Solution Brief

Addressing PCI DSS 3.2

Enabling Cardholder Data Security with ForeScout CounterACT®

Organizational Challenges

- Securing the evergrowing landscape of devices while keeping pace with regulations
- Enforcing appropriate access for compliant and non-compliant endpoints
- Requiring tools that provide visiblity, control and information sharing across the payment card ecosystem

Solution

- ForeScout CounterACT unifies security management and supports a wide-range of PCI DSS 3.2 compliance objectives
- CounterACT dynamically identifies and evaluates network devices and applications the instant they connect to your network
- CounterACT enables a broad range of host controls and network access, allowing organizations to quarantine or restrict access

Benefits

CounterACT helps organizations address PCI DSS compliance by:

- Transforming network security through visibility of managed, unmanaged and IoT devices
- Automating control and policy enforcement of endpoints on your network
- Granting network access to persons and devices—without intrusive intervention or staff involvement

Secure networks and drive compliance with PCI DSS 3.2, sidestepping considerable costs, disruptions and brand damage that can result from data breaches and compliance failures.

Cybercriminals constantly look for—and find—opportunities to compromise retail environments. As breach disclosures continue unabated, organizations need better ways to secure point of sales (POS) systems, automated teller machines (ATM), kiosks and other endpoints while keeping pace with regulations. Adding to the complexity, institutions face threats from a multitude of internal and external sources. Employees and contractors misuse and abuse corporate data resources—intentionally or otherwise—and their personally owned devices can wreak havoc on network security and stability, making the path to compromise much easier.

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that governs the way entities store, process and transmit cardholder data. If you are an organization that accepts payment cards for any service or product, you are obligated to comply with PCI DSS. All major credit card issuers support this standard, including payment card brands, acquiring banks, retail organizations and service providers.

Following these standards helps to ensure overall good organizational health and decreases the chance of customer cardholder data theft that can damage a business's reputation and result in fines.

Delivering on these compliance standards presents organizations with a complex set of challenges from a people, process and technology point of view. Discover why a grownning number of enterprises have made ForeScout CounterACT® a core component of their cybersecurity strategies to address PCI DSS 3.2 standards.

- **Average cost per compromised record in the retail industry is $172.[1]**
- **Payment card breaches had a much higher median of documented record loss than protected health information (PHI) or personally identifiable information (PII).[2]**
- **POS devices continue to be a reliable source for stolen payment card data.**

Keeping Cardholder Data Secure with ForeScout CounterACT

Whether its helping organizations build and maintain a secure network, drive a vulnerabiity management program, implement strong access control measures, monitor and test networks, or maintain an information security policy, CounterACT plays a vital role in helping to keep cardholder data secure.

No industry, location or organization is immune when it comes to the compromise of payment card data, and new threats can target any business at any time. Cybercriminals also continue to target financial information that is held by retailers, healthcare providers, financial services organizations and other customer-facing businesses. To keep cardholder data safe, companies need to be able to continously validate that their cyberdefense strategy is functioning properly with the ability to mitigate potential threats.

Designed to help ensure that merchants meet minimum levels of security when they store, process and transmit cardholder data, PCI DSS covers six objectives that are mapped to 12 specific requirement areas. It is up to each organization to implement these in ways that are best suited to their business. Compliance with all of these requirements greatly reduces the chance that data will be compromised and result in fraudulent transactions.

Most organizations find without compliance, there's chaos. The CounterACT platform offers a set of unique technologies that works with your devices—managed and unmanaged, known and unknown, PC and mobile, IoT, embedded and virtual. CounterACT helps ensure that endpoints on your network are compliant with your anti-virus policy, properly patched and have the proper policy-sanctioned software. CounterACT automatically identifies policy violations, remediates endpoint security deficiencies and measures adherence to regulatory mandates. In the retail industry, it is important to have reliable and efficient systems. CounterACT physically installs out of band, avoiding latency or issues related to the potential for network failure, and works in heterogenous environents. It can be centrally administered to dynamically manage tens or hundreds of thousands of endpoints from one console. ForeScout CounterACT provides organizations an efficient way to drive compliance toward a set of PCI DSS 3.2 requirements.

ForeScout CounterACT in the PCI DSS 3.2 Framework

The PCI DSS framework includes 12 categories, each with a set of requirements, testing procedures and guidance. CounterACT is uniquely positioned to help address a set of requirements in eight of the 12 key categories PCI DSS 3.2 mandates. Several examples are shown below.

Build and Maintain a Secure Network and Systems:

- Install and maintain a firewall configuration to protect cardholder data. CounterACT can provide a list of open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, identify traffic attempts from the Card Holder Data Zone outside of the Demilitarized Zone (DMZ) and deny or limit access to endpoints without firewall software.
- Implement one primary function per server and only enable necessary services and protocols required for the function of the system. CounterACT verifies that web, database and DNS services are dedicated to their primary function and detects insecure File Transfer Protocol (FTP), Telnet and NetBIOS services on PCI servers.

Maintain a Vulnerability Management Program:

- Protecting systems against malware and regularly updating anti-virus software and programs. CounterACT can detect hosts without an installed anti-virus application, validate that an anti-virus program is running with up-to-date threat signatures and continuously monitor endpoints to determine if the anti-virus becomes inactive. In addition, CounterACT can automatically quarantine them based on set policies.

- Developing and maintaining secure systems and applications. CounterACT can identify endpoints without the latest security patches, monitor traffic between the various PCI development, test and production zones, as well as track and block users attempting unauthorized access to servers.

Implement Strong Access Control Measures

- Restricting access to cardholder data by business need to know. CounterACT provides device and role-based network authentication and authorization, limiting individuals and their devices to appropriate network access as determined by Virtual Local Area Networks (VLANs) or Access Control Lists (ACLs). Enforcing network segmentation helps limit access to system components and cardholder data to those individuals whose job requires such access.
- Assigning a unique ID to each person with computer access. CounterACT integrates with a variety of third-party authentication systems to validate users prior to getting role-based network access and can provide acceptable policies to users who attempt to access the Card Holder Data Zone.

Monitor and Test Networks

- Regularly test security systems and processes. CounterACT can monitor and detect authorized and unauthorized wireless access points connected to the PCI network, create policies to isolate rogue access points as well as notify personnel of the discovery. In addition, CounterACT can provide real-time vulnerability scans as well as detect malicious activity by leveraging information sharing capabilities with third-party Advance Threat Detection, Vulnerability Assessment and Security Information and Event Management systems.

Information Security Policy

- Maintain a policy that addresses information security for personnel. CounterACT provides an avenue to present the company's Information Security policy to employees, requiring them to acknowledge reading and understanding it. This provides organizations a route to establish, publish, maintain and disseminate a security policy.

The CounterACT Security Platform

ForeScout CounterACT sees desktops, laptops, tablets, smartphones, IoT endpoints, peripherals and rogue devices the instant they connect to your network—even if they don't have security agents installed. CounterACT delivers real-time visibility and automates control of devices. It gathers in-depth insights about device types, users, applications, operating systems and more while continually monitoring those devices. CounterACT lets you allow, deny or limit network access based on device posture and security policies. It handles a full spectrum of control actions, making it simple to grant the identified level of network access to people and devices as you define and deploy controls at your own pace.

These capabilities help organizations processing credit card payments address components of PCI DSS 3.2 and more effectively secure their network, sidestepping the considerable costs, disruptions and brand damage that can result from data breaches and compliance failures.

PCI Objectives & Requirements[3]:

Objectives	Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI Requirements Addressed by CounterACT[3]

PCI Requirement 1

Install and maintain a firewall configuration to protect cardholder data.

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems.

Req	Definition	ForeScout CounterACT
1.1.6	Documentation of business justification and approval for use of all services, protocols and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Provides a list of open TCP and UDP ports found open on PCI servers. Entity should review the list of open ports and close ports that are unnecessary for business.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Identifies traffic attempts from the Card Holder Data Zone outside of the DMZ. CounterACT can restrict user and device access to the cardholder network using device and role-based access control. CounterACT provides authentication and authorization for wired, wireless and VPN access.
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: specific configuration settings are defined, personal firewall (or equivalent functionality) is actively running, personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	Endpoints attempting to access the network without personal firewall software that is both installed and operational can be denied access, quarantined and forced to remediate before being allowed access.

PCI Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters.

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Req	Definition	CounterACT Solution
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers and DNS should be implemented on separate servers.)	Verifies that Web, Database and DNS Servers are dedicated to their primary functions. Review the list of non-dedicated servers and close unnecessary ports to help ensure the servers are dedicated to their original role.
2.2.2	Enable only necessary and services, protocols, daemons, etc., as required for the function of the system.	Detects potentially insecure FTP, Telnet and NetBIOS services on PCI Servers.

PCI Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

Req	Definition	CounterACT Solution
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Detects hosts without an installed anti-virus application. Endpoints attempting to access the network without anti-virus software that is both installed and operational can be denied access, quarantined and forced to remediate before being allowed access.
5.1.1	Ensure that anti-virus programs are capable of detecting, removing and protecting against all known types of malicious software.	Can verify that the anti-virus is running and has updated threat signatures before granting network access.
5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirements 10.7.	Detects hosts without an active up-to-date anti-virus application. Verifies that anti-virus software is active and up-to-date with current signatures. CounterACT can monitor endpoints to determine if the anti-virus becomes inactive, and based on policy, quarantine the endpoint and require the endpoint to be remediated before getting network access.

PCI Requirement 6

Develop and maintain secure systems and applications.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

Req	Definition	CounterACT Solution
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Identifies endpoints without the latest known security patches. Based on policy, these endpoints can have quarantined network access until they are patched. Patching can be automated.
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Identifies traffic attempts between PCI Development, Test and Production Zones. Can enforce role-base access using VLANs or ACLs to segregate test, development and production environments.
6.4.2	Separation of duties between development/test, and production environments.	Identifies users attempting to access servers they are not authorized to access to by their Active Directory group.

PCI Requirement 7

Restrict access to cardholder data by business need to know.

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access right are granted to only the least amount of data and privileges needed to perform a job.

Req	Definition	CounterACT Solution
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Identifies users attempting to access cardholder information they are not authorized access to by their Active Directory group. CounterACT provides device and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.

PCI Requirement 8

Identify and authenticate access to systems components.

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Req	Definition	CounterACT Solution
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Integrates with a variety of third-party authentication systems to validate unique identity and users prior to getting role-based network access. User ID can also be associated with the device MAC address, device name and network access entry point to define and enforce specific access policies.
8.4	Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised	Present the use policies to the users that attempt to access the Card Holder Data Zone.

PCI Requirement 11

Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Req	Definition	CounterACT Solution
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	CounterACT can monitor and detect authorized and unauthorized wireless access points connected to the PCI network.
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	Policies can be created to automatically isolate rogue access points as well as notify personnel of discoveries.
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Can help to ensure real-time vulnerability scan compliance with various third-party vulnerability scanners. Can perform vulnerability scans for endpoints on network connections and periodically on the network determined by policy.
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines and signatures up to date.	Detects malicious activity using CounterACT Threat Protection engine. Integrates with third-party Advanced Threat Detection and Security Information and Event Management systems. These insights can provide actionable threat information that CounterACT's policy can use to isolate or initiate remediation actions.

PCI Requirement 12

Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

Req	Definition	CounterACT Solution
12.1	Establish, publish, maintain and disseminate a security policy.	Presents the company's Information Security Policy to employees and requires employees to acknowledge reading and understanding it.

[1] An acquiring bank (or acquirer) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant. Wikipedia

[2] Data Breach Investigation Report, Verizon, 2016

[3] Requirements and Security Assessment Procedures, Payment Card Industry (PCI) Data Security Standard, v3.2, April 2016

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

Version 9_16