Quest

Change Auditor

Change Auditor

针对Microsoft平台环境的实时更改审核

企业中的应用程序和服务的事件日志及更改报告既繁琐又费时，有时甚至无法使用原生审核工具来完成。由于没有中央控制台，您必须为每个服务器重复该过程，并且最终获得大量没有上下文的数据和众多报告。

这意味着，证明合规性或者快速对事件做出响应一直是个难题。由于原生事件详情稀疏零散并且很难解读，数据的安全性也处于风险之中。因此，您可能无法及时了解问题。由于原生工具无法阻止特权用户清除事件日志，因此您可能会失去日志数据，无法实现最初的审核目的。

幸运的是，Quest® Change Auditor可以提供帮助。该产品系列使您无需启用原生审核功能，即可实时对所有Active Directory (AD)、Azure AD、Exchange、Office 365、SharePoint、Skype for Business、VMware、EMC、NetApp、SQL Server和Windows文件服务器更改以及针对AD的LDAP查询进行审核、发出提醒和提供报告。

您可以通过一个中央控制台轻松地安装、部署和管理您的环境。您可以空前轻松地跟踪创建、删除、修改和访问尝试，并了解发生的情况，因为每个事件和所有相关事件都通过简单的术语显示，便于您了解五大要素：执行者、内容、时间、位置和源工作站，以及以前和当前的设置。

借助Change Auditor，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。

> “Change Auditor是目前为止在功能和成本方面最好的解决方案。我们非常喜欢这款工具的简洁性和易用性，通过它无需任何特定的专业技术即可创建查询。”
>
> *Stephane Malagnoux,*
> *BPCE Insurance计算机部门主管*

优势：

- 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，从而确保持续访问应用程序、系统和用户。
- 通过自动解释隐藏数据及其严重性，以便更快、更好地做出决策，从而减轻压力和降低复杂性。
- 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。
- 通过收集事件，而不是使用本机审核，降低对服务器性能的影响。
- 简化单独针对内部策略和外部法规（包括SOX、PCI DSS、HIPAA、FISMA、SAS 70等）的合规性报告。
- 向管理人员和审核人员证明相应的IT控制，让他们高枕无忧。

“Change Auditor是非常直观且功能非常强大的工具，使我能够了解员工所做的更改。它帮助我强制实施策略、限制访问权限以及检索有关数据泄露的警报。”

中型企业专业服务公司的高级IT架构师

来源：TechValidate。TVID：B4A-A84-619

产品
Change Auditor Threat Detection
Change Auditor for Active Directory
Change Auditor for Active Directory Queries
Change Auditor for EMC
Change Auditor for Exchange
Change Auditor for FluidFS
Change Auditor for Logon Activity
Change Auditor for NetApp
Change Auditor for SQL Server
Change Auditor for SharePoint
Change Auditor for Skype for Business
Change Auditor for VMware vCenter
Change Auditor for Windows File Servers

这种广泛的数据分析使您可以在出现问题时（例如特定用户和工作站进行了其他哪些更改）立即采取措施，消除了其他的不确定性和未知的安全问题。无论您要尝试满足安装合规性需求还是满足内部安全策略，Change Auditor都是您可以信赖的解决方案。

功能

通过关联的视图进行混合环境审核 — 审核混合环境，包括AD/Azure AD、Exchange/Exchange Online、SharePoint/SharePoint Online/OneDrive for Business以及AD登录和Azure AD登录。与本机审核不同，Change Auditor可为混合环境中的活动提供单个关联视图，从而确保发生的所有更改（在内部部署或云环境中）的可见性。

更改防范 - 防止更改AD、Exchange和Windows文件服务器（包括特权组、组策略对象和敏感邮箱）中的关键数据。

可直接呈递审核员的报告 — 生成全面的报告，符合SOX、PCI DSS、HIPAA、FISMA、GLBA、GDPR等法规的妥善做法和法规合规性要求。

包含On Demand Audit的托管控制板 — 通过具有响应快速的搜索、交互式数据可视化和长期事件存储功能的托管SaaS控制板查看AD和Office 365混合活动。

通过Change Auditor Threat Detection进行前瞻式威胁检测 — 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。

高性能审核引擎 — 消除审核限制并捕获更改信息，而无需使用原生审核日志，从而可以更快速地生成结果并节约大量存储资源。*

帐户锁定 - 捕捉造成帐户锁定事件的原始IP地址和工作站名称，查看交互时间表中的相关登录和访问尝试。这有助于简化内外部安全威胁的检测和调查。

随时随地获得实时警报 — 向电子邮件地址和移动设备发送关键更改和模式警报，以提醒立即采取措施，让您即便不在现场也能针对威胁更快做出响应。

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IBM 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。

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。

* 不适用于FluidFS、SharePoint、EMC、NetApp和VMware。

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

DataSheet-ChangeAuditor-US-KS-zh_CN-WL-40681