Change Auditor for Active Directory

实时审核Active Directory和Azure Active Directory

Active Directory (AD)问题会导致成本高昂的意外服务中断和造成业务波动的网络停机。同样，有害的数据泄露和违反SOX、PCI、HIPAA、GDPR等规定也会给您带来严重的经济损失。您需要使用Active Directory审核和安全功能，以确保在AD和Azure AD出现重要更改时您能实时收到通知。

Quest® Change Auditor for Active Directory通过跟踪所有关键配置更改，然后将它们整合在单个控制台中，从而提高AD和Azure AD的安全性并增强对其的控制力。Change Auditor可以跟踪、审核和报告影响内部部署和云环境的更改并发出相关警报，省却了启用本机审核所产生的额外开销。借助Change Auditor for AD，您可以获得所有更改以及任何相关事件详细信息的标准化视图，包括更改前后的值以及关联的内部部署和云身份。您还可以添加注释来说明执行某项特定更改的原因，以便符合审核要求。借助Change Auditor for AD，您可以快速、高效地审核所有关键更改，从而保护宝贵数据和资源的安全。

审核所有重要更改

获取对所有关键AD和Azure AD更改的广泛且可自定义的审核与报告，包括对组策略对象(GPO)、域名系统(DNS)、服务器配置、嵌套组等内容的更改。与本机审核不

借助Change Auditor for Active Directory，您可以了解所有更改的执行者、内容、时间、位置以及来源工作站，并且所有项目均按时间顺序列出，包括关联的内部部署身份和云身份。

优势：

- 只需几分钟即可完成安装，并且可通过快速事件收集来即时分析Windows环境
- 可从单一客户端实现整个企业范围的内部部署和云审核与合规性
- 基于用户行为模式前瞻性地检测威胁
- 通过跟踪所有事件以及与特定事件相关的更改，消除未知的安全问题，从而确保应用程序、系统和用户的持续访问
- 无论用户是否在办公室，均可通过任何设备接收实时警报，从而立即做出响应，因此，仅需几秒钟便可降低安全风险
- 通过防止进行不需要的更改来加强内部控制，并限制对授权用户的控制
- 通过主动故障排除来解决帐户锁定问题，提高可用性
- 通过收集事件，而不是使用本机审核，降低对服务器性能的影响并节省存储资源
- 简化对公司与政府政策和法规（包括SOX、PCI DSS、HIPAA、FISMA、SAS 70等）的合规性
- 将信息转化为智能的详细取证数据，供审核人员和管理人员使用

“总体来说，Change Auditor非常有用。经过我们的评估，其他产品都无法提供可与之匹敌的实时审核和保护，而且借助这款产品，我们无需启用Windows审核功能即可对所有Active Directory更改进行审核。”

Patrick Rohe
陶森大学
高级IT架构师

系统要求

有关系统要求的最新详细列表，请访问quest.com/products/change-auditor-for-active-directory。

同，您将获得AD和Azure AD环境中所有内部部署、云和混合AD更改活动的整合视图，以及随着时间的推移有关与其他事件的关系的深入取证数据，这些内容按时间顺序列出。此外，借助主动警报，您可以从任何位置以及任何设备上，对发生的重要策略更改和出现的安全漏洞保持持续关注并能做出响应，从而降低与日常修改相关的风险。

跟踪用户活动并阻止进行不需要的更改

通过跟踪导致帐户锁定的用户和管理员活动以及对重要注册表设置的访问，在整个企业范围内严密监控更改并加强对策略的控制。通过主动控制在第一时间防止发生重要更改，提供24x7的警报以及执行深入的分析，而且借助还原先前值功能和报告功能，保护AD和Azure AD环境免受任何可疑行为和未经授权访问的侵害，并确保始终符合公司和政府标准。

包含ON DEMAND AUDIT的托管审核控制板

升级到On Demand Audit Hybrid Suite for Office 365，其包含Change Auditor for Active Directory和On Demand Audit。只需点击几下即可轻松将它们搭配使用，在单个托管视图中查看AD、Azure AD、Exchange Online、SharePoint Online和OneDrive for Business中所做的所有更改。通过响应快速的搜索和交互式数据可视化简化调查，并可将审核历史记录保留长达10年。

主动式威胁检测和CHANGE AUDITOR威胁检测

通过分析异常活动并排列贵公司中最高风险的用户顺序来简化用户威胁检测、识别潜在的威胁以及减少来自错误警报的干扰。

将不相关的数据转化为有意义的信息，以确保安全性与合规性

跟踪重要更改，然后将原始数据转换成有意义的智能分析结果，从而帮助保护基础架构的安全与合规性。Change Auditor for AD可帮助您了解更改的执行者、内容、时间、位置和来源工作站以及任何相关的事件详细信息，包括更改前后的值，以便您可以在担忧安全性的情况下快速做出决策。您还可以通过Change Auditor的高性能审核引擎消除审核限制。无需本机审核日志，您可以更快获得结果并节省存储。

集成的事件转发

轻松与SIEM解决方案相集成，将Change Auditor事件转发到Splunk、ArcSight或QRadar。此外，Change Auditor与Quest® InTrust®相集成，实现20:1的压缩事件存储和集中化的本地或第三方日志收集，进行解析和分析并对可疑事件发出警报和自动执行响应操作。

针对公司和政府法规自动生成报告

借助内置的合规性库以及可自定义的报告，证明符合政府标准（如GDPR、SOX、HIPAA、PCI DSS、FISMA和SAS 70）变得轻而易举。

关于QUEST

Quest致力于为瞬息万变的企业IT领域提供软件解决方案。我们帮助简化数据爆炸、云扩展、混合数据中心、安全威胁以及合规要求所带来的挑战。我们的产品组合包括用于数据库管理、数据保护、统一端点管理、身份和访问管理以及Microsoft平台管理的解决方案。

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

DataSheet-ChangeAuditor4AD-US-KS-zh_CN-WL-40680