FORTINET®

Complying with PCI SSF Without Sacrificing Customer Experience

What to Look for in a Security Solution

Table of Contents

Executive Overview 3

Introduction: The Need for Agile Security 4

Building a Secure Network: The Power of Integration 6

Protecting Cardholder Data, in Motion and at Rest 8

Managing Vulnerabilities: Building Security Into Development 9

Access Control: Effective Verification and Segmentation 11

Monitoring and Testing: An Ongoing Reality Check 12

Conclusion: A Proactive Stance Toward Security and Compliance 14

FORTINET®

Executive Overview

CIOs at retailers are pulled in two different directions. On the one hand, they need to build systems that connect with customers in a rapidly changing marketplace, while on the other hand, they need to comply with Payment Card Industry (PCI) standards to protect their organizations' brand and bottom line.

Accomplishing both goals requires a new approach to security. Rather than maintaining a disaggregated security architecture in which different tools are disconnected and manual correlation and threat response is required, CIOs should seek an end-to-end, integrated security solution. Such an architecture enables true automation of security policies and threat response, resulting in a more secure, more operationally efficient stance.

Integrating the security infrastructure is especially helpful for PCI compliance. Central control for the entire attack surface means that PCI data is protected both in motion and at rest. Identity verification and access control can protect PCI data from unauthorized internal access and from threat actors moving laterally within the network. And automated, on-demand reporting informs an organization of its current compliance posture and offers actionable advice on how to improve it. This eBook explores these elements of an effective PCI compliance posture and offers specific features and functionality to seek in a solution.

The Payment Card Industry Data Security Standard (PCI DSS) will be retired in 2022.
The PCI Software Security Framework (PCI SSF) will replace it and is already being phased in.[1]

Introduction: The Need for Agile Security

CIOs at retail organizations face intense competitive pressure as consumers' buying habits and preferences evolve rapidly. Creating and perfecting a consistent, omnichannel customer experience is a key to success.[2] Such an effort requires an agile IT infrastructure and innovation on the part of developers. For the CIO, keeping a sprawling network operating smoothly for customers and employees is a challenge in itself.

Another nonnegotiable priority is compliance with PCI standards. Noncompliance with the PCI Data Security Standard (PCI DSS) and its soon-to-be successor, the PCI Software Security Framework (PCI SSF), can bring hefty fines to retailers.[3] Even more devastating would be a breach of cardholder data caused by a lack of adherence to the security best practices that the PCI standards require. Beyond the cost of remediation and compensation of customers whose data was compromised, media coverage of such events diminishes brand value and reduces revenue.[4]

These two critical priorities compete for the CIO's time and resources, and at times it may seem that both goals cannot be accomplished at the same time. Even if the CISO's team is in a parallel silo, security issues impact the CIO's digital transformation (DX) initiatives that promise to bring better customer engagement. For example, manual security processes and disaggregated security tools can inhibit network performance and impact time to market for DX projects.

Whether or not a retail CIO is responsible for security, it is in that CIO's best interest for the organization to streamline its security operations so that security is as agile as the DX initiatives it is protecting.

Compliance with PCI DSS is headed in the wrong direction. Verizon's latest Payment Security Report found that just 52.4% of organizations were in full compliance with PCI DSS, compared with 55.4% the year before.[5]

Building a Secure Network: The Power of Integration

While compliance is sometimes viewed as a separate function from security, PCI standards are built around seven security best practices that can help protect cardholder data—as well as an organization's other IT assets. One thing that gets in the way of these best practices is the complexity of today's enterprise networks. Organizations now commonly operate in multiple public and private clouds, Internet-of-Things (IoT) devices are proliferating at the endpoint, and network traffic now often travels on the public internet.

As the attack surface has grown, security teams have scrambled to secure new elements using point solutions that do not talk to each other, and often use the vendor-provided security tools for each public cloud they operate in. The result is multiple security silos, and this creates gaps in visibility and control. This also means that preparing for PCI audits requires manual correlation of data from different security solutions, driving operational inefficiency and distracting team members from their core responsibilities.

The only way to address these inefficiencies is to build an end-to-end, integrated security architecture with transparent visibility of the entire network, plus centralized control of all security solutions. Such an infrastructure is required for true automation of security processes, which helps prevent the human error that is behind many data breaches. CIOs should look for these features in an integrated solution:

- Single-pane-of-glass visibility for the entire infrastructure
- Centralized control of all security tools
- Automated security policy management across the infrastructure
- Automated configuration management in the data center and across all clouds
- Automated threat detection and response, based on comprehensive threat intelligence powered by artificial intelligence (AI) and machine learning (ML)

Integration issues are among the top 3 security issues for 32% of CIOs, but 78% lack an end-to-end, integrated security architecture.[6]

Protecting Cardholder Data, in Motion and at Rest

If all cardholder data was permanently stored in a single repository within a corporate data center, it might be easier to protect. But retail transactions occur at multiple store locations and online, and consumers' payment card information routinely travels from place to place within a retail organization's network—including multiple public and private clouds.

This means that, in order to protect PCI data, an organization's entire attack surface needs to be protected. Retailers need to know all the specific locations where consumers' payment card information is stored and ensure robust protection to those places. And PCI data needs to be flagged and protected while in motion. CIOs should look for these features:

- **Next-generation firewall (NGFW).** Traditional firewalls focus their protection on the perimeter of a corporate data center and are inadequate with widely distributed networks. The NGFW should be configured to protect cardholder data, and configuration management should be automated to prevent human error.
- **Endpoint protection with secure remote and wireless access.** As retailers use customer-facing Wi-Fi networks in stores to facilitate the omnichannel experience, and often conduct transactions with wireless devices, endpoint security is more important than ever.
- **Web application firewall.** As cloud-based ecommerce platforms proliferate, protecting web applications is a matter of PCI compliance. Look for a solution with in-line, AI-based threat intelligence to intercept fast-moving threats.
- **Encryption of cardholder data in motion.** As network traffic increasingly travels on public networks, this is nonnegotiable.

Misconfiguration of policies is by far the biggest cause of firewall breaches.[7]

Managing Vulnerabilities: Building Security Into Development

The need to innovate quickly has prompted many retail organizations to embrace DevOps methodologies to improve operational efficiency and time to market for customer-facing applications.[8] But it also presents security risks. Even though DevOps teams identify many vulnerabilities before production, problems persist post-production: 92% of organizations have seen at least one vulnerability slip into production in the past 12 months.[9] For applications that process transactions, this can pose problems for PCI compliance.

Despite these serious concerns, competitive pressures mean that security shortcuts are sometimes taken. One study found that 52% of respondents indicate they are willing to minimize security controls to meet a business deadline, and 68% say their CEOs demand no "security-related delays."[10] This places two of the CIO's two biggest priorities—customer engagement and PCI compliance—on a collision course.

Fortunately, it does not have to be that way. It is possible to secure DevOps environments without slowing DevOps processes. Automation is a key to accomplishing this for at least two reasons. First, security processes must be automated to eliminate the manual processes that cause delays in DevOps cycles. Second, automation is necessary to respond to threats that move at machine speed, creating the potential of delays caused by a security disruption.

When researching integrated security solutions, CIOs whose organizations have embraced DevOps should ensure that they enable the automation of the following:

- The integration of security into DevOps orchestration tools and containers
- Automation of security policy management in the DevOps environment
- Threat detection and response in the DevOps environment

85%

of companies operate in multiple clouds, and 39% have deployed DevOps processes and value chains across these clouds.[11]

Access Control: Effective Verification and Segmentation

Historically, cyberattacks moved at human speed, with actual people manually executing each step of an attack.[12] Now, cyber criminals are automating many of their practices to enable them to carry out attacks at machine speed. The result: it still takes months for an organization to discover the typical breach, but exfiltration of corporate data can now occur in a matter of minutes.[13] In other cases, threat actors penetrate quietly, and then move laterally around a network undetected until they can intercept the login credentials for a critical system.[14]

These trends mean that access to PCI data should be tightly controlled. Gone are the days when a username and password provided adequate protection—or when it was okay to leave a default administrator password in place on a system.

PCI data should be segmented from the rest of the network, but dynamic networking means that segmentation itself is more complex than it used to be. Further, the notion of trust is constantly changing, and thus binary, "yes/no" models of trust are no longer adequate. To control access to PCI data, CIOs should look for the following features in an integrated security solution:

- Inspection of both north-south and east-west traffic to prevent lateral movement by cyber criminals
- Intent-based segmentation, to align network segmentation with business outcomes and dynamic trust models
- Identity and access management that assigns a unique ID to each user based on role
- Two-factor authentication for critical systems such as PCI data repositories
- User and entity behavior analytics (UEBA) that identifies behavioral anomalies that might indicate access by malicious insiders or even unintentional exposure due to an insider

"Today's digital economy requires a security approach that allows data, applications, and workflows to move freely across a distributed network while avoiding an open environment where attackers can easily move and cause damage."[15]

Monitoring and Testing: An Ongoing Reality Check

To track and report intrusions, vulnerabilities, and other basic cybersecurity measures may seem obvious, but many companies do not do so. In a recent survey of CIOs at large enterprises, barely half of respondents said their organizations report on vulnerabilities and intrusions detected. It is likely that that many organizations forego basic tracking and reporting because doing so would require hours of manual work by already overwhelmed security staff to correlate the data in a digestible format. They likely reserve this "all-hands-on-deck" approach to reports required by auditors.

Having an enterprise view of an organization's security posture is important for several reasons, but PCI compliance tops the list for retail organizations. In addition, much of the data in transaction records is also subject to data privacy laws such as the EU's General Data Protection Regulation (GDPR) and the forthcoming California Consumer Privacy Act (CCPA).[17] It is incumbent on the CIO to regularly monitor and report on who accesses this data and for what reasons.

An integrated security solution should include the analytical tools to perform these assessments on demand, and executives should have access to a dashboard that summarizes their organizations' security and compliance posture at any given time. CIOs should look for the following features:

- Automated log management and real-time threat analysis
- Reporting templates for key standards like PCI, customizable to an organization's unique needs
- A tangible score that evaluates an organization's compliance against standards like PCI and includes comparisons against peer organizations
- Actionable recommendations on the prioritization of fixes to improve compliance

93%

of successful cyberattacks could have been prevented if routine scans and patches were implemented.[18]

Conclusion: A Proactive Stance Toward Security and Compliance

PCI compliance is all about following security best practices, and accomplishing it will improve an organization's security posture beyond the protection of cardholder data. Building an integrated security architecture not only simplifies audit preparation but also makes an organization safer in the following ways:

- By eliminating manual reporting, threat response, and other processes, security staff can focus on strategic initiatives.
- By automating threat-intelligence analysis and threat response, organizations can catch fast-moving threats before they cause a problem.
- By building security into the foundation of DevOps projects rather than adding it as an afterthought, vulnerabilities can be caught before they result in breaches.
- By effectively segmenting the network and inspecting all traffic—internal and external—organizations can ensure that only authorized people can view PCI data.
- By deploying centralized analytical tools, organizations can bolster their security in a strategic, prioritized manner.

The above enables CIOs to transform their security and compliance postures—from reactive to proactive. No longer will PCI compliance be seen as an annoying checkbox that must be checked. Rather, it will be a catalyst for a more resilient and secure enterprise.

"Bolt-on solutions are a thing of the past. Security is something you build, not something you do."[19]

[1] Laura K. Gray, "Just Published: New PCI Software Security Standards," PCI Security Standards Council, January 16, 2019.

[2] Peter Roesler, "New Survey Reveals What Consumers Want from Omni Channel Shopping Experience," Inc., May 28, 2018.

[3] "Fines for Non-compliance," PCI DSS Compliance, accessed August 8, 2019.

[4] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, March 6, 2019.

[5] "Verizon 2018 Payment Security Report," Verizon, accessed August 13, 2019.

[6] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[7] Asher Benbenisty, "Don't Go Once More Unto the Breach: Fix Those Policy Configuration Mistakes," Dark Reading, October 30, 2018.

[8] Bill Doerrfeld, "DevOps and Retail: Transforming Brick-and-Mortar to Brick-and-Click," DevOps.com, January 8, 2019.

[9] Ibid.

[10] "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, accessed May 22, 2019.

[11] Steve Cowley, et al., "Assembling your cloud orchestra: A field guide to multicloud management," IBM, October 2018.

[12] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

[13] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[14] Douglas Bonderud, "Lateral Movement: Combating High-Risk, Low-Noise Threats," Security Intelligence, June 11, 2019.

[15] Jonathan Nguyen-Duy, "Zero Trust is Not Enough: The Case for Intent-Based Segmentation," Network Computing, March 22, 2019.

[16] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[17] "3 Tips to CISO for Managing Privacy Laws Like GDPR," The CISO Collective, July 30, 2019.

[18] "Online Trust Alliance Reports Doubling of Cyber Incidents in 2017," Online Trust Alliance, January 25, 2018.

[19] David Linthicum, "Put security in DevOps first, not as an add-on," TechBeacon, accessed May 19, 2019.

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

399115-0-0-EN

August 24, 2019 2:06 PM

eb-compliance-with-pci-ssf