

# Meeting PCI DSS v3.2.1 Merchant Requirements With WatchGuard UTM and Total Security, Multi-Factor Authentication, and Wireless Solutions



# Table of Contents

## Contents

Introduction .....	2
PCI Certification .....	3
PCI DSS Merchant Levels .....	3
PCI DSS Requirements .....	4
PCI DSS 3.2.1 Update .....	5
PCI DSS and WatchGuard Total Security Suite .....	6
Implementation Guidance .....	6
Zoned Networks.....	6
Monitor Cardholder Data Access .....	7
Threat Detection and Response .....	7
DNS-Based Protection .....	7
Multi-Factor Authentication .....	7
Wireless Protection .....	7
Summary .....	7
Appendix I. PCI Requirements – WatchGuard UTM Alignment .....	8
About WatchGuard .....	9

## INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express. Governed by the Payment Card Industry Security Standards Council (PCI SSC), the compliance scheme aims to secure credit and debit card transactions against data theft and fraud.

While the PCI SSC has no legal authority to compel compliance, the PCI DSS has become a ubiquitous default requirement by the credit/debit card transaction-processing industry. PCI certification is also considered the best way to safeguard sensitive data and information, thereby helping businesses build long-lasting and trusting relationships with their customers. This paper will aim to explore how WatchGuard's award-winning network security, secure Wi-Fi, and multi-factor authentication solutions have helped thousands of customers build a PCI-compliant organization.



## PCI Certification

PCI certification ensures the security of card data at your business through a set of requirements established by the PCI SSC. These include a number of commonly known best practices, such as:

- Installation of firewalls
- Encryption of data transmissions
- Use of antivirus software
- Use of intrusion prevention systems
- Detection of rogue access points
- Deployment of multi-factor authentication



In addition, businesses must restrict access to cardholder data and monitor access to network resources.

PCI-compliant security gives customers confidence that your business can safely handle transactions. Conversely, the cost of noncompliance, both in monetary and reputational terms, should be enough to convince any business owner to take data security seriously. The investment in WatchGuard Total Security Suite goes a long way toward ensuring that other aspects of your commerce are safe from malicious actors.

## PCI DSS MERCHANT LEVELS

PCI compliance is divided into four levels, based on the annual number of credit or debit transactions a business processes.

The classification level determines what an enterprise needs to do to remain compliant.

<b>PCI</b> DSS COMPLIANCE LEVELS	<b>LEVEL 1</b>	6M + Transactions/ Year
	<b>LEVEL 2</b>	1-6M + Transactions/ Year
	<b>LEVEL 3</b>	20K-1M + Transactions/ Year
	<b>LEVEL 4</b>	< 20K-1M + Transactions/ Year

- **Level 1** – Applies to merchants processing more than six million credit or debit card transactions annually. They must undergo an internal audit once a year conducted by an authorized PCI auditor. In addition, once a quarter they must submit to a PCI scan by an Approved Scanning Vendor (ASV).
- **Level 2** – Applies to merchants processing between one and six million credit or debit card transactions annually. They're required to complete an assessment once a year using a Self-Assessment Questionnaire (SAQ). Additionally, a quarterly PCI scan may be required.
- **Level 3** – Applies to merchants processing between 20,000 and one million e-commerce transactions annually. They must complete a yearly assessment using the relevant SAQ. A quarterly PCI scan may also be required.
- **Level 4** – Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. A yearly assessment using the relevant SAQ must be completed and a quarterly PCI scan may be required.

## PCI DSS REQUIREMENTS

The PCI SSC has outlined 12 requirements for handling cardholder data and maintaining a secure network. Distributed between six broader goals, all are necessary for an enterprise to become compliant.

CATEGORY	REQUIREMENT
<b>SECURE NETWORK</b>	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
<b>SECURE CARDHOLDER DATA</b>	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
<b>VULNERABILITY MANAGEMENT</b>	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
<b>ACCESS CONTROL</b>	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
<b>NETWORK MONITORING AND TESTING</b>	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
<b>INFORMATION SECURITY</b>	12. A policy dealing with information security must be maintained



## PCI DSS 3.2.1 UPDATE

The Massachusetts-based organization announced on April 28, 2016 an upcoming change to the current PCI DSS (v.3.1) standard for safeguarding payment data, PCI DSS v3.2. This update included clarifications to existing requirements, new or evolving requirements, and additional guidance. PCI DSS v3.2.1, released in May 2018, provided further clarifications to existing requirements.

REQ #	DESCRIPTION	COMMENT
8.3.1	Incorporate multi-factor authentication for all non-console access into the cardholder data environment (CDE) for personnel with administrative access	<a href="#">See page 7 of this whitepaper</a>
10.8	<b>Additional requirement for service providers only:</b> Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to a failure of: <ul style="list-style-type: none"> <li>• Firewall</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivirus</li> <li>• Physical access controls</li> <li>• Logical access controls</li> <li>• Audit logging mechanisms</li> <li>• Segmentation controls (if used)</li> </ul>	<a href="#">See page 8</a>
10.8.1	<b>Additional requirements for service providers only:</b> Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: <ul style="list-style-type: none"> <li>• Restoring security functions</li> <li>• Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause</li> <li>• Identifying and addressing any security issues that arose during the failure</li> <li>• Performing a risk assessment to determine whether further actions are required as a result of security failure</li> <li>• Implementing controls to prevent cause of failure from reoccurring</li> <li>• Resuming monitoring of security controls</li> </ul>	<a href="#">See page 8</a>
11.3.4.1	<b>Additional requirement for service providers only:</b> If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods	<a href="#">See Page 8</a>
12.11	<b>Additional requirement for service providers only:</b> Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: <ul style="list-style-type: none"> <li>• Daily log reviews</li> <li>• Firewall rule-set reviews</li> <li>• Applying configuration standards to new systems</li> <li>• Responding to security alerts</li> <li>• Change management processes</li> </ul>	Although not directly applicable to WatchGuards firewall deployment, our Dimension product will produce a powerful view into firewall rule-sets to greater facilitate firewall policy reviews. <a href="#">See Page 8</a>

## PCI DSS AND WATCHGUARD TOTAL SECURITY SUITE

WatchGuard's comprehensive Total Security Suite, which includes 13 integrated security modules, managed under a single policy framework, provides visibility and control over network and endpoint data loss as well as comprehensive data discovery across enterprise storage systems. Our solution offers a comprehensive, approach towards network segmentation, protection, and detection that establishes WatchGuard as an ideal, award-winning choice for organizations where PCI compliance is a must.



## IMPLEMENTATION GUIDANCE

### Products required:

- WatchGuard Firebox UTM
- WatchGuard Threat Detection and Response
- WatchGuard AuthPoint
- Total Security Suite Subscription
- WatchGuard Cloud

## RECOMMENDED DEPLOYMENT:

PCI DSS Requirement		UTM Firewall + Basic Security Suite	UTM Firewall + Total Security Suite + AuthPoint	Cloud Wi-Fi
Requirement 1	Install and maintain a firewall configuration to protect cardholder data	✓	✓	
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters	✓	✓	
Requirement 3	Protect stored cardholder data			
Requirement 4	Encrypt transmission of cardholder data across open, public networks	✓	✓	✓
Requirement 5	Protect all systems against malware and regularly update antivirus software or programs		✓	
Requirement 6	Develop and maintain secure systems and applications	✓	✓	✓
Requirement 7	Restrict access to cardholder data by business need to know		✓	
Requirement 8	Identify and authenticate access to system components		✓	
Requirement 9	Restrict physical access to cardholder data			
Requirement 10	Track and monitor all access to network resources and cardholder data	✓	✓	✓
Requirement 11	Regularly test security systems and processes	✓	✓	✓
Requirement 12	Maintain a security policy that addresses information security for all personnel			✓

## ZONED NETWORKS

As required by PCI DSS, WatchGuard UTM's application proxy technology provides detailed control over the traffic that passes between network zones. Customizable and easy-to-configure firewall policy creation enables administrators to block all traffic by default and to define which traffic is allowed to pass between zones, including protocols, ports, content types (e.g., MIME types, 37+ file types, and URLs) and verbs (e.g., HTTP GET).

WatchGuard Total Security Suite allows businesses to leverage all components of WatchGuard's UTM appliance – including APT Blocker, Data Loss Prevention, Gateway AntiVirus, IntelligentAV, Reputation Enabled Defense, Intrusion Protection Service, WebBlocker, Network Discovery, Application Control, spamBlocker, Access Portal, DNSWatch, and Threat Detection & Response – providing a comprehensive network defensive scheme in pursuit of PCI DSS compliance.



## MONITOR CARDHOLDER DATA ACCESS

Practical monitoring of all the network components is best implemented with WatchGuard visibility solutions, including WatchGuard Cloud and WatchGuard Dimension. WatchGuard Cloud Visibility comes standard with WatchGuard's flagship UTM platform. It provides a suite of big data visibility and reporting tools that instantly isolate and distill key security issues and trends from the firewall log data, thereby accelerating the ability to set meaningful security policies across the network. Both WatchGuard Cloud Visibility and Dimension include a dashboard and a set of reports specifically for PCI compliance.

- Compatibility with the chosen identity management solution and complete logging of all authentication events.
- Comprehensive audit trail that tracks all changes to the firewall.
- IDS, IPS, DLP, and antivirus solutions – the actions of which must also be logged.
- Wireless networks require special attention as they are fundamentally insecure. Every precaution must be taken to secure against wireless hacks.



Ask your WatchGuard partner to see a sample, generated by WatchGuard Cloud Visibility, for a more complete look at the kind of information WatchGuard can correlate for your business to achieve and maintain PCI compliance. For on-premises requirements, WatchGuard Dimension is also available.

## THREAT DETECTION AND RESPONSE

WatchGuard Threat Detection and Response is a collection of advanced malware defense tools that correlate threat indicators from Firebox appliances and Host Sensors to stop known, unknown and evasive malware threats. At its core is ThreatSync, a Cloud-based correlation engine that analyzes event data from Host Sensors and Firebox appliances to identify malicious behavior. Threats are scored based on severity for automated remediation. TDR is licensed as part of WatchGuard's Total Security Suite and addresses key anti-malware requirements as part of PCI DSS.

## DNS-BASED PROTECTION

WatchGuard's DNSWatch is a DNS-based service that brings threat intelligence to outbound network traffic. DNSWatch is included with Total Security Suite, which includes all the features of a UTM appliance developed for protection against modern threat landscapes. Combining analysis from 37+ threat intelligence vendors with its own detection capabilities, DNSWatch applies anti-malware defense to network traffic by providing anti-phishing protection before a malicious URL has a chance to resolve to the intended destination. Additionally, DNSWatch provides redirection to training modules that can assist with automated and behavioral-based anti-phishing training, building awareness and threat prevention within your organization's first-line of defense: employees!

## MULTI-FACTOR AUTHENTICATION

WatchGuard's AuthPoint service is a crucial tool for PCI compliance, offering multi-factor authentication (MFA) to assist implementation of authentication, authorization and accounting. AuthPoint offers token-based authentication through traditional RADIUS-based means, Security Assertion Markup Language (SAML) 2.0, one-time passcode (OTP), and off-network-based protection. With a mobile application – supported on both iOS and Android platforms – and centralized Cloud management, AuthPoint brings targeted security for both the on-premises and remote user workforce.

## WIRELESS PROTECTION

WatchGuard access points (APs) help merchants to prepare for PCI compliance by offering monitoring capabilities on its 802.11ac platform. Leveraging the wireless AP's ability to monitor 2,000 active wireless devices per AP sensor, compliance and security officers wield powerful wireless intrusion prevention system (WIPS) technology to lock trusted devices to authorized networks and keep sensitive cardholder data processing systems secure and prevent any wireless 'honeypot' attacks.

## SUMMARY

No single vendor or solution can provide complete compliance with the Payment Card Industry Data Security Standard. The WatchGuard family of UTM products is ideally suited to providing merchants the means to build a thorough set of policies, processes and practices – including network segmentation – supported by an essential set of technological countermeasures to enforce them. In this regard, the WatchGuard UTM security platform is an invaluable solution that delivers:

- strong least-privilege access and authentication control for segmenting cardholder data environment
- support for a considerable cross-section of the PCI DSS requirements
- capabilities that far exceed PCI DSS's baseline standards to more thoroughly protect cardholder data

For more information and demonstrations visit us at [www.watchguard.com](http://www.watchguard.com) or contact your authorized WatchGuard reseller.

## APPENDIX PCI REQUIREMENTS – WATCHGUARD UTM ALIGNMENT

PCI DSS REQUIREMENT		SUPPORTED SUB-REQUIREMENTS	CAPABILITY DESCRIPTION
<b>Requirement 1:</b>	Install and maintain a firewall configuration to protect cardholder data	1.2, 1.2.2, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8	The WatchGuard UTM enables the enforcement of strict network segmentation by blocking all traffic by default and defining a proxy policy that allows only approved traffic to pass environment.
<b>Requirement 2:</b>	Do not use vendor-supplied defaults for system passwords and other security parameters	2.2.2, 2.2.3, 2.3	<p>WatchGuard UTM appliances support the implementation of preventative controls to reduce attack surfaces. These controls include changing vendor passwords; enabling only necessary services, protocols and daemons and removing unnecessary functionality and web servers.</p> <p>This is partly achieved by blocking all traffic by default and defining a proxy for those specific protocols that are allowed. Furthermore, all management communications with WatchGuard UTM appliances are done via a secure encryption-based protocol. Web interfaces and all management components use TLS 1.3.</p>
<b>Requirement 3:</b>	Protect stored cardholder data	N/A	N/A
<b>Requirement 4:</b>	Encrypt transmission of cardholder data across open, public networks	4.1, 4.1.1, 4.2	<p>WatchGuard UTM appliances support IPsec, IKEv2, L2TP, and SSL VPN communication. All certificates are based on SHA-256 or stronger cryptographic algorithms including full Suite B compatibility. In addition, WatchGuard wireless solutions fully support 802.11i authentication methods.</p> <p>WatchGuard UTM appliances can detect and prevent unauthorized loss of credit card information over email and web networks.</p>
<b>Requirement 5:</b>	Protect all systems against malware and regularly updated anti-virus software or programs	5.1, 5.1.1, 5.1.2, 5.2, 5.3, 5.4	WatchGuard Total Security provides three layers of anti-malware on at the gateway, as well as Threat Detection and Response, which provides protection for endpoints with a host sensor capable of detecting and blocking malware. In addition, appliance logs are updated in the event of malware intrusion from sandboxing service, APT Blocker or from our dual antivirus engines.
<b>Requirement 6:</b>	Develop and maintain secure systems and applications	6.1, 6.6	In combination with an application firewall, the UTM provides an additional layer of protection with HTTP/S proxies. These proxies perform content filtering and thoroughly examine web traffic to identify suspicious content, which can be a virus, spyware, or other type of intrusion. The WatchGuard TDR solution includes file signature analysis, heuristics analysis, and behavioral analysis to detect and classify malware. Through a process of correlation, TDR uses multiple sources of threat intelligence, as well as indicators from other security services on the Firebox platform, to establish a numeric threat score (1-10) that corresponds to risk.
<b>Requirement 7:</b>	Restrict access to cardholder data by business need to know	7.1, 7.2	With WatchGuard UTM, administrators can enforce granular policies - “least privilege” practices - based on individual users or groups, as well as segment network traffic so that access to data is bound by least privilege rights regardless of the user, device, or network.
<b>Requirement 8:</b>	Identify and authenticate access to system components	8.1.1, 8.2, 8.2.1, 8.3	WatchGuard UTM appliances support two-factor authentication, including RADIUS, RSA SecurID, VPN certificates, and WatchGuard’s multi-factor authentication service, AuthPoint. All management communications with Firebox appliances are done via a secure encryption-based protocol, and Firebox appliances store their password information in an encrypted format.



PCI DSS REQUIREMENT		SUPPORTED SUB-REQUIREMENTS	CAPABILITY DESCRIPTION
<b>Requirement 9:</b>	Restrict access to cardholder data by business need to know	N/A	N/A
<b>Requirement 10:</b>	Track and monitor all access to network resources and cardholder data	10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.6, 10.6.1, 10.6.2, 10.6.3	<p>All WatchGuard UTM appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated.</p> <p>WatchGuard Dimension can be installed on a secure machine to provide secure and convenient visibility for audit trails and provide key data including:</p> <ul style="list-style-type: none"> <li>• Audit trail of configuration changes</li> <li>• Authentication failures</li> <li>• Policy violations</li> <li>• IPS, DLP, and antivirus events</li> <li>• NTP synchronized</li> </ul>
<b>Requirement 11:</b>	Regularly test security systems and processes	11.1, 11.2	<p>WatchGuard wireless access points and WatchGuard UTM appliances with integrated wireless have the functionality to enable scanning for and detection of "rogue" wireless access points. This capability has been expanded with our Cloud-based rogue access point detection offerings.</p> <p>WatchGuard UTM bundle comes with our award-winning Intrusion Prevention Service (IPS). IPS scans traffic on all major protocols, using continually updated signatures to detect and block all types of threats.</p>

## ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit [WatchGuard.com](http://WatchGuard.com).

