

## THE PCI STANDARD: A MANDATE FOR CARDHOLDER SECURITY

It's no secret that cardholder data presents a tempting target for cybercrime. That's why the major credit and debit card providers have established the Payment Card Industry (PCI) Data Security Standard, which applies to all merchants and service providers that store, process or transmit cardholder data.

The PCI Standard mandates basic security best practices that include implementing and ensuring the effectiveness of defenses and procedures including firewalls, anti-virus applications, security patches, intrusion detection and prevention systems (IPS and IDS), and end-user awareness and incident-response programs.

## Security testing for PCI validation and compliance

The PCI Standard requires the same set of security measures for all merchants and service providers, regardless of transaction volume or card acceptance channel (e.g., in-store vs. e-commerce). Organizations must not only implement these measures but also validate that they are working effectively to achieve PCI compliance.

Using CORE IMPACT Pro to test your security measures is one of the easiest things you can do to comply with and validate multiple PCI requirements. IMPACT Pro enables you to run regular, controlled and safe data breach attempts against your network, endpoint and web application security infrastructure. As a result, you can quickly and easily demonstrate whether your security defenses and response plans are in-place and working as mandated by the PCI Standard. What's more, regular IMPACT Pro security tests help to ensure the ongoing efficacy of your overall security posture.

## CORE IMPACT ensures compliance with the following mandates:

### Requirement 1.1.1

Establish a formal process for testing network connections and changes to the firewall.

With CORE IMPACT Pro, you can stay on top of potential security exposures created by new network connections and changes to firewalls and other defensive infrastructure. The product's penetration testing capabilities incorporate industry-standard best practices into a repeatable methodology for testing the security of evolving network and endpoint systems, as well as web applications.

### Requirement 2.2

Assure that system configuration standards address security vulnerabilities and are consistent with industry-accepted system hardening standards.

CORE IMPACT Pro is continually updated with the latest Commercial-Grade Exploits designed to safely test your organization's exposure to newly discovered vulnerabilities in operating systems and services. Each exploit tests as many target OS configurations and methods of attack as possible. You can also test live cardholder systems with confidence, since exploits are designed to prevent service disruptions or alert you when disruptions could occur.

### Requirement 5.1.1

Ensure that anti-virus programs are capable of detecting, removing, and protecting against malicious software.

You can test the effectiveness of your entire security infrastructure, including anti-virus programs and other PCI-mandated applications, with CORE IMPACT Pro. In addition, the product makes it easy to tune security applications by testing them against specific attacks and generating reports that help you identify necessary patches and configuration issues. IMPACT Pro also documents each test with audit trails that you can compare against those from security applications to determine if attacks are being detected as expected.

### Requirement 5.2

Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

### Requirement 6.1

Ensure that all system components and software have the latest vendor-supplied security patches.

CORE IMPACT Pro gives you confidence in the integrity and effectiveness of all patches. After installing a patch, you can test its effectiveness by using IMPACT Pro to safely execute the attack that the patch was designed to stop. In addition, you can ensure that customer data remains protected by re-testing your entire network for new vulnerabilities potentially exposed by the patch.

### Requirement 6.3.1

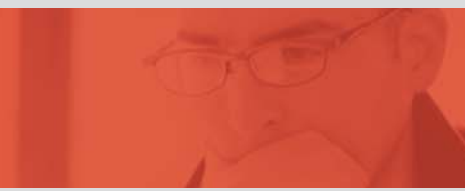
Test all security patches and system and software configuration changes.

**Meet the penetration testing requirement - and more ...**

PCI Requirement 11.3:

*Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification ...*

Testing your security infrastructure and policies with CORE IMPACT Pro allows you to directly comply with Requirement 11.3 while validating compliance with a number of additional PCI mandates (see table).



### Requirement 6.6

Ensure web applications exposed to the public Internet are protected against the most common types of malicious input.

CORE IMPACT Pro is the only automated penetration testing software solution that allows you to test both commercial and proprietary web applications for cross-site scripting, SQL injection (including blind SQL injection) and PHP file inclusion vulnerabilities. In addition to meeting PCI compliance requirements, IMPACT Pro helps organizations stop privilege escalation attacks on front-end web applications that can be used to tunnel through to back-end data.

### Requirement 11.1

Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

CORE IMPACT Pro enables you to determine if attackers can actually exploit network, endpoint or web application\* vulnerabilities. By automating previously manual and expensive processes, IMPACT Pro considerably shortens the testing process and reclaims the cost of hiring outside consultants or developing custom exploits in-house. The product also documents each test in a variety of reports that assist with auditing and compliance validation.

### Requirement 11.2

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

Scanning applications can provide a key component to the vulnerability management process by offering an understanding of your organization's potential vulnerabilities. Penetration testing with CORE IMPACT Pro builds on this process by identifying which vulnerabilities are real and determining if and how they can be exploited. Test results are presented in IMPACT Pro's PCI Vulnerability Validation report, which can help you prioritize remediation efforts, effectively allocate security resources, and satisfy auditing requirements.

### Requirement 11.3

Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification ...

Using IMPACT Pro provides direct compliance with the network-layer penetration testing section of Requirement 11.3. It also addresses top web application testing elements of the mandate, including SQL injection, cross-site scripting and PHP file inclusion. By regularly testing your security posture with IMPACT Pro, you can stay ahead of the latest threats and validate your compliance with other PCI mandates. This simplifies the compliance process, whether you need to complete the PCI Self-Assessment Questionnaire or prepare for an external audit by a Qualified Security Assessor.

*\*The PCI Standard allows you to perform in-house penetration testing, regardless of your merchant or service provider level.*

### Requirement 11.4

Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems ... Keep all intrusion detection and prevention engines up-to-date.

While intrusion detection and prevention systems can detect and block unwanted network traffic, they require ongoing, custom configuration and regular updates (e.g., new attack signatures) to be effective. CORE IMPACT Pro allows you to test the effectiveness of these defensive technologies and gives you the information you need to configure them to properly detect and protect against the latest threats.

### Requirement 12.9.2

Implement an incident response plan and test it annually.

In addition to emulating external network threats, CORE IMPACT Pro enables you to safely target end users with phishing, spear phishing and other social engineering attacks. You can simulate a full range of data incidents and evaluate how defensive infrastructure, employees and contractors react. The product's client-side reports provide a full audit trail of each end-user test, including phishing emails sent, exploits launched, test results, and details about compromised users and their systems.

## Learn More

Want to learn more about security testing and the PCI compliance? Please visit our website ...

<http://www.coresecurity.com/PCI>

### Headquarters

41 Farnsworth St.  
Boston, MA 02210  
Ph: (617) 399-6980  
Fax: (617) 399-6987

[www.coresecurity.com](http://www.coresecurity.com)