QUEST SOFTWARE

DATASHEET

InTrust®

Event Log Management for Security and Compliance

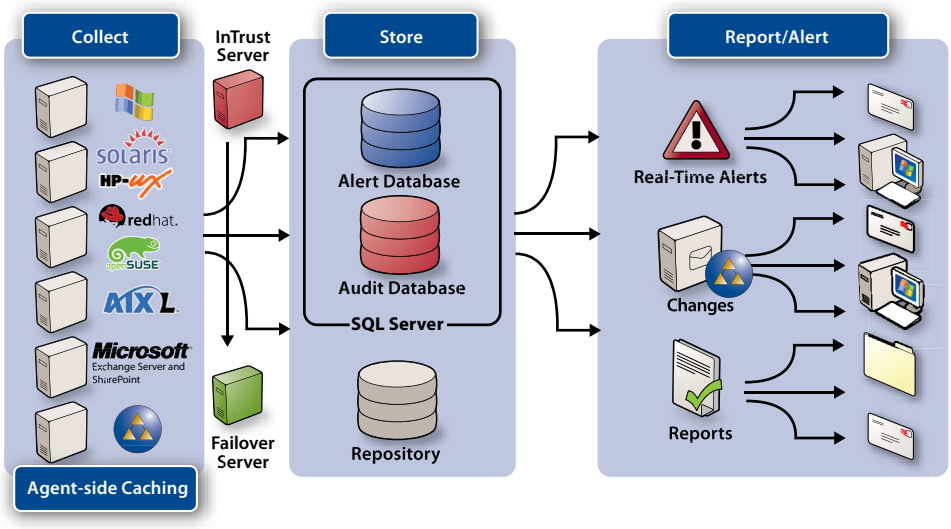
Keeping track of user and administrator activity is at the heart of keeping your environment secure and complying with various IT regulations.

Historically, monitoring user activity on critical network resources has been a challenging task – one that involves processing vast amounts of data scattered across numerous systems. Huge volumes of logs, expensive storage hardware, lack of in-house expertise about events, event log diversity and mediocre native tools for log analysis and reporting further complicate this task.

InTrust from Quest Software is the only event log management solution in the market that addresses all of these concerns in heterogeneous environments composed of Windows, Unix and Linux servers, databases, business applications and network devices.

With InTrust, you can securely collect, store, report and alert on event log data, helping you comply with external regulations, internal policies and security best practices. You can achieve regulatory compliance by auditing user access to critical systems and detecting inappropriate or suspicious access-related events.

Using this single solution to monitor access to critical systems on multiple platforms reduces the complexity of event log management, saves storage administration costs, improves information assurance, mitigates risk and helps to reduce cost and improve efficiency of security, operational and compliance reporting.



"InTrust was attractive to us because it provides a single user interface to both policy compliance monitoring and real-time, business-critical security event alerting."

— Colin Harrison
Principal Project Manager
IT Systems Architecture
Experian, UK, Ltd

BENEFITS

- Reduces costs by automating the collection and compression of event log data across heterogeneous environments
- Addresses regulatory and policy compliance by compressing and storing critical event log data for audits
- Ensures tamper free audit logs via agent-side caching, securing the audit log data from modification or loss
- Improves internal security by identifying user accounts that are being used in violation of corporate policy, proactively alerting in real time
- Sends real-time notification so you can respond immediately to the most critical events
- Automates responses to certain events, such as disabling an offending user or reversing a change

Features and Benefits

Key to Compliance: Addresses regulatory compliance by collecting and reporting on event logs across the entire IT stack, monitoring user access to critical systems and applications and allowing you to perform forensic analysis of user and system activity based on historical event data.

User Activity Tracking: Collects events on user and administrator activity from diverse and spread-out systems and applications and presents them in an easy-to-use and complete form suitable for ongoing reporting and ad hoc analysis. Extracts all the essential details of user access such as who performed the action, what that action actually entailed, which server it happened on and which user workstation it originated from.

Automated Log Collection: Automates the secure collection of event logs, decreasing your workload.

Log Data Compression: Provides unparalleled long-term compression, versus storing the same amount of event data in a database.

Log Integrity: Enables you to create a cached location on each remote server where logs can be duplicated as they are created, preventing a rogue user or administrator from tampering with the audit log evidence.

Forensic Analysis: Provides tools for interactive searching through historical event log data for on-the-spot investigation of security incidents and policy violations and preparation of evidence suitable for submission to the court.

Real-Time Alerting: Sends real-time alert notifications about unauthorized or suspicious user activity directly to you via email or to third-party monitoring applications such as Microsoft Operations Manager (MOM).

Flexible Reporting: Gives you unprecedented access to predefined and customizable reports, supporting a wide variety of file formats, including HTML, XML, PDF, CSV and TXT, as well as Microsoft Word, Visio and Excel.

Fault Tolerance: Provides automated server redundancy in the case of failure, enabling you to quickly move all configurations and jobs from a crashed server to a backup server to handle all activity and reducing the possibility of lost log files due to server failure.

About Quest Software, Inc.

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for **administration and automation**, **data protection**, **development and optimization**, **identity and access management**, **migration and consolidation**, and **performance monitoring**, go to **www.quest.com**.

TARGET PLATFORMS

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows NT 4.0 Service Pack 6 or higher
- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Sun Solaris
- HP-UX
- IBM AIX
- Red Hat Enterprise Linux AS
- Red Hat Enterprise Linux ES
- SUSE Linux Enterprise Server

For a list of supported operating system refer to the System Requirements document.

QUEST SOFTWARE®

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | EMAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.