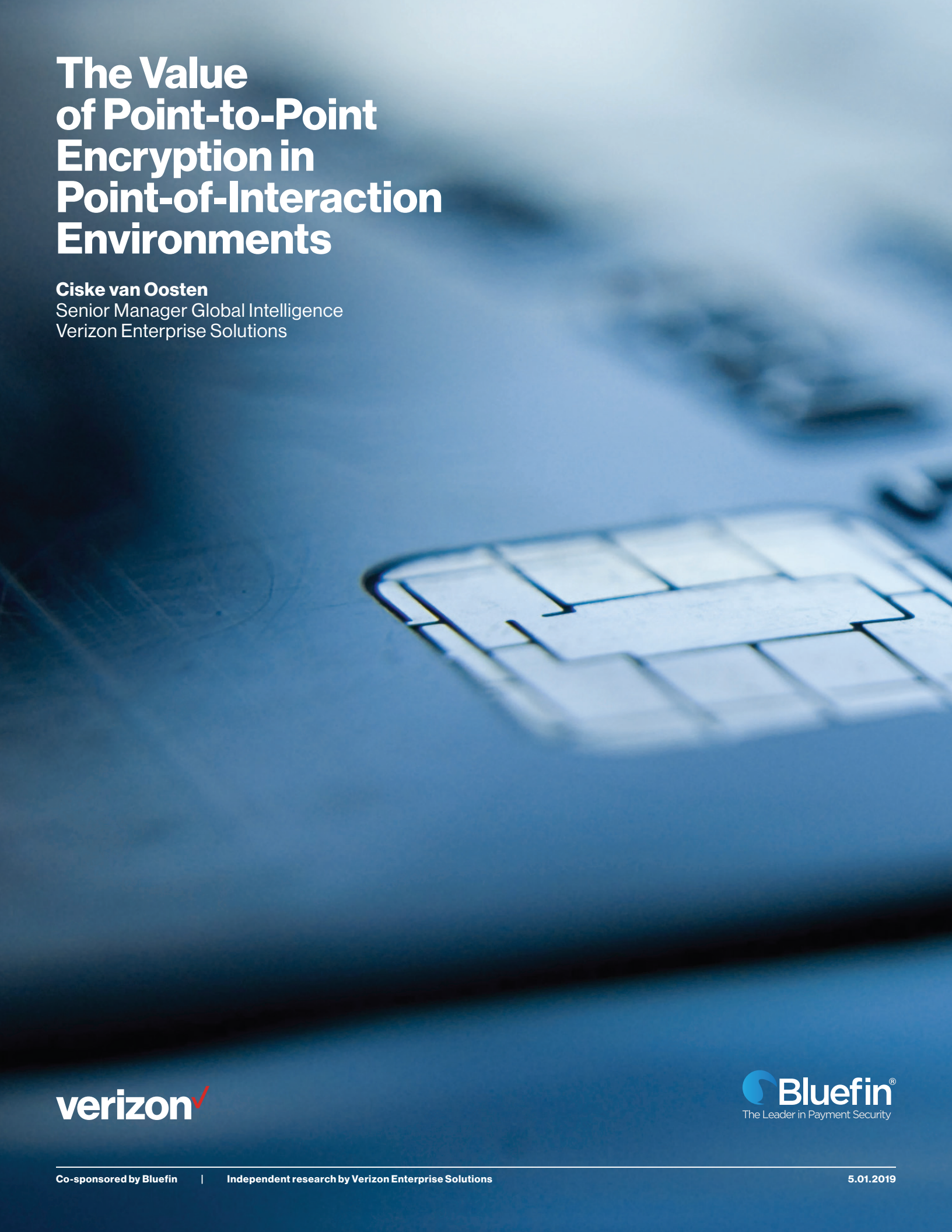
The Value of Point-to-Point Encryption in Point-of-Interaction Environments

Ciske van Oosten
Senior Manager Global Intelligence
Verizon Enterprise Solutions



verizon

Bluefin®
The Leader in Payment Security

Co-sponsored by Bluefin | Independent research by Verizon Enterprise Solutions **5.01.2019**

Table of Contents

Executive Summary

Malicious hackers continue to adversely impact nearly every industry. Threat actors attempt to steal data from point-of-sale (POS) systems using various methods, such as payment card skimmers, POS intrusions and web app attacks. They particularly take advantage of organizations that fail to reduce the size of their attack surfaces. While organizations cannot stop all security breaches, they can prevent or at least mitigate the possibility of sensitive data being compromised.

Significant effort and substantial annual investments in time and resources are necessary to protect cardholder data (CHD) and meet Payment Card Industry Data Security Standard (PCI DSS) compliance requirements. About half of organizations worldwide consistently fail to sustain security controls that support data security compliance initiatives. Traditional methods for securing CHD can be risky and inadequate.

The good news is that simpler, more effective, less expensive technology and methods to prevent data breaches do exist. Adoption of these technologies has grown rapidly as awareness and understanding has taken hold. Early adopters have been wise enough to move beyond the question "How can I protect CHD?" to "How can I reduce or even eliminate CHD?" These adopters of next-generation payment data security have implemented PCI-validated point-to-point encryption (P2PE) solutions that devalue CHD and reduce the scope of PCI DSS compliance. P2PE addresses the data breach risk by essentially removing the data that risks being breached.

This helps create the capacity, capability, and competence to comply with industry data security regulations and develop a sustainable control environment to maintain effective security controls. The purpose of this paper is to review the benefits of PCI-validated P2PE solutions in point-of-interaction (POI) environments. In addition to highlighting the various compliance management and scope reduction benefits, it aims to explore the POI threat landscape, detailing how criminals obtain access to CHD.

The P2PE concept has been around in different forms for over 20 years with varying names, terms, approaches and security practices associated with it. The main objective achieved by a P2PE solution is that it devalues sensitive data by securely encrypting it before it enters the POS environment. Among other things, this helps to prevent malware from extracting CHD from the memory of the system when it is decrypted.

In 2011, the Payment Card Industry Security Standards Council (PCI SSC) created the PCI P2PE standard to establish uniform encryption requirements (PCI P2PE v3.0 is expected sometime in Q4 2019 to Q1 2020). Today's validated P2PE solutions offer a high level of assurance of encryption capability and a tightly locked down CHD environment with little wiggle room for exploitation.

Only PCI-listed P2PE solutions offer substantial scope reduction, risk reduction and compliance simplification. The PCI SSC does not endorse the use of non-listed encryption solutions, since they have not been validated as fully meeting the PCI P2PE standard for security and cannot ensure a reduced PCI DSS validation effort.

Furthermore, this paper examines the merits of a layered approach to data security and fraud prevention, combining different technologies such as EMV, P2PE and tokenization – a configuration that provides opportunities for efficiencies and compliance simplification and the strongest protection offered with current technology.

The value of Point-to-Point Encryption in Point-of-Interaction environments

A profusion of sizable and high-profile payment card data breaches in the past decade has proven that traditional methods for securing CHD can be risky and inadequate. While compliance with the PCI DSS continues to improve, nearly half of companies fail their interim security assessments.[1] Studies indicate that organizations consistently fail to sustain security controls that support compliance initiatives. Instead, they should refocus their efforts on simplifying and standardizing control environments to maintain effective controls and better manage compliance. In short, they should take care of the basics and then worry about being excellent.

Most organizations realize that passing a security compliance assessment is not the only proactive step that could reduce the chances of a data breach. Investing resources to secure data and endpoints can be exhausting for businesses of all sizes. Enterprises must substantially simplify their control environments and reduce the surface area and complexity for defense. While organizations cannot stop all security breaches, they can prevent or at least mitigate the possibility that data is compromised.

The design of a corporate data protection strategy can reduce risk with the added benefit of minimizing the time and effort spent managing compliance. Two approaches that are effective in protecting sensitive data are “Defend the Fort” and “Devalue the Data.”

The Defend the Fort approach typically requires a substantial investment of time, money and effort to achieve and maintain a protective barrier around systems and data. While circling and maintaining the castle with a protective wall seems straightforward to implement, it is challenging to maintain defenses in an ever-changing threat landscape that requires stronger, higher and more expensive walls to keep threat actors out.

Devalue the Data is an efficient alternative. In this approach, organizations employ security technology, such as a PCI-validated P2PE solution, to devalue sensitive data through encryption, rendering it useless to hackers if exposed. An organization can then survive by mitigating the impact of a breach, protecting its brand and customers, and remaining secure and resilient to fight another day.

[1] Verizon 2018 Payment Security Report - https://enterprise.verizon.com/resources/reports/payment-security/

What is P2PE?

The P2PE concept has been around in different forms for over 20 years, with varying names, terms, approaches, and security related to it. A P2PE solution combines processes, applications and payment devices to securely encrypt and protect data during transit from the POI device/terminal or POS system. Payment card data is encrypted at the POI by read-head hardware regardless of whether the data enters into the POI device by swiping, dipping, tapping or typing. The encrypted data is then transferred via a secure tunnel until it reaches the solution provider's secure decryption environment. Strong encryption at the POI is used to devalue the CHD to anyone other than the payment processor who controls the cryptographic encryption and decryption keys. As additional protection, the processor sends the merchant a token, which can be used in subsequent transactions to protect information stored in databases.

According to Troy Leach of the PCI Security Standards Council (PCI SSC):

"P2PE provides merchants with one of the most significant ways to minimize where criminals can attempt to steal cardholder data by immediately encrypting at the earliest point of entry in their stores. That achieves one of the most fundamental security objectives, which is to reduce the attack surface. An attack surface represents all the different ways a criminal could potentially exploit a merchant location. And with all the recent advancements in hacking techniques, the more a merchant or other entity can reduce the potential attack surface and limit where cardholder data is exposed, the less risk they are required to manage."[2]

P2PE prevents memory scraping attacks involving malicious software (malware) harvesting clear-text CHD from the POS system's volatile memory (see page 12 for more details). Without P2PE, CHD is available in clear-text in RAM and virtual memory of the receiving systems between the POI and the payment processor. But with P2PE, cyber criminals cannot access clear-text CHD, which reduces risk to CHD and the PCI DSS scope of compliance and validation.

Worldwide adoption of P2PE

Industry experts, including analyst firms such as Gartner,[3] recommend that merchants upgrade their security infrastructure to incorporate P2PE. The number of PCI-validated P2PE solutions grew by over 700% in the first four years since the PCI SSC announced the PCI P2PE standard in 2011. In March 2014, Bluefin introduced the first PCI P2PE solution to be listed by PCI SSC in North America. According to the PCI SSC P2PE Solutions register,[4] it was one of only four P2PE solutions worldwide at the time. Since then, 76 solution providers received validation, including acquirers and gateways in both the U.S. and overseas.

Some industry research predicts that by the end of 2019, between 80% and 93% percent of retailers will adopt P2PE, and between 61% and 89% will adopt tokenization.[5]

[2] https://blog.pcisecuritystandards.org/whats-next-for-the-pci-p2pe-standard
[3] http://blogs.gartner.com/avivah-litan/2015/01/13/the-hidden-problems-with-payment-card-security-technologies-and-pci/
[4] https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
[5] https://blog.rsisecurity.com/does-a-p2pe-validated-application-also-need-to-be-validated-against-pa-dss/ and https://nrf.com/on-the-hill/policy-issues/data-security

PCI-validated P2PE solutions

The PCI SSC created the PCI P2PE standard to establish uniform encryption requirements. The PCI P2PE v1.0 standard was published in 2012, and the improved v2.0 was published in 2015. Publication of the PCI P2PE v3.0 standard is expected between Q4 2019 and Q1 2020.

Before the PCI SSC established the P2PE security standard, many vendors created and adhered to their own P2PE standard. These encryption solutions – not evaluated by the PCI SSC but that still provide encryption within the POI terminal and decryption outside the merchant environment – are referred to as unlisted P2PE solutions or end-to-end encryption (E2EE) solutions.

PCI-validated P2PE solutions are the gold standard for CHD protection. These solutions contain three parts: validated hardware, validated software, and validated solution providers to cover payment terminal, terminal application, deployment, key management, and decryption environments. Depending on the size of the organization and its needs, a P2PE solution can be managed by a service provider or the merchant themselves.

Each solution is assessed by a P2PE Qualified Security Assessor (QSA). If the solution meets the PCI P2PE standard, it is listed on the PCI SSC website under "Approved P2PE Solutions."[4]

PCI P2PE-certified solutions include:

- PCI-Personal Identification Number (PCI-PIN) Transaction Security certified payment devices, with full device lifecycle history from manufacture to end of use
- Secure management of encryption and decryption devices, use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading and injection, administration and usage
- Secure encryption of payment card data at the POI
- PCI-validated P2PE application(s) at the POI
- Management of the decryption environment and all decrypted account data
- Use of a P2PE Instruction Manual (PIM)

Besides meeting the PCI P2PE standard, the decryption component of the solution must operate within a secure environment assessed to the full PCI DSS standard.

Merchants using a PCI-validated solution within their environment, and who keep this environment segmented from CHD in other channels (i.e., e-commerce), are eligible to complete the authorized P2PE self-assessment questionnaire (SAQ). The SAQ allows merchants to significantly reduce the scope of their PCI DSS assessments (see page 14).

Non-listed Encryption Solution Assessments (NESA)

The PCI SSC does not endorse the use of non-listed encryption solutions. Only PCI-listed P2PE solutions are endorsed, as they have been validated as fully meeting the PCI P2PE standard for security and can ensure reduced PCI DSS validation efforts.

Several encryption providers are still not PCI-listed for their P2PE solutions because they cannot currently meet the requirements of the standard. This is usually due to device operational gaps, or technical constraints with various software requirement limitations. Many of these solutions being used by merchants pre-date the PCI P2PE standard. By acknowledging that these solutions are available, the PCI SSC is encouraging the providers of these solutions to remediate gaps and eventually undergo a PCI P2PE assessment for listing on the PCI SSC website.

In November 2016, the PCI SSC published a new document as part of the P2PE program titled Assessment Guidance for Non-Listed Encryption Solutions; i.e., 'NESA,'[6] as well as a Frequently Asked Questions (FAQ) document.[7] The gap assessment guidance document offers an optional path toward a PCI-listed P2PE solution and guides P2PE QSAs on evaluating non-listed solutions against the PCI P2PE standard. A P2PE QSA can conduct a non-listed encryption solution assessment against the PCI P2PE standard to identify and document the gaps between the solution and the PCI P2PE standard, and to show how the use of the solution impacts a merchant's PCI DSS assessment.

It is important to note that a NESA assessment potentially may not result in any PCI DSS scope reduction. There is no guarantee it will result in fewer PCI DSS requirements for the users of the non-listed encryption solution. Only PCI P2PE solutions can guarantee a reduction in PCI DSS requirements.

[4] https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
[6] https://www.pcisecuritystandards.org/documents/Assessment_Guidance_Non-Listed_Encryption_Solutions.pdf
[7] https://www.pcisecuritystandards.org/documents/FAQS_Assessment_Guidance_Non-listed_Encryption_Solutions.pdf

What is POI?

A point-of -nteraction (POI) is the initial point where data is read from a payment card. It consists of hardware and software that accepts electronic transactions and is hosted in approved equipment to allow a cardholder to perform a card transaction. The POI can be an attended or unattended POS payment terminal, ATM, kiosk, automated fuel dispenser, etc. Typically, POI transactions are card-based transactions done via integrated circuit (chip) or magnetic stripe.

POI device:
This device is used by the cardholder to swipe, insert, key or tap a payment card during the transaction. With P2PE, these devices must be evaluated and approved by the PCI PIN Transaction Security (PCI PTS) program.[8] Secure reading and exchange of data (SRED) should be enabled and listed as a "function provided." The POI device is responsible for securely encrypting the data before it leaves the device.

Hardware/host Security Module (HSM):
This device decrypts data encrypted by the POI device so it can be processed. It is physically and logically protected and provides a secure set of cryptographic services used for cryptographic key-management functions and the decryption of account data. For P2PE, these devices must be approved and configured to FIPS140-2 (level 3 or higher), or approved to the PCI HSM standard.

[8] https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

EMV does not secure data in transit

EMV (Europay, MasterCard and Visa) describes the chips embedded in payment cards to make transactions more secure. EMV is a global standard for processing credit and debit cards that works with P2PE and tokenization to create a holistic approach to payment fraud prevention.

Unlike P2PE – which ensures payment card data is unreadable by cryptographically protecting it from the POI to the secure point of decryption – the purpose of EMV is two-fold:

1. Validate consumer identity
2. Prevent fraud

EMV technology is crucial in payment security because it validates consumer identity in real-time at the POS device. EMV provides authentication, ensuring that you are you, and that your card is being used by you. A significant amount of data is exchanged in real-time between the payment card issuer and the payment terminal to confirm that a transaction is not fraudulent. EMV prevents fraud because its chip technology makes it difficult to clone payment cards, whereas magnetic stripe cards are easier to duplicate.

EMV became a focal point following major PCI breaches in 2014. However, EMV is not a data security solution; it would not have prevented the major retail breaches in the U.S., which made headlines. EMV is not designed to protect sensitive data in transit through POS environments. It also does not encrypt or protect payment card data within POS systems.

Encryption, as it relates to payment card processing, is a means of making sensitive data unreadable by unauthorized parties. When consumers complain about fraudulent credit card charges, it's often because their payment card data was stolen due to a data breach within the merchant environment.

Data interception methods are increasingly sophisticated, with malware now being used to steal payment card data from POS systems. A P2PE solution – not EMV – could protect against these attacks.

The value of tokenization

Tokenization is an integral payment technology for every merchant, along with EMV and PCI-validated P2PE. Each of these solutions plays an important role in a holistic payment security strategy. Tokenization, like P2PE, can effectively render sensitive data useless to hackers. However, tokenization and P2PE serve two very different purposes within a merchant environment.

Tokenization is the act of substituting sensitive data, such as a payment card number, with a random string of characters, a "token," that has no direct relationship back to the original data. This means that if the tokenized data is compromised, it cannot be reverse engineered to identify the original sensitive data.

During the past 10 years, numerous major retailers in the U.S. experienced payment card data compromises. In the majority of cases, payment card data, estimated at over 150 million records, would still have been compromised regardless of whether payment card data was tokenized. The reason? Most of the breaches took place at the POS terminals before the data would have been tokenized. Tokenization occurs only after the transaction traverses from the POS system through the network and then to the processor for authorization. On the way back from the processor, a "token" is sent back to the POS terminal with the approved authorization. The payment card data is not protected in the memory of the payment terminal.

When properly implemented, the use of tokenization, instead of storing actual CHD, is valuable for securing data at rest. Merchants should tokenize sensitive data as quickly as possible and replace CHD with tokens wherever it is stored.

Tokenization enables merchants and enterprises to safely store CHD for use in future transactions. Tokens are versatile – they can be engineered to preserve the length and format of the data that was tokenized. Tokens can also be generated to preserve specific parts of the original data values; by adapting to the formats of conventional databases and applications, tokens can eliminate the need to change the database scheme or business processes. The merchant can treat tokens as if they were the actual payment card account numbers. Tokenization allows merchants to perform all payment functions; for example, managing customer dispute resolution, recurring or subscription payments, conducting card-on-file billing, performing targeted marketing and conducting analytics.

There is merit in having a layered approach to data security and fraud prevention. Effectively protecting payment card data requires three different technologies:

EMV, P2PE, and tokenization

- EMV is an authentication and fraud prevention technology for card-present transactions. As discussed on Page 8, it does not secure data in transit.
- PCI-validated P2PE protects sensitive data in transit by encrypting CHD upon the point of entry in the retail device. This prevents the data from being available as clear-text when transmitted through the environment where it could be exposed in the event of a security breach.
- Tokenization mainly protects the storage of card data, securing payment card data against attacks on databases or servers, i.e., data at rest.

The POI threat landscape

The Verizon Data Breach Investigations Report (DBIR) highlights attacks on POI systems (i.e., PoS Intrusions) and shows most POI attacks occur at smaller retail organizations not properly equipped to address security. Although merchants of all sizes must comply with PCI DSS, smaller organizations generally are less compliant due to limited resources.

Payment card data is highly sought after by criminals because it is easily monetized. To access payment card data in merchant systems, the primary target for hackers has mostly been POS technology, including server, payment card terminals, and PIN entry devices (PEDs).

The mistake many organizations make when securing and monitoring POS technology is placing too much focus on endpoints and not enough on back-end systems. To improve security, businesses should design and maintain security to address application and database layers. A holistic security approach is needed as the cyber threat landscape continues to evolve in tactics and motivations.

Data breach trends

93%

The Verizon DBIR categorizes incidents into nine classification patterns, which account for the majority of data breaches. The 2018 DBIR indicates 93% of the data compromised was payment-related.

Outsiders are behind the majority of cyberattacks – 73% of cases. Organized crime groups carried out 50% of all data breaches with 12% involving actors known as nation-state or state-affiliated. Meanwhile, 28% of data breaches were perpetrated by internal actors. Nine out of ten times, the main drivers motivating threat actors were financial gain and espionage.

It takes cybercriminals just minutes, or even seconds, to compromise a system – but only 3% of breaches are discovered as quickly. In most cases, breaches are not discovered for months. When the breaches are discovered – typically by external sources such as by common point of purchase (CPP) analysis or trough law enforcement investigations – the data thieves usually are long gone, and in doing so, sometimes leaving behind a trail of destruction.

90%

POS Intrusions are over 40 times more common in accommodation and food services businesses than in other business industries. POS intrusion patterns account for 90% of all breaches within the accommodation and food services industries. Some 86% of the accommodation industry breaches occurred at small businesses. These attacks are overwhelmingly motivated by financial gain and often perpetrated by organized crime groups.

86%

Restaurants and small stores are targeted more frequently than hotel reservation systems, according to Verizon investigations. Of these hospitality breaches, only 1% involve insiders, who typically compromise POS systems through hacking and malware that captures and exports CHD. Furthermore, 96% of malware-related breaches utilize RAM scrapers to stealthily collect credit card data.

For retailers, web application attacks taking advantage of input validation weaknesses or stolen credentials are fairly common. Roughly one-third of all confirmed breaches in retail involved a web application. Common attack types include SQL injection and stolen credentials to compromise systems. Slightly more than half (53%) of the breaches recorded in the retail industry affected a server, which may be related to the frequency of web application attacks.

33%

Another one-third of breaches follow a pattern that is specific to brick-and-mortar retailers: payment card skimming. Most skimmers were discovered on gas station pumps (87%). About one-third of the assets compromised in retail data breaches were kiosks or terminals.

Business data protection strategies must include a defined approach to address all four key payment infrastructure vulnerabilities: configuration, volatile data (data in memory), data in transit, and application code. PCI security standards, such as PCI DSS, payment application data security standards (PA-DSS) and PIN, provide only partial protection against these vulnerabilities by offering minimal protection for CHD temporarily residing in memory.

How criminals obtain access to payment card data

Threat actors take advantage of organizations that fail to reduce the size of their attack surfaces. These attackers attempt to steal data from POS systems using various methods. Some of the most popular methods are described below:

Payment card skimmers:
Card skimming is a popular method used to capture payment card data. It usually involves installing additional hardware at the POI, which is then used to read track 2 data from the magnetic stripe on payment cards. Often, this hardware has been modified by the attacker and swapped out using the PED and Bluetooth, or it is overlaid on the legitimate hardware. Physical tampering of POI devices to implant external skimming devices is still an issue, especially for unattended payment systems, such as ATMs and fuel pumps, according to the 2018 Verizon DBIR. Today, organizations take active risk mitigation actions to prevent threat actors from implanting external skimmers on POI devices. Detection requires frequent physical inspections of devices to check for signs of tampering. With a PCI SSC validated solution, unauthorized replacing or swapping of POI devices makes the devices nonoperational. P2PE validation requires each POI device to authenticate, and opening the POI device will instantly render the device unusable.

POS intrusions:
POS intrusions require physical access to the retail and accommodation environments, rendering these attacks on a large scale impractical. Some hackers may attach a monitoring device to the POS system, but remote hacking elicits more gains and does not require highly specialized skills. Criminals can optimize POS malware to stealthily steal payment card data. It is relatively easy to create malware to run on POS systems because most are Windows-based. Malware can sneak past antivirus programs and traditional firewalls, capture/collect, and then extract card payment data.

By targeting major hospitality, retail and other organizations with this malware, criminals can accrue data from millions of payment cards in a single campaign. A well-known case of criminals using this technique occurred between 2003 and 2008, when a crime spree hacking campaign orchestrated by Albert Gonzalez led to the theft of data from about 180 million payment cards. Gonzalez was convicted and is serving two concurrent 20-year sentences, but the theft cost companies, banks and insurers nearly $200 million.[9] Several years later, in 2013 and 2014, POS malware was used by cybercriminals in large-scale infiltration of POS systems at various major retailers, such as Target and Home Depot. Although the majority of high-profile breaches involve the retail sector, organizations in hotel and tourism, food services, health care, financial services and education are also targeted by hackers. To defend against such breaches, organizations must make sure preventive and detective measures are in place. Operating systems must be patched, continuously updated, and properly configured to thwart potential attackers from finding soft spots to steal credentials, move laterally on a network, deploy malware or scrape memory for CHD.

Getting a foothold in the network

In technical terms, POS malware has not made significant strides. This is simply because it has not been necessary. Malware in one shape or form has been successfully and continuously around since 2005. POS malware kits are widely available in the cybercrime underground. The source code for some malware, such as BlackPOS, is also publicly available. Today, various POS RAM scraper malware variants exist, such as Alina, BernhardPOS, BlackPOS, Backoff, CenterPOS, Cherry Picker, Chewbacca, Dexter, FastPOS, FrameworkPOS, JackPOS, PoSeidon, PunkeyPOS, MajikPOS, MalumPOS, Multigrain, NewPosThings, RawPOS, Rdasrv, and VSkimmer. With this ease of availability, attackers can net millions of dollars in unauthorized payment transactions.

Businesses should consider the following recommendations when trying to secure their networks.

Supply chain integrity:
For hacking, as indicated earlier, POS systems differ little from regular computer systems. When software is purchased by an organization for use on a POS terminal, attackers can exploit vulnerabilities within the operating system. Most organizations assume that when buying a POS system, it's secure. Many POS products are installed by third-party resellers that may not specialize in security. These factors can put businesses at risk.

Remote connectivity:
POS terminals usually connect to a corporate network. They should not openly connect to the internet, yet sometimes they do. In most mature retail environments, the CDE is appropriately segmented to reduce risk (and PCI DSS scope). However, even in these environments, pathways still exist from the general corporate network to the CDE. Attackers, therefore, attempt to infiltrate the corporate network first through email phishing of employees, store managers, and other connections. Most POS endpoints are not regularly used for internet browsing. Attackers often exploit weaknesses in other external-facing systems, such as using standard query language injection on a web server, or finding a peripheral device that still uses the default manufacturer password.

Once in the network, attackers use hacking tools to gain access to the network segment hosting the POS systems. From there, memory scraping malware can make it to the POS terminal. This can be via a poisoned update of the endpoint software delivered from a central IT server, direct system penetration of higher-privilege systems and even internally by malicious individuals within the organization. After the POS malware is installed, attackers may take steps to hide their activity.

[8] https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html

These steps could include tampering with security software, scrubbing log files, changing time stamps, and having the malware surreptitiously exfiltrate CHD in the middle of the night, for example.

Memory scrapers:
Typically, POS malware is memory (RAM) scraping malware, also known as memory scrapers. The malware scans the memory of system components for data that matches the pattern of the card's magnetic stripe track 2 data. Track data is especially lucrative because it allows criminals to use the data for card-not-present transactions, and attackers can clone cards for fraudulent use at brick-and-mortar stores (see EMV on page 8). When a card is swiped or inserted into a POS device, its details are briefly processed and reside in clear-text in the POS terminal's memory while being transmitted to the payment processor. This process provides a brief window for malware on the terminal to copy the card data.

Hackers use memory parsing (scraping) software to find CHD before it is encrypted on the POS device. The malware resides in a place where it can monitor memory for when the data is unencrypted and can be captured and transmitted. The malware may be set to start when POS application or related applications run. Once executed, the malware can deploy key-logging routines and scrape the memory searching for track 2 data that contains the primary account number (PAN), expiration date, service code, and CVV/CVC/CID number. Using regex and the Luhn algorithm, malware can validate the card details before copying and saving the data in a file that the attacker retrieves later. The data also can be exfiltrated to a command-and-control server. Because this technique minimizes software or hardware tampering, virtually no attacker footprints exist.

Data exfiltration:
Many forms of POS memory scraping malware use FTP and HTTP, and sometimes the domain name system (for example, DNS tunneling) to transmit CHD out of the cardholder data environment (CDE). CDEs and other sensitive network segments that process card data often monitor, restrict or block FTP and HTTP to prevent CHD exfiltration to other environments. While these common internet protocols may be disabled within a restrictive card-processing environment, DNS is necessary to resolve hostnames within a corporate environment and therefore is unlikely to be restricted. Without effective DNS logging and monitoring, the bad actor's activity can go unchecked, and an attack can persist with CHD captured and exfiltrated for months or even years before detection.

P2PE compliance management and scope reduction benefits

Protecting CHD and meeting PCI DSS compliance requirements means significant annual effort and a substantial investment in time and resources. Configuration and connectivity weaknesses exist within the payment infrastructure. Lack of standardization introduces complexity, which is the enemy of effective and sustainable data protection. Incorrectly scoped CHD environments, incompletely documented CHD flows, and inaccurate system component inventories can cause exposures that may sometimes be difficult to detect proactively. No one wants to experience a security breach – especially one due to oversimplifying an approach to data protection and compliance validation.

Organizations must consistently monitor and continuously harden the security of POS endpoints and connecting components and routinely test the payment processing environment to look for critical and high vulnerabilities. Implementing and maintaining a basic security baseline will include a series of control tasks. Ten areas essential to check are:

1. Inventory control:
   Maintain inventory control to record and track all system components and prevent forgotten infrastructure elements, which may cause vulnerabilities going undetected for long periods.

2. Patching:
   Maintain strict patch management discipline for all in-scope components. The majority of successful attacks do not come from zero-day attacks but instead from known vulnerabilities for which patches are available. Patching is crucial to effective data protection. Access control and authentication go a long way to prevent security breaches.

3. Access control and monitoring:
   Allow access only from known IP addresses. Enable remote connectivity only when needed. For example, restrict access to the service provider for established periods, and disable remote access when not in use. Use the latest version of remote management applications, and ensure that the latest patches are installed before deployment and maintained throughout use. Enable logging on remote management applications, and examine logs regularly to detect anomalous and suspicious activity.

4. Authentication:
   Verify that a unique username and password exist for each user. Do not use default or easily guessed passwords. Use strong passwords and multi-factor authentication (something you know, something you have, and/or something you are) with strict password management and layered privileged account permissions to limit user privileges as much as possible.

5. System hardening:
   Do not use outdated or unsupported operating systems. Harden security around remote access to the POS system, using whitelisting and IP filtering to prevent unauthorized remote access. Block removable media on risky endpoints, especially any POS systems.

6. Network isolation:
   Maintain network segmentation to isolate the POS network from other networks. Fully secure Wi-Fi and Bluetooth connections to POS terminals and handheld card swipe machines to prevent the signal and data from being intercepted remotely. Separate guest Wi-Fi from internal network segments.

7. Endpoint protection:
   Deploy endpoint protection solutions to protect against malware and malicious URLs by using next-generation antivirus software. These solutions include host-based anti-virus, firewalls and data loss prevention. Continuously scan web applications for potential vulnerabilities.

8. Change control:
   Maintain strict change control and configuration management. Use file integrity monitoring to detect system changes. Changes in host-generated receipts, for example, could cause CHD leakage. Detect and prevent unauthorized key changes and the deployment of terminals before encryption is enabled with the capability to operate in a legacy mode.

9. Training:
   Provide role-based training to limit the potential for a physical breach, malicious tampering with equipment and employee misuse.

10. Vendor contracts:
    Manage vendor responsibilities contractually. The contract must require encryption in all stages of transmitting data and cover how data is captured, stored, processed and transmitted, including baseline compliance requirements such as with the PCI DSS.

As seen in this list of tasks, preventing attacks on POI environments can be a time-consuming, resource-intensive endeavor. All organizations within the payment card industry ecosystem – merchants, service providers, acquirers, processors and the card brands – want to simplify their PCI DSS compliance to save time, effort, headaches, money and complexity. Simplifying compliance starts with scope reduction and the standardization of system components and processes.

When the PCI SSC announced P2PE in 2011, there was an immediate demand for approved P2PE solutions because it offers substantial scope reduction, risk reduction and compliance simplification. The PCI DSS tasks and documentation are reduced when all clear-text CHD is removed from the merchant's POS and network environment.

Benefits to segmentation

Without isolation of components, PCI DSS controls remain applicable to all CDE and connected-to components. The workload to maintain these security controls throughout the environment can be substantial. The benefit of implementing a PCI-validated P2PE environment is that the requirement to isolate payment devices from other merchant systems is substantially reduced, because the CHD is securely encrypted through the merchant infrastructure to the P2PE payment provider. When payments are only accepted via an approved P2PE solution and the POI is the only place where CHD is introduced electronically into your environment, then the POI may be one of the few system components – or the only one – that remains in scope of PCI DSS compliance validation. P2PE solutions substantially reduce, and often completely remove, the applicable requirements on connected-to devices. This approach simplifies compliance maintenance and validation, and can substantially reduce the time, effort and cost of compliance.

Reduction in P2PE compliance validation

SAQs are validation tools designed to support merchants and service providers permitted by payment brands or their acquiring banks to self-evaluate compliance with PCI DSS. There are eight SAQs: A, A-EP, B, B-IP, C, C-VT, D, and P2PE. Under PCI DSS version 3.2, PCI SAQ C has 144 questions, and SAQ D has 329 questions. By comparison, the P2PE SAQ has only 35 questions and doesn't require validation of a vulnerability scan or a penetration test. This results in a significant reduction of controls, making PCI compliance validation much easier and faster for merchants using P2PE.

The P2PE SAQ is a substantially shorter proof of compliance, primarily because properly maintaining and implementing the P2PE payment terminal reduces many security issues related to card data. This compliance validation is intended for merchants who use approved hardware payment terminals with no electronic CHD storage, removing the core elements of the merchant environment from the scope. The POS, operating system and network, and validation requirements – such as network and application vulnerability scans and penetration test evidence – are not required.

SAQ P2PE Compliance Validation

The SAQ P2PE was first released in 2012 and updated with each new version of the PCI DSS. PCI DSS requirements in the SAQ P2PE include:

- Requirement 3: Protect CHD
- Requirement 9: Restrict physical access to CHD
- Requirement 12: Maintain a policy that addresses information security for all personnel

PCI compliance validation efforts can be reduced further if the merchant is using a PCI-validated P2PE solution and does not have access to any paper records (such as merchant receipts, mail order forms or reports) containing CHD. For example, the 12 questions of Requirement 3 and those in Requirement 9 relating to paper records would not be applicable. This model does not apply to e-commerce channels.

SAQ P2PE Version 2 was a major improvement over the initial SAQ version, which lacked flexibility. One of the significant changes was simplification of the certification process, which vendors complained was overly complicated and cumbersome in Version 1 (SAQ P2PE-HW). PCI SSC responded by simplifying the certification process and adopting a more modular approach. Also, the number of requirements was reduced in the SAQ through the removal of requirements to mask PAN data and not email unprotected PANs. This is likely because if a validated P2PE solution is in place and functioning as intended, access to an unmasked PAN is not possible.

Beginning with SAQ P2PE Version 2, merchants could take control of their own crypto key management. P2PE vendors drove this change when they found that large merchants needed to be able to manage POI encryption keys for transaction switching between processors.

Who qualifies for SAQ P2PE?

SAQ P2PE merchants must confirm that they do not have access to clear-text CHD on any computer system and enter account data only via hardware payment terminals from a PCI SSC-approved P2PE

solution. This includes verifying there is no legacy storage of CHD from other payment devices or systems, and they do not store, process or transmit any CHD on any system or electronic media (computers, portable disks or audio recordings) outside of the payment terminal used as part of the PCI SSC-listed P2PE solution.

SAQ P2PE merchants must confirm for the payment channel:

- All payment processing uses a PCI-validated P2PE solution approved and listed by the PCI SSC.
- The only systems in the merchant environment that store, process or transmit account data are POI devices approved for use with the validated and PCI-listed P2PE solution.
- The entity does not otherwise receive or transmit CHD electronically.
- No legacy storage exists of electronic CHD in the environment.
- If the entity stores CHD, such data is only in paper reports or copies of paper receipts and is not received electronically. Additionally, the entity must confirm it has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE solution provider.
- P2PE environments are adequately segmented (isolated) from any non-P2PE payment channels, and confirmation exists that there are no other payment channels.

DSS Report on Compliance validation

A similar reduction in the efforts to achieve and maintain PCI DSS compliance can be achieved for merchants and service providers that need to validate PCI DSS compliance by completing a Report on Compliance (RoC) assessment. A PCI-validated P2PE solution can reduce the same amount of applicable requirements (security controls) and system components that remain in scope within the cardholder data environment.

Merchants who accept transactions through a PCI-validated P2PE service may qualify to apply through their acquirers for card brand-specific incentive programs, such as the:

- Visa Technology Innovation Program
- Visa Secure Acceptance Incentive Program
- MasterCard PCI DSS Compliance Validation Exemption Program
- American Express Security Technology Enhancement Program

What is a semi-integrated approach, and how does it differ from a fully integrated payment environment?

Configuring a semi-integrated CDE is a network configuration approach complementary to P2PE. It helps streamline payment processes, enhance payment security and manage PCI scope. By decoupling POS from payments, the payment terminal handles the payments and the POS system handles the sales of goods and services. The two need not mix.

A configuration of in-store payment systems is used by some smaller retailers where the cashier does the math and enters the total into the PIN pad. This non-integrated system has a cash register, a calculator to add up the total of items sold and a payment terminal with a PIN pad – which are all separate.

Most payment systems evolved to fully integrated payments, where the PIN pad is peripheral to the POS, using the POS internet connection. A fully integrated payment environment is composed of the POS system, POS terminal, electronic cash register (ECR), merchant back office, and transaction processor. In a typical payment transaction, the amount due is generated by the ECR and sent to the POS terminal, where the cardholder is prompted to use a payment card. Once the card is inserted or swiped, the CHD travels to the terminal through the ECR and into the merchant's back office infrastructure where the information is stored. The back office infrastructure then forwards the CHD to the transaction processor for payment authorization. The authorization response is returned to the ECR to complete the transaction. Under this fully integrated approach, CHD goes through the POS system, and P2PE is often used. Otherwise, the POS system falls within the PCI DSS scope of compliance and validation.

A semi-integrated payment environment is composed of the same elements as a fully integrated payment environment. The transaction amount due is generated by the ECR and sent to the POS terminal. The terminal can directly communicate with the payment gateway. The payment terminal is a hardened, locked-down device that is more secure than the average personal computer or tablet. Once the cardholder inserts or swipes their card, the CHD travels directly from the POS terminal to the transaction processor for payment authorization. The authorization response from the processor is sent directly to the terminal, which then forwards the confirmation to the ECR. Integration of the terminal solution and the payment gateway can be implemented in different ways, but the POS system is not involved in their communication and does not touch card data. It might stay out of PCI DSS scope. In this payment environment, sensitive CHD never touches the ECR or the merchant's back office infrastructure, strengthening payment security and reducing the PCI scope. Communication between these elements is limited to the payment terminal and the ECR system with only non-sensitive commands.

If malicious attackers obtain unauthorized access into the ECR, they will not find CHD because the ECR never touches it. The P2PE-protected, EMV-enabled terminal will keep the payment data devalued and protected against tampering and secure the transmission of data.

A semi-integrated approach by itself will usually not yield the same benefits as when it is implemented in conjunction with a PCI-validated P2PE solution. With the addition of an appropriately configured and validated P2PE solution, the local network can be removed from scope of PCI DSS assessments.

Conquer the challenges

Businesses should no longer ask "How can I protect CHD?" but rather "How can I reduce or eliminate CHD?" Instead of banks asking merchants to provide proof of PCI compliance, merchants are now shopping around and asking banks for proof of validated P2PE solutions that can effectively remove all CHD from their POS environments.

From a compliance perspective, a validated P2PE solution places more of the compliance burden on the solution, application and component providers. The primary responsibility of protecting CHD is shifting from the merchants back to the card brands and acquiring banks. A well-informed merchant would consider doing business only with an acquirer or processor that offers solutions to keep payment card data away from the merchant's POS environment, potentially without incurring additional compliance fees or PCI Security responsibilities.

Merchants know that meeting only the compliance requirements is not sufficient to effectively and predictably prevent security breaches and protect CHD from compromise. They need assurance that security controls are effective and sustainable. Expanding payment infrastructure, increasing complexity in technology, and an ever-changing threat landscape can increase the burden on an organization's financial and operational resources. Therefore, modern-day corporate data protection and compliance strategies have evolved to establish control environments that are viable and can be upheld with the number of resources and assigned organizational supports. The goal is to achieve and maintain a secure payment processing environment that operates according to required levels of performance and security in a stable and predictable manner. In essence, businesses want lifecycle management with uninterrupted, controlled operation of system components and security controls.

Today's validated P2PE solutions enable organizations to lower risk while reducing the scope of PCI DSS compliance. They offer a high level of assurance of encryption capability and a tightly locked down CHD environment with little wiggle room for attackers to exploit. It is strongly recommended that merchants today use a validated P2PE, semi-integrated solution that supports EMV. This configuration provides opportunities for efficiencies and compliance simplification, and is the strongest protection offered with current technology.

As P2PE solutions become available to mixed-processing environments – including call center, online and face-to-face transactions – many organizations are poised to benefit from PCI-validated P2PE solutions. Almost all organizations with an estate of POI devices connected to POS systems can improve payment card risk mitigation and reduce PCI scope significantly, saving time and money while complying with PCI DSS. Organizations will experience greater efficiencies across all departments and business units, depending on how much business is directly and indirectly subject to compliance requirements.

This approach will reduce cost and effort in several key areas:

- Achieving compliance: remediation for out-of-compliance systems and processes directly or indirectly subject to PCI DSS compliance
- Compliance maintenance: sustaining PCI DSS compliance for all remaining in-scope components
- Compliance assessments: validating PCI DSS compliance

These benefits can mean hundreds of thousands of dollars in savings when considering the time and money to implement compliance correctly.

The key to data protection and compliance today is simplification – setting up for success by using a validated P2PE solution to devalue CHD and reduce the scope of compliance. This helps create the capacity, capability and competence to develop a sustainable control environment to maintain effective security controls.

Resources

PCI Security Standards Council

P2PE at a Glance - Securing Account Data with the PCI Point-to-Point Encryption Standard
https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf

PCI SSC Validated P2PE Solutions Register
https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Assessment Guidance for Non-Listed Encryption Solutions (NESA)
https://www.pcisecuritystandards.org/documents/Assessment_Guidance_Non-Listed_Encryption_Solutions.pdf

NESA FAQ
https://www.pcisecuritystandards.org/documents/FAQS_Assessment_Guidance_Non-listed_Encryption_Solutions.pdf

PCI SSC PIN Transaction Devices
https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

Verizon

Payment Security Report
https://enterprise.verizon.com/resources/reports/payment-security/

Data Breach Investigations Report
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Insider Threat Report
https://enterprise.verizon.com/resources/reports/verizon-threat-research-advisory-center/

Verizon Security Assurance
https://enterprise.verizon.com/products/security/

Bluefin

Bluefin Security Solutions
http://www.bluefin.com

P2PE Education
https://www.bluefin.com/about/media/

Contact Us

Verizon, with co-sponsorship from Bluefin, conducted an independent study of P2PE in POI environments for the effective and sustainable protection of payment card data.

verizon

About Verizon Security Professional Services

Verizon is a global security consultancy and a trusted voice in the PCI Security community, having conducted over 16,000 security assessments since 2009 for Fortune 500 and large, multinational companies. Verizon manages over 4,000 customer networks worldwide, and operates one of the world's largest global IP networks providing a unique perspective on security operations. Verizon offers various consulting and assessment programs related to payment security and compliance (PCI-DSS, PA-DSS, P2PE, EI3PA, PIN and ECB) and healthcare security and compliance (HIPAA, ONC Health IT, ConCert by HIMSS). Verizon also offers security testing and certifications for security hardware, software, solutions and IoT (through Verizon ICSA Labs), and threat and vulnerability testing. And when needed, the Verizon Threat Research Advisory Center (VTRAC) is positioned to provided investigative response and cyber threat intelligence support to data breaches and cybersecurity incidents, to include PCI Forensic Investigations.

For more information, please visit enterprise.verizon.com/products/security/

Verizon Enterprise Solutions

1 Verizon Way,
Basking Ridge,
New Jersey 07920

Phone: (908) 559-2001
paymentsecurity@verizon.com

Bluefin®
The Leader in Payment Security

About Bluefin

Bluefin provides the leading payment security platform that supports payment gateways, processors and ISV's in 30 countries. Bluefin's secure payment platform is key to the holistic approach to data security. Designed to complement EMV and tokenization, Bluefin's PCI-validated Point-to-Point Encryption (P2PE) solutions provide a solid security defense against current and future data breaches. Bluefin supports point of sale solutions for retail, mobile, call center and kiosk/unattended environments, and secure Ecommerce technologies.

Bluefin became the first North American company to receive PCI validation for a P2PE solution in March 2014. Bluefin is headquartered in Atlanta, with offices in New York, Chicago, Tulsa, and Waterford, Ireland.

For more information, please visit http://bluefin.com

Bluefin Payment Systems LLC

Corporate Headquarters
8200 Roberts Drive, Suite 150
Atlanta, GA 30350

Greg Cornwell
Head of Global Sales
Phone: +1 770-709-7745
gcornwell@bluefin.com

verizon

Bluefin®
The Leader in Payment Security