



# Fact Sheet

## Dell InTrust 10.7 Reduces Complexity of Event Log Management

### What is Dell InTrust?

Dell InTrust helps organizations address regulatory compliance and internal security risks through the secure, real-time collection and compression of event logs. Using InTrust, administrators can reduce the complexity of event log management across a heterogeneous network, reduce storage administration costs and improve the efficiency of security, and operational and compliance reporting. Specifically, Dell InTrust 10.7:

- Monitors user access to critical systems and applications, and enables forensic analysis of user and system activity based on historical event data
- Collects events on user and administrator activity from diverse and widely dispersed systems and applications, and presents them in an easy-to-use and complete form suitable for ongoing reporting and ad-hoc analysis
- Provides unparalleled long-term data compression to meet compliance requirements versus storing the same amount of data in a database, providing storage savings
- Creates 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
- Conducts an interactive search 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

### Key new Features Make InTrust an Integral Part of the Connected Security Ecosystem:

- **Rich data feed for SIEM (SecureWorks Integration):** Enriches SIEM with intelligent data feeds that capture crucial aspects of user activity on Windows systems, which can detect internal threats in less time and with less overhead
- **Privileged Accounts Audit (TPAM/SUDO Integration):** Audits the use of shared and super user accounts to meet compliance-driven requirements and implement accountability of the shared accounts usage. This minimizes security risk by knowing what was done during privileged or sensitive access
- **Event Archive That Lasts:** Compresses and indexes event logs as they are collected in real time, and enables fast searching through the event archive no matter how old the data is. This saves on storage costs by leveraging better event compression in the online searchable event archive, and meets both internal security and external compliance requirements

## Why It Matters

It is difficult to know what security events are occurring in your network, and audit log data may not be complete, accurate and tamper-proof. InTrust gives users the capabilities to successfully manage the following potential situations that could have a significant impact on your business:

- Immediate decisions without visibility and intelligence may compromise your organization's systems and policies
- Security policies and procedures that are not followed result in under-performance of your network and employees
- External regulations require long-term retention of all records, resulting in significant storage costs
- You're not sure how much data there is and don't know where or how you will store it. Storage is expensive
- Rogue administrators or users can access logs and tamper with them, which erodes their integrity for use in forensic investigations
- Lost log files due to a crash might destroy evidence of inappropriate behavior
- Manual methods for detecting suspicious activity are cumbersome and prone to failure
- Reporting flexibility is important to meet disparate user needs. How do you get information to the people who need it?
- Inability to take action on security violations as they happen

## Quotes

### **Tim Sedlack, senior product manager, Dell Software**

"From Windows, to Unix and Linux, InTrust allows you eliminate the silos of gathering, analyzing and reporting on suspicious event data from disparate IT environments. From the time users log on until the time they log off, Dell InTrust provides a complete and connected view of the security events happening in your environment. Having all of this tamper-proof information easily at your fingertips helps users address internal security policies and achieves regulatory compliance."

## Pricing & Availability

InTrust 10.7 is immediately available with pricing starting at \$15 per enabled user account or \$995 per managed server.

## Connected Security

Dell Connected Security gives organizations the power to solve their biggest security and compliance challenges today, while helping them better prepare for tomorrow. From the device to the data center to the cloud, Dell helps mitigate risks to enable the business. To learn more about Dell's Connected Security vision, visit [Direct2Dell](#) and read the blogs by Patrick Sweeney, executive director, product management, and Tom Kendra, vice president and general manager, Dell Software.

## About InTrust

Dell InTrust helps organizations address regulatory compliance and internal security risks through the secure, real-time collection and compression of event logs. InTrust helps administrators reduce the complexity of event log management across a heterogeneous network, reduce storage administration costs and improve the efficiency of security, and operational and compliance reporting.

# # #