Quest

身份系统的 5 大关键风险因素及如何降低风险

Active Directory 可能会影响您业务的各个方面。

当身份服务不可用或遭到入侵时，您的业务会停止、公众声誉会受损，成本也会迅速增加。数十年来，Active Directory (AD) 和 Azure AD（现为 Microsoft Entra ID）一直是身份服务的支柱，正因如此，恶意分子会专门设计针对二者的方法和勒索软件，任何行业都无法幸免于难。举例来说，AD 攻击近期造成了多起跨行业功能的中断，例如：

- 全球运输和供应链
- 机票和航班信息
- 石油管道
- 金融交易
- 医疗保健服务

因此，控制框架和风险登记簿详细说明了为保证业务连续性、安全性和合规性，必须具备的特定 AD 功能。这些要求看似繁重，但实施得当的控制措施能让您摆脱“事后救火”的模式，消除流程和服务中的摩擦，让您先人一步，获得竞争优势并防范恶意分子。

> **高管应该认识到，其组织至少有 90% 的部分依赖于 Active Directory 运作，90% 到 100% 的身份验证的可用性依赖于 Active Directory。**
>
> *企业服务副总裁，*
> *托管服务提供商*

给 AD 造成风险的五个关键要素

AD 和 Azure AD 对于组织身份服务的运行和业务策略的执行至关重要，但它们也是主要的风险来源。具体来说，了解以下五个风险因素至关重要，若能通过近期的安全评估了解它们，便再好不过：

- **M&A 项目** — 兼并、收购和剥离均为重要的商业战略。但每个项目都需要集成和 / 或整合两个或更多 IT 环境。这通常意味着要接手另一个组织陈旧、复杂且配置不当的 AD，其中很可能包括随时有可能被攻击者利用的陈旧用户帐户和服务帐户，以及因配置流程欠佳而导致的权限过高的帐户。
- **技术债务和复杂性** — 随着身份服务的无序扩张，AD 日渐陈旧，各种安全控制措施的实施难度加大。特别是，AD 的调整、自定义和扩展会影响威胁检测、故障排除和响应以及灾难恢复的速度和可靠性。结果，更多的漏洞浮出水面，更多的漏洞隐匿无踪。
- **受攻击面不断扩大** — 混合 AD 中的可滥用特权链和错误配置形成了数以千计的攻击路径，让横向移动和权限升级成为可能，导致出现未知漏洞和难以承受的风险。只要有一条攻击路径被利用，组织就会遭受重大安全事故。
- **IT 和安全团队人手紧张** — 您的重要身份和访问控制掌握在一小群技术娴熟的专业人员手中。每当有人退休或跳槽到更有吸引力的工作时，都会增加部分关键知识随之流失、部分重要任务无法完成的几率。

- **法规和 SCRM** — 实施不断扩充的必要控制措施（从数据隐私、供应链风险管理到信用卡处理等）很容易会使组织无法集中精力和预算关注核心业务目标。但如果将这些控制措施视为负担，又未免过于短视。故此，可以使用一套全面的控制措施来衡量您的内部情况，以及与供应链中其他组织的对比情况，从而为占据领先地位、提高安全性创造机会。

量化身份和 Active Directory 风险

Active Directory 对于业务运营乃至企业生存都有着至关重要的意义，不能单纯将其归入技术范畴。如今，组织还需要从业务风险的角度审视 AD。

对于每个组织，以下风险因素的表现形式不尽相同，但展示一个 AD 环境风险登记簿的不完整示例（见图 1）非常有用，这个风险登记簿中包含风险发生的可能性以及可能对组织造成的影响程度。

借 Quest 之力降低风险

组织需要能够发现、评估并优先应对 AD 相关风险，并与值得信赖的顾问合作，提供一套广泛而可靠的 M&A 集成、迁移和网络安全风险管理解决方案，从而有效降低风险。

在尽可能降低身份系统风险方面，Quest 是 AD 和 Azure AD 领域的专家，拥有以深度防御和数十年的可靠性而著称的产品组合。实际上，Gartner 在其 2022 年 IAM Active Directory 最佳实践研究中将 Quest 列为示例供应商的次数是其他供应商的两倍以上。数以千计的客户（包括 82% 的财富 100 强公司和 46% 的财富 1000 强公司）已选择与 Quest 合作来大幅降低固有风险，使之变为可接受的剩余风险（见图 2）。

原因	影响	可能性	严重性	固有风险分数
M&A 迁移期间和之后的复杂性，以及未能执行最小特权模式。	• 错过最后期限和里程碑 • 收入和生产力损失 • 更高的违规风险 • 更高的合规性惩罚风险	5	4	**20**
因 AD 帐户遭到入侵而导致数据泄露。	• 罚款 • 生产力损失 • 声誉受损	4	5	**20**
勒索软件攻击造成 AD 脱机。	• 恢复成本，可能包括勒索赎金 • 罚款 • 收入和生产力损失 • 声誉受损	5	5	**25**
IT 团队无法了解谁能访问关键系统和数据。	• 更高的数据泄露风险 • 在审核中发现不利情况并遭受合规性罚款的风险更高 • 收入和生产力损失 • 声誉受损	4	4	**16**

图 1. Active Directory 固有风险示例，按照从 1（最小）到 5（最大）的分值来计算分数，其中固有风险的计算方式是将可能性与严重性相乘

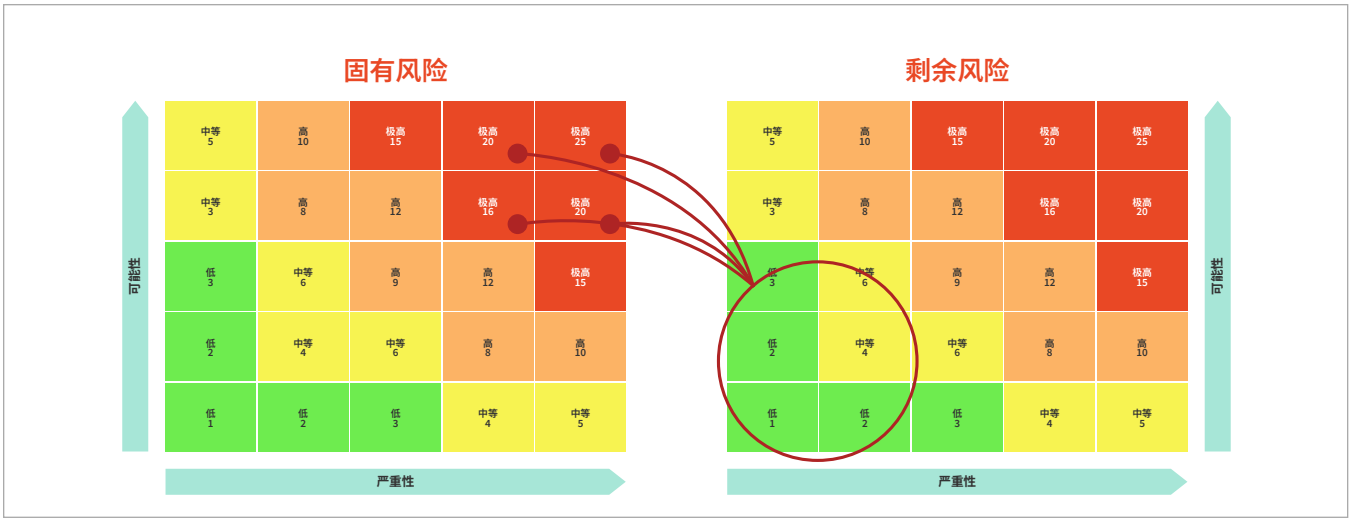

图 2. 使用 Quest 时的风险变化示例

评估投资回报率

Quest 客户在降低各种安全和运营控制措施的风险方面取得了显著成果，其中包括：

迁移

Quest 迁移客户可高效规划和执行迁移，尽可能减少工作量、降低风险。此外，他们还能大大减少对技能娴熟的 IT 资源的需求，并降低代价高昂的时间超支风险（见图 3）。

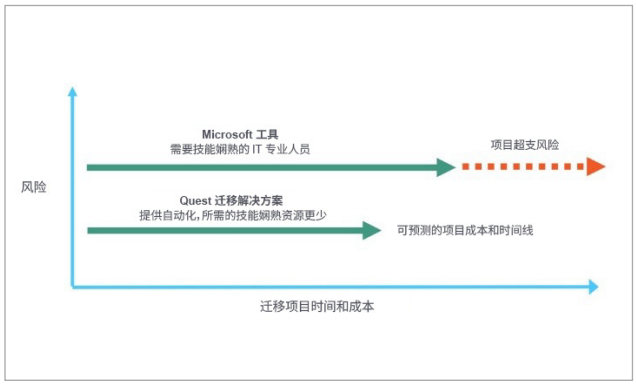

图 3. Quest 迁移工具降低了项目超支的风险。

恢复

Forrester Consulting 的一项研究发现，在发生 AD 故障后，如果使用 Quest Recovery Manager for AD Disaster Recovery Edition (RMAD DRE)，组织的恢复时间可缩短多达 90%，相当于每次恢复可节省 1970 万美元（见图 4）。

> **“根据我们先前的预计，迁移项目需要 14 个月的时间，但借助 [Quest 迁移解决方案]，我们得以将该时间缩短 6 个月。”**
>
> *Curtis Mavity，Avera Health 高级系统工程师*

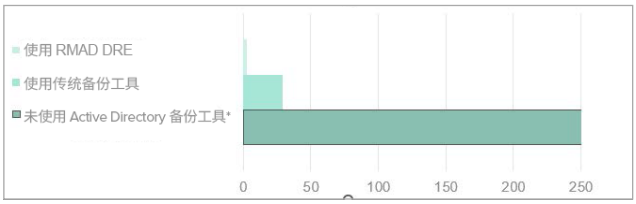

图 4. Quest 工具将恢复时间缩短多达 90%。

研究参与者之一、某消费类包装商品公司的目录服务高级主管表示：“从根本上来说，与攻击可能造成的收入损失相比，[RMAD] DRE 的成本几乎可以忽略不计。”

受攻击面管理

Quest 客户可以轻松地对 Active Directory 中的攻击路径进行可视化和优先排序，并准确了解如何同时缓解一整组攻击路径。这样，他们就能快速缩小受攻击面。

> **这非常令人兴奋，因为我们作出更改后，能够在可视化图示中看到其通过减少攻击路径数量所带来的确切影响。我们可以用可量化的方式跟踪所采取的措施，并向管理团队证明投资的价值。**

美国某州运输局
信息系统管理员

安全性和合规性审核

Quest 审核客户可获得其混合 IT 环境中活动的单一关联视图。IT 团队不必手动从多个服务器收集并研究难以理解的本地日志，而是可以实时查看可行的情报，快速排查故障。此外，有关关键更改的详细警报让他们可以缩短响应时间，甚至可以主动防止对最关键 AD 对象的更改，从而更大限度地提高安全性和系统可用性。

> **以前，调查某个问题很容易就会花费一小时的时间。Change Auditor 可以将该时间缩短至 5 到 10 分钟。**

Dennis Persson，Region Halland 的 IT 系统技术人员

即刻安排身份和 AD 安全风险评估

无论您是在规划 M&A 集成、迁移或现代化项目，还是需要加强安全性和合规性控制措施，最好都从风险评估入手。立即注册，我们可以评估您当前的安全状况和最重要资产的潜在攻击路径。通过此风险评估，可以：

- 了解数以千计或数以百万计的身份攻击路径
- 获得精准、规范的指导，帮助您通过尽可能少的工作来降低风险
- 获得切实可行的风险补救措施，而无需对环境做出重大改变
- 获得控制措施，衡量您的身份安全状况随时间推移所取得的改进

即刻安排身份安全风险评估。

确保合规性并超越供应链管理需求

选择 Quest 解决方案，您就可以获得一家拥有成熟供应链风险管理实践的合作伙伴。我们运用主动安全措施来识别并尽可能降低供应链风险。

尤其是，Quest：

- **使用 Zero Trust 研发体系结构**
- **不在有安全顾虑的国家 / 地区开展开发工作**
- **对所有新供应商进行广泛的可信度评估**
- **控制供应链的每一个环节对产品的访问**
- **严格限制对敏感业务区域（包括产品开发区域）的访问**
- **100% 符合 NIST SP800-218（基于 Coalfire 对 12 种美国联邦 / 国防部首选产品的评估）**
- **已取得多项认证，包括 SOC 2 Type 2 以及 ISO 27001、27017 和 27018**
- **采用超越行业标准的气隙安全装配流程**

关于 Quest

Quest 提供软件解决方案，在越来越复杂的 IT 环境中带来新技术的优势。从数据库和系统管理到 Active Directory 和 Office 365 管理，以及 网络抗风险能力，Quest 都可帮助客户在当下解决其面临的下一个 IT 挑战。在全球范围内，有超过 130,000 家公司和 95 % 的财富 500 强企业依赖 Quest 为下一个企业计划提供主动管理和 监控，为复杂的 Microsoft 挑战寻找下一个解决方案，以及针对下一个威胁做到 防患于未然。Quest Software。Where Next Meets Now.

如果您对可能使用的本材料存有任何问题，请联系：

www.quest.com/cn-zh/company/contact-us.aspx