Active Directory research. Thousands of customers, including 82% of the Fortune 100 and 46% of the Fortune 1000, have partnered with Quest to dramatically reduce inherent risk into acceptable residual risk (see Figure 2).

Cause	Impact	Likelihood	Severity	Inherent Risk Score
Complexity and failure to enforce a least privilege model during and after M&A migration.	• Missed deadlines and milestones • Revenue and productivity losses • Increased risk of breaches • Increased risk of compliance penalties	5	4	**20**
Compromise of an AD account leads to data breach.	• Fines • Productivity losses • Reputation damage	4	5	**20**
Ransomware attack takes AD offline.	• Recovery costs, possibly including ransom payment • Fines • Revenue and productivity losses • Reputation damage	5	5	**25**
IT teams lack visibility into who has what access to critical systems and data.	• Increased risk of data breaches • Increased risk of audit findings and compliance fines • Revenue and productivity losses • Reputation damage	4	4	**16**

Figure 1. Inherent risk example for Active Directory using a scale from 1 (least) to 5 (greatest) to calculate score, where inherent risk is calculated by multiplying liklihood and severity

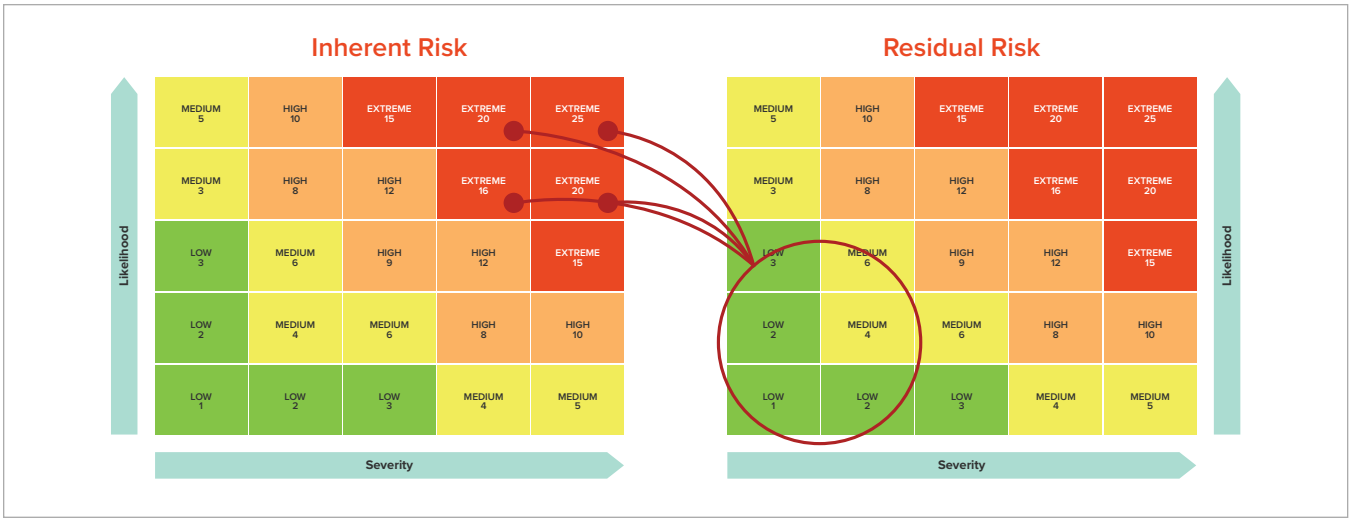

Figure 2. Example change in risk with Quest

Assessing your return on investment

Quest clients have demonstrable results in reducing risk across a wide range of security and operational controls, including:

Migration

Quest migration customers can efficiently plan and execute their migrations to minimize effort and risk. Moreover, they can dramatically reduce the need for highly skilled IT resources and the risk of costly timeline overruns (see Figure 3).

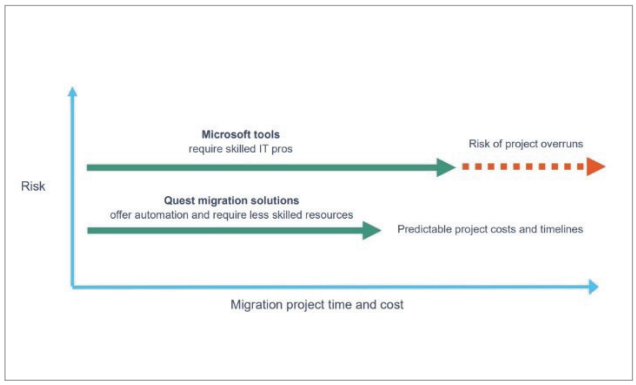

Figure 3. Quest migration tools reduce the risk of project overruns.

Recovery

A Forrester Consulting study found that in the wake of an AD outage, organizations using Quest Recovery Manager for AD Disaster Recovery Edition (RMAD DRE) experienced up to 90% faster recovery times — translating into a savings of $19.7M per recovery (see Figure 4).

> **We had projected that the migration project would take 14 months, but with [Quest migration solutions], we were able to shave six months off that timeline.**
>
> *Curtis Mavity, Senior Systems Engineer, Avera Health*

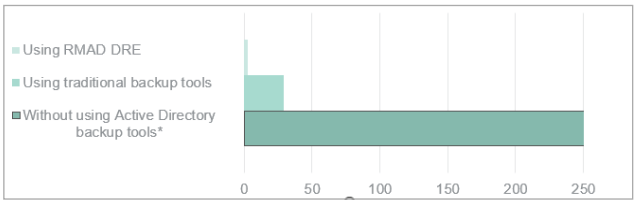

Figure 4. Quest tools slash recovery time up to 90%.

"Essentially, the cost of [RMAD] DRE is a rounding error compared to the potential revenue loss from an attack," said one of the study participants, the directory services senior lead at a consumer packaged goods company.

Attack surface management

Quest customers can easily visualize and prioritize the attack paths in their Active Directory — as well as exactly how to mitigate a whole set of attack paths at once. As a result, they can quickly slash their attack surface area.

> 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.

Information Systems Manager at the Department of Transportation for a U.S. State

Security and compliance auditing

Quest auditing customers get a single, correlated view of activity across their hybrid IT environment. Instead of manually collecting and poring through cryptic native logs from multiple servers, the IT team can review actionable intelligence in real time to quickly troubleshoot incidents. Moreover, detailed alerts about critical changes enable them to slash response time, and they can even proactively prevent changes to the most critical AD objects to maximize both security and system availability.

> Previously, investigating an issue could easily take an hour. Change Auditor cuts that time to just 5–10 minutes.

Dennis Persson, IT Systems Technician, Region Halland

Schedule an identity and AD security risk assessment today

Whether you are planning for an M&A integration, migration or modernization project or need to tighten your security and compliance controls, it's best to start with a risk assessment. Sign up now and we'll review your current security posture and potential attack paths to your most critical assets. This risk assessment will provide:

- Visibility into thousands or millions of identity attack paths
- Precise and prescriptive guidance to help reduce risk with minimal effort
- Practical risk remediations without drastic changes to your environment
- Controls to measure your identity security posture improvements over time

Schedule an identity security risk assessment today.

Ensuring compliance and exceeding supply chain management requirements

By choosing Quest solutions, you gain a partner with mature supply chain risk management practices. We apply proactive security measures to identify and minimize supply chain risks. In particular, Quest:

- **Uses a Zero Trust R&D architecture**
- **Performs no development in countries of security concern**
- **Puts all new suppliers through an extensive trustworthiness assessment**
- **Controls access to the product in each step in the supply chain**
- **Strictly limits access to sensitive areas of the business, including product development**
- **Has achieved 100% compliance with NIST SP800-218 (based on Coalfire's assessment of 12 US Federal/DoD preferred products)**
- **Has earned multiple certifications, including SOC 2 Type 2 and ISO 27001, 27017 and 27018**
- **Uses an airgap-secured assembly process that exceeds industry standards**

Quest

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. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.