SIMPLIFY PCI COMPLIANCE FOR MULTI-SITE BUSINESSES

An Affordable, Easy-to-Implement Approach Using Secure SD-WAN
3 Climbing the Mountain of PCI Compliance
4 Which Comes First: Network or Applications?
5 Essential Enabling Practices
   Partition the Network End-to-end
   Encrypt Data In Flight and At Rest
   Employ Multi-layered Security
10 Sustainable, Affordable Deployment
11 Secure SD-WAN
12 Accelerate with Cloud-managed SD-WAN
13 Monitoring
14 Scaling
15 Scaling with Ease
16 Chicago Scoops Gets the Scoop on PCI Compliance
18 Beyond Checklist PCI Compliance
20 PCI DSS at a Glance
21 Next Steps
22 References
CLIMBING THE MOUNTAIN OF PCI COMPLIANCE

For most retailers, the technology burden of maintaining PCI compliance can be overwhelming. Hundreds of pages of guidelines, standards and procedures and a confusing array of technology and vendor options paralyze retailers who are wrestling with business-critical questions such as:

• How do I go about implementing PCI compliance?
• Is there an affordable strategy to achieve PCI compliance system-wide?
• Can I scale out PCI compliance to multiple sites without on-site IT resources?
• How do I sustain PCI compliance in a constantly evolving threat landscape?
WHICH COMES FIRST: NETWORK OR APPLICATIONS?

This primer will help you answer those questions without having to climb a mountain of regulations or becoming a security expert.
In an ironic application of the Pareto principle, while roughly 80% of breaches occur at the application level, 80% of security spending is focused on the network. Consequently, when someone asks us, “Should I focus on application security or network security?” we say, “Yes.”
ESSENTIAL ENABLING PRACTICES

This document offers a roadmap to minimize the technical friction associated with PCI compliance and establish consistent security standards across the brand for cross-franchise adoption.
PARTITION THE NETWORK END-TO-END

PCI standards recommendation:

• Scope the infrastructure to identify all components located within or connected to the cardholder data (CHD) environment
• Reduce the scope through segmentation to isolate the CHD environment from the rest of the network

This approach leads to a focus on the network when you should actually address both the network and the applications.
Why restrict partitioning to just applications that use CHD, such as POS and loyalty programs? Every application should have access to only the data relevant for that application. Enable a pragmatic approach to PCI compliance through cloud-managed micro-segmentation, isolating every app into its own virtual network.

- Enforce security policies per application
- Reduce the risk of lateral breach propagation
Encrypt Data
In Flight and At Rest

Sensitive data appears at many points in your network, from a POS card scanner to mobile applications to payment information entered on a web page, transmitted through your network, and stored in various systems. As EMV gains wider adoption, counterfeit card fraud may be declining, but card-not-present fraud is surging. Every source, destination, and path of sensitive data must be secured.
EMPLOY MULTI-LAYERED SECURITY

PCI standards recommend multiple security layers. These mature technologies should be considered:

- Segmentation
- VPN
- Multi-factor authentication
- IDS/IPS
- Firewall
- Encryption
- Malware protection
- Antivirus protection

This defense-in-depth strategy should be launched with granular security policies customized per application instead of applied to the entire network.
Most retailers are looking for a sustainable PCI solution, i.e. an affordable, low-touch solution that achieves true application and network security. This is particularly important when securing networks prone to attack, such as those carrying CHD. Low friction PCI compliance solutions free up retail IT budgets currently spent on maintenance, upgrades and integration (these make up a whopping 81% of IT costs) for more strategic revenue initiatives that drive the customer experience and direct revenue growth.
SECURE SD-WAN

• Accelerate secure operations across multi-site businesses
• Consolidate multiple security and network functions—VPN, firewall, IDS/IPS, MFA, malware protection, antivirus protection—in a simple device that can be installed by on-site retail personnel without IT or security training
• Avoid both the capital and operational expenses of costly and difficult to maintain multi-device network solutions
ACCELERATE WITH CLOUD-MANAGED SD-WAN

• Configure and enforce security policies centrally
• Automate updates to all locations for a consistent, standardized security approach
• Maximize system-wide adoption
• Respond to the evolving threat landscape quickly
• Deploy on top of existing networks as a virtualized software layer, preserving network investments while optimizing application security and performance
MONITORING

Monitoring is an important enabler for sustained PCI compliance. Cybera includes continuous network monitoring as an essential component of the managed, secure SD-WAN service. When emerging or resurging threats are detected in one part of the network, a response can eliminate that threat, and updates can be proactively propagated to the rest of the network.
Implementing defense strategies can be daunting when working with a traditional VPN, which is complex and labor intensive, and MPLS, which is costly and can take months to get up and running. These technologies can diminish time-to-market advantages and add unnecessary delays to your growth plans.
SCALING WITH EASE

The flexibility and scalability of a properly-designed SD-WAN simplifies and automates this process to extend enterprise-grade, multi layered security to the edge of the network without requiring on-site IT and security professionals.
Through acquisitions and organic growth, Chicago Scoops expanded their footprint to span 31 locations across 10 states at a very rapid clip of one month. “Most acquired stores had minimal security systems in place,” said Chicago Scoops president, Kyle Welch. “There were stores with unprotected Wi-Fi, and the residential internet access was shared on the same connection as the payment network.”

Welch considered security as essential to the business as sanitary food-handling practices. “We wanted to be proactive about protecting our customers and brand from day one.”
With no in-house IT expertise, Chicago Scoops needed a simple, uniform approach to protect their CHD environment, reduce their data breach exposure and achieve PCI compliance at two levels.

• Standardize security across all locations using an easy, template-based approach that can scale for future store growth while still being able to handle franchise exceptions as they invariably arise
• Secure connectivity inside each store regardless of the existing network

Chicago Scoops turned to Cybera to enable sustainable, affordable PCI compliance.
The elements of managed, secure SD-WAN come together to enable an affordable, secure, PCI-compliant infrastructure that your retail locations can deploy on their own broadband connections in minutes with absolutely no IT or security training. The benefits go beyond checklist PCI compliance solutions that may or may not be truly secure.
The ease of use and performance associated with an SD-WAN solution frees up time and dramatically reduces cost. Franchisees and owners can channel budget and time toward innovation where it matters, in the core business. Deploy customer-experience-enhancing initiatives, such as unified commerce, mobile payments, guest Wi-Fi, beacons and other emerging technologies that directly drive revenue growth. Significant reduction in TCO frees up the budget to pay for them.
## PCI DSS AT A GLANCE

| Build and maintain a secure network and systems | 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 |
NEXT STEPS

For more information on the advantages of managed, secure SD-WAN and tips on selecting the best option, see the blog

REFERENCES


ABOUT CYBERA

Cybera is a leading provider of secure, software-defined WAN (SD-WAN) solutions to many of the world’s top enterprises and has been named a Gartner Cool Vendor and recognized 7 times by Inc. 5000 as one of America’s fastest growing private companies.

Cybera provides a simple solution for the growing complexity distributed enterprises face at remote locations by automating application-centric security and performance in the cloud and providing greater customer choice and faster time-to-market through best-of-breed partnerships and services. By virtualizing security functions in the fabric of the network, Cybera offers advanced enterprise-grade security for any location, no matter how remote.

For more information visit www.cybera.com