零售连锁店确保PCI DSS合规性

大型零售商通过使用Quest®解决方案，顺利通过其年度PCI DSS审核，并维护企业范围的强大安全性。

“为实现PCI DSS合规性，我们需要打开所有本地日志记录并为审核员提供过去一年的完整日志…倘若没有InTrust，我们的空间恐怕早已耗尽。”

大型零售连锁店企业管理员

客户概况

行业	零售
国家/地区	美国

业务需求

为通过年度PCI DSS审核和确保安全性，一家大型零售连锁店需要企业级日志管理和经济高效的长期数据存储，以及高级Active Directory监控和变更审核。

解决方案

依托Quest® InTrust®，该公司现在可以从其受监管的零售IT环境中的4,000个POS终端及其他系统收集数据，并将所有数据以高度压缩的格式存储数年，同时仍支持轻松、安全的访问以进行合规性审核和安全调查。与此同时，Quest的Change Auditor和Active Roles借助诸如安全授予管理职责和对象保护等功能，为公司的业务IT环境提供全面的安全性。

优点

- 能够有效收集和经济高效地存储PCI DSS审核所需的所有数据
- 能够强有力地控制Active Directory，从而提高安全性
- 确保一致性并且能够安全地委派管理任务，从而节省时间
- 阻止更改管理员帐户和其他关键AD对象，从而阻止攻击

解决方案一览

- Microsoft平台管理

现代零售组织需要遵守支付卡行业数据安全标准(PCI DSS)，并在年度审核期间证明此合规性。审核失败可能导致完全被禁止接受信用卡支付 — 这会危及整个业务。有一项PCI DSS要求可能特别难以满足：为前一年生成完整的IT审核跟踪记录。然而，通过使用Quest Software提供的解决方案，一家大型零售连锁店可以从其整个零售IT环境收集所有需要的日志数据，并根据要求经济高效地存储这些数据，同时在其业务IT环境中维护强大的安全性。

> “我们在Active Roles中设置的策略让我们的Active Directory保持条理分明，并确保所有操作完成方式一致，从而简化了管理员和我的工作。”
>
> *大型零售连锁店*
> *企业管理员*

PCI DSS合规性对于任何现代零售业务都至关重要

零售商需要收集其整个受监管的IT环境中的日志数据，以维护PCI DSS合规性。但是，现代IT生态系统非常繁忙，有很多不同的系统用于收集大量关键日志数据。一家大型零售连锁店的IT团队认识到，脚本和其他手动方法根本不是可行的审核通过方法。相反，他们需要一个企业级解决方案，该解决方案要能够从各种系统（包括数十个远程位置的约4,000个销售点[POS]终端）收集所有所需的数据，并根据PCI DSS要求经济高效地将所有这些数据至少存储一年。

除了受监管的POS环境外，IT团队还负责用于处理常规业务操作的系统，这些系统对于每个现代组织必不可少，例如Exchange和HR系统。随着威胁局势的快速发展，他们迫切希望能够更好地保护其Active Directory免受外部攻击、恶意内部攻击以及管理员造成的错误或不当行为的影响。为实现这种严格的安全性，他们需要通过某种方式来保持其AD的有序性并密切监控对AD对象（包括用户和组）的所有更改。

出自ACTIVE DIRECTORY专家之手的出色解决方案

在对市场上各项方案进行仔细评估之后，该零售商选择了Quest的四个解决方案。InTrust®是一款可扩展的智能事件日志管理工具，可用于监控Windows、UNIX/Linux、数据库、应用程序、网络设备及其他设备中的所有用户工作站和管理员活动。此外，其20:1的数据压缩让您可以经济高效地存储这些事件日志达数年之久。InTrust甚至可以提供实时警报和自动化操作，以确保即时响应可疑活动。

Active Roles可精简用户和组管理，从而大幅提升安全性。您可以通过自动、一致且全面的方式，从单一管理平台轻松管理您内部部署或混合AD环境中的所有系统。

产品及服务

软件
Active Roles
Change Auditor for Active Directory
Change Auditor for Windows File Servers
InTrust

Change Auditor for Active Directory和Change Auditor for Windows File Servers可用于跟踪、审核、报告所有重要配置更改并发出警报 — 甚至可以在第一时间主动保护关键对象（例如管理帐户和组）免遭更改。

借助INTRUST确保并证明PCI DSS合规性

该公司快速设置了InTrust，以从其受监管的零售IT环境中的多个系统收集数据。“我们每一个POS终端均有InTrust，”企业管理员表示，“我们还使用InTrust从SQL服务器、终端服务器、FTP和IIS收集日志。我还从一台服务器提取自定义文本日志，并且我们还收集一些系统日志。”

所有这些数据都经过高度压缩并存储在中央InTrust存储库中，并且可经济高效地存储满足合规性和安全需求所要求的时长。“对于PCI DSS合规性，我们需要打开所有本地日志记录并为审核员提供过去一年的完整日志，”管理员解释道，“因为我们有这么多的终端和这么多的活动，数据量如此之大 — 任何时候都有约800 GB的日志。倘若没有InTrust，我们的空间恐怕早已耗尽。这会对企业造成灾难性影响：如果我们无法满足PCI要求，那么从长远来看，我们将无法使用信用卡。”

可喜的是，得益于InTrust提供的高级压缩功能，公司不再需要担心无法提供审核员所需的数据。“InTrust具有非常高的压缩率，”企业管理员报告说，“它实实在在为我们节省了大量空间，让我们能够存储为确保PCI DSS合规性所需的所有日志数据。实际上，倘若没有InTrust，我根本不知道可以收集所有数据，更别说存储这些数据，因为传输这么多未压缩数据需要大量带宽。”

轻松搜索、预构建报告和高级警报

此外，InTrust确保IT团队能够快速访问其所需的特定数据，以执行安全调查、快速回答审核员的问题以及维护安全性。“利用InTrust存储库中的高级索引，搜索非常快速且简单，”管理员表示，“随附报告几乎涵盖我所需的一切数据；我不用寻找任何未配置的内容。”

主动警报对于确保安全性和合规性同样必不可少，公司对于InTrust中的实时警报功能感到非常满意。“我在InTrust中为Active Directory中完成的几乎一切操作都设置了警报，无论是创建新用户还是加入机器，”管理员提到，“这对于通过审核至关重要。例如，如果一个技术人员更换了一个终端，则需要重新加入，并且我们会收到该操作的相关警报。审核员需要查看该警报以证明我们是根据相应帮助台票证的要求更换了终端。通过InTrust警报，我可以获取所需的一切信息，包括审核员需要的所有信息。”

借助ACTIVE ROLES和CHANGE AUDITOR保持AD的有序性和安全性

在用于办公和仓库业务操作（如Exchange消息传送）的IT环境中，公司依赖Active Roles维护严格的安全性。“我们使用Active Roles已有五六年，”管理员表示，“以前，Active Directory是一团乱麻，管理员如此之多，操作五花八门。现在，只有约十几个管理员可以访问Active Directory，并且Active Roles是他们可以进入Active Directory的唯一途径。我们在Active Roles中设置的策略让我们的Active Directory保持条理分明，并确保所有操作完成方式一致，从而简化了管理员和我的工作。例如，Active Roles现在从一开始就强制管理员在适当的组织部门(OU)创建所有计算机帐户，这样我以后就不必使用PowerShell频繁移动这些帐户。”

> “我们请几位渗透测试专家进来测试，令我们惊讶的是，他们无法穿过Change Auditor对象保护屏障。”
>
> *大型零售连锁店*
> *企业管理员*

“即使我们拥有所有许可证，我也几乎从不寻求支持；一年可能只有一次。但只要我寻求支持，支持团队总是大力相助，帮助我解决问题。”

大型零售连锁店
企业管理员

Active Roles还让首席管理员能够精细地向其他管理员授予权限，这样他即可分散工作负载又不会失去控制权。“Active Roles帮我节省了大量时间，这一点很重要，因为我身兼数职且全天候待命，”他解释道，“以前，我只能向极少数管理员委派任务，因为我不能让帮助台人员更改Active Directory中的内容。而利用Active Roles，我可以委派更多任务，因为我可以控制每个人可执行和不可执行的操作。例如，我们每家商店都有一个主管。如有主管呼叫帮助台，请他们重置密码，帮助台无法执行此操作；只有可验证请求人员身份的区域经理可以更改主管的密码。”

这两个Change Auditor解决方案进一步增强了环境的安全性。“Change Auditor对象保护功能堪称大救星，”Clark表示，“我设置了此保护以防止对我们文件服务器上特定目录中的ACL进行更改，以及保护所有管理帐户。我们请几位渗透测试专家进来测试，令我们惊讶的是，他们无法穿过Change Auditor对象保护屏障。”

顶级支持

企业管理员还主动向Quest支持公开表达致意。“即使我们拥有所有许可证，我也几乎从不寻求支持；一年可能只有一次，”他提到，“但只要我寻求支持，支持团队总是大力相助，帮助我解决问题。Quest社区的支持论坛也很实用 — 有些功能我们以前没有充分利用，在这里我们获得了很好的相关想法和建议。”

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、安全威胁以及合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、统一终端管理、身份和访问管理以及Microsoft平台管理的解决方案。

若需查看更多案例分析，请访问Quest.com/Customer-Stories

CaseStudy-RetailerPCIDSS -US-KS-zh_CN-WL-55478#