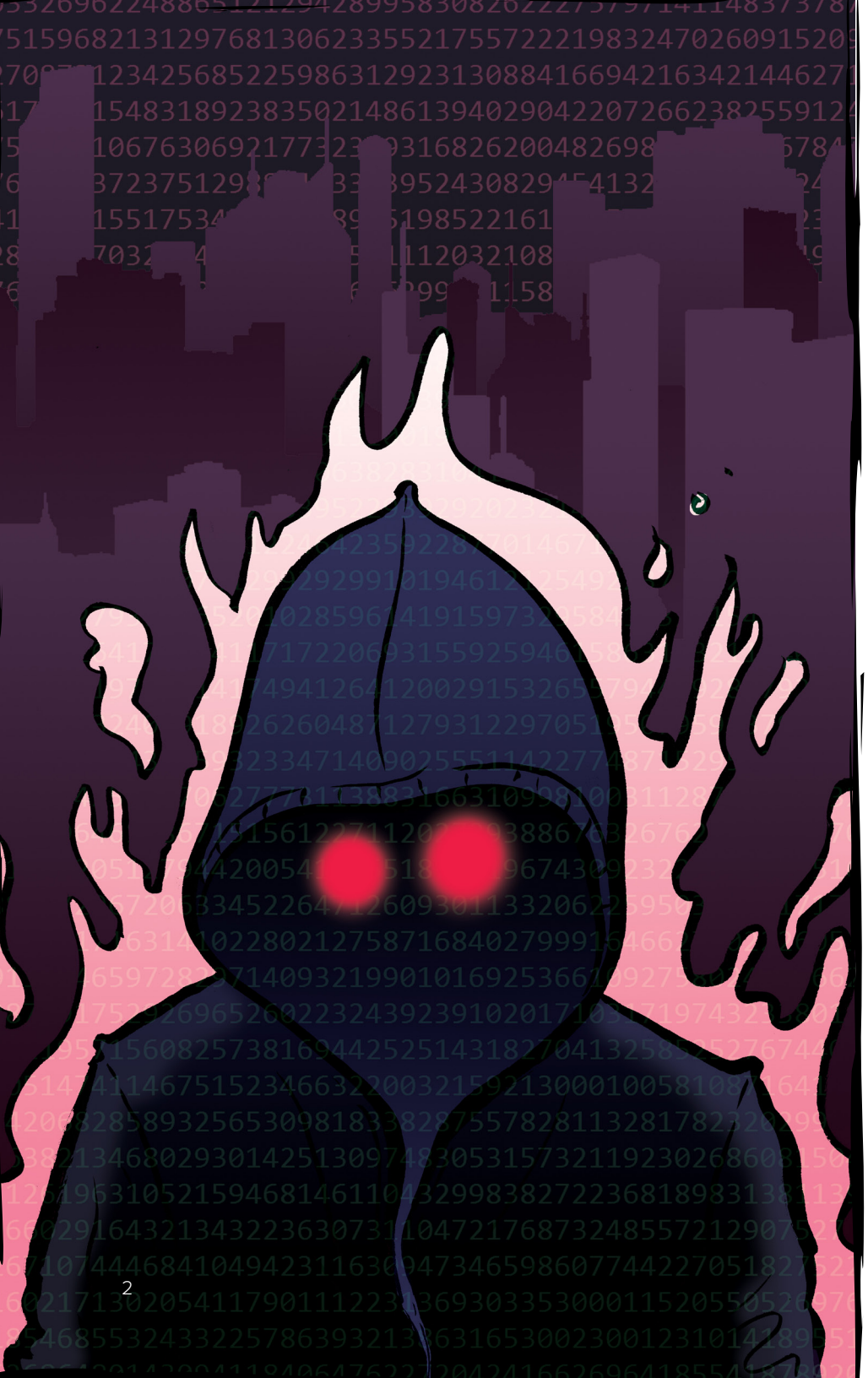
令人震撼的网络抗风险能力：AD 安全杀手应对指南

保护您的混合 Active Directory
免遭风险、威胁和灾难。

Quest



简介

在网络安全领域，Active Directory (AD) 至关重要。Active Directory 是每个组织的支柱，为环境中的每项重要资源提供身份验证和授权。可以说，确保 Active Directory 得到妥善管理和保护对于保障业务连续性和迈向成功至关重要。

遗憾的是，考虑到 AD 环境较为复杂且不断演变，这说起来容易做起来难。此外，Active Directory 的价值使其成为不法网络犯罪分子的头号目标。这些攻击者既聪明又无情，极其危险。他们深知控制 Active Directory 就意味着控制整个企业，因此不断研究新策略、工具和方法来实现其目标：统治 AD。

Microsoft 报告称，2021 年针对 Azure AD 帐户的暴力攻击超过 250 亿次。《Microsoft 2022 年年度数字防御报告》(2022 Annual Microsoft Digital Defense Report) 显示，88 % 受影响的客户没有采用 AD 和 Azure AD 安全最佳实践。此外，Microsoft 报告强调，在从攻击中恢复的客户中，不安全的 Active Directory 配置是首要问题之一。

攻击威胁真实存在，它并不是“是否发生”的问题，而是“何时发生”的问题。无论是勒索软件、内部威胁、错误配置还是其他灾难，危险都在悄然而至。混合 Active Directory 已然成为常见攻击媒介，攻击者利用关键身份系统中的错误配置和较弱的安全状况，来获得更广泛的访问权限，以及对企业造成更大的影响。

好消息是前景并非一片黯淡，毫无希望。在本电子书中，您可探索 Quest 如何助您在混合 AD 的整个生命周期内实现网络抗风险能力，从而在攻击之前、期间和之后都能缓减风险。披上斗篷，带上面具，我们即将征服 AD Active Directory 安全威胁。

Quest

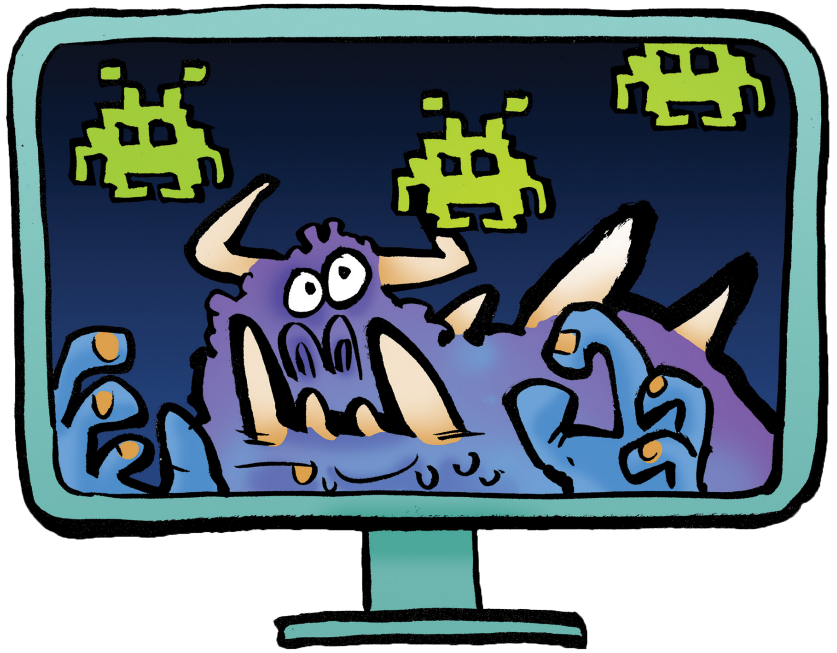
建立混合 AD 网络风险管理框架

为消除安全基础架构中的缺口，许多公司将其安全风险管理计划调整为常用框架，例如 NIST（或其他特定于地区、行业或国家的替代框架）。NIST 框架设定了一系列标准、指导准则和做法，您在保护基础架构免遭网络安全风险时应考虑这些标准、指导准则和做法。

NIST 框架由以下支柱或原则组成：

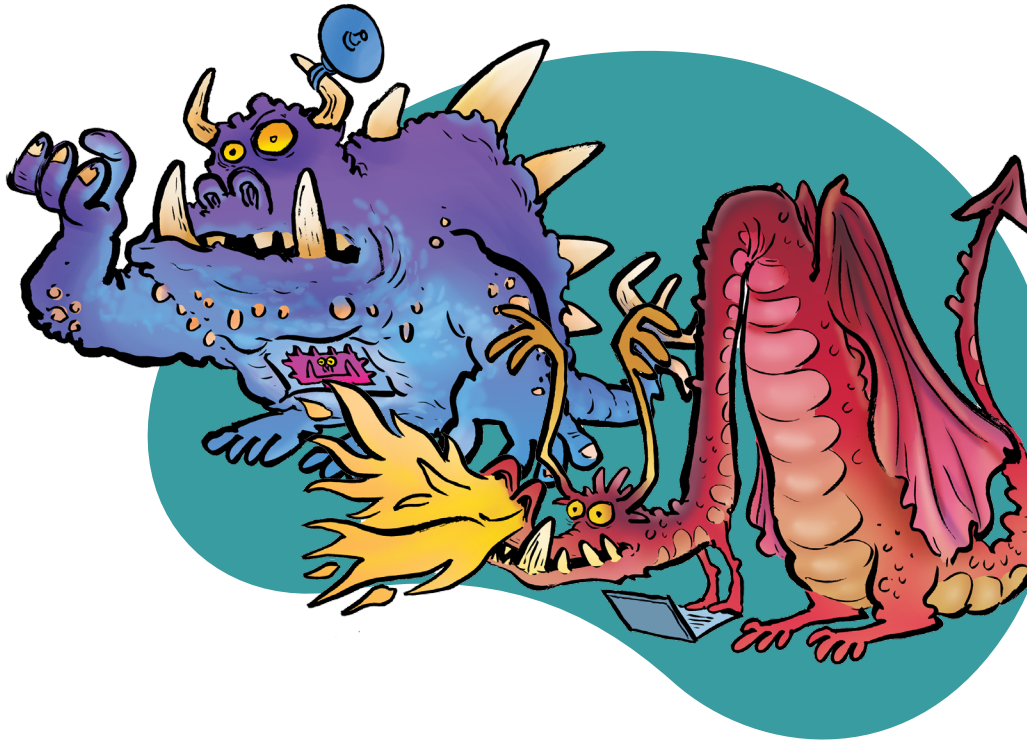
- **识别**：确认哪些资产需要保护，以及存在哪些薄弱之处
- **保护**：建立防护和抵御措施以保护关键资产
- **检测**：调查安全事件
- **应对**：制定应对措施以遏制安全事件
- **恢复**：发生灾难时还原各项功能和数据

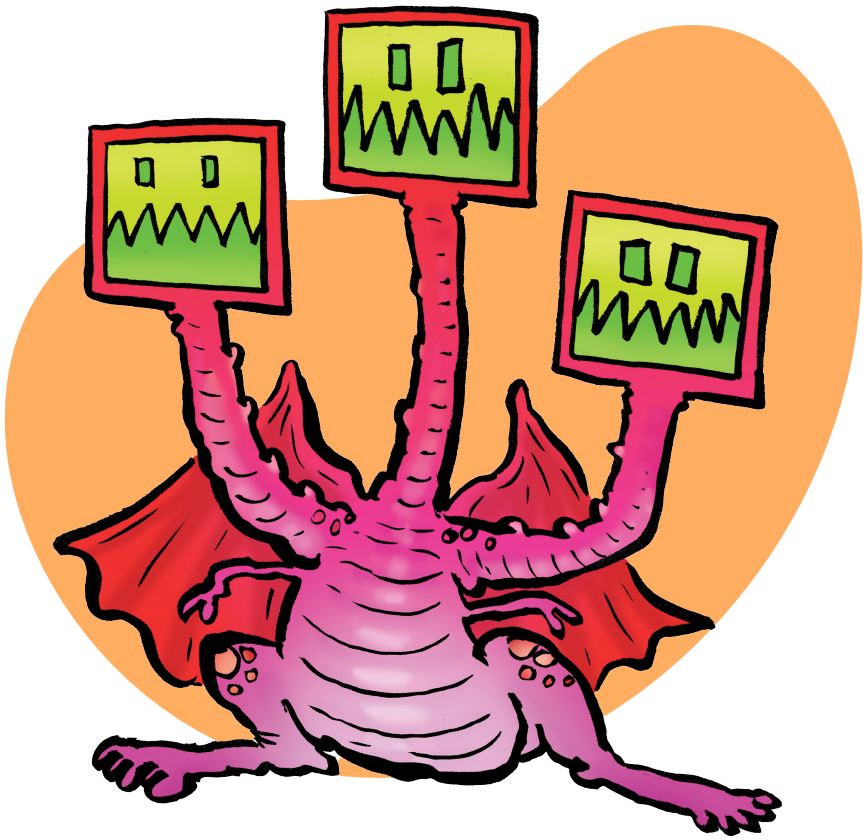
每个支柱落实到位是确保 Active Directory 安全的关键所在。然而，许多公司都发现，在尝试实现每个 NIST 原则的目标时，他们面临种种挑战。



Quest

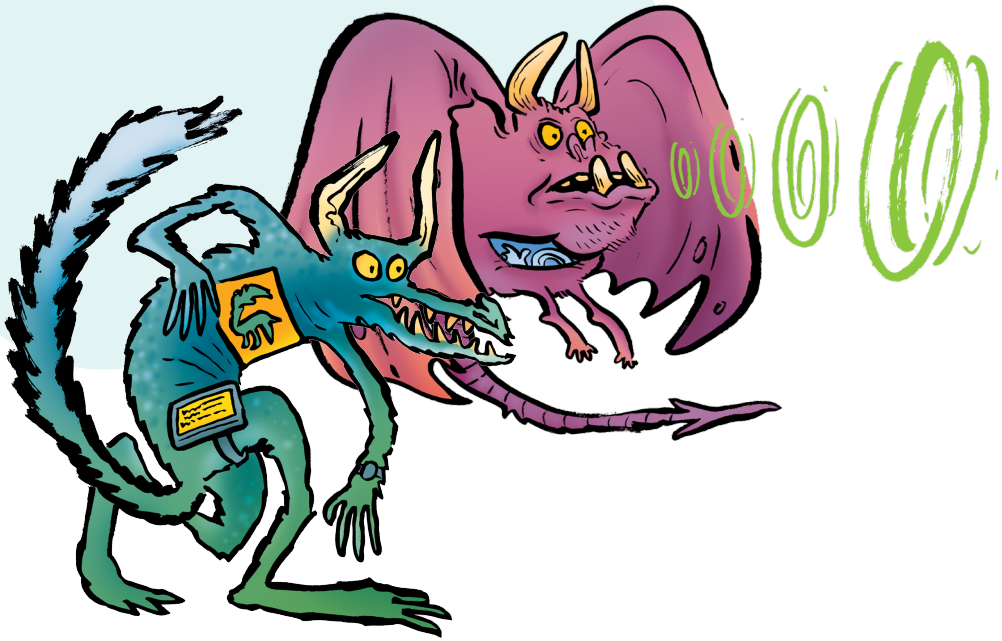
- **识别相关的挑战**：随着组织的发展（无论是在本地还是云端的发展），他们常常发现自己对 Active Directory 的关键方面（如用户、组、权限和应用程序）缺乏可见性。这意味着他们不确定谁可以访问哪些信息！此外，许多组织无法识别自己最关键的资产是什么 — Tier Zero 资产。在最终识别风险过程中，了解 AD 中存在哪些权限以及 Tier Zero 资产是什么是向前迈出的一小步。如何识别攻击者会利用的现有途径和漏洞？您能指出作为通向整个基础架构的通道的关键媒介吗？若不了解 Active Directory 的这些重要组件，几乎不可能做到保护自己免受日常威胁并真正了解自己的风险状况。





- **保护相关挑战**：目前，组织纷纷采用 Azure AD 和 Office 365，这会增加对 Active Directory 的依赖，同时会使攻击面翻倍并给勒索软件和其他攻击创造更多机会。遗憾的是，针对 AD 的漏洞管理繁琐复杂、耗费时间，而且通常无法使用系统自带的审核工具。组策略对象 (GPO) 的控制和管理可能非常棘手，尤其是在如下情况下会更加复杂：一个被遗忘已久的团队创建了一个 GPO，而后该 GPO 又被放弃，缺少该 GPO 可能导致对您网络中数千个系统的安全状况造成巨大不利影响。如何管理和保护规模将会变得越来越庞大的 Office 365 租户？ Active Directory 环境在不断演变和扩展，这意味着您需要涵盖的漏洞和资产也在不断演变和扩展。

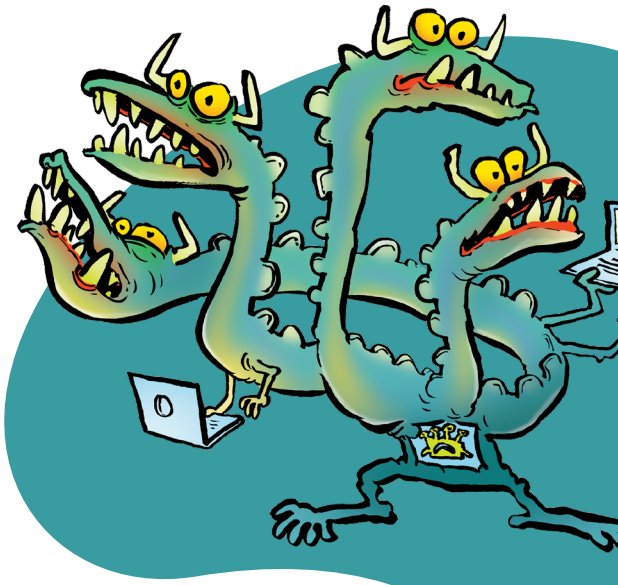
Quest



- **检测相关挑战** 虽然检测本地和云端的配置、用户和管理员更改以及活动，对于保障安全至关重要，但 Office 365 和 Azure AD 安全日志并不提供本地和云端活动的整合视图。系统自带的工具无法轻松识别漏洞利用、漏洞和可疑活动，让您只能努力准确找出新的异常情况，以免为时已晚。
- **应对相关挑战**：谈到“为时未晚”，假设您已意识到有异常活动在进行 — 现在该怎么办？大多数组织发现自己缺少有效的应对系统，一个能让他们快速调查、分析并在需要时还原发生任何更改前正在运行的设置和权限的系统。依靠 IT 部门的能力以及系统自带的工具，只会导致对上述配置和异常进行令人沮丧而耗时的搜索，同时让您认识到自己无法确定接下来应该怎么做。
- **恢复相关挑战**：最糟糕的情况是，测试灾难恢复计划时发生灾难。然而，情况往往就是如此。Microsoft 的“Active Directory 林恢复指南”概述了约 40 个概要步骤，若这些步骤无法自动执行，将很容易出错且耗费时间。执行手动流程或使用本机工具只会带来恶意软件再次入侵、停机时间延长且损失增加的风险。如果您拥有备份的访问权限，但无法自信地使用这些备份，便会让攻击者有机可乘，让他们能造成更多损害，并致使您的组织遭受更多经济和名誉损失。您知道首先要恢复哪些域和用户吗？您的沟通计划如何？遭到入侵已经非常糟糕，使用未经测试的计划延长这一情况只会雪上加霜。您可能认为投保是一种解决办法，但您上一次阅读保单细则是什么时候？您是否尽一切努力来弥补损失，让运营恢复正常？ 造成这一切的原因可能有很多，例如工具效率低下、使用的各项工具之间缺乏连贯性、支持存在误导性、对外围安全投资过度（和部署不力），以及对身份保护投资不足。

在 Active Directory 安全方面，必须对网络抗风险基础架构的各个方面保持警惕。如果有一个方面很薄弱，那么整个 Active Directory 就都存在崩溃的风险，进而导致整个企业面临风险。

如果网络抗风险框架的一个方面被忽视，攻击者会异常兴奋，因为对他们说，这相当于欢迎他们进入 Active Directory 环境的其余部分。



Quest

那么，是否有办法确保 NIST 框架的所有方面都得到开发，可以接受大量 AD 安全挑战？是否有英雄可召唤？

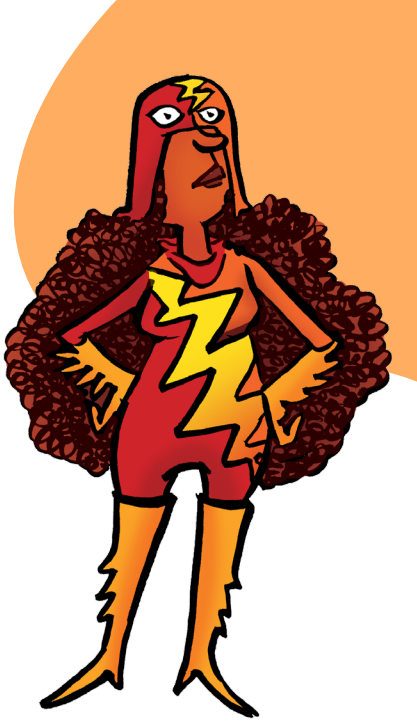
寻求网络抗风险能力

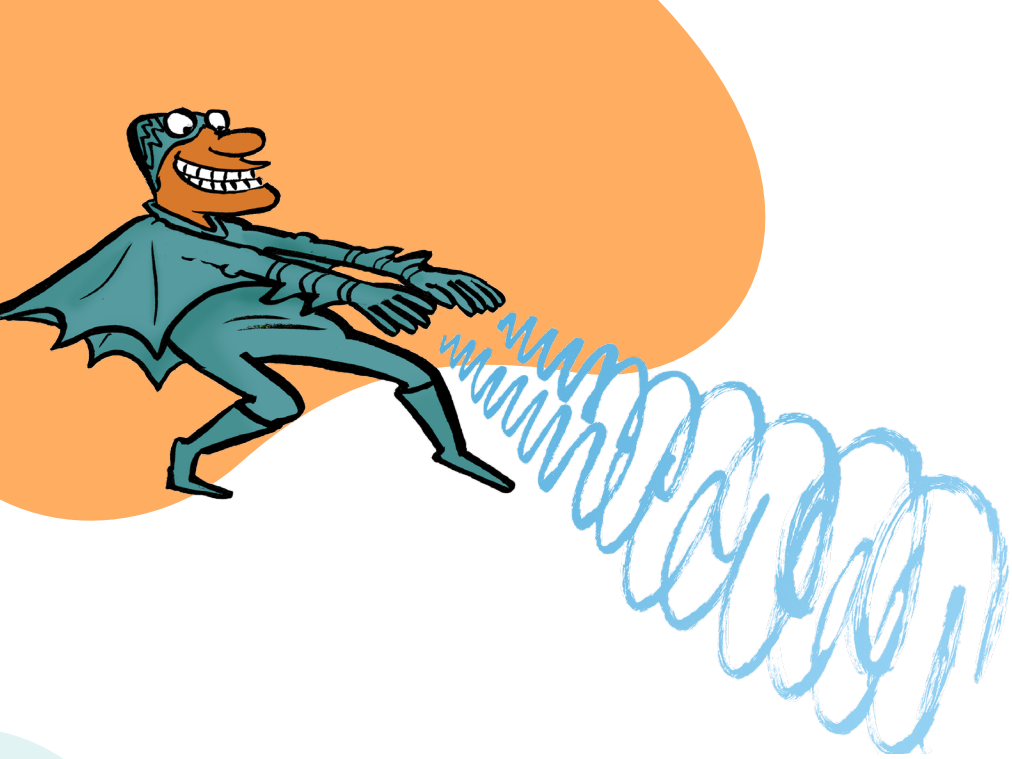
Quest 提供混合 AD 网络抗风险方案。该方案提供深度防御，能够降低 NIST 框架每一层的风险，从而让您能在攻击之前、期间和之后做好准备。

我们混合 AD 网络抗风险套件中的各项解决方案互相补充，协同实现动态、全面的防御，让您能够：

- **识别**暴露指标 (IOE)，并确定攻击者可能用来入侵您环境的攻击路径的优先级。
- **保护**您的环境，让攻击者无法更改关键组、GPO 设置或渗透您的 AD 数据库以窃取凭据。
- 通过实时审核、异常检测和警报功能来**检测**入侵指标 (IOC)。
- **应对**威胁并快速收集信息以加速调查。
- 无需花费数天、数周或数月时间，只需数分钟即可从各种规模的攻击中**恢复**，并恢复业务运营、数据完整性和客户提议按。

但是，这组强大的解决方案是如何严谨配合以保护混合 AD 环境免遭各种威胁的呢？通过将它们放到各自的套件中，我们能够接力发挥它们的功能，并阐释它们如何相辅相成。





Quest AD Risk Assessment Suite

AD Risk Assessment Suite 结合了我们的两款旗舰产品 Change Auditor 和 On Demand Audit Hybrid Suite，以及强大的 SpecterOps BloodHound Enterprise，让您能识别、防御并检测环境中的潜在威胁。利用 Quest AD Risk Assessment Suite，您可以：

- 审核 AD 和 Azure AD 环境中的所有安全更改（包括用户和组更改）以及漏洞，例如通过离线复制或未授权的域复制造成 AD 数据库渗漏
- 及早检测威胁（包括未经授权的域复制、脱机提取 AD 数据库以及 GPO 链接），以减轻甚至避免代价高昂的勒索软件攻击
- 阻止攻击者首先更改关键组、GPO，或阻止其过滤您的 AD 数据库以窃取凭据 — 无论他们已劫持何种权限

Quest AD Risk Protection Suite

通过 AD Risk Protection Suite，您可以从 Risk Assessment Suite 和 GPOADmin 获得所需的一切功能；GPOADmin 是我们一款强大的解决方案，能够简化 GPO 的管理与监管工作。AD Risk Protection Suite 可助您：

- 在部署之前确保更改符合更改管理最佳实践，这是 Active Directory 组策略管理中的重要一步
- 通过自动化认证持续验证 GPO — 这是任何第三方组策略管理解决方案的必备功能
- 通过以不同时间间隔对 GPO 版本进行高级横向比较，改进 GPO 审核流程，并轻松快速地验证设置一致性
- 如果 GPO 更改产生非预期效果，可快速还原到有效的 GPO。只需数秒，即可让环境重新恢复正常运行。

Quest

Quest Hybrid AD Cyber Resiliency Suite

前两个套件涵盖了 NIST 框架原则的过半内容（识别、检测和保护），最后一个套件 Hybrid AD Cyber Resiliency Suite 则涵盖了框架的其余部分（应对和恢复）。有了 Hybrid AD Cyber Resiliency Suite，您可以确信，无论发生什么网络事件，您都已充分增强安全性。除其他套件中包含的产品外，Hybrid AD Cyber Resiliency Suite 还添加了 IT Security Search、Recovery Manager Disaster Recovery Edition 和 On Demand Recovery。IT Security Search 用于响应事件，Recovery Manager Disaster Recovery Edition 和 On Demand Recovery 用于处理您本地及云端所有大大小小的恢复需求。您将能够：

- 自动执行手动 AD 林恢复过程的每一步。
- 保护 AD 备份免遭入侵，并消除再次感染恶意软件的风险
- 恢复未通过 Azure AD Connect 同步的仅限云的对象
- 展示并验证混合 AD 备份和灾难恢复计划

总结

通过 Quest，您会收到全面且持续的 AD 和 Office 365 网络抗风险生命周期，它为映射到 NIST 网络安全框架的许多防护层带来了深入的防御。我们的解决方案协同工作，相辅相成，能够确保您实现网络抗风险能力目标及业务成果，而不会出现任何让您在日后饱受困扰的缺口。

全球的网络罪犯请注意 — Quest 网络抗风险故事才刚刚开始。

Quest

关于 Quest

Quest 致力打造软件解决方案，在日益复杂的 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 Microsoft 365 迁移和管理，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. 有关详细信息，请访问: www.quest.com。

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