



# InTrust®

“InTrust 既可用于 IT 政策执行情况的管理，也可用于监控或实现实时的关键业务安全事件报警。”

— Colin Harrison  
首席项目经理  
Experian

- 通过自动收集和压缩事件数据，降低成本
- 压缩和储存重要事件数据用于审计，以实现法规遵从
- 通过代理端缓存确保审计日志不会被篡改，保护审计日志数据不被修改或丢失。
- 通过识别违规用户账户，改善内部安全，并实时预警。
- 提供实时详细的 Exchange 信箱内部活动预警和跟踪
- 接受实时报警，响应与 AD 和 GPO 变更相关的重要事件：通过立即锁定违规用户或取消不当操作对敏感安全事件进行及时响应。

## 安全企业的审计及法规遵从

当今企业必须时刻注意遵守内外部法律法规和内部安全策略，安全制度建立后，还要不断对其进行测试和改进。Quest InTrust 可帮助系统管理员以安全方式，对异构环境下的事件日志进行收集、储存和分析，生成与安全管理和法规遵从有关的管理报告。

InTrust 提供的法规遵从报告，包括应用、系统和用户活动跟踪信息，支持跨平台安全数据采集和企业级扩展性，是企业法规遵从工作的关键。

### 安全采集事件日志

InTrust 通过消除用户错误和降低日志数据丢失的可能，确保数据的一致性和日志文件的安全。另外，通过在传输前对事件日志进行加密和压缩，InTrust 的提供了额外的安全保护功能。

### 在线存储更多数据

InTrust 提供了最快捷、最具性价比的日志信息访问方式。其基于元数据库的解决方案，非常适合长期存储海量数据，实现高效的审计和法规遵从状况审计。与 IT 系统自身的日志文件和其它将日志存储于数据库中的管理方案不同，InTrust 实现了最高的数据压缩率。

### 智能报表

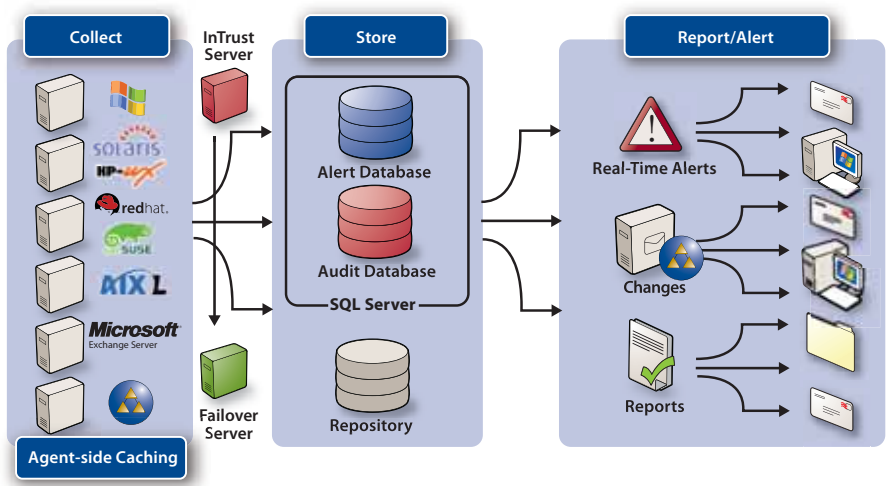
利用 InTrust，可以生成和发布企业内部或外部审计所需的相关信息。内置报表和可定制的报表生成功能，能够通过多种灵活的输出格式满足用户对管理信息的需求。

### 改善系统安全和性能

InTrust 通过实时报警，报告系统中异常的用户和管理员活动（如，试图在下班后访问文件，或经过多次失败尝试后成功登录等关键的安全事件），改善系统安全。同时，InTrust 可以对系统本身的异常活动进行报警，保证服务器或工作站未受黑客的操纵。报警信息可以直接通过电子邮件发送给管理人员，或提交给第三方监控工具。

### 确保 Exchange 系统安全

InTrust Exchange 插件提供实时、深入的用户活动和非授权访问追踪，以及针对 Exchange 信箱和服务器授权的变更及配置审计。



## 系统要求

### 操作系统

- Microsoft Windows 2000 SP3 或更新版本
- Microsoft Windows XP SP1
- Microsoft Windows Server 2003
- Sun Solaris 8.0 (标准安装), 外加 patch 112439-01
- Sun Solaris 9.0 (标准安装)
- Red Hat Enterprise Linux AS 3.x
- Red Hat Enterprise Linux ES 3.x
- SUSE Linux Enterprise Server 9

### 平台

- Intel x86
- SUN SPARC
- 32 及 64bit

### 内存

- 建议 512 MB 或更多

### 硬盘空间

- 至少 400 MB



北京东城区东长安街1号东方广场C1办公楼501室  
邮编: 100738

电话: (86)-10-85185651

传真: (86)-10-85151322

上海静安区北京西路1701号静安中华大厦2210室

邮编: 200040

电话: (86)-21-62884984/4994

传真: (86)-21-62884974

广州天河区天河北路183号大都会广场1013室

邮编: 510620

电话: (86)-20-87554820/6920

传真: (86)-20-87554860

e-mail: info.china@quest.com

www.quest.com/china

## 针对 Active Directory 的全面活动追踪和变更审计:

InTrust 可提供针对所有域控制器的审计、报表功能, 为 AD 和 Group Policy 的变更提供详细的跟踪报告。

### 主要特色:

**支持法规遵从:** 通过监控关键系统访问和发现与访问相关的可疑日志项目, InTrust 可以满足企业的法规遵从需求。利用该产品, 可以采集、分析和报告异构系统中任何访问相关的事件, 实现实时事件报警功能。

**全面自动化:** 利用 SecureCollect 技术, InTrust 可以实现事件日志的自动采集。这种功能既可降低管理工作量, 还能将采集工作安排到系统较为空闲的时段, 降低网络流量和IT资源竞争。

**用户活动跟踪:** 通过 UserTrack 技术, InTrust 可以收集异常用户及系统管理员活动的相关信息, 并通过关联处理, 自动向管理人员发出报警信息。

**日志完整性:** InTrust 可为远程服务器创建日志文件的缓冲存储, 以便对日志文件进行及时备份。消除了人为原因导致审计日志丢失的可能。

**冗余设计:** InTrust 为系统故障提供了自动化的冗余机制。InTrust 服务器接管可帮助企业通过快速、自动化的方式, 将事件日志管理的相关配置和作业, 从故障服务器迁移到新的后备服务器, 实现接管功能。这种配置消除了服务器故障导致日志文件丢失的可能。

**数据压缩和元数据库存储:** InTrust 提供了独特的 StoreMore 两层存储架构, 利用元数据库, 实现高压缩比、大数据量的长期事件日志存储, 比基于数据库的日志存储方案更加出色。

**异常分析:** InTrust 简化了网络趋势分析和安全事件管理, 方便对网络用户登录 / 注销等活动进行模式分析和对比, 简化了异常分析。

**实时报警:** InTrust 的 NotifyNow 技术确保用户能够实时获取 UserTrack 报警信息。报警信息可以直接通过电子邮件发送给管理人员, 或提交给第三方监控工具, 如 Microsoft Operations Manager (MOM)。

**灵活的报表:** InTrust FlexReport 技术使用户可以方便访问预定义报表和用户自定义报表。

InTrust 支持多种文件格式, 包括 HTML、XML、PDF、CSV、TXT, 以及微软的 Word、Visio 和 Excel。

**快速安装和部署:** InTrust 中的 QuickStart 向导可帮助用户快速安装、部署和配置该产品, 或对其配置功能进行优化。其配置向导可帮助用户全面部署日志管理解决方案, 包括站点创建、策略应用, 以及任务和实时报警规则的定义。

### 关于 Quest Software, Inc.

Quest Software, Inc. 提供的创新的产品能够帮助企业提高其应用程序、数据库和 Windows 架构的性能和工作效率。通过深入的 IT 运营技能和对最佳 IT 实践的持续关注, Quest Software 帮助全球 50,000 多个客户满足他们对企业 IT 的更高期望。Quest Software 在世界各地设有办事处或分支机构; 其公司网址为: [www.quest.com/china](http://www.quest.com/china)

©2007 Quest Software, Inc. 版权所有。Quest 和 Spotlight on Exchange 为 Quest Software 注册商标。其它商标或产品名称为相关公司所有。

DSW-InTrust-US-VC