



Achieving PCI Compliance at the Point of Sale
Using Bit9 Parity™ to Protect Cardholder Data

PCI: Protecting Cardholder Data

As the technology used by merchants and their partners has evolved, card fraud has become more sophisticated. Any business that stores or transmits cardholder account data is a potential target, and recent data indicates that 4 out of 5 cardholder breaches occur at the point of sale.

In response to this evolving threat, the major credit card companies (American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International) have created a set of security standards to protect their customers from security breaches and identity theft.

What are the PCI Data Security Standards?

The Payment Card Industry Data Security Standards (PCI DSS) includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

By following the standardized, industry-wide procedures of PCI DSS, organizations can:

- Protect their customers' personal data.
- Boost customer confidence through a higher level of data security.
- Insulate themselves from financial losses and remediation costs.
- Maintain customer trust and safeguard the reputation of their brand.
- Provide a complete 'health check' for any business that stores or transmits customer information.

The Pressure to Comply

Retailers are under heavy pressure to comply with PCI, and it does not look like that will ease any time soon. If anything, the payment industry is more intent on enforcement than ever before. And while only a third of the largest companies were considered compliant at the end of 2006, that number is expected to grow to between 50% and 75% by the end of 2007, with smaller companies following suit.

As of June 30, 2007, the PCI Data Security Standards are scheduled to be enforceable. This means that companies who are not compliant with the standard could face financial penalties. At an expected rate of \$10,000 to \$100,000 per month, these fines will place a heavy burden on organizations that have not complied.

Learn More

- > See a product demonstration
[▶ http://www.bit9.com](http://www.bit9.com)
- > Browse our resource library
[▶ http://www.bit9.com/resources](http://www.bit9.com/resources)
- > Watch a recorded webinar
[▶ http://www.bit9.com/webinars](http://www.bit9.com/webinars)
- > Contact Bit9 today!
[▶ http://www.bit9.com/contactme](http://www.bit9.com/contactme)

PCI Data Security Standards (DSS)

Build and Maintain a Secure Network

- Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
- Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3:* Protect stored cardholder data
- Requirement 4:* Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5:* Use and regularly update anti-virus software
- Requirement 6:* Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7:* Restrict access to cardholder data by business need-to-know
- Requirement 8:* Assign a unique ID to each person with computer access
- Requirement 9:* Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10:* Track and monitor all access to network resources and cardholder data
- Requirement 11:* Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12:* Maintain a policy that addresses information security

Facts About Data Protection

- Recent data indicates 4 out of 5 cardholder data breaches occur at the point of sale.
- Fines for non-compliance with PCI range from \$10,000 a month to \$100,000 a month depending on circumstances.



■ Achieving PCI Compliance at the Point of Sale *(Continued)*

Protecting Data Where It's Most Vulnerable

The PCI Data Security Standards are designed to thwart identity theft and fraud by establishing controls around how customer data is handled within a company's information architecture. These guidelines place requirements on systems that stretch from the central data repository all the way to the point of sale.

As companies work their way through these guidelines, many are discovering their greatest exposure is at the endpoint. PCs deployed in the field, at stores and retail outlets, and at remote locations are more susceptible to hackers and malicious software.

Computers in stores are often used for many different purposes—not just transactions—and therefore need to provide access to a wider group of individuals. These PCs are frequently offline making centralized patching or auditing difficult, and other systems management processes are hindered by the simple lack of on-site IT resources. All of this creates a difficult environment for establishing security.

Whitelisting: Ease the Security Burden

Let's face it—your store employees are just not data security experts. Your security policies must be simple if you want them to be implemented effectively. This will make it easier for both your field staff and your central IT department to achieve your compliance requirements.

Bit9 protects data at these endpoints where it is most vulnerable by locking down PCs to a standard software configuration known as a "whitelist." Any and all unauthorized software is prevented from running and access to personal storage devices is brought under control. Malware, spyware, and rogue applications and devices are all blocked to ensure the integrity of the computer and its critical data.

Because this whitelist is controlled centrally, your PCs can not be modified in the field. And your store personnel never need to be given responsibility for complex IT tasks such as updating signatures, patching systems, or manipulating security configurations.

■ How Bit9 Helps You Comply with the PCI Data Security Standards

Here's how Bit9 addresses the PCI Data Security Standards.

Build and Maintain a Secure Network

PCI DSS Specification	Bit9 Functionality
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).	By controlling the installation and execution of software, systems are prevented from drifting from their desired state. From a central console, vulnerable software can be centrally identified, making it easy to prioritize patch activity.
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).	By creating a whitelist of approved software, Bit9 ensures only approved services and software are allowed to run on any Windows-centric device.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	By creating a whitelist of approved software (scripts, drivers, subsystems, web applications), Bit9 ensures only approved services and software are allowed to run on any Windows-centric device.



How Bit9 Helps You Comply with the PCI Data Security Standards *(Continued)*

Maintain a Vulnerability Management Program

PCI DSS Specification	Bit9 Functionality
<p>5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers).</p> <p>5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.</p>	<p>Bit9 blocks any software that is not pre-approved to run. A cryptographic hash (a unique identifier) is taken for each new file that is written to disk. Before this file is allowed to run, the hash is created and then compared to a list of approved hashes that were created by an automated software approval process. If the hash is on the list of approved hashes, the file is allowed to run. If the hash is not on the list of approved hashes, it is completely blocked from execution. If a file is changed, it changes the cryptographic hash for the file and because the hash is no longer on the list of approved hashes, it too will not run. While there are obvious benefits to Bit9's approach to preventing viruses, spyware, and adware, there are also significant benefits from preventing illegal and unlicensed software from running.</p>
<p>5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>Unlike traditional anti-virus solutions that need constant signature updates to stay effective, Bit9's non-signature antivirus approach continuously blocks all unwanted software without the burden of keeping signature files up to date. Ultimately, Bit9's non-signature antivirus approach eliminates zero-day attacks.</p>
<p>6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.</p>	<p>Because Bit9 has a software inventory of all software currently installed on Windows computers, a Bit9 user can centrally identify the presence or absence of vendor-supplied security patches.</p>

Regularly Monitor and Test Networks

PCI DSS Specification	Bit9 Functionality
<p>6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.</p>	<p>Every new file is looked up in the Bit9 ParityCenter™ knowledgebase of more than 2 billion file records and hundreds of thousands of known vulnerabilities to determine the threat level of the newly discovered software. Bit9 ParityCenter is updated daily with legitimate and potentially malicious software.</p>
<p>6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:</p> <ul style="list-style-type: none"> • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security. • Installing an application layer firewall in front of web-facing applications. 	<p>Bit9 has the ability to act as an application firewall on web-facing applications. Any new application or program that is not pre-approved is blocked from installing or executing. This ensures the highest levels of system and application security. This whitelisting approach is the safest way to ensure only approved software is allowed to run.</p>



■ How Bit9 Helps You Comply with the PCI Data Security Standards *(Continued)*

Implement Strong Access Control Measures

PCI DSS Specification	Bit9 Functionality
7.1 Limit access to computing resources and cardholder information only to those individuals whose jobs require such access.	Portable storage devices can be an easy source of data leakage and loss. Bit9 can set controls on the ability to read/write/execute software on portable storage devices, preventing information leakage and accidental loss of sensitive, confidential information.
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	When a user logs into a system, the user will be restricted to run only the applications that have been pre-approved. All other applications will be restricted from use based on the user's policy and need to know.
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.	Bit9's device control policies ensure only authorized staff are allowed to copy cardholder data to portable storage devices, helping to control the distribution of cardholder data.
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	Bit9's device control policies ensure only authorized staff and computers are allowed to copy cardholder data to portable storage devices, controlling the storage, accessibility, and portability of confidential information.

Regularly Monitor and Test Networks

PCI DSS Specification	Bit9 Functionality
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	To prevent malicious software, every executable that is introduced (downloaded/installed/copied) to a Windows computer is tracked to a specific user on a specific computer. To prevent data leakage, every file (executable or data file) that is copied to and/or from a portable storage device is tracked to a specific user on a specific computer.
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Bit9 Parity blocks unauthorized writes to log data files and ensure only authorized processes write to log data files.
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Installing an application layer firewall in front of web-facing applications.	Bit9 will log all activity related to new software and alert should an application begin to propagate across a number of computers over a time period. All new applications that get written to a system get logged and then compared to the Bit9 ParityCenter knowledgebase of 2 billion database records to gauge the threat level of the file.



■ How Bit9 Helps You Comply with the PCI Data Security Standards *(Continued)*

Maintain an Information Security Policy

PCI DSS Specification	Bit9 Functionality
<p>11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files.</p>	<p>Bit9 Parity prevents unauthorized modification of critical system files and content files and ensures only authorized processes can write to critical system files and content files.</p>
<p>11.6 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files and configure the software to perform critical file comparisons at least weekly.</p>	<p>With Bit9, only approved software is allowed to run. Should a hacker tamper with the bits of an application, it would change the cryptographic hash of the file and therefore render the new application inoperable. Ultimately, this protects hackers from tampering with applications to make them perform malicious activity.</p>
<p>12.5.5 Monitor and control all access to data.</p>	<p>Data leakage is a serious problem and difficult to control. Only approved users should have access to data. By controlling who can and cannot read/write data to portable storage devices, a layer of control is added to prevent data leakage. Malicious applications and spyware can also gain unauthorized access to data. Bit9 allows only approved software to run and malicious software is therefore unable to gain access to confidential information.</p>

- To learn more about how Bit9 can help your organization become PCI compliant, contact us at +1.617.393.7400 or contact@bit9.com.

About Bit9, Inc.

Bit9 is the leader in enterprise application whitelisting. The company's award-winning solutions provide real-time configuration audit and change control to improve the security and integrity of Windows computers. Unlike legacy reactive security solutions that try to scan and prevent the never-ending list of unauthorized software, the Bit9 Parity™ solution ensures only authorized and trusted applications are allowed to run, eliminating the risk and operational costs associated with malicious, illegal and unauthorized software. For forensics and complete visibility into applications, Bit9 provides the Bit9 Global Software Registry™, the largest most complete source of information to help identify, authenticate and trust software. Bit9 customers include companies in a wide variety of industries, such as government agencies, retail, financial services, healthcare, e-commerce, and telecommunications.



Bit9, Inc.
 266 Second Ave.
 Waltham, MA 02451
 p: +1.617.393.7400
 f: +1.617.393.7499
www.bit9.com