A PRACTICAL GUIDE TO MERCHANT CYBERSECURITY:

Understanding how PCI DSS, Point-to-Point Encryption (P2PE), Next-Gen Firewalls, and Advanced Threat Protection work together to secure your business.

Netsurion™
Powering Secure and Agile Networks

"I'm thinking we'll switch to P2PE so I won't need anything else to protect my business."

"My point-of-sale (POS) system is PCI compliant so I'm all set."

"My bank said I'm PCI compliant already by using their payment processing services."

"My business is too small. Nobody is going to hack my POS."

Chances are you've heard one or more of these phrases, or perhaps you've uttered them yourself. Cybersecurity is complex enough as it is. But merchants, particularly those in the retail, restaurant, and hospitality space, are dealing with misinformation that further compounds the complexity, causing undue frustration and intolerable levels of risk.

The goal of this whitepaper is to clearly outline cybersecurity concerns of the merchant business, untangle the web of overlapping technology solutions and compliance regulation half-truths, and provide clear practical guidance to implementing a reasonable cybersecurity strategy.

Security Considerations for Merchants

Let's begin with a breakdown of the broad topic of "cybersecurity". What are the areas of concern for a merchant when it comes to protecting data and IT assets?

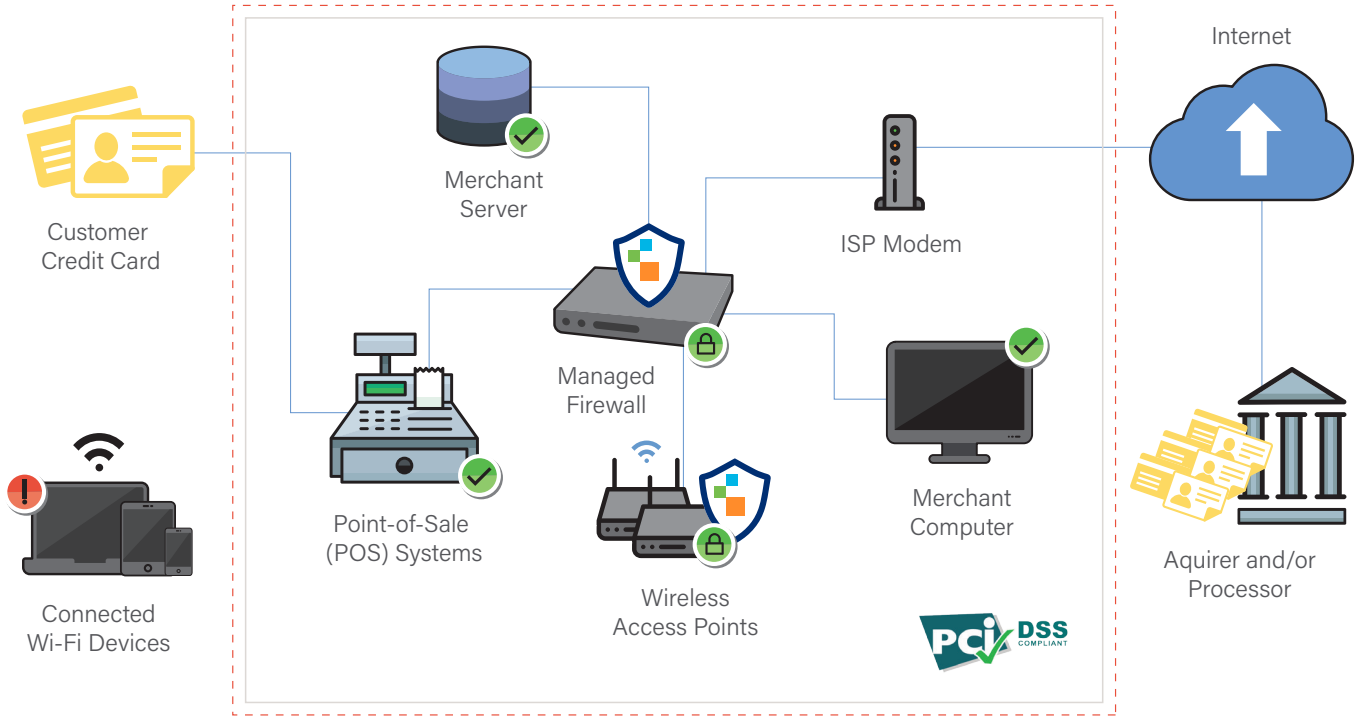
Point-of-Sale (POS) and the Cardholder Data Environment (CDE)

While there are other areas of concern, let's first talk about the primary area of concern for merchants – the CDE. This is the group of IT systems that process, store, and/or transmit cardholder data or sensitive payment authentication data. The POS system is one of those systems, perhaps the most important, in the CDE. Cardholder data includes the Primary Account Number (PAN) plus any of the following:

- Cardholder name
- Expiration date
- Service code

It is crucial that adequate network segmentation, which isolates the CDE from other systems, be implemented.

Retail, restaurant, and hotel merchants suffered the greatest from POS intrusions in 2016. The study included 212 incidents. (Verizon 2017 DBIR)



SEGMENTED CARDHOLDER DATA ENVIRONMENT (CDE)
The group of IT systems that process, store, and/or transmit cardholder data or sensitive payment authentication data including the Primary Account Number (PAN), cardholder name, expiration date, and/or service code.

POS intrusions continue at an alarming rate and are indiscriminate in their targets. Large brands and independent merchants alike are at risk of POS malware, ransomware, and other advanced persistent threats.

The Bottom Line: Don't cut corners when securing the CDE. By virtue of processing transactions at a POS system, you are vulnerable. It's not worth the risk. A multi-layered security strategy to protect your CDE should include managed network security services and monitoring, data encryption technology, EMV technology, and advanced threat protection – all backed by adherence to the Payment Card Industry Data Security Standard (PCI DSS) compliance practices. We'll discuss these further below.

Retail Experience Technologies

$

Businesses are at different points in their digital transformation: 73% agree there is a business need to prioritize technology, 66% plan to invest in IT infrastructure and digital leadership, 72% expect to expand their software development capabilities. (Dell Technologies-2017)

There's no doubt that as a merchant, competition is fierce. The need to differentiate and meet consumer expectations is a reality. As a result, a digital transformation is happening in retail, restaurants, hotels, and more. Examples of these technology-based experience enhancements are self-serve kiosks, online ordering, loyalty programs, mobile POS, mobile payment, digital signage, restaurant table tablets, in-store beacons,

and guest Wi-Fi. Each one of these initiatives rely on your network, and is a potential attack vector for cybercriminals.

The Bottom Line: All technologies outside the CDE that touch your network need to be secured. First and foremost, proper network segmentation from the CDE will prevent any of these technologies from becoming a point of infiltration or exfiltration. But for their own sake and the other sensitive data they may hold (personally identifiable information of customers or employees, business financial, or legal information), they should be responsibly secured. This should at minimum include a properly managed firewall, proper network segmentation, and implementation of a cybersecurity practices policy for all employees and vendors to follow.

PCI DSS Compliance

When it comes to the compliance discussion, things can get confusing fast. Merchants have many voices telling them various bits of information about their compliance – the bank, the payment processor, the POS solution provider, the POS integrator, and so on. Most of the time, the information provided is out of context, incomplete, or flat-out incorrect. Naturally, most people when unsure, choose the path of least resistance. Which may seem like the right choice in the short term, but in the long-term may be posing considerable risk to the businesses' future.

Let's lay out some basics:

- PCI DSS is the Payment Card Information Data Security Standard
- It is governed by PCI SSC, the Payment Card Information Security Standards Council
- The PCI SSC was founded by five global payment brands – American Express, Discover, JCB International, Mastercard, and Visa
- Enforcement of compliance and non-compliance penalties are carried out by the individual payment brands, not the Council
- PCI SSC has two priorities, those simply being:
  - Help merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data
  - Help vendors understand and implement standards for creating secure payment solutions
- PCI Compliance is actually comprised of three security standards:
  - PCI DSS for Merchants and Service Providers
  - PCI PA-DSS for Payment Application Software Developers
  - PCI PTS for Manufacturers of PIN Entry Devices
- Achieving PCI DSS compliance involves:
  - Meeting the requirements (see below)
  - Performing external vulnerability scans quarterly with an ASV (Approved Scanning Vendor)
  - Attesting to compliance annually by submitting the PCI DSS SAQ (Self-Assessment Questionnaire)

When your POS system representatives says "Yes, we're PCI compliant", that means their solution is PCI PA-DSS compliant, but it has zero influence on you, the merchant, being PCI DSS compliant. **Each organization that plays a role in payment transactions is responsible for their own compliance.**

Why Be PCI DSS Compliant?

The Data Security Standard (DSS) should be considered just that… a "standard"… a "minimum requirement" to having the privilege to handle and process sensitive credit card data. Gaining and maintaining PCI DSS compliance is a minimum expectation and indicates you have some basic required security in place. By all means, you should strive for more to protect your greatest assets… your customers, your business, and your brand.

You may not be fined for non-compliance until there's a reason for your compliance to be inspected – a data breach, a fraudulent credit card purchase, or even a suspected incident. When that happens, a PCI DSS compliance audit is conducted and that's when the additional fines and penalties come in.

Quick Steps to Basic Security and Compliance

A model framework for security, the PCI Data Security Standard integrates best practices forged from the years of experience of security experts around the world.

The standard works for some of the world's largest corporations. And it can work for you.

- Buy and use only approved PIN entry devices at your points-of-sale.
- Buy and use only validated payment software at your POS or website shopping cart.
- Do not store any sensitive cardholder data in computers or on paper.
- Use a firewall on your network and PCs.
- Make sure your wireless router is password-protected and uses encryption.
- Use strong passwords. Be sure to change default passwords on hardware and software – most are unsafe.
- Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or "skimming" devices.
- Teach your employees about security and protecting cardholder data.
- Follow the PCI DSS.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	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. Use and regularly update anti-virus 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. Assign a unique ID to each person with computer access 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 employees and contractors

Trends

Cybersecurity is by nature an ever-evolving battle... an "arms race" in which hackers find new ways to thwart defenses and IT security professionals enable new defenses.

Customer Experience Technology: Merchants are being pushed to integrate more and more digital experiences in their stores and restaurants. Having a strong cybersecurity strategy and scalable infrastructure is fundamental in being able to keep up with these demands. Thus, cybersecurity and infrastructure management is not just an IT concern, it is a business growth and success concern.

POS Ransomware: Typical credit card malware must successfully persist on a network for months, while a ransomware attack needs only minutes to complete the mission. Cybercriminals are always looking for quicker, more efficient ways to make money. Deploying a ransomware attack that shuts down the POS system can effectively hold a business hostage, bringing revenue to a screeching halt. Ransomware could be the next big threat. What would you be willing to pay to unlock your POS systems?

You can find out your risk level and revenue impact potential with this free online POS Ransomware Risk Assessment. netsurion.com/ransomware-risk-assessment

IMPLEMENTING A REASONABLE CYBERSECURITY STRATEGY

Managed Firewalls

Firewalls manage the flow of computer data traffic allowed into and out of your network, for example to or from a server that hosts a payment system, or a back-office PC. Depending on its configuration, a firewall will permit or restrict access and the passage of data to or from specified hosts and networks.

The firewall device is a standard security measure, core aspect of network segmentation, and requirement #1 for PCI DSS. However, it is critical to understand that 24/7 monitoring and active configuration management is necessary for the firewall to be effective.

Benefits of Managed Firewall

This is where your security begins... managing what traffic is allowed to flow through your network and also enabling the fundamental segmentation of your network to separate the CDE from the rest of your business.

Threats to Managed Firewall

The primary threat to the managed firewall is it not being properly managed. Ensure your firewall is actively managed by a network security provider that can also aid in PCI DSS compliance. Other threats include:

- Firewall circumvention: The physical device can simply be circumvented with rogue devices plugged directly into the broadband connection. Look for a managed firewall service provider that delivers "circumvention detection" to alert you to such activity.
- DNS Tunneling: Hackers use a variety of DNS tunneling utilities as well as several known malware that use DNS as their communication channel. Because DNS is rarely monitored and analyzed, hackers are able to use DNS tunneling to slip under the radar until something else draws attention to the breach. Ensure your managed network security provider uses a next-generation firewall and/or SIEM technology capable of detecting DNS tunneling.

- Guest Wi-Fi: If not properly configured and segmented, your guest Wi-Fi can be a point of entry for a data breach. In addition to proper segmentation and family-friendly configuration, ensure your wireless network security detects the Wireless Access Points in the area around the firewall and reports on the detected SSIDs, wireless channels in use, and associated MAC addresses and can alert regarding any unknown or unauthorized wireless access points detected.

Advanced Threat Protection

Advanced threat protection (ATP) refers to a category of security solutions that defend against sophisticated malware or advanced persistent threats targeting sensitive data.

In today's world, basic security controls like firewalls and anti-virus are simply not enough to reasonably protect data networks... particularly those of a merchant. Advanced threat protection solutions encompass more advanced technology that until recently was not available to the SMB market. That has changed though. Solutions that include capabilities like Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) have now been made practical and affordable for merchants with any number of locations.

Value of Advanced Threat Protection

ATP solutions provide immediate detection, alerting, automated remedial action, and containment of modern threats like malware and ransomware which have particularly plagued the POS of merchants. Even the most capable anti-virus and anti-malware products at best state they "detect all of the currently known variants of point-of-sale malware". But that's just it, they can only detect what is already known to be malware and the current challenge is the rate at which new strains of malware are created along with mutated versions of old malware. Advanced threat protection delivers detection and alerts of both known and unknown threats.

Challenges of Advanced Threat Protection

An effective ATP solution must make sensor distribution simple. The sensor is a lightweight piece of software installed on all devices at all locations to be protected.

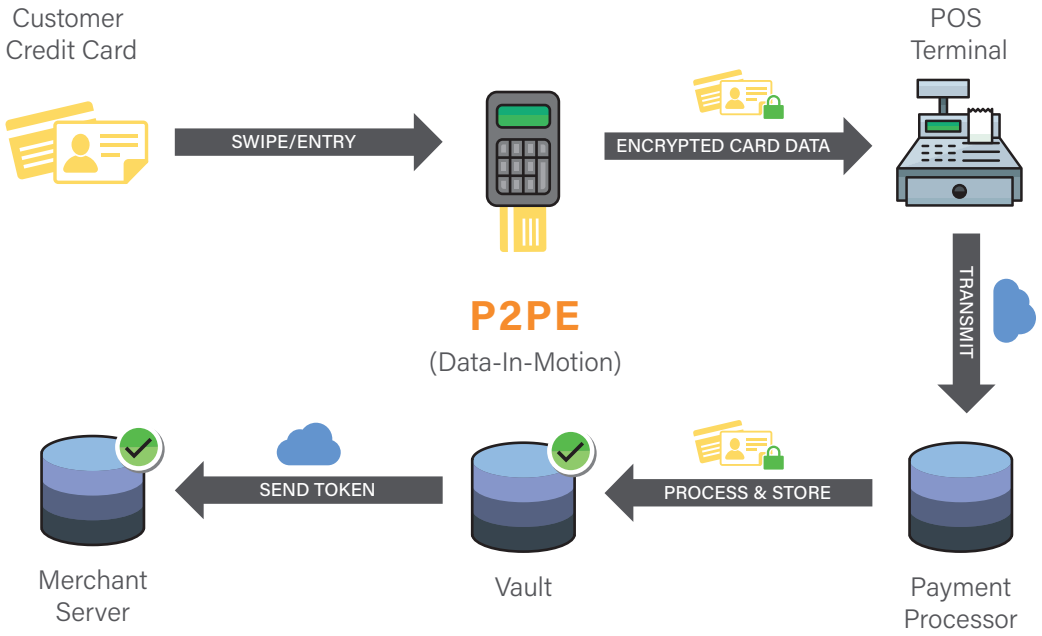
Also, while humans are known to be the weakest link in a cybersecurity chain, they can also be the strongest. 24/7 monitoring and management needs to be a component of the ATP solution. It cannot be considered a "set it and forget it" solution. Advanced persistent threats evolve and mutate. Your ATP solution must constantly keep pace. And if a critical security incident occurs, an email notification is simply not enough. A 24/7 SOC (Security Operations Center) staffed by professional security analysts must be available to help a merchant resolve the incident

Point-to-Point Encryption (P2PE)

When correctly implemented, point-to-point encryption (P2PE) solutions may simplify merchants' and acquirers' PCI compliance programs by eliminating clear-text cardholder data from their environment and reducing the scope of PCI DSS requirements. The Security Standards Council validates the conformance of P2PE solutions and provides a list of approved solutions. The Council urges merchants and acquirers to consider the use of validated solutions for implementation in their payment environments.

P2PE significantly reduces the risk of credit card fraud by instantaneously encrypting confidential cardholder data at the moment a credit card is swiped.

PCI-approved P2PE solutions reduce where and how PCI DSS requirements apply to your business. This should save you time and money on overall compliance efforts, without sacrificing the security of your customers' data.



Much confusion has crept in about the promise and capabilities of P2PE. While this technology is a significant enhancement to any cybersecurity strategy, it is not a replacement for all other security measures.

Threats to P2PE

To ensure that a P2PE solution effectively minimizes risk, it is important to first understand the risk to cardholder data within these environments, including:

- The risk that plain-text Card Holder Data (CHD) will be intercepted prior to encryption by circumventing security controls at the point of interaction (POI)
- The risk that plain-text CHD will be intercepted after decryption by circumventing security controls at the point of decryption
- The risk that an attacker will obtain decryption keys. This risk grows when an organization retains keys to decrypt ciphertext
- The risks posed by inadequate key management. Encryption and decryption keys must be protected with robust key management practices including key generation, loading, distribution, usage, administration, and injection
- The potential for exposure of cardholder data via a breach remains as long as the PAN and other sensitive cardholder data is of value and is present – even in encrypted form.

Merchants should evaluate their environments carefully for these types of scenarios and ensure that any plain-text cardholder data is adequately protected.

- If the POI device falls back to non-encrypted output for payment card transactions, any part of the merchant environment that transmits, processes or stores the plain-text CHD is still a part of the CDE and is in scope for PCI DSS compliance.

- Any legacy data and processes (such as billing, loyalty, or marketing databases) within the merchant's environment that may still store, process, or transmit plain-text CHD remain in scope for PCI DSS. Entities should have an ongoing data discovery methodology to demonstrate that legacy information is not resident in the environment before considering whether the footprint of the CDE can be reduced by a P2PE implementation.
- In cases where a merchant issues a pre-paid "gift" card or where a non-card scheme card is used, that card's account data may need to be exported in plain-text form. A device may implement a white-listing approach to prevent these cards from being encrypted prior to output. White-listing presents a significant threat to the security of a P2PE solution, should the white-listing process be subverted. For this reason, the entity operating the whitelisting should be subject to PCI DSS review.
- The physical impression taken during a card-present transaction must at some point be converted to electronic data for transmission to the acquirer/processor. Use of encryption at the point of data entry and electronic conversion can produce benefits and significantly reduce the scope of the CDE, but there will still be points at which CHD is available in plain-text form. PCI DSS validation scope is unchanged until the data is encrypted.
- Should a merchant later obtain plain-text CHD from an acquirer/processor as part of dispute resolution or chargeback processing, this data remains in scope of PCI DSS.

The Bottom Line: P2PE is an enhancement to your data security and can streamline PCI DSS compliance. It is one important component of a comprehensive merchant cybersecurity strategy.

"We're seeing more and more that cybersecurity can actually become a remarkable way to help a company innovate and move faster. In certain kinds of digital innovation, the security considerations, controls and capabilities, alongside a frictionless means of authentication, are essential to the design and development of these new products and services."
(David Burg, PwC, Global Cybersecurity and Privacy Advisory Leader)

Recommendations

Deploy a comprehensive and multi-layered IT infrastructure security strategy. This is not just an IT initiative, but one that a merchant's business growth, customer satisfaction, and overall success will depend on.

When it comes to security versus compliance, both are important to manage the risk to your merchant business.

Don't rely heavily on one solution or a disjointed set of pointed solutions. Ensure you have a security partner who can deliver technology, service, and process to predict, prevent, detect and respond to security incidents.

For more information about Netsurion's services, visit netsurion.com

Netsurion™
Powering Secure and Agile Networks