Making Sense of Your IT Data for On-the-Fly Investigations

Abstract

Analyzing user activity on files, folders and other network resources involves processing huge amounts of data scattered across disparate systems, devices and applications. The difficulty in managing, maintaining and searching on "big IT data" hampers security and compliance efforts and slows down investigations.

This tech brief introduces InTrust 11.0, which consolidates, stores, searches through and analyzes the millions of files and billions of events that comprise IT data. InTrust provides organizations with the inside track on log management, security, compliance and IT data analytics.

Introduction

In the world of governance, risk and compliance (GRC), your business depends on being prepared for an audit at any time. That means being able to quickly get your hands on data about system configuration, user access and recently accessed files, wherever in the organization that data may reside.

In fact, being compliant is probably not the hardest part; staying compliant is. As regulations, software and business processes change, it becomes more difficult to know exactly where in the mountains and silos of data a given document is stored, who last accessed it and what that person did with it.

This tech brief describes new features in InTrust 11.0 designed to help businesses make sense of all their IT data with on-the-fly investigations. InTrust is a GRC product in Dell's assess-audit-remediate-manage model of continuous compliance, used for security investigations, log management and compliance. From this tech brief, administrators, security officers and compliance staff will take away a clear picture of how they can use InTrust 11.0 to analyze the IT data residing on their own networks and see the 5 W's — who, what, when, where and workstation.

In fact, being compliant is probably not the hardest part; staying compliant is.

The quest for continuous compliance

For IT departments, the essence of GRC is ensuring that company data is secure, available and compliant. That means tracking IT data like system configurations and being able to quickly identify which users have access to which files and how they have used that access.

In most organizations, that is easier said than done. While most people assume that "big data" refers to vast quantities of data located somewhere on the Internet, IT teams know that big data is alive and well right inside their own network. Continuous compliance means tracking huge amounts of IT data on users, groups, computers, shares, files and events scattered among disparate systems, devices and applications.

For IT to get its arms around and make sense of all the data it needs for audits, security investigations and day-to-day operations — in other words, to be continuously compliant — it needs to regard this as a big data problem.

Three avenues, three sets of stakeholders

Furthermore, to make sense of huge quantities of data, IT must pursue the three different avenues shown in Figure 1, each of which poses its own set of obstacles:

1. Log management. Server logs hold useful clues about threats, but IT teams face the obstacles of securely collecting and archiving logs across a diverse enterprise network, then figuring out how to automate the review process and make sense of log data out of context.
2. Security and compliance. IT must be able to conduct full investigations of security incidents and fraudulent activity — especially of insiders, since many security threats are internal — yet at best they manage a patchwork investigation. They are unable to pass audits and they have trouble showing proof of the controls they have put in place.
3. IT data analytics. Forced to use an assortment of one-off and native tools, IT cannot apply suitable analytics to its big data problem.

Those obstacles impede the quest for continuous compliance, with unsatisfying results for three sets of stakeholders:

- Administrators are not able to troubleshoot widespread issues should an incident occur. Nor are they able to quickly answer common questions like "Who has access to this file?" "How was access granted?" and "How was the access used?"
- Security officers are unable to perform forensic analysis and investigate fraud because the data they need resides in different locations with different outputs.
- Compliance officers have to produce multiple reports from multiple systems to prove compliance.

The inability to locate and make sense of IT data puts organizations in reactive mode, setting them up for security breaches, compliance failures and even system downtime.

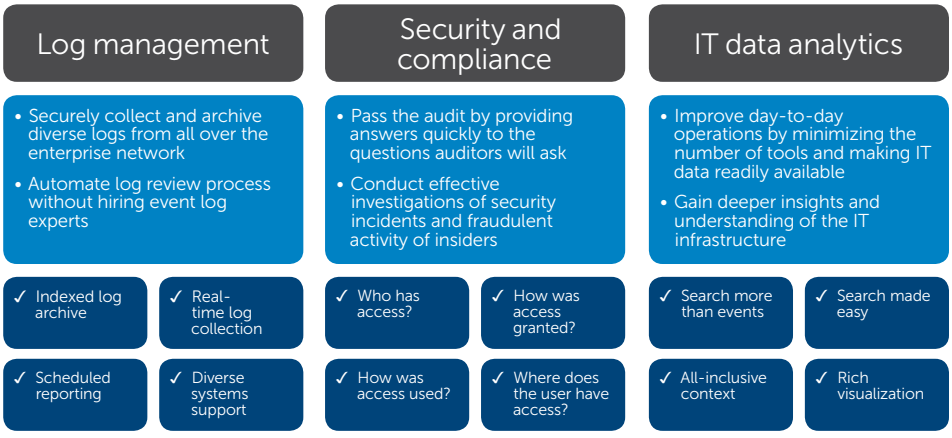

Figure 1: Three avenues of continuous compliance

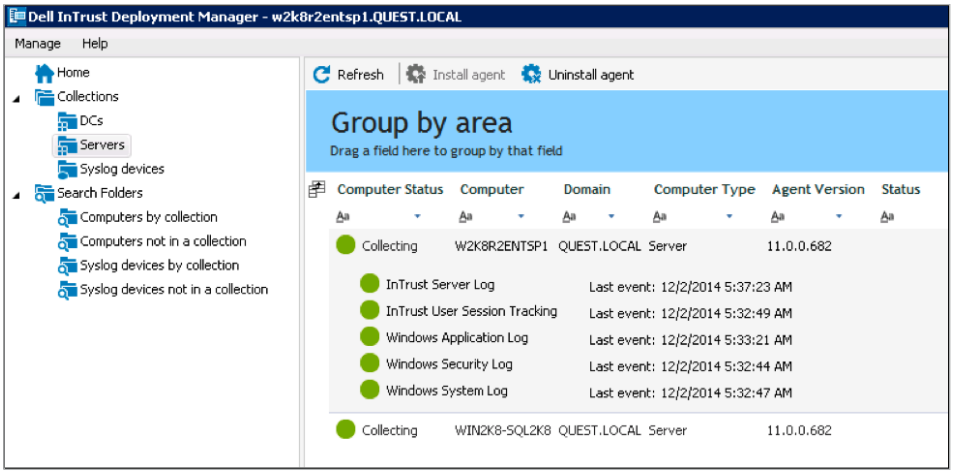

Figure 2: Configuring the collection of event log data

Continuous compliance and Intrust 11.0

Intrust 11.0 from Dell is specifically designed to collect, archive and correlate IT data and user activity from across the enterprise. With InTrust, organizations can make sense of IT data throughout the network with on-the-fly investigations.

By storing event log data in a highly compressed, indexed repository, InTrust becomes the big data analysis tool at the heart of continuous compliance. Administrators, security officers and compliance officers can use InTrust to see the 5 W's in their event log data without being event log experts.
IT teams configure automated, real-time gathering of event logs from one console. Figure 2 shows collection from Windows domain controllers, servers, workstations and syslog devices.

InTrust works across platforms, silos and formats to correlate event data from multiple sources:

- Microsoft Windows
- Sun Solaris
- Red Hat Enterprise Linux
- Oracle Linux
- SUSE Linux
- IBM AIX
- HP-UX
- VMware — vCenter, ESX and ESXi

Agents are available for those platforms, and InTrust can collect event log data from other platforms without agent support, including in-house applications and custom-formatted event logs. Across all types of event logs, InTrust normalizes IT data into the 5 W's: Who, What, When, Where and Workstation, as shown in Figure 2. By representing billions of events from diverse systems by those five parameters, InTrust allows non-experts to make sense of the data.

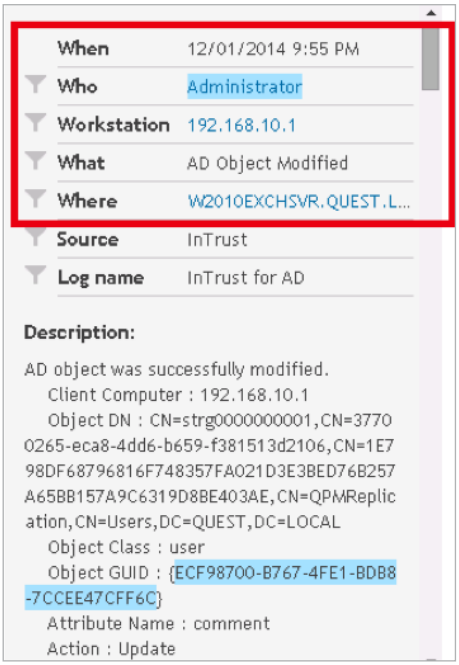

Figure 3: The 5 W's

Administrators, security officers and compliance officers can use InTrust to see the 5 W's in their event log data without being event log experts.

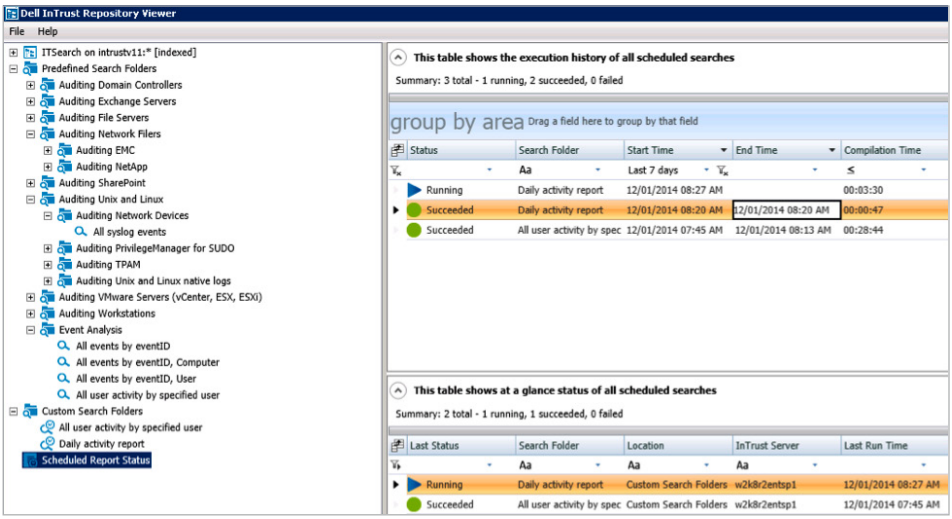

Figure 4: Status of scheduled reports

Addressing all three avenues

InTrust lets administrators, security officers and compliance officers pursue all three avenues needed for continuous compliance.

1. Log management

InTrust manages event logs in real time by compressing them at up to a 20:1 ratio and archiving them for up to seven years in a flat-file repository. It indexes the data for fast searching and reporting, then allows users to create ad hoc and regularly scheduled reports, as shown in Figure 4. Users can choose from a variety of report formats (.pdf, .csv, .xml, etc.), with automated distribution.

The left side of Figure 4 also illustrates the wide range of network resources whose IT data InTrust can collect and whose particular audit needs InTrust addresses.

Because logs often serve as proof of compliance and legal evidence, InTrust offers tamper-proof log collection by creating a protected copy of the event log on each source system, in case the original is deleted. InTrust collects events in real time, so the data is available for searches and reports almost immediately. Additionally, the repository itself can

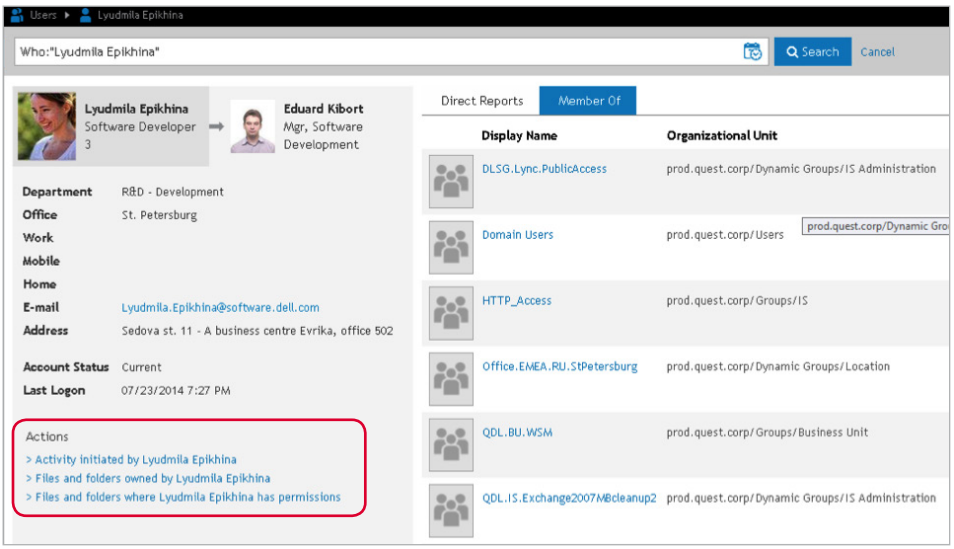

Figure 5: Relationships (in red) among events and state-based data

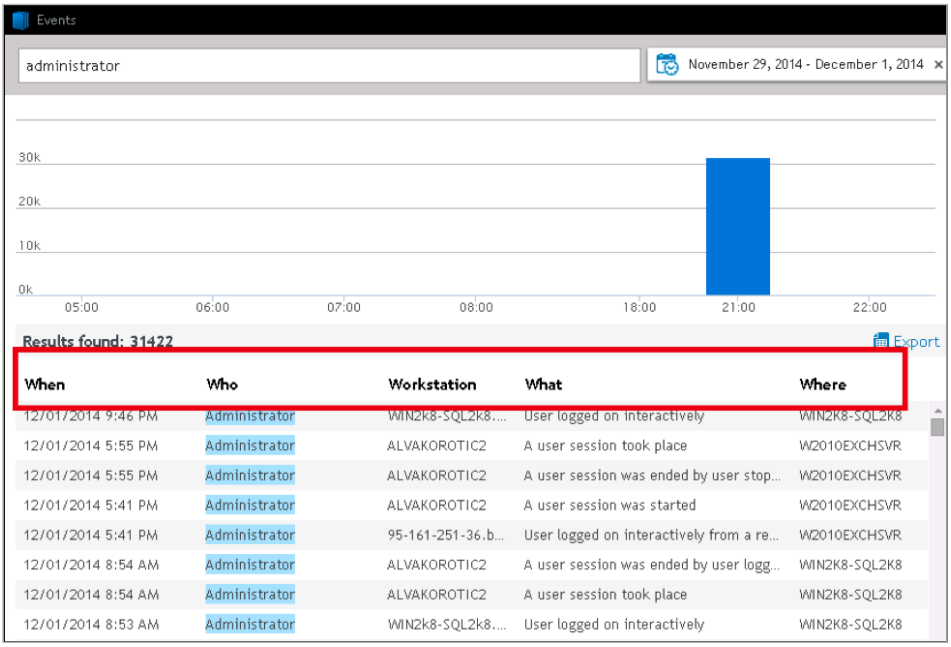

Figure 6: InTrust IT Search - Events

be protected from unauthorized modification either on the storage hardware or with Dell ChangeAuditor.

2. Security and compliance

IT Search, a new feature in InTrust 11.0, goes beyond event log management to the big data tools and Web interface needed to make sense of IT data — changes, file permissions, user entitlements — with on-the-fly investigation. IT Search can analyze multiple data streams from a single, easy-to-use interface and exploit relationships among events and state-based data (see Actions in Figure 5) using its full-text search and correlation engine.

InTrust lets organizations quickly obtain the answers to the questions auditors pose most often:

- Who has access?
- To what do they have access?
- How was access granted?
- How was the access used?

When security and compliance officers can easily list the 5 W's as shown in Figure 6, they switch from reactive to ready mode and can more effectively examine security incidents, investigate potentially fraudulent activities of insiders and set up alerts for unauthorized user activity.

For security and compliance, InTrust provides preconfigured reports required by regulations including SOX, PCI DSS and HIPAA. The reports include IT data that shows, for example, what type of activity is performed by privileged accounts like domain administrators and local server administrators.

InTrust also accommodates ad hoc reporting by saving or converting search results that officers can use to document an investigation.

InTrust provides preconfigured reports required by regulations including SOX, PCI DSS and HIPAA.

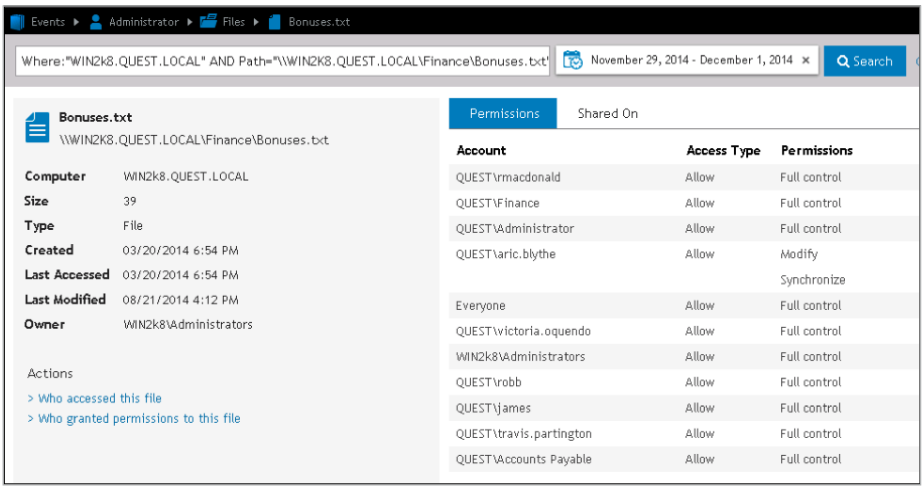

Figure 7: InTrust - File permissions

IT data analytics

InTrust aggregates and correlates multiple streams of IT data:

- Event-based data from native security logs of computers and network devices for security and compliance reporting
- Granular user activity data not found in native event logs due to their limitations
- State-based or configuration data, such as group membership and permissions on files and folders (see Figure 7), to offer granular, real-time insight

It aggregates that data from millions of files and billions of events to make it easier to spot event trends and determine who is behind them. Then it correlates all three streams of data, giving additional context for every access that occurs in the environment.

For example, every time users access a file or folder on the network, InTrust shows this access in the context of current permissions configured on those same files and folders. Administrators can review particular events and decide whether they should be investigated now and prevented in the future.

Most important, IT Search serves as the analytics tool for finding and breaking out IT data quickly, then capturing the results. In access auditing, for example, questions often arise about the number of users with permission to access a given resource. Who is the manager for those users? Who gave file access to the particular users? What did the user do with the access (as shown in the What column in Figure 8)?

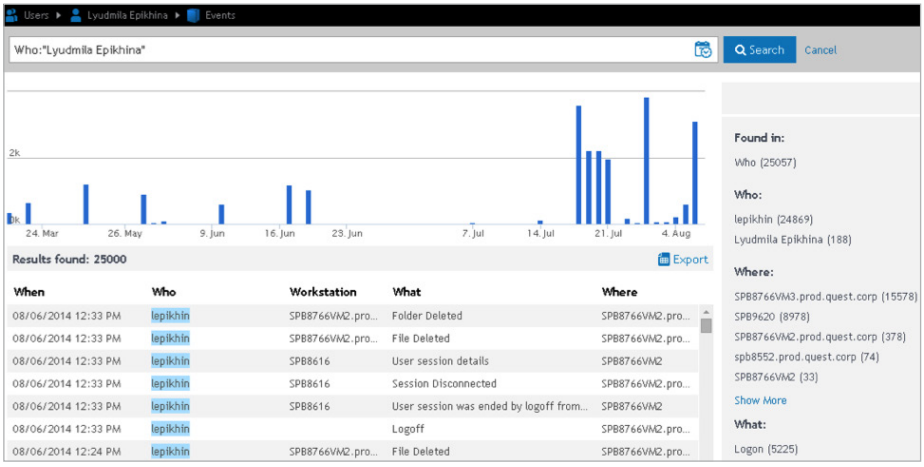

Figure 8: Resources accessed by a given user

Those seem like simple questions, but a great deal of investigation and data may go into answering each of them. By aggregating and correlating multiple streams of data, InTrust can present a simple answer and give security and compliance officers a way to drill in to the details behind it.

Integration with SIEM tools

Providing the context to make sense of huge amounts of IT data is not a feature of most security information event management (SIEM) tools. InTrust complements and integrates with SIEM tools (for example, HP ArcSight, TIBCO LogLogic and Novell Sentinel).

As InTrust collects event log data, it can stream it to SIEM appliances in the syslog format for real-time correlation and security monitoring. Also, InTrust consumes data from Dell Change Auditor and Dell Enterprise Reporter for more-granular auditing data and analysis of user activity. The combination of high-quality data and tools to quickly search within that data can speed up investigations in ways that SIEM tools alone cannot do.

In general, InTrust provides superior auditing, log archiving and reporting for Windows platforms, while SIEM tools discover and respond to a wider set of security threats including logon policy violations and unauthorized attempts to access/modify files and folders.

Conclusion

IT data in the form of event logs, changes, file permissions and user entitlements takes on big-data proportions in organizations that rely on it for security and compliance. In spite of how strong the connections among systems, devices and applications may be, silos invariably develop, making it difficult to collect and analyze IT data.

InTrust makes sense of the IT data residing on numerous systems and platforms in real time with on-the-fly investigations. It provides an interactive search and store engine, IT Search, that goes beyond log management tools to cover security, compliance and IT data analytics.

With InTrust, administrators, security officers and compliance officers have the inside track on continuous compliance. They can quickly produce answers to common audit questions and investigate fraudulent activity by insiders.

With InTrust, administrators, security officers and compliance officers have the inside track on continuous compliance.

For More Information

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. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.