



# InTrust® for Databases

## Build Confidence in the Security of Your Database

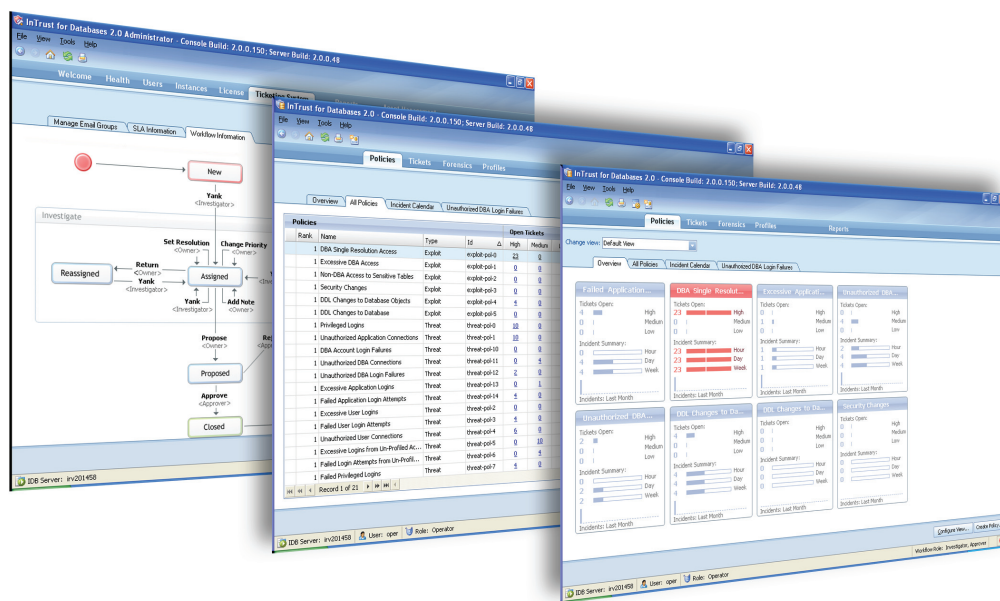
Organizations must comply with external regulations that place the burden of database security and auditing on IT management. Once controls are implemented, IT is responsible for ensuring continuous compliance, and managing data threats, security and auditing in a scalable manner.

Compliance requirements are extremely expensive and complex to implement, especially with increasingly high volumes of data. Database administrators (DBAs) need to secure their data from intrusion, theft and fraud. Although the auditing capabilities of the native relational database management system (RDBMS) may be enabled, they can be intrusive as well as difficult to manage and scale. Furthermore, additional tools are needed to add value to the volumes of audit data that are generated.

## Compliance and Security for the Database

InTrust® for Databases is a multi-featured, database auditing solution that secures corporate database assets. It automates corporate data policies in real time by detecting intrusions, theft and anomalies. In addition, it provides forensic analysis, ticketing workflow, incident alerting and reports to help you resolve these issues. You can remain confident that:

- your corporate database systems are under constant watch
- data is secured to accepted standards
- you are ready to pass your next audit



The InTrust for Databases policy overview interface provides a single view of the audit policy status across all databases.

### Core Differentiators:

- Streamlines processes and reduces costs associated with implementing database audit controls
- Informs security and database personnel of any security violations by interpreting high volumes of audit data in real time
- Tracks any audit policy violations, and provides forensics and workflow methodology in line with auditor requirements
- Scales to the continuously growing database environment
- Enforces audit policy management across database platforms

## System Requirements:

### SQL Server Agent:

- Operating System – one of:
  - Windows 2000, 2003
- SQL Server:
  - 2000, 2005 – 32-bit versions only

### Server:

- Operating System – one of:
  - Solaris 9 or 10: 32 & 64 bit
  - HP-UX 11 or 11i: 32 & 64 bit
  - Linux RH ES: 3.0 or 4.0: 32 bit
  - AIX 5: 64 bit
  - Windows 32-bit
- Oracle Database:
  - V8.17, 9.2, 10.1, 10.2

### InTrust Management Server:

- Operating System – one of:
  - Linux RedHat ES 3.0 or 4.0
  - Linux Suse LE 9 or 10
  - Windows 2000 Server SP4 or
  - Windows 2003 Server SP1 or
  - Windows XP SP2

### Console:

- Windows 2000, 2003, XP
- .NET Framework version 2.0
- 70 MB free disk space
- 512 MB RAM or more

## InTrust for Databases:

- Delivers real-time, detailed notification of critical events such as intrusion detection, data theft and fraud
- Tracks any audit policy violations
- Provides forensics and workflow methodology in line with auditor requirements
- Creates artifacts of the investigation and resolution process for any incidents or policy violations on the database
- Documents and catalogues data assets including databases, tables and users
- Features flexible reporting options for database compliance for faster decision-making on data protection
- Retains of audit trails for both short-term and long-term compliance requirements

### Data Theft and Privacy

When policy violations such as intrusions and excessive data reads occur, InTrust for Databases ensures that all stake holders, management, security and database staff are alerted. The incident ticketing workflow and historical reporting tools guarantee that exceptions are processed appropriately.

### Data Fraud and Integrity

InTrust for Databases allows you to identify and track who is manipulating sensitive data tables or making changes to data structures. Armed with this information, you can intervene or protect your data.

### Incident Analysis

InTrust for Databases provides and preserves the connection between an incident ticket and raw audit data. It quickly displays the relationship between an incident and session by clearly exposing the cause of the incident.

### Complete Audit

By using InTrust for Databases, you can capture information on all remote and local DBA operations -- including privileged sessions -- right down to the object level. You also can perform a forensic investigation on these activities.

### Compliance Strategy

InTrust for Databases is a part of the larger Quest compliance strategy. This includes a total solution for the compliance requirements, both internal and external, for database, applications and Windows management. It covers requirements such as Sarbanes-Oxley, HIPAA, FISMA (SP800-53), CPI and other regulatory compliance standards.

### About Quest Software, Inc.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 50,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at [www.quest.com](http://www.quest.com).

© 2007 Quest Software Incorporated. ALL RIGHTS RESERVED. Quest Software and InTrust are trademarks and registered trademarks of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.



[www.quest.com](http://www.quest.com)  
e-mail: [info@quest.com](mailto:info@quest.com)  
Please refer to our Web site for international office information.