SOLUTION BRIEF

Fortinet PCI Compliance Solutions

Supporting PCI DSS and PCI SSF Without Sacrificing Performance or Innovation

Executive Summary

In a world of very thin profit margins, retail CIOs face pressures to innovate while maintaining compliance with payment card standards. But a disaggregated security architecture makes achieving both aims at the same time very difficult. The Fortinet Security Fabric provides a broad, integrated, and automated approach to security that covers the entire attack surface with single-pane-of-glass visibility and control. Reporting is automated, eliminating the mad scramble to prepare for audits that can distract team members from their core responsibilities. Further, the Security Fabric enables organizations to move to a proactive, risk management-based stance with actionable insights that assist with strategy.

"The breach or theft of cardholder data affects the entire payment card ecosystem. Customers suddenly lose trust in merchants ... Merchants ... lose credibility (and in turn, business)."[1]

Protecting PCI Data While Engaging Customers

For CIOs at retail organizations, compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the forthcoming PCI Software Security Framework (PCI SSF) are not optional. However, a piecemeal approach to security and compliance can result in operational inefficiencies that threaten the CIO's other duties—providing a functional, efficient network and delivering digital transformation (DX) initiatives that improve customer engagement. Such initiatives are often critical in a quickly evolving and intensely competitive marketplace.

Protecting a retail organization's overall infrastructure and complying with PCI SSF are not separate tasks. Doing both effectively involves a new, more holistic approach to security, built on an end-to-end, integrated security architecture with transparent visibility and centralized control.

Fortinet PCI Compliance Solutions: A Comprehensive Network Security Portfolio

Fortinet offers retailers a broad, integrated, automated security solution that supports PCI DSS and PCI SSF compliance while protecting the network from advanced threats. Automation of key security processes frees up security team members' time to focus on strategic priorities, while improving protection against threats that move at machine speed. The following elements of the Fortinet security solution support retail organizations as they strive to protect PCI data:

- **Integrated security fabric.** The Fortinet Security Fabric enables seamless integration of all security elements across the entire attack surface. It features full, single-pane-of-glass visibility and centralized control. In addition to Fortinet's broad and comprehensive security toolset, Fabric Connectors enable the integration of third-party products sold by Fortinet Fabric-Ready partners. In addition, organizations can develop their own integrations with a robust representational state transfer application programming interface (REST API).

  The Security Fabric is powered by FortiGate next-generation firewalls (NGFWs), which deliver protection at every point of sale—including wireless and ecommerce. They protect the entire infrastructure, including the data center, public and private clouds, and all connections between store locations. And every solution in the Security Fabric benefits from threat intelligence powered by artificial intelligence (AI) and machine learning (ML) from FortiGuard Labs.

- **Reporting and analysis for audit preparation.** PCI audits no longer need to be an "all-hands-on-deck" emergency. Logs from all Security Fabric solutions are automatically aggregated and reconciled with automated, customizable reports. And, as the PCI framework delineates, complying with PCI requirements is easier with customizable policy management and configuration management.

- **Endpoint, application, and user protection.** From checkout stands to the warehouse, protecting endpoints and verifying users is critical to protecting sensitive assets. Fortinet delivers next-generation endpoint protection that includes secure remote access with built-in virtual private networks (VPNs), single sign-on (SSO), and two-factor authentication—all integrated into the Security Fabric for automated compliance tracking and reporting. This can be combined with identity and access management, user and entity behavior analytics (UEBA), and intent-based network segmentation for comprehensive verification of users at every access attempt.
- **Proactive risk management.** Moving an organization from a reactive stance toward security to a proactive one, accurate information and analysis is key. The Fortinet Security Rating Service provides a compliance check to ensure operations comply with auditor requirements, a tangible score against PCI DSS standards and against peer organizations, and actionable information about how to prioritize and resolve PCI DSS compliance issues. Additional analysis and event management tools add to this comprehensive view of where an organization stands and what steps need to be taken to bolster security and compliance.

Conclusion

Retail CIOs face pressure from many angles. Competitive pressures often require innovation in the areas of customer engagement and omnichannel experience—which in some cases may be a key to an organization's profitability in an industry with razor-thin profit margins. Nevertheless, complying with PCI DSS—and soon, PCI SSF—is mandatory. Tackling PCI in a comprehensive, strategic way actually brings about operational efficiencies that make DX initiatives more effective. The Fortinet Security Fabric, with its broad, integrated, and automated security architecture, can bring this about.

[1] "Why Security Matters," PCI Security Standards Council, accessed August 8, 2019.

August 23, 2019 1:28 PM

399156-0-0-EN

D:\Fortinet\Work\2019\August\082319\sb-fortinet-pci-compliance-solutions