# InTrust®

智能且可扩展的事件日志管理工具

您的企业的宝贵资产是数据和对其有访问权限的用户。对于IT和安全部门来说，跟踪用户和特权帐户活动（尤其是在工作站或最终用户设备上）是保护其环境安全和遵守各种行业法规的核心。但是，这是一项非常困难的任务，因为大量数据散布在分散的系统、设备和应用程序中。收集、存储和分析这些数据通常需要大量存储、耗时地收集事件数据和关于所收集的事件数据的内部专业知识。

借助Quest® InTrust®，您可监控所有用户工作站和管理员活动，从登录到注销以及其间发生的一切都包括在内。通过20:1的数据压缩削减存储成本，并存储来自Windows、UNIX/Linux服务器、数据库、应用程序和网络设备的长达数年之久的事件日志。InTrust实时警报功能通过自动响应可疑活动，使您可以即时应对威胁。

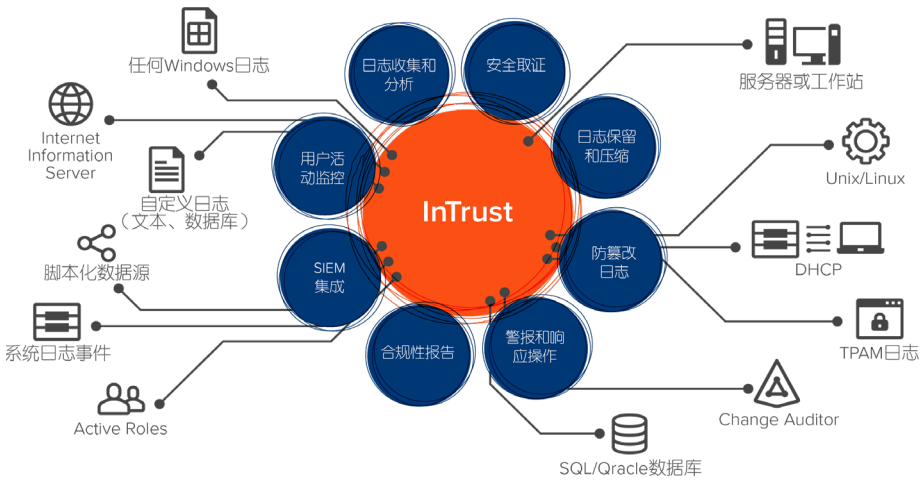
## 功能

### 单一管理平台

通过一个可搜索的位置收集并存储来自各种系统、设备和应用程序的所有原生或第三方工作站日志，而且提供即时可用性，从而实现安全性与合规性报告。InTrust提供Windows事件日志、UNIX/Linux、IIS和Web应用程序日志、PowerShell审核跟踪、终端保护系统、代理和防火墙、虚拟化平台、网络设备、自定义文本日志以及Quest Change Auditor事件的统一视图。

### 用户工作站日志监控

通过监控用户和管理员活动，从登录到注销以及其间发生的一切都包括在内，从而保护您的工作站以抵御现代网络攻击，例如哈希传递、网络钓鱼或勒索软件。收集并存储有关用户访问的所有重要详细信




*高效监控所有用户工作站和管理员活动，从而保护您的宝贵资产，即数据。*

> “我们使用InTrust从域控制器进行日志收集，并监控事件以进行SOX合规性审核。我非常喜欢存储库查看器，它非常适合研究帐户锁定和其他登录事件来确保安全性。”
>
> *S&P 500专业服务公司的工程师*
>
> TVID：726-084-5E5

## 优势：

- 通过高度压缩和建立了索引的日志存储库，降低存储成本并确保持续合规性
- 从单个位置轻松搜索所有最终用户和特权帐户活动
- 快速报告安全事件并进行故障排除和调查
- 通过标准化的本机事件日志了解数据
- 与您的现有SIEM解决方案轻松集成在一起
- 通过实时警报和自动化响应即时应对威胁
- 通过对创建的事件进行复制，避免事件日志数据被篡改或销毁

“我相信该产品提供非常宝贵的安全报告和警报功能。尽管其他产品也提供类似的功能，但是我认为InTrust的定位是实现快速实施，可在审核与合规性领域即时带来价值。”

*财富500强汽车和运输公司的高级IT经理*

TVID：D2B-CDB-505

**系统要求**

| 支持的平台 |
| --- |
| Microsoft Windows事件 |
| Microsoft IIS事件 |
| Microsoft Forefront Threat Management Gateway和ISA Server事件 |
| Microsoft DHCP Server事件 |
| Solaris事件 |
| Red Hat Enterprise Linux事件 |
| Oracle Linux事件 |
| SUSE Linux事件 |
| Debian GNU/Linux事件 |
| Ubuntu Linux事件 |
| IBM AIX事件 |
| HP-UX事件 |
| VMware vCenter事件 |
| VMware ESX和ESXi事件 |

有关详细信息，请参阅系统要求文档。

息，如谁执行了操作、该操作涉及什么、执行于哪一台服务器以及源于哪一台工作站。

### 简化的事件日志分析

将来自分散源的加密事件日志整合成一种简单的标准化格式，其中包含相关用户、内容、时间、位置、源和对象，以帮助您了解数据。尤其是，不同应用程序的系统日志数据截然不同。利用InTrust®，您可以检测系统日志事件中的结构化数据，并正确解析这些数据。独特的全文索引功能使长期事件数据易于进行搜索，从而实现快速的报告、故障排除和安全调查。

### 智能且可扩展的事件日志压缩

收集大量数据并存储在高度压缩的存储库中（在建立索引的情况下实现20:1的压缩率，在不建立索引的情况下实现40:1的压缩率），从而使您可以节省多达60 %的存储成本，并确保持续符合HIPAA、SOX、PCI、FISMA等要求。此外，一台InTrust服务器每秒可以处理多达60,000个事件且支持10,000个代理程序同时写入事件日志，使您实现更高的效率、更大的可扩展性和巨大的硬件成本节省。如果您需要更多容量，只需添加其他InTrust服务器并划分工作负载 - 可扩展性几乎是无限的。

### 实时警报和响应操作

监视未授权或可疑的用户活动，例如超出阈值限制的文件创建、使用已知勒索软件攻击的文件扩展名或使用可疑PowerShell命令。通过实时警报即时响应威胁。InTrust使您可以轻松触发对可疑事件的自动化响应，例如阻止活动、禁用违规用户、撤消更改和/或启用紧急审核。

### 防篡改日志

通过在可对创建的日志进行重复数据删除的每台远程服务器上创建缓存位置，保护事件日志数据，以防止篡改或销毁。

### SIEM集成

通过适用于Splunk和IBM QRadar的InTrust连接器，大大降低您的年度SIEM许可费用。通过InTrust长期存储事件日志数据，以及根据行业妥善做法过滤数据并仅将相关数据转发到SIEM解决方案进行实时安全性分析。

### 通过IT Security Search提高洞察力

在一个位置便可利用所有Quest®安全与合规性解决方案提供的宝贵洞察力。借助IT Security Search，您可以在一个类似于Google的IT搜索引擎中关联来自InTrust、Change Auditor、Enterprise Reporter、Recovery Manager for AD以及Active Roles的数据，实现更快的安全事件响应和取证分析。通过丰富的可视化和事件时间表轻松分析用户授权和活动、事件趋势、可疑模式等。

### 自动化妥善做法报告

轻松将调查结果转换为多种报告格式，包括HTML、XML、PDF、CSV和TXT以及Microsoft Word、Visio和Excel。借助内置的事件日志专业技术，安排报告的生成时间并自动将其分发给各团队，或从内容丰富的预定义妥善做法报告库中进行选择。通过数据导入和整合工作流，您甚至可以将数据的子集自动转发到SQL Server以进行进一步的高级分析。

## 关于QUEST

Quest致力于为瞬息万变的企业IT领域提供软件解决方案。我们帮助简化数据爆炸、云扩展、混合数据中心、安全威胁以及法规要求所带来的挑战。我们的产品组合包括用于数据库管理、数据保护、统一端点管理、身份和访问管理以及Microsoft平台管理的解决方案。

Quest
quest.com/cn
有关当地办事处信息，请访问 (quest.com/cn-zh/locations)


DataSheet-InTrust-US-KS-zh_CN-WL-39601