

THE GROWING OBLIGATION TO PROTECT CONSUMER INFORMATION

The payment card industry presents a prime target for hackers seeking access to credit card numbers, social security numbers and other consumer information. This problem jeopardizes any organization that conducts payment card transactions, including retail merchants, online vendors, universities, government agencies and payment processors. Network security breaches can bring direct financial losses, threaten company reputations and customer loyalties, attract negative press, and trigger significant fines and penalties. These risks necessitate unwavering protection of your customer data.

THE PCI STANDARD: A MANDATE FOR NETWORK SECURITY

Ensuring network security is no longer an option for merchants and payment processors. That is why MasterCard® and Visa® have established the Payment Card Industry (PCI) Data Security Standard, which applies to all members, merchants and service providers that store, process or transmit cardholder data. The PCI Standard offers a single approach to safeguarding sensitive information for all card brands and is endorsed by Discover® and American Express®.

The PCI Standard outlines required data security measures, including network penetration testing. Specifically, Requirement 11.3 calls for network penetration testing to be performed at least once per year and, more importantly, after any significant infrastructure or application upgrade or modification. Penetration testing solutions, such as CORE IMPACT, provide the information you need to both protect customer data and comply with the PCI Standard.

ACHIEVE PCI COMPLIANCE AND PROTECT YOUR CUSTOMERS WITH CORE IMPACT

CORE IMPACT is the first automated, comprehensive penetration testing product for assessing specific information security threats to an organization. Specifically, Requirement 11.3 calls for network penetration testing to be performed at least once per year and, more importantly, after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

You can safely exploit network weaknesses, replicate the kinds of access an intruder could achieve, and identify actual attack paths that must be eliminated.

PCI Standard Requirement 11.3:

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

The Consequences of Non-Compliance

Payment card companies impose fines, up to \$500,000 per incident, on any non-compliant organization that is compromised. There is a \$100,000 penalty for failing to report an incident, and over 20 states have legislation requiring disclosure. Regardless of your current merchant level, a single breach automatically subjects your organization to the most stringent and extensive regulations.

CORE IMPACT ENSURES COMPLIANCE WITH THE FOLLOWING PCI MANDATES:

Requirement 6.1

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

CORE IMPACT gives you confidence in the integrity of all patches. After installing a patch, you can test its effectiveness by using CORE IMPACT 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 6.2

Establish a process to identify newly discovered security vulnerabilities ... Update your standards to address new vulnerability issues.

The PCI Standard requires quarterly vulnerability scans for merchants at Levels 1-3. However, vulnerability assessment and management tools uncover all possible network weaknesses, leaving you guessing as to which pose real, imminent threats to customer data. CORE IMPACT quickly distinguishes real vulnerabilities from false positives, eliminating the expense of addressing conceptual vulnerabilities and allowing IT resources to focus on actual network threats.

Requirement 11.1

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

CORE IMPACT is the only product that tests network security by determining if attackers can actually exploit a vulnerability. By automating previously manual and expensive tests, CORE IMPACT considerably shortens the testing process and reclaims the cost of hiring outside consultants or developing custom exploits in-house. Flexible reporting enables users to generate CORE IMPACT's reports as HTML, PDF, Microsoft Word® and other popular formats that can easily be customized and shared with auditors and other parts of the organization.

Requirement 11.3

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

Requirement 11.4

Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

We run CORE IMPACT regularly and frequently, which enables us to fix vulnerabilities as they are uncovered. This gives us confidence in our network security and means we're better prepared for our annual external penetration test - which we pass with flying colors.

Major University

CORE IMPACT enables us to quickly and easily determine which vulnerabilities are false positives, allowing us both to save time and to focus our remediation efforts. This helps us cost-effectively meet the PCI standards.

Major Retailer

CORE IMPACT comprehensively evaluates your entire network against the latest threats, providing direct compliance with this requirement. By allowing you to launch multiple, simultaneous attacks, CORE IMPACT also improves the speed and ease with which you evaluate network defenses.

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. Penetration testing is the only way to truly test the effectiveness of these defensive technologies against the latest threats. CORE IMPACT provides an updated, automated solution for safely probing network defenses and revealing tangible risks to customer data.

STAY AHEAD OF NETWORK THREATS AND KEEP PACE WITH PCI REGULATIONS

The assaults on consumer information, and the mandates for its protection, show no signs of slowing. Attacks are evolving in sophistication and automation, the number of vulnerabilities expands every day, and technology is increasing both the connectivity among users and the complexity of networks. In response, most industry experts predict that regulations will become stricter, placing greater demands on merchants and payment processors. At the same time, basic compliance with industry standards doesn't necessarily mean that your network is 100% impenetrable. CORE IMPACT allows you to comply with expanding PCI regulations and protect customer data against evolving threats, without compromise.

KEY BENEFITS FOR MERCHANTS AND PAYMENT PROCESSORS

Meet regulatory requirements and avoid penalties

Comply with the PCI Standard as well as other regulations including GLBA and Sarbanes-Oxley.

Prioritize remediation efforts

Enable IT staff to focus on real vulnerabilities by obtaining information on actual attack paths.

Avoid network outages and downtime

Prevent breaches that consume IT resources, hamper employee productivity and threaten revenues.

Preserve corporate image and customer loyalty

Avoid data incidents that put your organization's goodwill and reputation at stake.

Increase staff productivity

Automate penetration testing and eliminate the need to manually create exploits.

Justify existing security investments

Evaluate the effectiveness of other security products in detecting and preventing attacks.

Headquarters

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

www.coresecurity.com