Software

InTrust®

Gain IT insights with on-the-fly data investigations

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 Dell 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.

InTrust enables you to securely collect, store, search and analyze massive amounts of IT data from numerous data sources, devices and SIEM solutions in one place. Get real-time insights into user activity for security, compliance and operational visibility. With one view know what resources users have access to, how that access was obtained and how it was used.

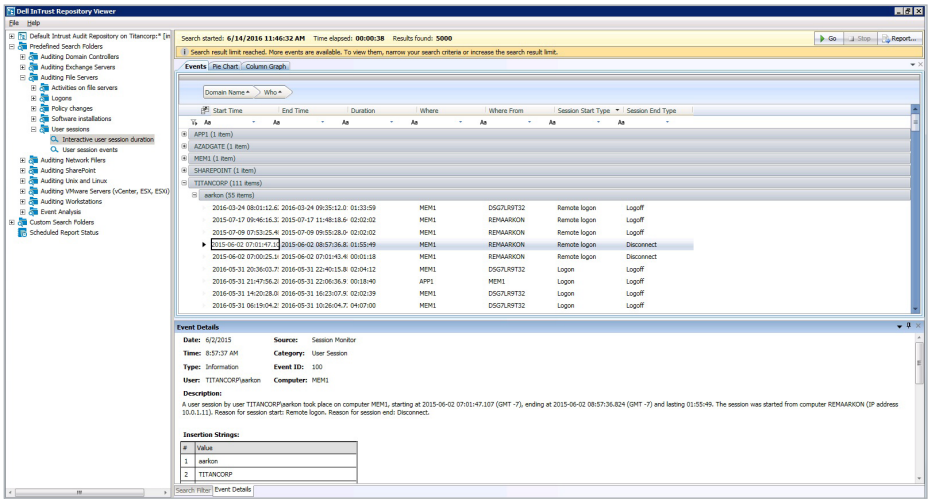

Figure 1. Use built-in reports to zero in on critical event data.

"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:

- 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 machine data in one searchable place
- Troubleshoot widespread issues should an incident occur
- Save on storage costs and adhere to compliance event log requirements (HIPAA, SOX, PCI, FISMA, etc.) with a highly-compressed and indexed online long-term event log repository

System requirements

Target platforms
Oracle Linux
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
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Sun Solaris
HP-UX
IBM AIX
IBM AIX 7.1
Red Hat Enterprise Linux AS
Red Hat Enterprise Linux ES
SUSE Linux Enterprise Server
For a list of supported operating systems, refer to the System Requirements document.

Features

Improved insights with IT Search — Correlate disparate IT data from numerous systems and devices into an interactive search engine for real-time search and analysis. Include user entitlements and activity, event trends, suspicious patterns and more with rich visualizations and event timelines.

On-the-spot security and compliance view — Pass audits, review security incidents and reveal any malicious insider activity in less time and with more confidence. One view quickly answers tough questions including what resources users have access to, how that access was obtained and how it was used afterwards.

Dynamic investigation paths — Start investigations into users, groups, shares, files or events and quickly pivot into other views as new details emerge for a more complete investigation.

Real-time log collection and analysis — Automate, secure and scale the collection of event logs across servers, network devices and workstations with immediate availability for analysis, security and compliance reporting.

Automated best practice reporting — Easily convert investigations into multiple report formats. Schedule reports and automate distribution across teams or choose from a vast library of pre-defined best practice reports with built in event log expertise.

Tamper-proof logs — 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.

Indexed repository — Archive and conduct full-text search on long-term event log data for compliance and security purposes in a highly compressed and indexed online repository, saving storage costs and time spent searching for events.

Single pane of glass — Run smart searches on auditing data from Dell Enterprise Reporter and Change Auditor to improve security, compliance and operations while eliminating information silos from other tools.

Monitor and alert on activity — 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).

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.

Diverse systems support — Get a unified view into event log data from Windows, Unix/Linux, network devices, custom text logs and more. Make sense of log events by leveraging their simplified and normalized representation of who, what, when, where and workstation.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results.

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

© 2016 Dell, Inc. ALL RIGHTS RESERVED. Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.
Datasheet-InTrust-US-GM-23290