Quest

90%

的企业感到易于受到内部威胁的攻击。[1]

检测、防范内部攻击并从内部攻击中恢复

您已构建了出色的外围防御，但是是否为已在网络内部的威胁做好准备?

挑战

似乎每周都有新数据泄露事件见诸新闻头条。每个人都担心黑客攻击，因此企业以前在外围防御上投入了大量资金。但是，现实是超过 一半的泄露事件是由已在网络内部的某个人 导致的，[2] 例如某个员工窃取知识产权以带到新工作中，或某个手指较大的管理员犯了重大配置错误。通常，实际上是外部攻击者获取了合法的帐户 - Microsoft报告称每天有9500万的AD帐户成为网络攻击的目标[3] 而且每天有1000万次Azure AD登录尝试是网络攻击。[4]

因此，安全专家建议采用“假设数据泄露”思维：认定迟早有人会在您的网络中四处搜寻，企图造成损害或窃取您的重要数据。即使最好的外围防御也无法阻止他们，因此还拥有强大的Active Directory安全与监管非常重要。

这对您有何影响

为了有效应对内部威胁，您必须：

- **通过实施新技术（以安全的方式实施）来满足业务需求。**更快迁移到云或扩展自带设备会推动业务目标，但是您必须大大降低安全风险。
- **保护您的所有敏感数据。**近年来，数据飞速增长，其中很多数据是非结构化数据，它们位于SharePoint Online和OneDrive等云存储库中，而不是直接位于办公楼内锁着的数据中心上的一些数据库中。因此，了解您所拥有的内容就困难得多，更不用说保护它们的安全了。
- **遵循 数量不断增加且日益严格的数据隐私法规。**不久以前，只有某一些行业存在严格的法规，而且获得ISO认证就已足够。但是，现在诸如PCI、GDPR和CCPA等法规正在深入各行各业。您不仅必须建立合规性，还必须随着法规的不断涌现和发展而持续保持合规性。
- **通过审核并避免影响极大的头条报道。**数据泄露会产生巨大的成本损失 — 平均为386万美元。[5] 审核失败会导致巨额罚款，甚至使您的企业破产。保护业务靠您自己。

为了实现这些目标，您需要控制用户权限，并紧密监控每个人的活动。但是，利用原生工具无法轻松做到这些；实际上，62 % 的用户承认他们拥有超出需求的访问权限。[6] SIEM提供对用户活动的更好可见性，但是它们的许可费用太昂贵，且难以配置和使用。此外，它们的表现取决于您为其提供的数据，而且原生日志存在巨大的差距，在重要方面缺乏保真度。无怪乎攻击者平均能够潜伏101天才会被发现。[7]

1 Cybersecurity Insiders，《Insider Threat 2018 Report》（2018年内部威胁报告）。

2 同上。

3 ZDNet，《Active Directory czar rallies industry for better security, identity》（Active Directory要求行业实现更好的安全和身份），2015年6月9日。

4 Softpedia News，《Microsoft Sees Over 10 Million Cyberattacks per Day on Its Online Infrastructure》（Microsoft发现每天针对其在线基础架构的网络攻击超过1000万次），2016年5月6日。

5 Ponemon Institute，《2018 Cost of a Data Breach Study》（2017年数据泄露成本分析）。

6 Ponemon Institute，《Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations》（填补保护企业数据的安全缺口：美国和欧洲企业研究）。

7 FireEye，《M-Trends 2018 Report》（2018年M-Trends报告）。

“以前，我需要控制对管理组进行的任何更改。借助Change Auditor，我只需在我的邮件中查看某个文件夹，便可轻松监控这些重要更改。”

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

您可信赖的安全性与合规性解决方案

更好的方式

如果您可以通过确保每个人仅具有进行工作所需的访问权限，从而限制用户或窃取了用户凭据的其他人可以造成的损害，会怎么样？如果您可以在任何人执行存在风险的操作时立即收到相应警报，会怎么样？如果您可以为每个人建立正常行为基准并快速发现任何偏差，会怎么样？如果您可以快速调查并应对威胁，会怎么样？

只能依赖QUEST完成的任务

Quest是可信赖的供应商，提供适用于任何内部部署或混合Microsoft环境的安性与合规性解决方案。我们提供全套的解决方案，使您可以像严密保护外围一样保护内部环境，并确保持续的合规性。

修复和缓解

抵御内部威胁始于适当的监管。Quest® 解决方案可自动执行管理任务，包括用户配置和取消配置，消除安全漏洞以及降低风险。基于审批的工作流 增加了额外的一层监管和控制。

前瞻性地发现漏洞

IT环境是动态的，因此您还需要定期检查漏洞。Quest解决方案提供自动化且整合的报告功能，报告涵盖内部部署环境、混合环境或云环境，因此您可以轻松确定谁有权访问什么内容以及其如何获得该访问权限。此外，您 可以直接在报告中调整权限。您还可以发现非常敏感的数据所在的位置，以便确保其受到保护，轻松查看GPO，甚至在第一时间阻止对重要对象的更改。

检测 可疑活动并发出警报

Quest解决方案还提供对用户和管理员活动的实时审核，以及有关权限提升、不当更改和 其他可疑活动的警报，从而使您可以更快敲响警钟。高级用户行为分析可对各个用户行为模式进行建模，并检测异常操作。您甚至可以实现响应自动化，例如阻止活动、禁用用户或者撤销更改。

快速调查攻击并从攻击中恢复

企业平均需要69天才能控制数据泄露。[8] 借助Quest，您可以通过集中化数据收集以及类似Google的搜索和取证调查引擎来快速轻松地查明安全事件的根源。此外，您可以建立虚拟测试实验室以进行灾难恢复规划，并 将冗长的原生AD林恢复流程简化为图形用户界面驱动的简单流程。

保持并证明合规性

这些功能结合在一起，使您可以建立、保持并证明对广泛法规的合规性。另外，Quest解决方案还提供智能、可扩展的日志压缩，使您可以经济高效地将审核数据存储数年之久，同时确保其可用于安全调查和审核检查。

8 Ponemon Institute，《2018 Cost of a Data Breach Study》（2017年数据泄露成本分析）。

Quest
quest.com/cn
有关当地办事处信息，请访问 (quest.com/cn-zh/locations)

SolutionBrief-MPM_SecurityCompliance-US-zh_CN-WL-38251