



Endpoint Security Considerations for Achieving PCI Compliance

Contents

- PCI Requirements and Endpoint Security 3
- Overview of the PCI Data Security Standard 3
- Developing a PCI Compliance Plan 4
- Endpoint Security Technologies and PCI DSS 4
- Best Practices for Deploying Endpoint Security Technologies 4
- Endpoint Security Controls Defined in the PCI Standard 5
- Learn More 6

PCI Requirements and Endpoint Security

Electronic theft of personal and financial data is a serious and growing problem that drives up costs for credit card issuers and the merchants they serve, and undermines consumer confidence and loyalty. In response, the Payment Card Industry has developed the PCI Data Security Standard (PCI DSS). This multi-faceted security standard includes requirements for endpoint security, security management, policies, procedures, network architecture, software design and other critical protective measures.

The old adage ‘a chain is only as strong as its weakest link’ provides the best analogy for challenges that merchants must address when planning to comply with new PCI standards. Recent studies demonstrate that the endpoints of a payment card processing system are in fact that ‘weakest link’. The endpoints of your system—POS terminals, networked cash registers, kiosks, etc.—are typically deployed in exposed environments, vulnerable to criminals who leverage increasingly sophisticated tools and methods of attack to steal valuable cardholder data and account information. Tellingly, more than half of the PCI DSS requirements are now dedicated to defining controls for endpoint security.

Overview of the PCI Data Security Standard

PCI DSS is an industry-driven set of six goals and 12 requirements for protecting cardholder data. The standard is managed by the PCI Security Standards Council which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc. Any organization that accepts, or plans to accept payment cards, must comply with PCI DSS.

PCI DSS 1.2 goals and requirements	
Goals	Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for employees and contractors.

“Check Point provides a solution that is secure for us and transparent to the users. Check Point has been great. We wouldn’t dream of moving to any other solutions provider.”

Connie Wiseman
IT Technical Manager
RPS Group Plc

Developing a PCI Compliance Plan

PCI compliance requires actions based on an organization’s classification level, as defined by the PCI standard. As a baseline, organizations must implement security controls required by PCI DSS, regularly assess the state of security affecting cardholder data, remediate vulnerabilities, and submit an annual compliance report. Validation requirements include an annual security self-assessment, an onsite review and quarterly network security scans. Qualified Security Assessors and Approved Scanning Vendors can help with compliance planning and validation. A compliance failure can result in serious penalties for merchants—including revocation of the rights to accept and process payment cards.

Endpoint Security Technologies and PCI DSS

Certain PCI DSS requirements can be satisfied through deployment of endpoint security technologies and controls. These essential technologies provide a robust and comprehensive multi-layered defense against endpoint exploits, and should be carefully considered when developing compliance plans for PCI, as well as other security regulations.

Essential endpoint security technologies
Firewall — Blocks or allows traffic based on criteria defined by endpoint security policies.
Intrusion Detection / Prevention System — IDS/IPS technology analyzes network traffic for malicious code and attacks.
Program Control — Restricts network access on a per-program basis thereby limiting exposure to vulnerabilities and attacks.
Network Access Control — NAC restricts access by unknown users by enforcing policy compliance at endpoints and offering auto-remediation.
Antivirus / Anti-spyware — Automatically scans files based on a variety of criteria to identify viruses and malware, and responds according to policy.
Data Security — Protects data stored on endpoints through a combination of user authentication, data encryption and port control.
Secure Remote Access — Establishes a virtual private network (VPN) allowing remote users to safely access corporate resources.

Best Practices for Deploying Endpoint Security Technologies

Prior to deployment of endpoint security technologies, several strategies must be considered to ensure flexibility, reliability and long term viability of the overall solution. Best practices should include:

Deploy integrated solutions— choose solutions from reputable vendors that address multiple requirements. Integrated solutions can optimize management and administration efficiencies. This may not be possible with individual point solutions.

Be holistic— deploy solutions that address core security capabilities and facilitate compliance with multiple regulations and industry guidelines.

Add value— use solutions that enhance fundamental business value and differentiate your business, such as adding new sales channels.

Ensure future scalability— deploy solutions that will adapt to and grow with changing business requirements.

Check Point Endpoint Security for PCI Compliance

Check Point Endpoint Security™ is the first and only single agent for total endpoint security; simplifying deployment, eliminating the need to manage multiple security agents and incorporating the strongest, most comprehensive suite of endpoint security components. Key benefits include:

- Single agent for all your endpoint security needs
- Easy configuration and deployment
- Eliminates the need to manage multiple security agents
- No testing or compatibility issues between separate agents
- Reduced administration requirements lower total cost of ownership

Endpoint Security Controls Defined in the PCI Standard

In order to prevent cardholder data that is processed or temporarily stored at endpoints from being stolen or tampered with, the PCI DSS defines key endpoint security requirements and associates them with specific endpoint security controls. Consultants will refer to these definitions when conducting PCI audits. The following table conveniently summarizes these endpoint security requirements and controls.

Endpoint security controls for PCI DSS compliance	
PCI Endpoint Requirement	Endpoint Security Control
1.4: Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet, which are used to access the organization's network.	Endpoint Firewall. Solely using server-based firewalls does not meet the requirement for PCI 1.4. Personal firewall software also must be installed on each endpoint with Internet access that is used to access a merchant's network.
3.4: Render PAN, at a minimum, unreadable anywhere it is stored. Options include one-way hashes, truncation, index tokens and pads, or strong cryptography with associated key-management.	Endpoint Encryption. Endpoint cryptography solutions simplify compliance with PCI 3.4 via full disk encryption, media encryption, and encryption for mobile devices such as personal digital assistants and smart phones.
4.1: Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	Encryption for Remote Transmission. Endpoints must use remote access technology that protects cardholder data transmitted over public or wireless networks.
5.1: Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Anti-Virus. Endpoints must run anti-virus technology to automatically eliminate viruses and other malware. Virus and rootkit defenses may include combinations of signatures, behavior blockers, and heuristic analysis.

<p>5.2: Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>Anti-Virus Updates. Anti-virus technology on endpoints must include a mechanism that automatically ensures every machine has the most recent software activated and logging all incidents.</p>
<p>7.2: Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.</p>	<p>Endpoint Access Control. Endpoint access control technology must automatically regulate network access based by anyone based on policy conforming to requirements of PCI 7.1 and 7.2.</p>
<p>10.2: Implement automated audit trails for all system components to restrict any of seven specified security events.</p>	<p>Security Audit Trails for Each Endpoint. Each security control implemented on an endpoint must automatically post security events to audit log files.</p>
<p>11.4: Use up-to-date intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises..</p>	<p>Intrusion-Detection or Prevention. IDS/IPS technologies must include each endpoint that can access the cardholder data environment. Endpoint IDS/IPS must be integrated with the organization's standard security alert system.</p>
<p>11.5: Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system, configuration, or content files.</p>	<p>Endpoint Program Control. Endpoint program control technology can perform this task with an inventory of critical files and MD5 hash values. Policy and rules will use this information to confirm legitimate applications and block unauthorized access attempts.</p>

Learn More

For more information about PCI DSS ver. 1.2 requirements or to view the online PCI Quick Reference Guide, please visit the Council's website at: www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

For more information about how Check Point Endpoint Security solutions can help you achieve PCI compliance, please contact your local Check Point sales representative, call Check Point at 800-429-4391, or visit: www.checkpoint.com/products/datasecurity/index.html



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is the leader in securing the Internet. Check Point offers total security solutions featuring a unified gateway, single endpoint agent and single management architecture, customized to fit customers' dynamic business needs. We are unique in this offering as a result of our leadership and innovation in the enterprise firewall, personal firewall/endpoint, data security and VPN markets.

Check Point's pure focus is on information security. Through its NGX platform, Check Point delivers a unified security architecture to protect business communications and resources, including corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market-leading endpoint and data security solutions with Check Point Endpoint Security products, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm solutions protect millions of consumer PCs from hackers, spyware and identity theft. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMSecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.