Simplifying PCI Compliance
An Affordable, Easy-to-Implement Approach Using the Cybera Network Services Platform
Executive summary

For most retailers, the technology burden of maintaining PCI compliance can be overwhelming. Instead of focusing on core business functions, you must understand hundreds of pages of guidelines, standards, and procedures—along with a confusing array of technology and vendor options.

Still, you likely end up asking business-critical questions such as:

- How do I go about implementing PCI compliance?
- Is there an affordable way to achieve system-wide PCI compliance?
- Can I scale out PCI compliance to multiple business sites without onsite IT resources?
- How do I sustain PCI compliance in a constantly evolving threat landscape?

This paper is designed to help you answer those questions without having to sort through endless regulatory documents or become a security expert. It all starts with the Cybera® Network Services Platform, an intelligent solution to help retailers rapidly deploy, secure, and optimize their applications and services.

*The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that manage branded credit cards from the major card schemes.*
Essential Enabling Practices

Simplification starts with minimizing the technical friction associated with PCI compliance and establishing consistent security standards across your distributed enterprise. The most important considerations when developing a security plan are:

1. Separating PCI and non-PCI data and applications
2. Encrypting data in flight and data at rest
3. Managing user access to data
4. Employing multi-layer security

Separating PCI and Non-PCI Data and Applications

PCI standards advocate scoping your IT infrastructure to identify all components located within or connected to the card holder data (CHD) environment—and then reducing the scope by isolating the CHD environment from the rest of the network. Although this aspect of PCI leads to a focus on the network, it’s important to address both your network and your applications.

For instance, every application should have access to only the relevant data for that particular application. You can take a pragmatic approach to PCI compliance through cloud-managed micro-segmentation, partitioning every app into its own virtual network to isolate it from other apps (including payment apps, loyalty apps, corporate apps, franchisee apps, IoT apps, etc.). This approach allows security policy enforcement on a per-application basis, thereby reducing the risk of lateral breach propagation across applications (see Figure 1).

Figure 1.
The cloud-managed Cybera Network Services Platform allows security policy enforcement on a per-application basis.
Encrypting Data in Flight and Data at Rest
Sensitive data typically appears at many points in your network, from a point of sale (POS) card scanner and mobile applications to payment information entered on a web page, transmitted through your network, and held in various storage systems. As EMV (a technical standard for smart payment cards) gains wider adoption, counterfeit card fraud may be declining, but card-not-present fraud is surging. As a result, you should secure every source, destination, and path of sensitive data as part of your PCI compliance strategy.

Managing User Access to Data
Multi-factor authentication (MFA) safeguards data access through a variety of verification methods while satisfying the desire of users for simple logins. Using a centralized cloud-based network solution can help you ensure a scalable approach to policy configuration and enforcement across multi-site deployments. This type of solution can help you automate consistent security standards, eliminate manual configuration errors, and accelerate security updates across locations.

Employing Multi-Layer Security
PCI standards recommend using multiple security layers, including firewalls, encryption, malware protection, and antivirus protection. This defense-in-depth strategy should also include granular security policies customized for each application (instead of being applied to the entire network).

Sustainable, Affordable Deployment
Most retailers are looking for a sustainable PCI solution: an affordable, low-touch solution that delivers true application and network security. This is particularly important when securing networks that are prone to attack, such as those carrying sensitive CHD. Low-friction PCI compliance solutions can free up IT budgets currently being spent on maintenance, upgrades, and integration for more strategic revenue-focused initiatives that enhance the customer experience.

In fact, forward-thinking retailers who have few or no onsite IT staff are identifying innovative yet easy ways to enable PCI compliance for their networks. Many are deploying secure, software-defined WAN (SD-WAN) solutions.
These solutions accelerate secure business operations across multiple sites by consolidating many security and network functions (such as VPN, firewall, intrusion detection, and MFA) in a single device. Using a simple plug-and-play appliance that can be installed by onsite retail personnel with no IT/security training, you can avoid both the capital and operational expenses of costly and complex multi-device network solutions.

A cloud-managed SD-WAN solution enables you to:
• Centrally configure and enforce security policies across all locations for a consistent, standardized security approach
• Automate security updates so all remote locations receive them quickly, improving response times in a constantly evolving threat landscape
• Place the solution on top of your existing networks as a virtualized software layer, preserving existing network investments while optimizing application security and performance

Monitoring
Because monitoring is an important element of sustained PCI compliance, Cybera includes continuous network monitoring as part of its solution. When emerging or resurging threats are detected in one part of the network, a fast response can eliminate the immediate threats while the necessary security updates are proactively propagated throughout your distributed enterprise.

Scalability
Implementing these defense strategies can be daunting when working with traditional VPNs (which tend to be overly complex and labor-intensive) and MPLS (which is costly and can take months to get up and running). Both of these technologies can diminish your time-to-market advantage and delay your growth strategy.

The flexibility and scalability of a well-designed SD-WAN simplifies and automates this process to extend enterprise-grade, multi-layer security all the way to the edge of your network without requiring onsite IT and security professionals.

Cybera accelerates secure business operations across multiple sites by consolidating many security and network functions in a single device.
Going Beyond Checklist PCI Compliance

By being smart and proactive, you can embrace an affordable, secure, and PCI-compliant infrastructure that your retail locations can deploy on their own broadband connections in minutes—with no IT or security training. The resulting business benefits extend far beyond checklist PCI compliance solutions that might or might not be truly secure.

The ease of use and high performance associated with the Cybera Network Services Platform frees up time and dramatically reduces costs. As a result, you can redirect your IT budget and resources toward initiatives that enhance the customer experience—such as unified commerce, mobile payments, guest Wi-Fi, beacons, and other emerging technologies.

Learn more at www.cybera.com/pci.

<table>
<thead>
<tr>
<th>PCI DSS at a Glance</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goals</strong></td>
<td><strong>PCI DSS Requirements</strong></td>
</tr>
</tbody>
</table>
| Build and maintain a secure network and system | 1. Install and maintain a firewall configuration to protect cardholder data  
2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | 3. Protect stored cardholder data  
4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a vulnerability management program | 5. Protect all systems against malware and regularly update antivirus software or programs  
6. Develop and maintain secure systems and applications |
| Implement strong access control measures | 7. Restrict access to cardholder data by business “need to know”  
8. Identify and authenticate access to system components  
9. Restrict physical access to cardholder data |
| Regularly monitor and test networks | 10. Track and monitor all access to network resources and cardholder data  
11. Regularly test security systems and processes |
| Maintain an information security policy | 12. Maintain a policy that addresses information security for all personnel |

Footnotes

1 PCI Data Security Standard, December 2016