Closing PCI DSS Security Gaps with Proactive Endpoint Monitoring and Protection
Table of Contents

Introduction .................................................................................. 3
Positive versus Negative Application Security ................................ 3
Continuous Audit and Assessment of the Compliance Validation Process...... 4
FIM/FIC Reporting .......................................................................... 6
Correlated Contextual Logging ........................................................... 7
Risk Analysis and Measurement – Vulnerability Threat and Risk Weighting .... 8
Enterprise Configuration Delta Monitoring ............................................ 9
Policies and Procedures – Audit Consolidation and Security Awareness ........ 10
Summary ....................................................................................... 11
Introduction

IT security and compliance professionals at retail and other organizations involved in payment card processing face ongoing pressure to not only comply with the Payment Card Industry (PCI) Data Security Standard (DSS), but to ensure they also are keeping pace with rapidly shifting security threats. The risks associated with noncompliance and/or a security breach—including fines, litigation and reputation damage—are too great to ignore.

This white paper defines potential compliance and security gaps and identifies what effect these gaps can have on your organization. It also explores how a positive security solution can close these gaps to ensure the security of servers and endpoints, as well as compliance with PCI DSS. This will include a discussion of five core compliance controls:

1. Continuous audit and assessment of the PCI compliance validation process
2. File integrity control/file integrity monitoring and correlated contextual logging
3. Risk analysis and measurement of PCI compliance
4. Configuration delta monitoring
5. Policy and security awareness audit consolidation

The PCI Security Standards Council announced new guidance regarding application whitelisting and continual risk monitoring. See below for details.

Positive vs. Negative Application Security

The two approaches to system security most often discussed are ‘positive’ and ‘negative’ solutions. Both are entirely different in all of their characteristic behaviors. Signature-less security and signature-based security are two examples of positive and negative security rules, respectively.

Both positive and negative security approaches operate according to an established set of rules. However, positive, proactive security is based on a known/good model and focuses on what you want to allow on your systems according to a business process. Every rule added to a positive security model increases what is known and allowed.

Negative security is based on a set of bad applications that you already know exist and it denies access based on what was previously identified as bad. Negative security policies do not take into account how the application works; they only notice what accesses the application and if that access violates any negative security patterns or signatures.
Continuous Audit and Assessment of the PCI Compliance Validation Process

PCI DSS provides prescriptive recommendations about the type of security solution an organization should use to protect its endpoints against malware and vulnerabilities. The aim of many requirements, including the popular Requirement 5.x, is to ensure systems are not exposed to ANY potential vulnerability—and to account for “evolving malware threats”—that can endanger the integrity of the server/endpoint and risk the compliance state.

While PCI DSS 3.0 still calls for the use of antivirus (AV) software, this is a negative tool that worked in the early days of viruses and worms but has been proven ineffective against today’s dynamic advanced threats and zero-day attacks.

**December 2014 Update:** The PCI SSC has released new guidance, as detailed in a recent article, indicating a shift away from antivirus software in favor of application control, or whitelisting.

Negative solutions are constantly scanning and patching updates to the signature set, a process that is highly CPU-intensive and negatively affects endpoint performance, which in turn can negatively affect SLAs and increase administration requirements and costs. This can have significant consequences for today’s organizations, which need to be agile. The retail business cycle, in particular, requires a solution that consumes very few system resources so response times are acceptable and don’t negatively impact customer satisfaction.

Industry experts, including assessors and auditors associated with the PCI SSC, recognize the shortcomings of negative solutions and are now recommending that organizations make the shift to positive solutions that provide advanced protection against today’s threats. Many standards organizations have endorsed positive solutions, and businesses worldwide recognize them as the best practice for locking down and protecting POS systems, kiosks, servers and remote desktops/laptops.

A positive solution (1) requires very few system resources, (2) can proactively drive a security policy to the endpoints by allowing only trusted applications to run, and (3) detects, identifies, ranks, eliminates and blocks malicious software. In addition, a positive solution can:

- Provide visibility into what’s happening on all IT assets
- Categorize the risks, without relying on signatures
- Verify the security controls
- Perform continuous monitoring of these controls
- Provide reports that enable IT to take proactive, corrective actions and/or prove compliance

In summary, this is the first validation shift. The transition from a negative solution to a positive solution, such as Carbon Black Protection, provides continuous protection, enables full visibility of your in-scope enterprise assets to measure risk, verify controls, and continuously monitor endpoints.
Figure 1 is an illustration that shows how Cb Protection drift reporting is used to monitor good and bad change on an endpoint, and how that change can affect the compliance stance of the enterprise. Cb Protection can determine:

Approved drift — that which you expect to see as part of the regulatory policy (patches, updates and approved files with no known vulnerabilities that can affect or risk your compliance stance).

Unapproved drift — that which you do not want on your systems as it can affect your compliance policy and risk. Unapproved drift appears in two ways:

1. A new marked vulnerability within the Cb Protection regulatory template event view

2. An unexplained compelling compliance event caused by the introduction of a file or system that is out of compliance with the regulatory Cb Protection policy.

FIM/FIC Reporting
While segmenting cardholder data from the rest of the network is not required by PCI DSS, PCI does "strongly recommend" network segmentation so as to avoid the entire network being considered in-scope of the PCI DSS assessment. With Cb Protection you can easily scope 'out' PCI DSS information in order to quickly ensure the security of the infrastructure, while avoiding the complexity of the applicable compliance metrics usually associated with attempting to filter data intelligence on the back end.

Cb Protection offers file integrity control mappings to enable control and file integrity monitoring. This eliminates much of the white noise and enables you to address a smaller segment of the compliance scope, making for an easier—and more cost-effective—assessment. Cb Protection provides mapping of and templates for required critical files to control and monitor across many different operating systems.

**Correlated Contextual Logging**

Cb Protection takes the integrity process for PCI a step further, eliminating excessive noise by providing
correlated contextual logging out to third-party security information and event management solutions. Both the proof and measure on the integrity of the audit logs, as well as advanced threat information, is provided in direct context to the compelling event. This adds substantial value to the monitoring requirements of PCI DSS.

Figures 3 and 4 are examples of Cb Protection file integrity control and monitoring. The first is the "compliance enforcements" view. The list of enforcement events demonstrates that Cb Protection can enforce by policy. You use this to (1) demonstrate to assessors that you are enforcing policy and (2) correlate into the events that are critical to your business to build context around your data. This is a very powerful feature. It helps lower the administrative burden of compliance pre-assessment data gathering and produces a contextual report of all enforcements that are out-of-line with the compliance policy.

Figure 3: Compliance Enforcements view

Figure 4: File Integrity Control view, showing critical changes
Risk Analysis and Measurement — Vulnerability Threat and Risk Weighting

Requirement 6.1 of PCI DSS requires that covered organizations establish a process to identify and assign a risk ranking to files or versions of files with any security vulnerabilities. Cb Protection provides a logical, proactive alternative to threat and risk analysis of in-scope PCI assets, and assists in the collection of risk metrics utilizing the templates already incorporated within the solution.

Cb Protection introduces threat-driven policies to pinpoint the exact data that needs to be identified and quantified under Requirement 6.1. By providing a real-time analytic feed from Carbon Black Threat Intel, along with a comparison of the corporate golden image, Cb Protection will produce a risk analysis out of the gate, without the need for manual intervention.

Cb Protection also eliminates risk because it will block malicious code if the deemed risk is too high. The solution can apply risk ranking in the form of thresholds that will abide by the local PCI policy set within the central PCI risk posture that is used to drive enforcement across all the in-scope endpoints. The trust policy determines if a given execution is allowed to happen, and if the file in question measures higher on the risk scale than the PCI policy allows, it will not be able to execute. A complete record of the interaction along with all attributes are kept within the local event repository and can be utilized for re-assessment, investigation and auditing.

Cb Protection’s ability to both monitor the in-scope endpoints, as well as analyze the in-scope data, enables the total remediation of vulnerabilities on any of the endpoints to which it is applied. If a vulnerability appears, or is already on a new machine brought into the protected zone, Cb Protection will analyze it in real time, identify it, stop it from affecting the integrity of corporate systems through propagation or distribution, and lock it down in order for security staff to quickly remediate the situation in preparation for audit or inspection.

Cb Protection provides data that also can be used to categorize risk across the infrastructure, enabling you to set priorities and assign objectives in order to bring systems in line with compliance and security requirements.

Figures 5 and 6 are examples of reports that assess risk across the enterprise.

![Figure 5: Risk Trend Report](image1)

![Figure 6: File Risk Measurement Report](image2)
Enterprise Configuration Delta Monitoring

To help you meet Requirements such as PCI DSS 6.4, which stipulates that organizations “follow change control processes and procedures for all changes to system components,” Cb Protection provides enhanced, up-to-date file asset inventory information that enables you to build business intelligence around these file assets. This information is combined with Cb Threat Intel data, threat and malicious inventory, and IT trust data in order to help you proactively monitor your enterprise systems.

Through advanced delta comparison of endpoints, you can easily sift out any activity that is deemed untrustworthy or has a negative effect on your compliance posture. By utilizing threat and risk metrics across the enterprise, you can compare endpoints individually, or to a group of endpoints and get a snapshot of the status of the systems (see Figure 7). More importantly, you get a view into the status of all activity across the enterprise and the ability to control assets and enforce compliance.

Cb Protection’s delta monitoring also helps you comply with Requirement 2.2.2, as you are able to restrict the services, protocols, etc., to those that are necessary, and identify any that are not.

Figure 7: Comparison of endpoint risk across the enterprise
Policies and Procedures —
Audit Consolidation and Security Awareness

To help ensure compliance with Requirement 12.1, and assure that the organization is focusing on and proving out the BAUs (business as usual activities), 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.

Cb Protection adds a higher level of awareness and audit to PCI DSS. Using available templates, you can ensure that end users are directed to review and acknowledge their review of security and compliance policies. Cb Protection also can provide an audit trail confirming that the policy was consumed.

With Cb Protection’s high enforcement level, an end user is notified when an attempted application installation is outside of the internal security compliance policy. The application is blocked and the end user is notified and requested to both accept and acknowledge the policy. Once the end user clicks the necessary links, instructions or check boxes, he/she is allowed access to the endpoint. All of the associated audit information is archived within the Cb Protection repository and is used to produce a full compliance report for the validation process, audit or assessment.

Figure 8 illustrates several of Cb Protection’s compliance validation features that help enforce an audit compliance policy. This sample notification window helps compliance stakeholders understand their responsibilities and provides audit proof that the compliance policy is being disseminated, consumed and followed.
Summary

Cb Protection helps IT security and compliance professionals proactively prove continuous compliance with PCI DSS and avoid steep noncompliance fees and damage to their brand. While every organization is unique, all organizations face similar challenges in ensuring that PCI DSS requirements are met.

Cb Protection addresses the convergence of compliance and security, providing one agent that enables visibility, detection, response and protection and can automate and manage compliance for PCI-DSS.

About the Author

Christopher Strand is senior director of compliance and governance at Carbon Black. With more than 20 years of information technology experience, Strand is Carbon Black’s subject-matter expert on enterprise network and application security solutions and how organizations can deploy positive security to maintain and improve their compliance posture. Previously, Strand held security/compliance positions at Trustwave, Tripwire, EMC/RSA and Compuware. He holds a bachelor’s degree in environmental engineering from the University of Guelph in Ontario, Canada, and completed post-graduate work in IT and development at Humber College in Toronto.