InTrust

Smart and scalable event log management

Your organization's most valuable asset is its data and the users that have access to it. For IT and security departments, keeping track of user and privileged account activity — especially on workstations or end-user devices — is at the heart of keeping their environment secure and complying with various industry regulations. But this is a difficult task because of the massive amounts of data scattered across disparate systems, devices and applications. Collecting, storing and analyzing all this data generally requires large amounts of storage, time-consuming collection of event data, and in-house expertise about the event data collected.

With Quest InTrust, you can monitor all user workstation and administrator activity from logons to logoffs and everything in between. Slash storage costs with 20:1 data compression, and store years of event logs from Windows, UNIX/Linux servers, databases, applications and network devices. InTrust real-time alerting enables you to immediately respond to threats with automated responses to suspicious activity.

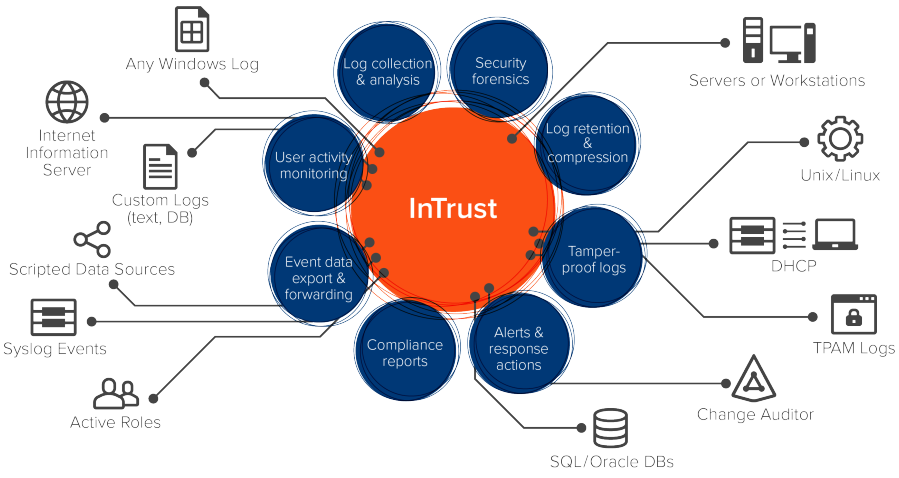
FEATURES

Single pane of glass

Collect and store all native or third-party workstation logs from various systems, devices and applications in one, searchable location with immediate availability for security and compliance reporting. InTrust delivers a unified view of Windows event logs, UNIX/Linux, IIS and web application logs, PowerShell audit trails, endpoint protection systems, proxies and firewalls, virtualization platforms, network devices, custom text logs, as well as Quest Change Auditor events.

User workstation monitoring

Protect your workstations from modern cyberattacks, such as pass-the-hash, phishing or ransomware, by monitoring user and administrator activity — from logons to logoffs and everything in between. Collect and store all essential



Efficiently monitor all user workstation and administrator activity to secure your most valuable asset — your data.

"We use InTrust for log collection from domain controllers and monitoring events for SOX compliance auditing. I love the repository viewer, it is great for researching account lockouts and other login events for security purposes."

Engineer, S&P 500 Professional Services Company

TVID: 726-084-5E5

BENEFITS:

- Slash storage costs and ensure continuous compliance with a highly-compressed and indexed log repository
- Easily search all end user and privileged account activity from a single location
- Quickly report on, troubleshoot and investigate security events
- Make sense of your data with normalized native event logs
- Easily integrate with your existing SIEM solution
- Immediately respond to threats with real-time alerting and automated responses
- Protect event log data from tampering or destruction by duplicating events as they are created

"I believe the product offers invaluable security reporting and alerting capabilities. While other products do similar things, I feel that InTrust is positioned to enable a quick implementation that delivers immediate value in the audit and compliance arena."

Senior IT Manager, Fortune 500 Automotive & Transport Company

TVID: D2B-CDB-505

SYSTEM REQUIREMENTS

SUPPORTED PLATFORMS
Microsoft Windows Events
Microsoft IIS Events
Microsoft Forefront Threat Management Gateway and ISA Server Events
Microsoft DHCP Server Events
Solaris Events
Red Hat Enterprise Linux Events
Oracle Linux Events
SUSE Linux Events
Debian GNU/Linux Events
Ubuntu Linux Events
IBM AIX Events
HP-UX Events
VMware vCenter Events
VMware ESX and ESXi Events
For more information, see the System Requirements document.

details of user access, such as who performed the action, what that action entailed, on which server it happened and from which workstation it originated.

Simplified log analysis

Consolidate cryptic event logs from disparate sources into a simple, normalized format of who, what, when, where, where from and whom to help you make sense of the data. Unique, full-text indexing makes long-term event data easily searchable for fast reporting, troubleshooting and security investigation.

Smart, scalable event log compression

Collect and store massive volumes of data in a highly-compressed repository, 20:1 with indexing and 40:1 without, so you can save on storage costs by up to 60% and ensure continuous compliance with HIPAA, SOX, PCI, FISMA and more. Additionally, one InTrust server can process up to 60,000 events per second with 10,000 agents writing event logs simultaneously, giving you more efficiency, scalability and substantial hardware cost savings. And if you need more volume, you can simply add another InTrust server and divide the workload — scalability is virtually limitless.

Real-time alerting and response actions

Watch for unauthorized or suspicious user activity so you can respond to threats immediately with real-time alerts sent directly via email or to monitoring applications like System Center Operations Manager. You can then automatically trigger responses to these suspicious events, such as disabling the offending user, reversing the change and/or enabling emergency auditing.

Tamper-proof logs

Protect event log data from tampering or destruction by creating a cached location on each remote server where logs can be duplicated as they are created.

Integration with SIEM solutions

Forwards all log data collected from Windows servers and network devices to a security information and event management (SIEM) solution of your choice. Supports customizable event output formats to seamlessly integrate with a wide variety of SIEM solutions.

Improved Insights with IT Security Search

Leverage the valuable insights from all of your Quest security and compliance solutions in one place. With IT Security Search, you can correlate data from InTrust, Change Auditor, Enterprise Reporter, Recovery Manager for AD, and Active Roles in a Google-like, IT search engine for faster security incident response and forensic analysis. Easily analyze user entitlements and activity, event trends, suspicious patterns and more with rich visualizations and event timelines.

Automated best practice reporting

Easily convert investigations into multiple report formats, including HTML, XML, PDF, CSV and TXT, as well as Microsoft Word, Visio and Excel. Schedule reports and automate distribution across teams or choose from a vast library of predefined best practice reports with built-in event log expertise. With data import and consolidation workflows, you can even automatically forward a subset of data to SQL Server for further advanced analysis.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

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-InTrust-US-KS-35123