Retail Chain Ensures PCI DSS Compliance

Large retailer aces its annual PCI DSS audits and maintains strong security enterprise-wide with Quest and One Identity solutions.

Country: **United States**

Industry: **Retail**

Modern retail organizations need to maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) and prove that compliance during annual audits. A failed audit could lead to being banned from accepting credit card payments altogether — which would jeopardize the entire business. One PCI DSS requirement in particular can be tough to meet: producing a complete IT audit trail for the preceding year. But one large retail chain collects all required log data from across its entire retail IT environment and stores it cost-effectively as mandated, and also maintains strong security in its business IT environment, with solutions from Quest Software and One Identity.

PCI DSS compliance is critical to any modern retail business

Retailers need to maintain PCI DSS compliance by collecting log data across their regulated IT environments. But modern IT ecosystems are busy places, with many different systems collecting huge volumes of critical log data. The IT team at one large retail chain recognized that scripting and other manual methods were simply not a viable approach to passing audits. Instead, they needed

About this case study

To pass annual PCI DSS audits and ensure security, a large retail chain needed enterprise-class log management with cost-effective long-term data storage, as well as advanced Active Directory monitoring and change auditing.

Solution

With Quest® InTrust®, the company can now collect data from its 4,000 POS endpoints and other systems in its regulated retail IT environment and store all the data in a highly compressed format for years while retaining easy, secure access for compliance audits and security investigations. Meanwhile, Quest Change Auditor and One Identity Active Roles provide comprehensive security for the company's business IT environment, thanks to features such as secure delegation of administrative responsibilities and object protection.

Benefits

- Enables efficient collection and cost-effective storage of all data required for PCI DSS audits
- Improves security by enabling strong control over Active Directory
- Saves time by ensuring consistency and enabling secure delegation of administrative tasks
- Blocks attacks by preventing changes to admin accounts

an enterprise-quality solution that could collect all the required data from a wide range of systems, including some 4,000 point-of-sale (POS) endpoints across dozens of remote locations — and store all that data cost effectively for at least a year, as required by PCI DSS.

Beyond the regulated POS environment, the IT team is also responsible for the systems that handle the normal business operations that every modern organization has, such as its Exchange and HR systems. With the threat landscape evolving rapidly, they were eager to better secure their Active Directory (AD) against external attacks, malicious insiders and mistakes or misdeeds by administrators. To deliver that tight security, they needed a way to keep their AD in order and closely monitor all changes to AD objects, including users and groups.

> **The policies we have in Active Roles keep our Active Directory organized and ensure that everything is done consistently, which simplifies things for the admins and for me.**
>
> *Enterprise Administrator*
> *Large Retail Chain*

Best-in-class solutions from the Active Directory expert

After careful evaluation of the options on the market, the retailer selected four Quest solutions. InTrust® is a smart, scalable event log management tool that empowers you to monitor all user workstation and administrator activity across Windows, UNIX/Linux, databases, applications, network devices and more. Moreover, its 20:1 data compression enables you to store those event logs cost-effectively for years. InTrust even delivers real-time alerting with automated actions to ensure immediate response to suspicious activity.

20:1

Data compression enables you to store those event logs cost-effectively for years.

One Identity Active Roles streamlines user and group management to dramatically improve security. You can easily manage all systems across your on-prem or hybrid AD environment from a single pane of glass in an automatic, consistent and comprehensive way. Change Auditor for Active Directory and Change Auditor for Windows File Servers enable you to track, audit, report and alert on all key configuration changes — and even proactively protect critical objects, such as administrative accounts and groups, from being changed in the first place.

Ensuring and proving PCI DSS compliance with InTrust

The company quickly set up InTrust to collect data from multiple systems across its regulated retail IT environment. “Every single one of our POS endpoints has InTrust,” says the enterprise administrator. “And we also use InTrust to collect logs from our SQL servers, terminal servers, FTP and IIS. I also pull custom text logs from one server, and we collect some syslogs as well.”

All of that data is highly compressed and stored in a central InTrust repository, where it can be kept cost-effectively for as long as required for compliance and security needs. “For PCI DSS compliance, we have to have turn on all native logging and provide auditors with complete logs for the past year,” explains the admin. “Because we have so many endpoints and so

much activity, that's a lot of data — we have roughly 800 gigs worth of logs at any time. Without InTrust, we would have run out of space a long time ago. That would have been disastrous for the business: If we couldn't meet PCI requirements, in the long run, we wouldn't be able to take credit cards."

Thanks to the advanced compression offered by InTrust, however, the company no longer needs to worry about not being able to supply the data that auditors require. "InTrust has a really high compression rate," reports the enterprise administrator. "It definitely saves us a lot of space, so we can store all the log data we need for PCI DSS compliance. In fact, I don't know that it would even be possible to collect all the data, let alone store it, without InTrust because of the amount of bandwidth that would be required to transmit so much uncompressed data."

> **"For PCI DSS compliance, we have to have turn on all native logging and provide auditors with complete logs for the past year.... Without InTrust, we would have run out of space a long time ago."**
>
> *Enterprise Administrator*
> *Large Retail Chain*

Easy searches, pre-built reports and advanced alerting

Moreover, InTrust ensures that the IT team can quickly access the specific data they need to conduct security investigations, promptly answer questions from auditors and maintain security. "With the advanced indexing in the InTrust repository, searches are very fast and easy," the admin says. "And the canned reports cover nearly everything I need; I don't go looking for anything that isn't already configured."

Proactive alerts are also essential to both security and compliance, and the company is very pleased with the real-time alerting functionality in InTrust. "I have alerts set up in InTrust for pretty much everything that gets done in Active Directory, whether it's creating a new user or joining a machine," notes the admin. "That's critical for passing audits. For example, if a tech replaces an endpoint, it will get rejoined, and we will get an alert on that action. The auditor will want to see that alert to prove that we replaced the endpoint as required by the corresponding helpdesk ticket. With the InTrust alerts, I get everything that I need, including all the information that the auditor requires."

Keeping AD orderly and secure with Active Roles and Change Auditor

In the IT environment used for office and warehouse business operations such as Exchange messaging, the company relies on Active Roles to maintain tight security. "We have been using Active Roles for five or six years," the admin says. "Before, Active Directory was a mess and everything was done differently by so many different admins. Now, about a dozen admins have access to Active Directory and Active Roles is the only way they can get into it. The policies we have in Active Roles keep our Active Directory organized and ensure that everything is done consistently, which simplifies things for the admins and for me. For instance, Active Roles now forces admins to create all computer accounts in the proper OU right from the get go, so I don't have to use PowerShell to move them around later."

Active Roles also enables the lead administrator to granularly delegate permissions to other admins, so he can spread out the workload without losing control. "Active Roles saves me a lot of time, which is important because I wear many different hats and I'm on call 24/7/365," he explains. "Before, I could delegate tasks to only a very few admins because I couldn't, for instance, have helpdesk staff changing things in Active Directory. Active Roles empowers me

to delegate more tasks because I can control what each person can and cannot do. For instance, we have a director at each store. If one them were to call the helpdesk and ask them to reset a password, the helpdesk could not do it; only the regional managers, who can verify the identity of the person who's make the request, can change a director's password."

The two Change Auditor solutions add even more security to the environment. "Change Auditor object protection is a lifesaver," the administrator says. "I have it set up to prevent changes to the ACLs on certain directories on our file servers, as well as to protect all administrative accounts. We've had pen testers come in and be very surprised that they could not get past the Change Auditor object protection."

> **We've had pen testers come in and be very surprised that they could not get past the Change Auditor object protection.**
>
> *Enterprise Administrator*
> *Large Retail Chain*

World-class support

The enterprise administrator also volunteered a resounding shout-out to Quest Support. "Even with all the licenses we have, I hardly ever call for support; it's maybe once a year," he notes. "But when I do call, the support team is always very helpful and gets me through the issue I'm having. The support forums on the Quest communities are also quite useful — we've gotten good ideas and suggestions about features that weren't really taking full advantage of before."

SOLUTIONS AT A GLANCE

- Microsoft Platform Management
- Active Roles

SYSTEM REQUIREMENTS

Services

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

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.