IT Security Search

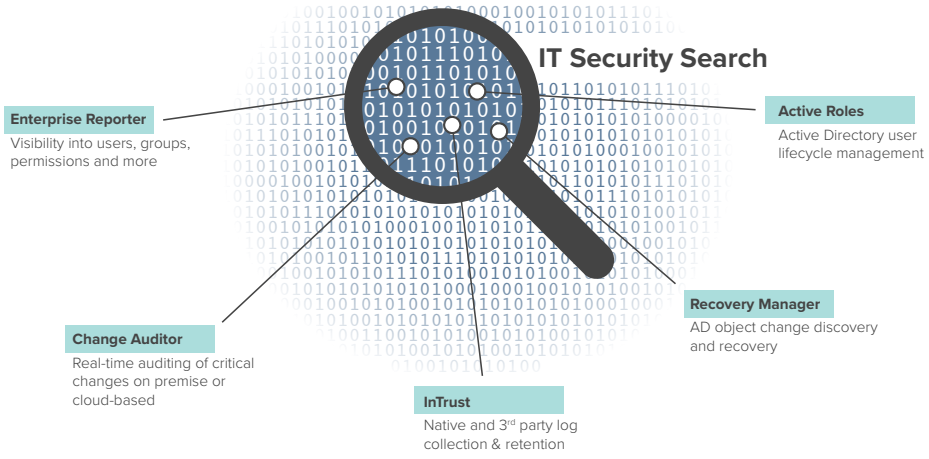
Correlate disparate IT data into an interactive search engine

Keeping track of who has access to data, how they obtained it and how they are using that access can be difficult in a disparate IT environment. Seeing the unseeable can be a challenge for IT. With billions of events to collect and review from a variety of sources, both on premises and in the cloud, it's difficult to find relevant data and make sense of it. And in the event of a security breach, either internal or external, the ability to locate where the breach originated and what was accessed can make a world of difference. Luckily, IT Security Search, a feature of several Quest® solutions, makes it easier than ever.

IT Security Search is a Google-like IT search engine that enables IT administrators and security teams to quickly respond to security incidents and analyze event forensics. The tool's web-based interface correlates disparate IT data from many Quest security and compliance solutions into a single console.

With a quick search, you'll be able to find out who did what, when and where, whether it's a change to critical Active Directory (AD) objects, elevated privileges granted to a user or group, or someone inappropriately accessing sensitive files or folder data. And additional rich visualizations and event timelines help to provide more valuable insights to management and stakeholders.

IT Security Search is available as part of several Quest solutions, including Enterprise Reporter, Change Auditor, InTrust®, Recovery Manager for AD and Active Roles, that pulls data and feeds it into a single pane of glass.From here, you can easily review and act upon all of the various activities in your on-premises or hybrid environment. Configure role-based access, enabling auditors, help desk staff, IT managers and other stakeholders to get exactly the reports they need and nothing more.



IT Security Search makes identifying security breaches, both internal and external, easier than ever.

IT Security Search uses simple, natural search language to help administrators and security teams quickly investigate insider attacks.

BENEFITS:

- Reduce the complexity of searching, analyzing and maintaining critical IT data scattered across information silos
- Speed security investigations and compliance audits with complete real-time visibility of your privileged users and server/file data in one searchable place
- Troubleshoot widespread issues should an outage or security breach occur
- Restore corrupted or maliciously changed AD objects with ease and speed
- Enable role-based access to provide all stakeholders with exactly the reports they need and nothing more

SYSTEM REQUIREMENTS

COMPATIBILITY

The following versions of data-providing systems are supported in this version of IT Security Search:

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

SOFTWARE REQUIREMENTS

Operating system: Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

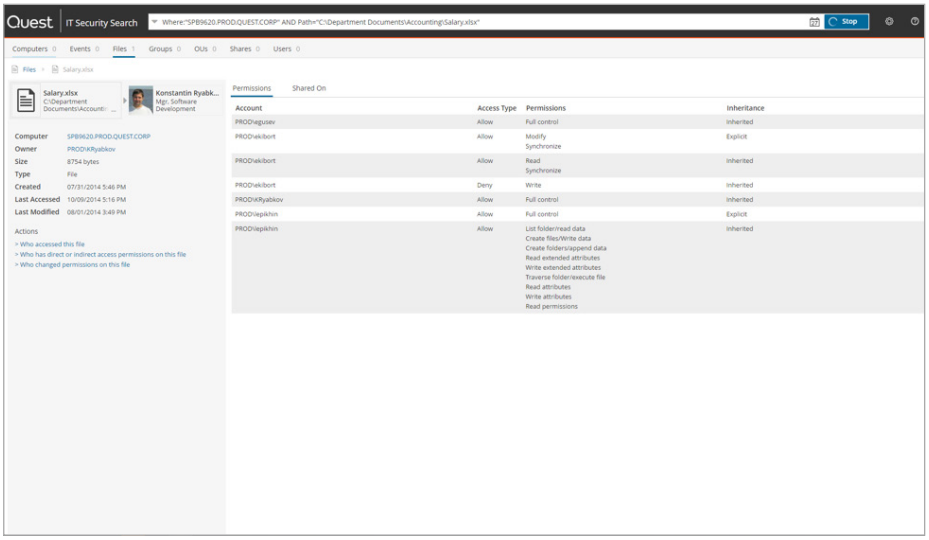
Microsoft Windows Server 2008 R2

Additional software: Microsoft .NET Framework 4.6.2 or later

Microsoft Windows PowerShell 3.0 or later

Microsoft SQL Server 2012 or later (all editions). This is a requirement of the IT Security Search Warehouse component, which needs it for internal configuration management.

For a detailed and current list of system requirements, please visit quest.com/products/it-security-search.



Easily understand the who, what, where and how of user access.

STATE-BASED DATA

- Gain critical insights into user, computer and group information; direct and nested group memberships; organizational unit (OU) and file/folder permissions; ownership; and more across on-premises, Azure and hybrid environments with Enterprise Reporter. Empower IT teams to comprehensively understand their state of security.
- View virtual attributes, dynamic group members, temporal group members and managed units from Active Roles.

REAL-TIME SECURITY AUDITING

- Search real-time information about changes to critical objects and sensitive data, whether on premises or in Office 365 and Azure AD, with Change Auditor.
- Supplement native audit details with the actual user who initiated a change to AD, even if it was initiated through Active Roles.

COLLECT AND ARCHIVE LOGS

Gather native (Windows server, Unix/Linux, workstation and more) logs as well as third-party logs from across your diverse enterprise network with InTrust® log management.

COMPRESSED, INDEXED, ONLINE REPOSITORY

Conduct full-text search on long-term event log data and other server data for compliance and security purposes with InTrust, saving time spent looking for events.

OBJECT RECOVERY

Discover which AD objects have changed, including before and after values, and restore them in a few clicks with Recovery Manager for AD.

ABOUT QUEST SOFTWARE

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-ITSS-US-KS-38937