Quest

Change Auditor

Change Auditor

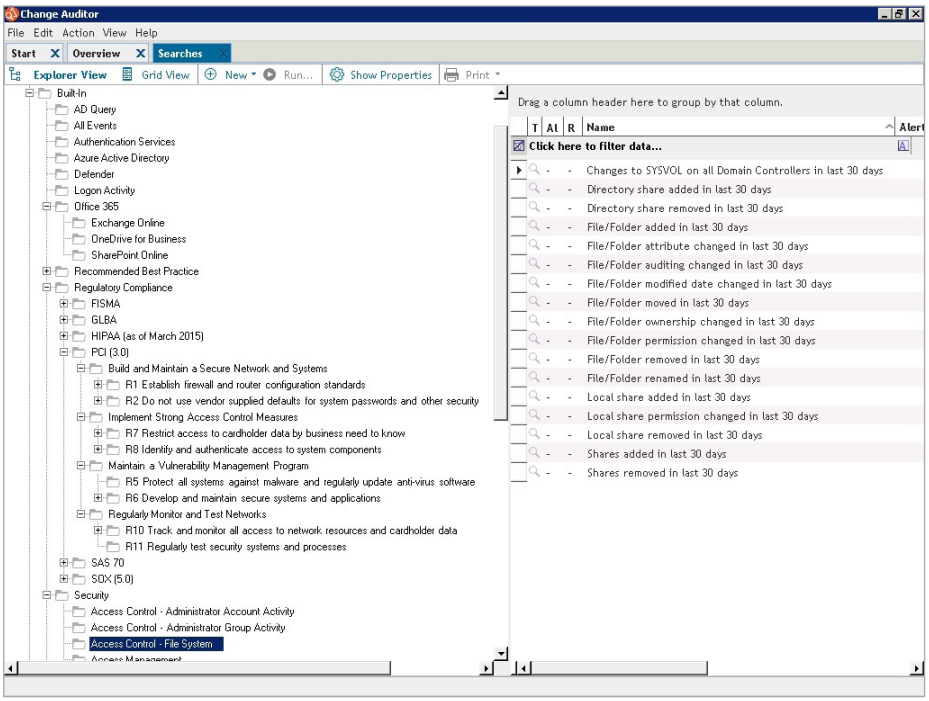
针对Microsoft平台环境的实时更改审核

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，有时甚至无法使用本机审核工具来完成。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。由于本机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。由于本机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，Change Auditor可以提供帮助。该产品系列使您无需启用本机审核功能，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



获得700多个立即可用的合规性和最佳实践报告事件，以及有关所有更改的执行者、内容、时间、位置和工作站的实时提醒。

> “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*

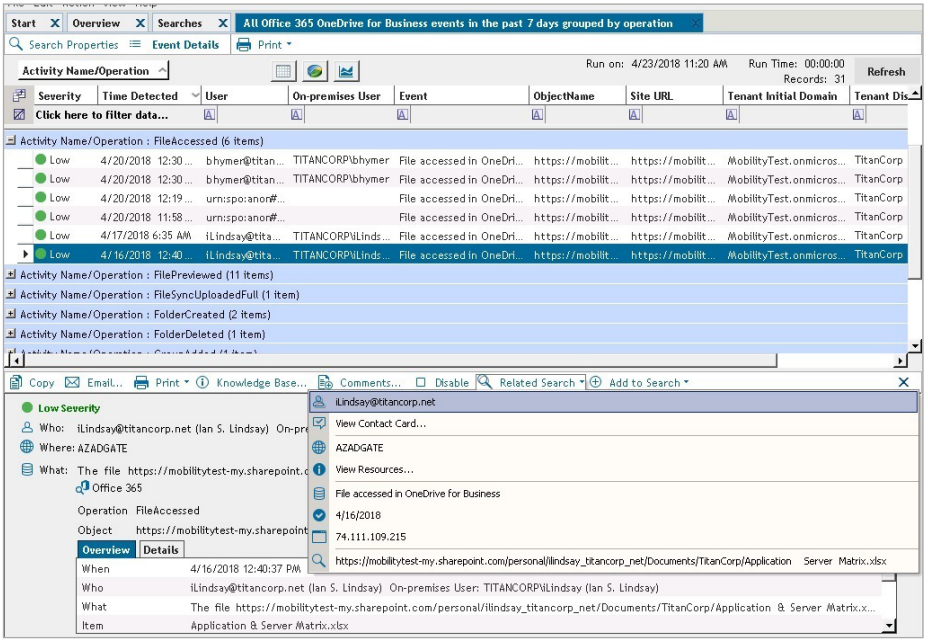
优势：

- 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



相关搜索通过提供有关特定用户以及他们进行的所有更改的详情，帮助您实现在特定环境下的安全性。

解6大要素：执行者、内容、时间、位置、工作站和原因，以及以前和当前的设置。

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。

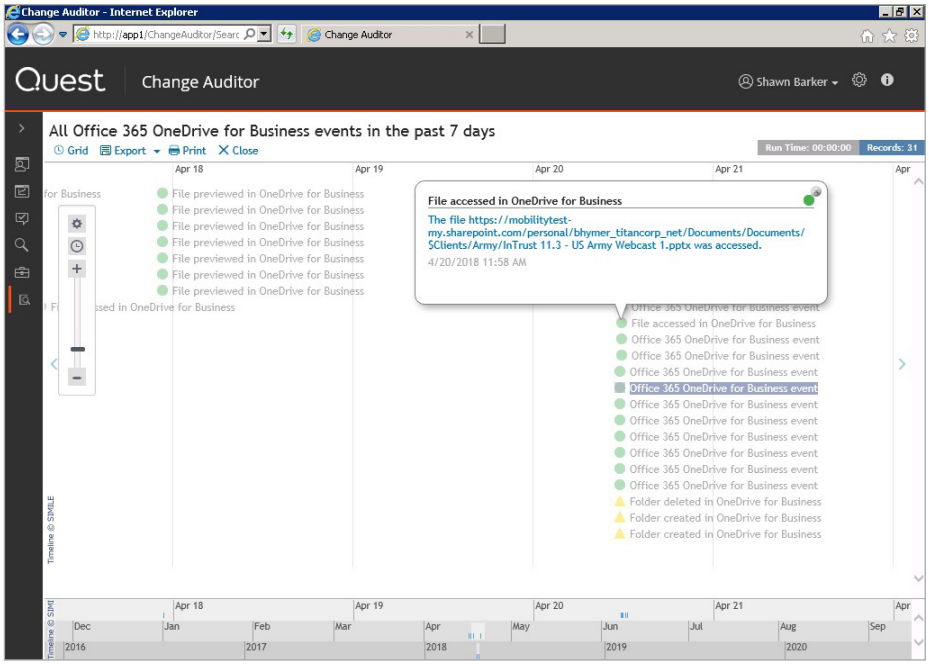
高性能审核引擎 - 消除审核限制并捕获更改信息，而无需使用本机审核日志，从而可以更快速地生成结果并节约大量存储资源。*

借助IT安全搜索提高洞察力 - 将大量系统和设备中不同IT数据关联到交互搜索引擎中，以加快安全事件响应和取证分析速度。通过丰富的可视化和事件时间表囊括用户授权和活动、事件趋势、可疑模式等。

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。

有关移动的实时警报 - 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。

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



从一个基于Web的控制台以事件时间轴的形式查看、报告和分析审核活动。

系统要求

有关详细要求的完整列表，请查看版本说明指南。

安全时间表 - 按时间顺序查看、突出显示和筛选您的AD和Microsoft平台中发生的更改事件，并发现这些事件与其他事件的关系，以便更好地进行取证分析和安全事件响应。

相关搜索 - 一键式即时访问有关您正在查看的更改的信息以及所有相关的事件（例如来自特定用户和工作站的其他更改），从而消除额外的不确定因素和未知的安全隐患。

时间归档 - 安排将两种旧数据归档到归档数据库，让企业能够在线保留关键数据及相关数据，同时改进搜索和数据检索的整体性能。

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、HP Arcsight或IBM QRadar。此外，Change Auditor还与Quest® InTrust®相集成实现长期20:1的压缩事件存储并聚合本机或第三方日志，以降低SIEM转发的存储成本和创建高度压缩的日志存储库。

基于角色的访问 - 配置访问权限，以便审核员无需更改任何应用程序配置，也无需管理员花费时间提供协助，即可运行搜索和报告。

基于Web的访问及控制板报告 - 使用Web浏览器可随时随地执行搜索，并且可以创建有针对性的控制板报告，因此，高层管理人员和审核员不必了解体系结构或管理情况即可访问所需的信息。

关于QUEST

Quest的宗旨是通过简单的解决方案解决复杂的问题。为实现此宗旨，我们秉持注重卓越产品和优质服务的理念，并且追求易于合作这一总体目标。我们的愿景是提供技术来避免在效率与有效性之间做出取舍，从而使您和您的企业可以减少用于IT管理的时间，并将更多时间用于业务创新。

Quest
www.quest.com/cn
如果您不在北美洲，可以在我们的网站上找到本地办公室信息。

DataSheet-ChangeAuditor-US-KS-zh_CN-WL-34738