



Business Problem

Isolate stored credit card data to meet PCI compliance. Segment access to credit card applications and servers to reduce scope of audit.

Benefits of ConSentry

The ConSentry LANShield platforms enabled this company to rapidly deploy access controls to credit card information, without having to make network changes. As a result, the company was able to move from non-compliant to passing its audit in just three weeks.

Credit Card Clearinghouse

Challenges of Achieving PCI Compliance

Facing fines of \$500,000 per day, this large credit card clearinghouse needed to rapidly and cost-effectively meet the Payment Card Industry (PCI) Data Security Standard. This Fortune 500 company was out of compliance with the requirement to protect stored cardholder data; specifically, with requirement 3.4 of the specification, which indicates that a cardholder's primary account number, at a minimum, must be unreadable anywhere it's stored.

Meeting this requirement is a tremendous challenge for all organizations handling credit card information. Ideally, every credit card-related application would encrypt data. The application vendors are moving in that direction, but it's a long-term solution. In the meantime, even organizations in the process of migrating from legacy systems to newer architectures are struggling to comply. Fortunately, credit card issuers are aware of this challenge and have revised the PCI standard to define acceptable compensating controls, which specify how a company can mitigate risk to achieve compliance without having to encrypt stored credit card data.

The compensating controls include segmenting traffic and restricting user access to credit card data. For this Fortune 500 company, the apparent option for implementing these compensating controls was to build out a separate network. Not only was this approach prohibitively expensive, but it also could not be accomplished in time to avoid fines. Fortunately, a qualified data security company (QDSC) was able to show this credit card clearinghouse how ConSentry Networks and its innovative LANShield access control platforms could provide the necessary compensating controls and quickly bring the company into PCI compliance.

Alternatives for Protecting Cardholder Data

According to Appendix B in the 1.1 version of the PCI DSS specification, companies unable to encrypt all stored data have the alternative to deploy

Corporate Office
ConSentry Networks
1690 McCandless Dr
Milpitas CA 95035

866-841-9100
408-956-2100



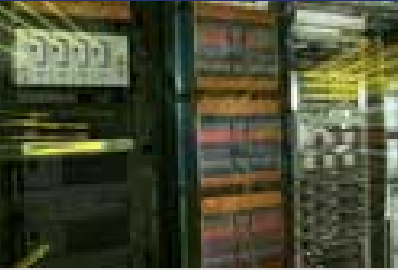
devices, applications, or other controls that meet *all* of the following conditions:

1. Provide additional segmentation/abstraction (for example, at the network layer).
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
 - IP address/MAC address
 - Application/service
 - User accounts/groups
 - Data type (packet filtering)
3. Restrict logical access to the database.
 - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).

Using ConSentry's LANShield Controller, this Fortune 500 clearinghouse has been able to provide all of the required compensating controls in a low-cost, non-disruptive fashion. In only three weeks, the clearinghouse went from evaluating to installing LANShield Controllers in six sites across the United States, becoming fully PCI compliant and avoiding fines.

In particular, the clearinghouse was able to use ConSentry's role-based policies to segment PCI users and resources from the rest of the network, effectively creating a virtual wall around the PCI system. Using ConSentry's InSight policy server and the role-based provisioning capabilities of the LANShield platforms, the clearinghouse created a role called "CI" and assigned it to those users who must handle credit card information as part of their job. Only those users are given access to the servers where credit card data is stored.

A Layer 2-7 aware device, ConSentry's LANShield Controller operates inline between wiring closet switches and core switches/routers, which gives it complete visibility into LAN traffic. Using stateful, deep-packet inspection, the Controller tracks all user activity and all traffic flows on the network, tying users to flows.



This type of detailed visibility into user activity allows IT to define a range of access control policies, including those based on MAC and IP addresses; applications and content at Layer 7 and above; users and roles; network destinations and/or zone; location; and time. Controls can be very granular because the LANShield Controller has visibility into *all* user activity, including login/logout time, applications run, resources reached, and transactions performed. It also provides information about specific application flows, even events within an application such as a file open, copy, delete, or edit. These capabilities enable specific access controls called for in the PCI specification.

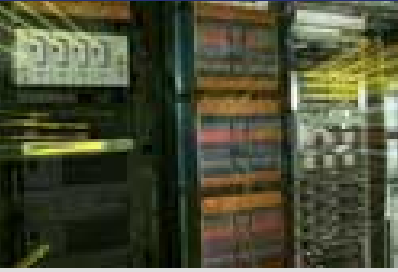
In addition, ConSentry provides threat control, protecting against both known and unknown threats. The LANShield Controller provides more accurate detection of attacks than security tools operating at lower layers, with blocking at a finer level of granularity. ConSentry's patent-pending application behavioral algorithms can detect zero-day or zero-hour worms by differentiating worm traffic from normal user behavior, for example. ConSentry gives IT the flexibility to define a policy to block all traffic from an infected user or just the infected application so that the user can continue to work and retain network access for remediation.

Additional Benefits

The clearinghouse was able to rapidly deploy the LANShield Controller because it's a completely transparent platform. The Controller requires no changes to the existing LAN design or hardware, has no impact on LAN traffic, has no dependencies on specific host or authentication infrastructure, and does not require users to interact with the network any differently. This plug-and-play capability enabled the clearinghouse to quickly achieve PCI compliance with minimal capital outlay and installation overhead.

In addition, the ConSentry LANShield Controller helps companies dramatically reduce the scope of a PCI audit. Because the LANShield Controller segments PCI users and resources from the rest of the LAN, only those devices and resources within the "virtual PCI domain" must be audited. Narrowing the scope of the audit to only those users and servers involved with PCI enabled the clearinghouse to cut its audit expenses by more than 50 percent.

ConSentry's InSight command center aids in documenting PCI compliance by enabling IT – and auditors – to view traffic on a per-user, per-flow basis for



detailed auditing, reporting, and forensics. With InSight, the clearinghouse is able to fully document what access control policies are in place and to whom they apply.

Likewise, InSight can document all user activity through both user-based and application/service-based reports. User reports indicate every application, server, and resource a user touched in a given timeframe while application/service reports detail all users who ran a particular application or hit a particular resource during a given period. InSight compiles information based on knowledge of user transactions, presenting IT with the user's name tied to all activities and access violations.

In addition to satisfying the compensating controls in Appendix B, the ConSentry platform can also help companies address aspects of Requirement 1 for firewalls, Requirement 7 for need-to-know access, and Requirement 10 for monitoring access.

With ConSentry Networks, this Fortune 500 clearinghouse was able to rapidly achieve PCI compliance as well as reap ongoing benefits from a streamlined auditing process.