Meet and Exceed PCI DSS 3.0 Requirements with Carbon Black

- Protect and secure in-scope and out-of-scope systems
- Ensure that security policies and operational procedures are documented, in use, and known to all affected parties
- Establish a process to identify security vulnerabilities and assign a risk ranking
- Control change, resulting in less data to analyze, which reduces administrative efforts
- Receive real-time alerts so you can act immediately to protect all of your critical systems and data

PCI DSS 3.0

Validates the Convergence of Security and Compliance

PCI 3.0 Requires a Proactive Approach to Security (and Compliance, too)

The Payment Card Industry Data Security Standard (PCI DSS) has evolved to now impact a greater number of merchants and customers than ever before. PCI DSS 3.0, and the subsequent update to version 3.1, have had a profound effect on the compliance validation programs of many organizations. Per the PCI Security Standards Council, version 3.0 changes “are designed to help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice.” This change strengthens the controls to protect companies from threats. It also demonstrates the convergence of security and compliance, and the need for measurable proof that security controls are actually protecting your systems.

PCI DSS 3.1 Security and Compliance Highlights

1. PCI DSS 3.1 improves the focus and scrutiny on the actual intent and effectiveness of the security controls used to meet the requirements, rather than just the requirement itself. This means that your organization must now have greater control over your in-scope infrastructure, and the security solutions that you use to protect it.

2. PCI DSS 3.1 requires that security goals are met within each requirement and that there are adequate measures to ensure and prove the fulfillment of those requirement goals. This means that your organization must have greater visibility into the infrastructure to ensure and prove your compliance position on an ongoing basis, rather than managing compliance based on a ‘snapshot’ view. You now need to make risk measurement a standard part of your “business as usual” activities, and have full real-time visibility into the business process in order to guarantee that compliance and security risk can be measured at any point in time.

3. PCI DSS 3.1 provides for enhanced testing procedures to ensure that the requirements are met and validated. By using a security solution that enables you to control critical changes and focus on the compelling changes that matter to your business, you will limit the scope of compliance pre-assessment data gathering, reduce the administrative burden and streamline the process.

4. The PCI Security Standards Council also has taken a stance to be much more technology-agnostic with version 3.1, which opens the door for your organization to consider using alternate technologies as your primary controls to meet many PCI requirements. This means your organization can consider various technology alternatives to build an iron-clad security stack to help meet compliance objectives and protect your organization.

Carbon Black.
Carbon Black Enables You to Meet and Exceed PCI DSS 3.1 Requirements

The Carbon Black Security Platform can help you meet and exceed both security and PCI DSS 3.0 requirements. Below are examples of how Carbon Black addresses selected requirements.

Requirement 5.1.1

The 5.1.1 requirement states that anti-malware programs must be capable of detecting, removing and protecting against all known types of malicious software. As guidance on this requirement, PCI also states that it is important to protect against “current and evolving malicious software threats.”

The PCI standard places greater emphasis on security protection while also emphasizing that your anti-malware solution must be able to stop all known types of malware. This is simply not possible using antivirus and other signature-based security solutions, as has been evidenced in numerous breaches where those tools were in place. However, Carbon Black Enterprise Protection, based on the industry’s most advanced application control, enables your organization to close the threat window against zero-day and targeted attacks to meet—and exceed—this requirement.

Requirement 5.1.2

PCI DSS 3.0 has added a new requirement for systems not commonly considered to be affected by malicious software. Requirement 5.1.2 requires you to perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue to not require antivirus software.

Malware attacks have become more sophisticated and advanced since the last version of the data security standard was published, and the intent with this requirement is to ensure better security coverage of outward systems that are integrated or perhaps attached to the processing systems that deal with credit card data. This new requirement is aimed at ensuring your business is protecting the entire enterprise from malicious attack, and is more aligned to handle the types of advanced exploits seen in the industry today. Cb Protection is an example of a security solution that can protect both your in-scope and out-of-scope systems, enabling you to exceed this requirement.

Why PCI DSS 3.1 is Important to Retailers

Types of Data Targeted

- Customer Records
- Payment Card Data, PII, Email Addresses
- Confidential Information & Intellectual Property
- Electronic Protected Health Information
- Business Financial, Account Numbers

“...The primary data type targeted by attackers in 2012, as in 2011, was cardholder data. There is a well-established underground marketplace for stolen payment card data: it is bought and sold quickly for use in fraudulent transactions. With such a vast number of merchants accepting payment cards (estimates from major credit card brands put the total in the United States between nine and 10 million merchants), and with so many available attack vectors, it is unlikely this market will change any time soon.”

- 2013 Global Security Report

PCI DSS 3.0 Validates the Convergence of Security and Compliance
ADVANCED THREAT PROTECTION FOR ENDPOINTS AND SERVERS

Assessing Your Current Security Posture

Visibility

*Know what’s running on every computer in real time.*

From a single console, get immediate visibility into the files, executions, and critical system resources on every machine under protection.

Detection

*Detect advanced threats and zero-day attacks in real time.*

Detects advanced threats, zero-day attacks, and other malware that can evade blacklisting and signature-based detection tools. Combine real-time sensors, Advanced Threat Indicators (ATI), and a Software Reputation Service to proactively detect advanced threats and malware.

Response

*A full audit trail accelerates analysis and response.*

When you suspect you have a threat incident, ensure you have the information you need to analyze, scope, contain, and remediate the problem.

Prevention

*Stop all untrusted software from executing.*

Implementing next generation endpoint security enables you to define the software you trust to run in your organization. Everything else is denied by default.

Integration

*Connect endpoint and server security solutions with network security.*

Acquire a holistic approach to enterprise security by correlating network data with real-time endpoint sensor and recorder data.

Requirement 5.3

This requirement, also new to PCI DSS 3.0, calls for organizations to ensure that antivirus programs cannot be changed or turned off, except as a temporary measure to address technical needs, and then only by authorized personnel whose approval to do so is granted on a case-by-case basis. This is a change to the previous version, which required businesses to ensure their antivirus programs remained “actively running.”

While antivirus software can easily be deactivated on client endpoints, Cb Enterprise Protection cannot be disabled, ensuring that your organization meets this requirement.

Requirement 5.4

Requirement 5.4 ensures that security policies and operational procedures for protecting systems against malware are documented, in use and known to all affected parties. This definition reflects the PCI Council’s stance to ensure proof that security controls are enforced. It will be crucial that your security solution:

- Enables the collection and dissemination of security policy
- Helps to enforce that policy across the entire organization
- Provides the audit proof to support it

Cb Protection can assist you in distributing and enforcing a compliance policy and put mechanisms in place to inform and educate end users on those established policies.

Requirement 6.1

PCI DSS 3.0 switched requirements 6.1 and 6.2, so requirement 6.1 now calls for your organization to establish a process to identify security vulnerabilities using reputable outside sources for security vulnerability information, and assign a risk ranking. While risk ranking was initially introduced in requirement 6.2 in the PCI 2.0 standard, it is now enhanced and requires use of security solutions that will help assign and measure the amount of risk that any vulnerability poses to the organization.

Cb Protection addresses this requirement by providing real-time visibility into your environment on the front end and real-time threat and trust measurement to the assets, reducing the administrative effort to meet this requirement. Cb Protection also applies threat and trust ratings to every file within your infrastructure, providing immediate analysis and risk ranking of any potential file vulnerability discovered.
**Requirement 6.2**

Requirement 6.2 now calls for organizations to ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied patches. Critical security patches must be installed within one month of release.

Adhering to this requirement can be a challenge when popular operating systems reach end of life. In many cases, organizations cannot upgrade to newer operating system versions because of software incompatibility and/or because the newer operating system upgrade requires an expensive upgrade of their hardware as well. Organizations that choose not to upgrade can consider paying for extended support, an extremely expensive alternative.

Cb Protection has been validated by Coalfire, an industry-leading QSA, as a as a compensating security control for regular patching and updates when they are no longer available, enabling your organization to extend the security window and protect your endpoints past their end of life.

**Requirement 11.5**

Requirement 11.5 calls for the deployment of a change-detection mechanism that can control and understand change and alert personnel to unauthorized modification of critical system, configuration or content files. Previously, the requirement called for a monitoring mechanism, and although this is a minor change it supports the concept of a proactive security environment that enables you to analyze change, understand it, and make decisions based on the authorization level of the change.

Cb Protection enables you to control change so you can stop unauthorized change. This means less change and less change data to analyze. Without Cb Protection, the large amounts of change data can be overwhelming to compliance and security personnel.

Carbon Black Enterprise Response provides change detection capabilities which track critical changes in real time and provide alerts of unauthorized activity.

Requirement 11.5.1 calls for organizations to implement a process to respond to any alerts generated by the change-detection solution. This is further proof that organizations must move away from passive security measures to a more proactive security approach that provides alerts in real time so you can act immediately to protect all of your critical systems and data.

**Summary**

The PCI SSC has increased the security control measurement in PCI 3.0 and now recognizes that proactive security measures must be integrated into the business process. This focus on security helps ensure that compliance is a cyclical, proactive measurement, not just a report on a company’s compliance posture at a specific point in time—or before the auditor arrives.

Proactive security measures require security solutions that can address both the security and compliance challenges your organization faces. Carbon Black’s next generation endpoint security exemplifies the convergence of compliance and security—providing the visibility, detection, response and prevention needed to automate and manage compliance for PCI DSS 3.0.

**Carbon Black.**