

Securing Endpoints for PCI DSS Compliance

Volume 1 • Number 2 | June 2012



KEY TAKEAWAYS

from this Bit9 Threat Advisor

- ✓ Constant updating of antivirus signature libraries can degrade performance and leave endpoints vulnerable to advanced attacks.
- ✓ Businesses are at risk of steep noncompliance and regulatory fines, which can range anywhere from \$10,000 to \$100,000 per month.
- ✓ Adopting a positive, trust-based security model improves protection against advanced attacks and provides auditable, continuous compliance with PCI DSS standards.



Get Started Today

The Bit9 Parity Suite 5-Day Free Trial is designed for IT security and forensics professionals interested in closing the endpoint security gap left open by traditional reactive security solutions. This cloud-based trial is a complete working deployment of the Bit9 Parity Suite 6.0, which includes the industry's leading Application Whitelisting solution. Sign up today at www.bit9.com/freetrial.

Advanced Threats and Endpoints: A Double Whammy

Endpoints, such as point-of-sale (POS) systems, ATMs, and pay-at-the-pump terminals, are the gateways through which credit card data and other personally Identifiable Information (PII) pass to the enterprise. But because these endpoints can be weak links in an organization's network, they are routinely used by criminal entities to gain a foothold in the infrastructure. The main reason businesses are often unable to adequately protect these systems is due to their continued reliance on ineffective antivirus solutions.

While the financial and market implications of a breach of customer data are worrisome in their own right, any organization processing credit cards must also grapple with continuous Payment Card Industry Data Security Standard (PCI DSS) compliance—or face increasing penalties.

POS devices, ATMs, and pay-at-the-pump terminals together were involved in 85% of data breaches, yet “96% of victims subject to PCI DSS had not achieved compliance.”

Verizon 2012 Data Breach Investigations Report

This Threat Advisor examines the double whammy associated with inadequate endpoint protection: PCI DSS noncompliance penalties and greater risks to the integrity of customer data. But the other, often unnoticed, danger is that malicious entities can use their ability to access endpoints as a way to launch an Advanced Persistent Threat (APT). *And any organization that processes credit card data at distributed endpoints is increasingly susceptible to these attacks.*

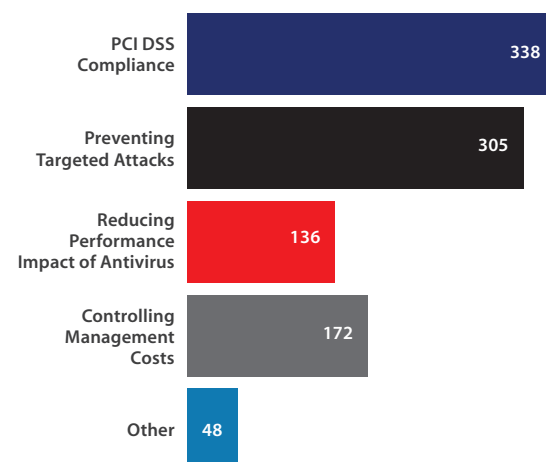
On the following pages, we'll look at how advanced attacks exploit gaps in endpoint antivirus protection and examine what you can do to better maintain PCI DSS compliance, secure your customers' personal information, and protect your revenue stream.

What, Me Worry?

In a 2011 Bit9 survey of 722 retail businesses, the top two IT/security concerns were maintaining PCI DSS compliance (47%) and preventing targeted attacks (42%). And 78% of the respondents were either not confident, or only somewhat confident, in their ability to stop an APT.

Their concern is warranted: In 2010, 90% of businesses fell victim to a cyber security breach at least once.¹ And, 85% of the breaches that occurred in 2011 involved POS terminals and servers.²

What is your biggest IT/Security concern today?



\$ FINANCIAL SERVICES COMPANY ACHIEVES GREATER APPLICATION CONTROL AND PCI DSS COMPLIANCE

Customer Challenge

The Chief Information Security Officer (CISO) of a financial services organization was concerned about the increasing frequency and sophistication of malware incidents—as well as the longer, undiscovered “dwell time” of each attack. However, the blacklisting strategies of the company’s existing antivirus solution could not effectively identify these threats, putting the organization’s ability to meet PCI DSS standards at risk.

Bit9 Solution

Bit9’s project team analyzed the organization’s endpoint environment and organized it into three distinct groups categorized by the sensitivity of data handled and the rate of change. The first group, which consisted of about 75% of all endpoints, was placed into Bit9 Parity’s application control environment.

Results

With the help of Bit9 Parity, malware infections have declined dramatically, and the company has not had to reimage a single machine. In addition, not only does Parity block more than 80 new nuisance applications per month, it has also dramatically reduced the analysis required to determine what malware had caused a breach, and what its impact might have been.



MORE SUCCESS STORIES

For more real world examples of how organizations meet the challenges of advanced threats, download [Advanced Threat Protection in Action](#).

The PCI Security Standards Council is responsible for the development, management, education, and awareness of the PCI DSS standards.³ There are four levels of PCI compliance based on the number and type of transactions a merchant processes each year. The definition of what volumes pertain to each level, however, is defined by the individual payment card brand. For example, Visa sets Level 1 as over 6 million transactions processed per year, Level 2 at 1 to 6 million transactions, Level 3 at 20,000 to 1 million e-commerce transactions, and Level 4 at up to 1 million transactions (and a maximum of 20,000 ecommerce transactions).

The June 2011 update to the PCI DSS Standard increased pre-audit pressure on all businesses, especially those classified as Level 2. Tightening this process has increased the costs of *maintaining compliance*, as PCI DSS requires both monthly and quarterly scans and reporting.

As endpoint networks continue to change—both in size and complexity—the pre-audit process becomes even more essential to controlling compliance costs. Different endpoint security solutions produce more and more noise, making it harder for businesses with distributed endpoint environments to control costs and maintain compliance. And being unprepared to adopt newer payment technologies, such as Europay, MasterCard, and Visa (EMV) chip and pin advancements, only increases an organization’s liabilities.

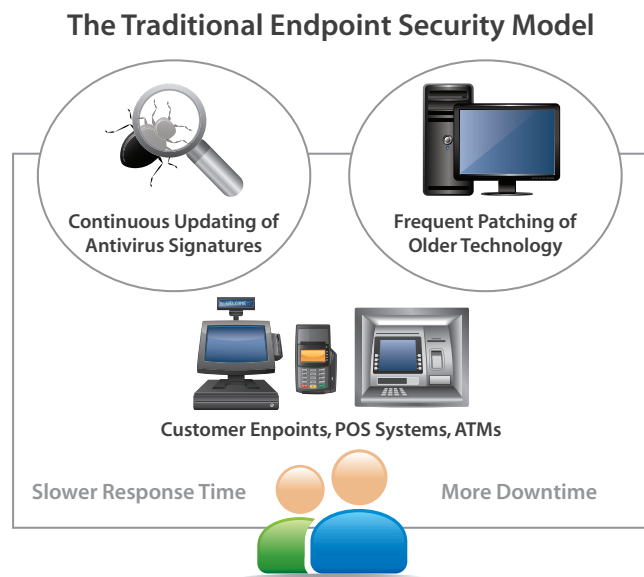
When Endpoints Leave You Open to Advanced Attacks

A large number of endpoints regulated by PCI DSS are running older, sometimes unsupported operating systems. But because they represent a substantial investment, many businesses, understandably, want to leverage them for as long as possible. However, patching these operating systems—if fixes are even available—can be time consuming and disruptive.

Endpoint protection has traditionally relied on a negative security model—one that depends on a list of known threats in an antivirus software library. Unfortunately, the ease with which malware can be acquired and tweaked has led to an exponential growth in antivirus signatures. According to report by Symantec Corporation, 403 million new variants of malware were created in 2011, representing a 41% increase over 2010.⁴ Because of the exploding size of antivirus libraries, and the need for constant updating, this model eats up precious processing time and slows down customer service at the endpoints.







For retailers and other customer-facing organizations, there are times when endpoint use is especially heavy—when transactions simply must flow through them at maximum levels. At these times, businesses often “freeze” antivirus updating and patching activities to maximize processing time. What’s more, expanding expectations for 24/7 business availability have also cut into network service windows, putting more pressure on IT.

Unfortunately, attackers are often well aware of the periods when endpoints might be more open to attack—such as the holiday shopping season.



ADDITIONAL RESOURCES FROM BIT9

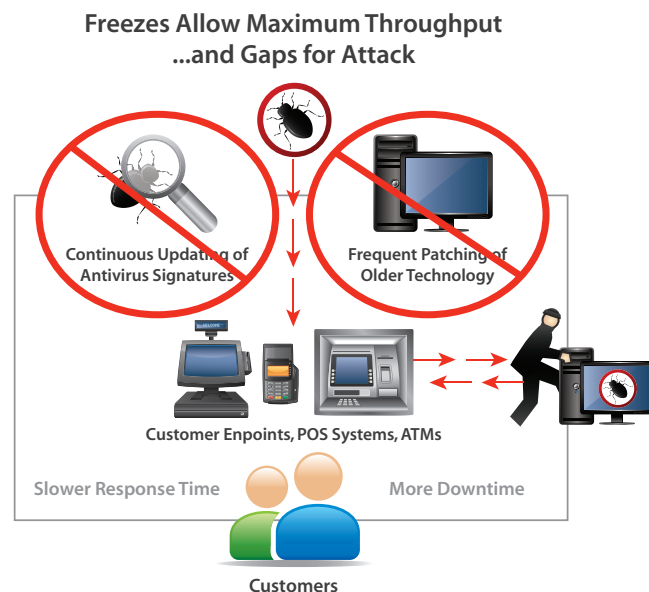
Below are some key resources to help you get started with the assessment of your current security environment.

-  View the web seminar [Beyond PCI Compliance to Advanced Threat Protection](#)
-  Read the articles in the [E-Guide](#) to learn about the 12 mandates for PCI DSS compliance and how to navigate through the PCI compliance landscape.
-  View the [Bit9 whiteboard video](#) on improving PCI DSS compliance, while increasing performance and eliminating antivirus solutions on retail endpoints.
-  Learn more about [Advanced Protection for Retail Systems](#) with Bit9 for POS Systems.
-  Read Chris Strand's blog: [Negative Security Model: 3 ways It's Not Making the Grade for Retail PCI](#)
-  Download [Getting \(and Staying\) Ahead of Advanced Threats: A Workbook for Assessing Your Environment for Advanced Threat Protection](#)

Negative Security Models Leave Dangerous Gaps

In addition to impacting endpoint availability and IT service windows, there are additional, serious liabilities introduced by a reliance on a negative security model. Employing a blacklist of "known" threats does not address the proliferation of today's more dynamic malware, especially when there are 55,000 new malware signatures distributed *every day*.⁵ Unless one is *continually updating* the endpoint blacklist, there will most certainly be periods of time when newer viruses will not be recognized on endpoints.

The reliance on a negative model is particularly problematic in the case of APTs, which tend to be customized for a specific target. According to a Gartner report, only 76% of advanced malware is actually detected by antivirus solutions.⁶ And, by definition, endpoint security based on blacklisting cannot detect zero-day attacks, which are commonly used in the initial stages of an APT.



Securing Endpoints Using a Positive Security Model

A positive, trust-based security model provides a more adaptive and proactive security posture. It begins with levels of trust. You need to have a clear, up-to-date understanding of the trustworthiness of all software running in, and attempting to enter, your enterprise. Two best practices in trust-based threat protection are IT-driven trust and cloud-driven trust. IT-driven means users rely on IT's track record and reputation for secure operations to trust what is pushed out to the endpoints. Cloud-driven means software can be pulled from the Internet and loaded onto endpoints only when it is above a threshold of trust defined by IT. Using these best practices, you can assign levels of trust by user or group within your network of endpoints.

...and Helps Enable PCI DSS Compliance

Endpoint security built on a positive model using defined levels of trust can help demonstrate continuous controls for PCI DSS standards, such as requirements 5 (Maintain a Vulnerability Management Program) and 11 (Protect Critical System Files).

Deploying Bit9 Parity on your endpoints reduces the risk associated with outdated data files, retail holiday freezes or reduced service windows, transactional activity, and zero-day attacks. The solution ensures that only trusted software can run on your endpoints (and, if implemented, on servers), preventing unauthorized modification of critical system and content files.

Maturing PCI DSS requirements, most recently the tighter pre-audit processes, are increasing the complexity and costs of maintaining compliance. Whether you opt for a vended QSA or an ISA approach, you must continue to show that there are no gaps in your overall security posture. By providing greater knowledge of, and reporting on, endpoint activity, Bit9 Parity helps provide the information required during the pre-audit process.

Advanced Threat Protection Platform

TRUST
 Build your enterprise trust with Software Reputation

DETECT
 Identify your risk with a real-time sensor

PROTECT
 Stop the APT with trust-based application control

MEASURE
 Monitor risk and compliance with a reporting and analytics engine

ASSESSING YOUR CURRENT SECURITY POSTURE

Prior to implementing a phased IP protection plan, you should assess your current security environment for risk and value of all your assets. There are four fundamental areas of best practices that make up an Advanced Threat Protection Platform: Trust, Detect, Protect and Measure.

TRUST: Taking a pro-active security posture begins with trust. You need to have a clear, up-to-date understanding of the trustworthiness of all software running in and attempting to enter your enterprise.

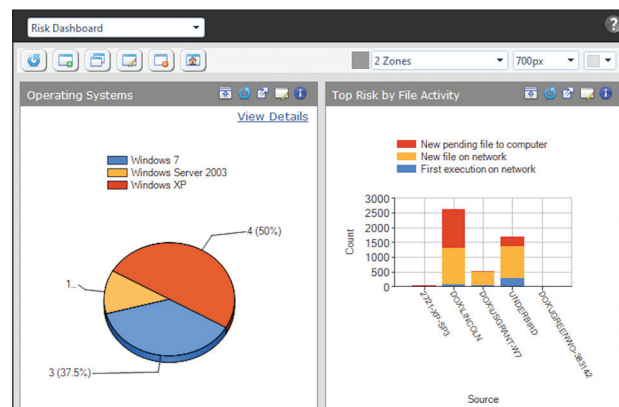
DETECT: You need to understand what is arriving, executing and propagating throughout your infrastructure, in as close to real time as possible, so you can identify and protect against untrusted software, applications and devices.

PROTECT: How dynamic, automatic are the protection controls and routines you have in place for applications in your environment? How responsive can you be enforcing user and context-based policies?

MEASURE: What reporting capabilities are in place to continuously monitor your security posture and make changes based on your evolving threat landscape? How timely and automatic is reporting?

And if your organization is somewhat smaller, Bit9 can help you better prepare for the SAQ. Bit9 Parity's constant endpoint monitoring and standard reports will help you build the business intelligence needed to achieve compliance around PCI DSS requirement 10 (Regularly Monitor and Test Networks).

Bit9's file integrity control capability tracks all changes and events by user, blocks unauthorized activities, and ensures that only authorized processes can write to log data files. You can leverage this controlled user interaction to enforce your security policies and educate employees. And, all event logs are captured and stored, providing a full audit trail and report on all activity and giving you further evidence that users are complying with your policies.



Bit9 Parity integrates with Security Incident and Event Management (SIEM) consoles to provide immediate intelligence about monitored assets and compelling security events—all from a single pane of glass. Integrating data with a SIEM allows you to more easily correlate endpoint events with other sources, such as an Intrusion Detection System (IDS), to filter out noise, reduce false positives, and enable your team to investigate and remediate incidents with greater speed and efficiency.

Summary

Constant updating of security patches and antivirus software libraries can slow response times and leave endpoints vulnerable to APT attacks. Endpoint protection based on detecting known malware is demonstrably ineffective—and has the potential to create numerous inefficiencies across your organization. Besides potential breaches of customer PII, a lack of endpoint control can also put you at risk for steep noncompliance and regulatory penalties—fines that can range anywhere from \$10,000 to \$100,000 per month.

Adopting a positive, proactive, trust-based security model provides better application control, improving endpoint protection against advanced attacks while helping to prove compliance with PCI DSS requirements.

Get Started Today

The Bit9 Parity Suite 5-Day Free Trial is designed for IT security and forensics professionals interested in closing the endpoint security gap left open by traditional reactive security solutions. This cloud-based trial is a complete working deployment of the Bit9 Parity Suite 6.0, which includes the industry's leading Application Whitelisting solution. Sign up today at www.bit9.com/freetrial.

1 Ponemon Institute.
 2 Verizon 2012 Data Breach Investigations Report.
 3 https://www.pcisecuritystandards.org/organization_info/index.php
 4 <http://www.symantec.com/threatreport/>
 5 McAfee
 6 Gartner – Burton IT1 Research. Application Control and Whitelisting for Endpoints, March 10, 2011.