5 Steps to Reduce the Complexity of PCI Security Assessments
Today’s PCI compliance landscape is one of continuing change and scrutiny. Given the number of recent high-profile breaches in the retail space, the pressures will only increase and organizations are facing significant questions, such as:

- What are the best practices for PCI assessments?
- How does an organization best use limited resources to meet compliance requirements and, more importantly, provide a truly secure environment?

In 2013, just over half (51%) of companies subject to the PCI Data Security Standards (PCI DSS) passed seven of the twelve requirements, and only 11.1% passed all twelve. These figures support the difficult nature of successful PCI assessments; getting the protection, monitoring, vulnerability scanning and enforcement elements right takes time and resources.

Further complicating the issue is the fact that, while compliance is the goal, it’s well-known that compliant does not always mean secure.

The matrix of individual requirements included in many North American compliance regulations (e.g., PCI, SOX and HIPAA) will vary slightly, but the underlying data or business logic that is used to demonstrate adherence to these controls is essentially the same. By taking a positive security approach that arms their endpoints, organizations can reduce the complexity of assessments, while lowering administration costs and accelerating attainment of a compliant – and secure - environment.
The following five steps outline a path to meet these goals.

1. **Adopt a proactive approach in order to speed up pre-compliance data gathering.**

   Compliance is not a one-time event or an annual project. While easier said than done, an ideal compliance program is constant and proactive, and allows IT to know and see what is on every endpoint and server. In many organizations, IT finds it difficult to know and identify all the assets and data needed to meet compliance requirements. This can lead to a "fire-drill" mentality during the data-gathering phase, as manual classification; discovery based on negative models (scanning and re-scanning data); and little business intelligence developed against data all lead to a cumbersome and static process.

   Instead, a proactive approach relies on defined trust sources and focuses on the business process of data gathering. Combining trust policies (IT trusted systems and applications) with business policies leads to a more efficient way to categorize data. This process helps to rapidly identify the “bad” by whitelisting and filtering out trusted files/processes, which in turn drives and optimizes prevention techniques and helps to enforce security and compliance policy. This process also delivers the ability to focus and prioritize on the high-risk files for security and compliance.

2. **Stop scanning your in-scope environment.**

   Over-reliance on scanning is an operational norm and, thus, a challenge many organizations face and, as malware evolves, scanning is increasingly ineffective. In addition, scanning provides volumes of data but in many cases little actionable information, leading to increased use of resources for little or no gain. Within PCI DSS 3.0, Requirement 5 recognizes the limits of scanning and suggests that scanning alone, even if one thinks they are identifying 100% of potential malware, won’t meet requirements.

   Traditional negative security is scan-based, and by nature is limited in its ability to identify and protect. Positive security, with real-time monitoring and threat intelligence capabilities delivered via the cloud, provides the full continuum of the threat landscape, and a real-time enforcement engine with endpoint and network integration. In addition, positive security can cover all network assets, including third-party elements. As recent history has shown, breaches often start via third-party access points, so a positive security posture can help identify and mitigate these threats.

3. **Apply real-time vulnerability and threat analysis to all in-scope systems.**

   Requirement 6 of PCI DSS 3.0 states that an organization needs to “establish a process to identify security vulnerabilities…and assign a risk ranking.” Further, these rankings have to identify all “high risk” and “critical” vulnerabilities, and patches must be installed within one-month, including unsupported systems. In a traditional scan-based system, this requirement is difficult to meet as it requires manual risk assessment. This manual scanning process can be based on news groups, updates and feeds, and is subject to human error.

   Compare this with a positive security approach using real-time assessment vulnerability analysis and response, delivered via the cloud and updated constantly. This process is not reliant on manual updates, includes recent modifications and alerts, and can cover unsupported elements of a system, e.g., Windows XP. This alternative delivers active intelligence in real time, allowing security teams to see the entire kill chain in seconds; from vulnerable processes to a persistent malicious service. In a scan-based environment, this could take days or weeks to re-create using traditional tools, during which time the organization is vulnerable to attack.
Control change rather than analyze it to plan and provide for continuous support of all the in-scope systems all the time.

PCI assessments, like many IT projects, can fall victim to “scope creep," where the original and mandated task grows exponentially to encompass extra work that may or may not produce fruitful results. One way to manage this issue is to focus on critical system and file changes, and avoid “analysis paralysis.” This can be done by filtering out all the irrelevant changes on the front-end, thus allowing the team to zero in on only authorized critical changes that are relevant to security and compliance.

When the IT team is able to scope out large amounts of data and focus instead on in-scope compliance endpoints, they can introduce control over critical infrastructure files, leading to better audit and chain of custody, and a lower administrative cost of change analysis. With this concentrated approach, systems and processes can be identified, protected and updated in real-time, enabling a more secure environment. This also allows the team to provide compensating controls even for systems at or near end-of-life. By focusing on, and protecting the critical data in legacy systems, IT teams can extend security coverage for endpoints. This strategy:

- locks down a full audit of all inventory;
- extends compliance coverage; and
- provides compensating controls for requirements 6.1 and 6.2, as well as a full audit and reporting of endpoint security.

Such a whitelisting approach is called out in the PCI FAQs*, which state:

“Examples of controls that may be combined to contribute to an overall compensating control include … properly-configured application whitelisting that only permits authenticated system files to execute, and isolating the unsupported systems from other systems and networks.”

*Available at [http://www.pcistandards.org/faq](http://www.pcistandards.org/faq)

Ensure you can validate and confirm coverage of the security policy across the Business-As-Usual processes.

As highlighted in the PCI DSS “Best Practices for Implementing PCI DSS into Business-as-Usual Processes,” the ability to enforce the standard on a continuous basis is critical. With proper enforcement, IT teams can ensure their systems are protected, and the burden of the assessment process is reduced with audit evidence that stakeholders are aware of the DSS requirements (see Requirement 12).

A positive security approach assists the organization in proving that PCI DSS policy has been distributed to stakeholders, as evidence is collecting that addresses the adherence to PCI DSS policies at mandated points across the enterprise. A positive security approach distributes these mandates to each stakeholder, ensuring the ownership and understanding of responsibilities. This provides audit information and an assurance that standards have been met and the organization is compliant, while ensuring that compliance data is collected within one place.
SUMMARY

PCI assessments are a key element for all covered entities and, if conducted properly, can lead to not just a compliant organization but a secure one. But in order to make this a reality, careful planning, adequate resources and the proper positive security approach need to be focused on the task. These five suggestions are a good starting point for a positive PCI assessment, but a constantly-aware and proactive approach to PCI compliance and a positive security strategy is the best preparation for a PCI assessment.

Visit [www.carbonblack.com](http://www.carbonblack.com) or contact us at [PCIConsultation@carbonblack.com](mailto:PCIConsultation@carbonblack.com) for more information or a free PCI consultation.