IT Security Search

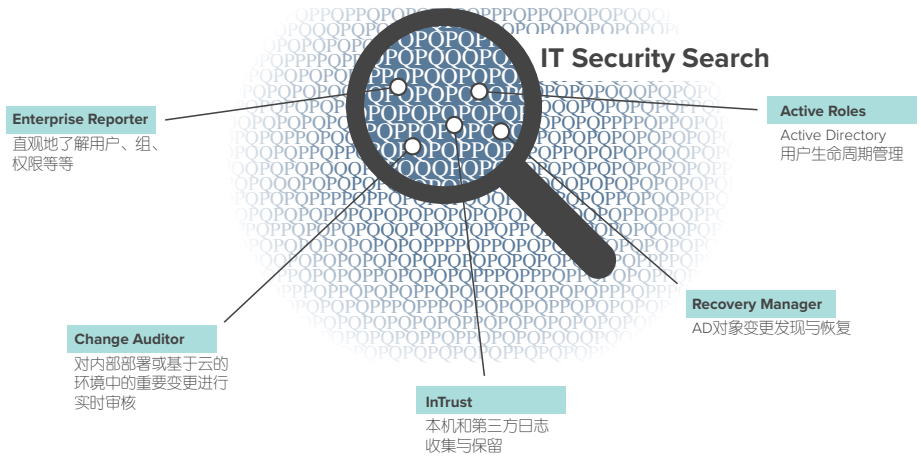
将不同的IT数据关联到交互搜索引擎

在分散的IT环境中很难持续跟踪谁有权访问数据、他们如何获得的访问权限以及他们如何使用该访问权限。查看不可见的内容是IT面临的一项挑战。面对各种不同来源（内部部署和云环境中）中要收集和审核的数十亿计的事件，很难找到相关数据并了解其意义。在内部或外部出现安全违规时，能够确定最初发生违规的位置和访问的内容可以使局面大大改观。幸运的是，许多Quest®解决方案中都提供IT Security Search功能，它可以大大简化上述工作。

IT Security Search是类似于Google的IT搜索引擎，使IT管理员和安全团队可以快速响应安全事件和分析事件取证。该工具基于Web的界面将来自许多Quest安全与合规性解决方案的分散IT数据关联在单个控制台中。

借助快速搜索，您可以查看谁执行了哪些操作及执行的时间和位置，Active Directory (AD)中的关键对象是否发生了更改，授予用户或组的特权是否得到了提升，或是否有人不当访问了敏感文件或文件夹数据。附加的丰富可视化和事件时间表有助于为管理层和利益相关方提供更多宝贵的深刻见解。

IT Security Search在多款Quest解决方案（包括Enterprise Reporter、Change Auditor、InTrust®、Recovery Manager for AD和Active Roles）中提供，可提取数据并通过单一管理平台呈现这些数据。在这里，您可以轻松查看内部部署或混合环境中的各种活动，并执行相应的操作。配置基于角色的访问，使审核人员、服务台员工、IT经理和其他利益相关方可以准确获得所需的报告。



使用IT Security Search，可以比以往更加轻松地发现内部和外部的安全违规情况。

IT Security Search使用简单的自然搜索语言，帮助管理员和安全团队快速调查内部攻击行为。

优势：

- 简化对信息孤岛上分散的关键IT数据的搜索、分析和维护工作
- 通过在一个可搜索的位置实时、全面地查看特权用户和服务器/文件数据，加快安全性调查及合规性审核的速度
- 在发生中断或安全违规时，对普遍存在的问题进行故障排除
- 轻松快速地恢复损坏或恶意更改的AD对象
- 支持基于角色的访问，为所有利益相关方准确提供其所需的报告

系统要求

兼容性

以下版本的数据提供系统在此版本的IT Security Search中受支持：

InTrust 11.4、11.3.2、11.3.1、11.3、11.2

Change Auditor 7.0、6.9.5、6.9.4、6.9.3、6.9.2、6.9.1、6.9、6.8

Enterprise Reporter 3.1、3.0、2.6、2.5.1

Recovery Manager for Active Directory 9.0.1、9.0、8.8.1、8.8、8.7.1、8.7

Active Roles 7.3.1、7.2.1、7.2、7.1、7.0

软件要求

操作系统：
Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

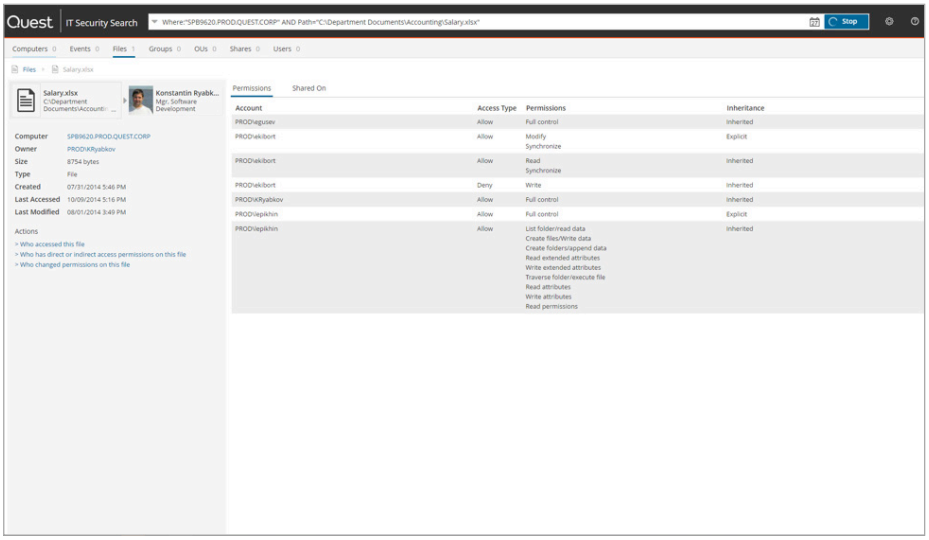
Microsoft Windows Server 2008 R2

其他软件：
Microsoft .NET Framework 4.6.2或更高版本

Microsoft Windows PowerShell 3.0或更高版本

Microsoft SQL Server 2012或更高版本（所有版本）。这是IT Security Search Warehouse组件的要求，其需要这些内容进行内部配置管理。

有关系统要求的最新详细列表，请访问quest.com/products/it-security-search。



轻松了解访问用户、内容、位置和访问方式。

基于状态的数据

- 通过Enterprise Reporter，可深入了解内部部署、Azure和混合环境中的以下方面的重要信息：用户、计算机和组，直接和嵌套组成员关系，组织单位(OU)和文件/文件夹权限，所有者等等。提高IT团队的能力，以全面了解其安全状态。
- 通过Active Roles查看虚拟属性、动态组成员、临时组成员和托管设备。

实时安全审核

- 通过Change Auditor，搜索有关内部部署环境或Office 365和Azure AD中重要对象和敏感数据更改的实时信息。
- 在本机审核详细信息中补充发起AD更改的实际用户，即使更改是通过Active Roles发起的也是如此。

收集和存档日志

通过InTrust®日志管理，跨多元化的企业网络收集本机（Windows服务器、Unix/Linux、工作站等）日志以及第三方日志。

压缩且编制了索引的在线存储库

通过InTrust对长期事件日志数据和其他服务器数据执行全文本搜索，以实现合规性和安全性，从而节省用在查找事件上的时间。

对象恢复

通过Recovery Manager for AD发现发生更改的AD对象（包括更改前后的值），而且只需单击几下即可将其还原。

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)

Quest、InTrust和Quest徽标是Quest Software Inc.的商标和注册商标。有关Quest标记的完整列表，请访问www.quest.com/legal/trademark-information.aspx。其他所有商标均归其各自拥有者所有。

© 2019 Quest Software Inc. 保留所有权利。

DataSheet-ITSS-US-KS-zh_CN-WL-38937