worldpay
from FIS

PROTECT YOUR REVENUE WITH POINT-TO-POINT ENCRYPTION

What it is and why it's important

15 HOURS

The time it takes for hackers to breach an organization, locate critical value data, and exfiltrate it. On average, it takes a targeted organization 200 to 300 days to discover it has been breached.

Source: The Black Report 2018, Nuix
https://www.nuix.com/sites/default/files/downloads/marketo/report_nuix_black_report_2018_web_us.pdf

Protect your Revenue with Point-to-Point Encryption:
What it is and why it's important

Information security is now seen as a strategic priority for modern businesses. With 76% of US companies reporting an attack within the last 12 months,[1] the risks are too severe to ignore.

The payment industry is always developing new ways to help protect businesses and their customers. One of the principal security developments in recent years is point-to-point encryption, or P2PE, which removes clear text data from an organization's network to help secure payments from the point of sale through authorization.

But before you choose a P2PE solution, there are some important things to consider.

THE RISKS AROUND DATA SECURITY ARE GREAT

In an increasingly technology-led world, protecting consumer data is more critical than ever. With more data passing between different systems, it's of little surprise that data breaches have increased over the past few years. During the first half of 2019, the number of reported breaches increased by 54% compared to the same time last year.[2]

In the US, the average total cost of a data breach is $3.92 million (2019), a 130% increase since 2006.[3] These costs include business disruption, lost sales, recovery of assets, fines and compensation. There's also non-monetary costs like brand erosion and reputational damage. With such steep consequences, it's imperative that organizations make security a top priority.

The challenge lies in understanding the complex regulatory and compliance requirements involved in payment security, and implementing a strategy that protects the business while reducing the time and effort to maintain compliance.

$3.92 MILLION

The average total cost of a data breach in the US, up 130% since 2006.[3]

76% of US companies reported an attack within the last 12 months.[1]

The number of reported breaches increased by 54% during the first half of 2019.[2]

CONTENTS

WHAT IS P2PE AND WHY WAS IT CREATED?

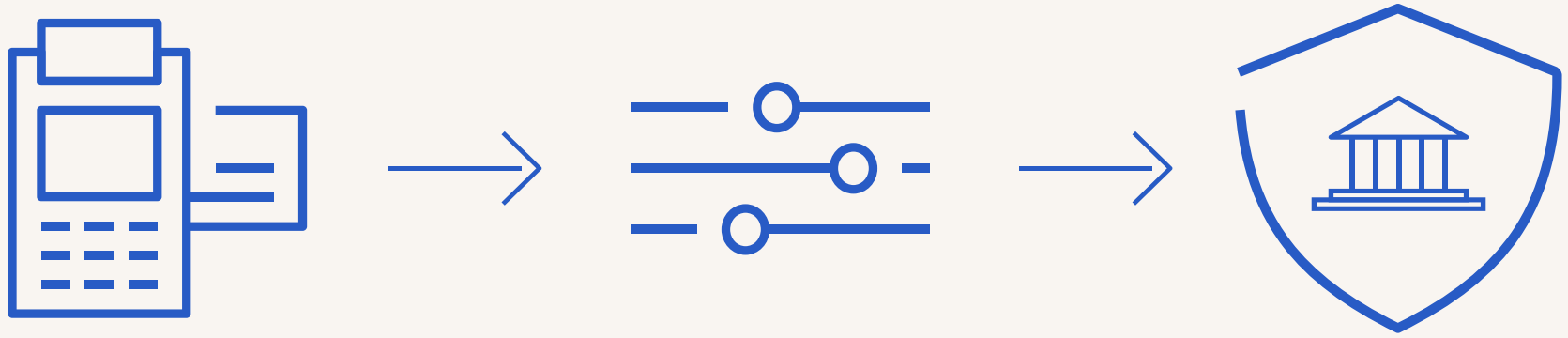
P2PE encrypts cardholder data from the point of payment to the solution provider's secure environment, where it is then decrypted. PCI P2PE is a standard established in July 2013 by the PCI Security Standards Council (PCI SSC), a global forum formed by Visa, Mastercard, American Express, JCB, and Discover, for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. Employing a PCI P2PE solution is not currently mandated by the Payment Schemes, but it has the potential to reduce the complexity and the costs of a meeting PCI DSS mandates.

Why was P2PE created?

P2PE was developed to counter the increase in data breaches involving unencrypted card data. P2PE removes clear text data from a business' network with a secure encryption process in which each transaction is created using a unique key. With P2PE, data is "de-valued" because it cannot be abused, even if stolen. P2PE offers peace of mind that any data passing through a business' network is protected.

P2PE ensures that confidential card payment data and information is encrypted at the point the payment is taken, thereby removing clear text data from a business' network.

Cardholder data is encrypted from the point of payment through to the solution provider's secure environment, where it is then encrypted



Card present transaction

Encrypted data transfer

Secure data centers

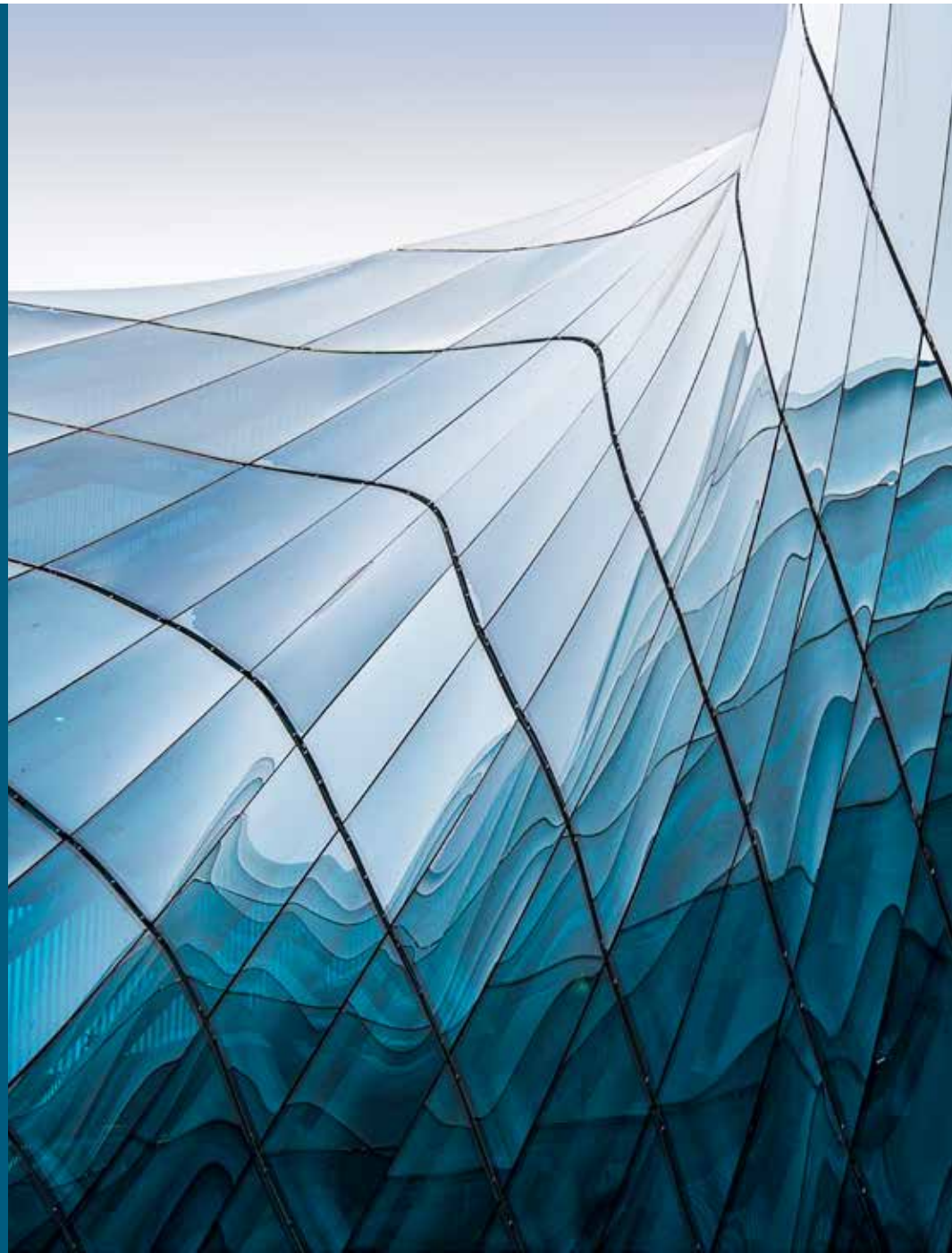
THE COMPONENTS OF A P2PE SOLUTION

A P2PE solution includes the following components:

1. PIN pads or portable terminals (PEDs – PIN entry devices) that have been assessed as achieving PCI PTS version 3 standard or higher, and which have been prepared in a highly secure, formally assessed environment
2. A certified key injection facility to prepare the PEDs securely
3. A payment application which has been listed as a PCI P2PE Application, and loaded onto a PCI-approved Point of Interaction (POI) device
4. A processing and decryption environment which is PCI DSS compliant

Each solution comes with:

1. A P2PE Implementation Manual (PIM), which provides guidance about implementing physical security for the PEDs while in operation
2. Additional implementation instructions as applicable to the solution



WHY CARE ABOUT P2PE

Benefits

Despite improvements in security and fraud prevention hardware and software, card payment fraud is still on the rise. And it's costly. According to LexisNexis Risk Solutions 2019 True Cost of Fraud study, the cost of each dollar of fraud has increased over 30% since 2016, to $3.13 in 2019.[4]

For businesses, it's critical to ensure that cardholder information is protected in an ever more challenging commercial environment. Many businesses have looked at P2PE to strengthen the security of their environment. P2PE offers businesses a recognized solution that provides the reassurance that cardholder data is protected end-to-end, helping reduce the costs and complexities of meeting PCI DSS.

THE BENEFITS INCLUDE:

Better security with greater reassurance

A P2PE listed solution provides the latest technology to help protect customers' data and businesses' reputations. Customer account data is devalued even if stolen. Businesses are therefore much less likely to be the victim of a profitable attack.

Simplified PCI DSS compliance process

PCI-listed P2PE solutions can help reduce the scope of a PCI DSS audit, saving time and money without sacrificing the security of customers' data. The scope reduction depends on how well the business environment is segregated from other payment channels or parts of the network that store, process, or transmit cardholder data.

Peace of mind through a managed service

Some P2PE solutions provide additional features that help ease day-to-day management, including PED device tracking and monitoring, which businesses must evidence as part of their PCI DSS assessment.

DISPELLING THE MYTHS

Exploring the common misconceptions of P2PE

It's important to understand what PCI P2PE means in terms of PCI DSS compliance.

Myth	Truth
P2PE is mandated	P2PE is not compulsory, although it is highly recommended by the Payment Schemes including Visa and Mastercard, American Express, Diners, Discover and JCB. The general consensus is that P2PE will not be mandated given that businesses can achieve PCI DSS compliance in other ways.
P2PE automatically reduces PCI scope	Scope reduction is not a given. However when managed correctly, P2PE should help to reduce the path towards compliance since it eliminates clear text information from an organization's environment.
Businesses no longer need to engage a QSA (Quality Security Assessor) if they implement a PCI P2PE compliant solution	Businesses still need to engage a QSA. However, the scope of the QSA assessment can be reduced as a result of implementing a P2PE-listed solution. But the business still needs to revalidate their compliance on an annual basis.
P2PE covers both in-store and online channels	P2PE only applies to in-store environments. Businesses with an eCommerce channel need a QSA to complete an assessment for the standard PCI DSS compliance program. It can be more difficult for large businesses supporting a mix of in-store and eCommerce channels, since there needs to be a clear demarcation between the channels. P2PE reduces the PCI burden and businesses should consult with a QSA to determine their level of scope reduction.

WHAT TO LOOK FOR WHEN CHOOSING A P2PE SOLUTION

There are a number of key considerations when looking for a P2PE solution provider. Here's what to look for:

The solution should meet the latest standard, PCI-P2PE version 2 A PCI-P2PE version 2-approved solution is necessary to meet the latest standards and allow for greater PCI DSS scope reduction. This helps avoid the disruption and added investment that businesses with PCI-P2PE version 1 will encounter over the next couple of years, and provides a longer "shelf-life" for the solution.

The provider should offer access to the newest PIN Entry Devices (PEDs) With tamper-resistant designs to reduce the risk of someone trying to extract data, PEDs are a critical piece of the whole P2PE solution. To help ensure protection and adherence to the latest standards, PEDs must be PCI PTS Version 3 or later. The latest devices in market now are PTS5 certified, with a current expiration date of April 2026. Look for a solution provider that can support a variety of PEDs and has the ability to introduce new devices without significant development work.

WHAT IS A P2PE SOLUTION PROVIDER?

A P2PE solution provider is a third-party entity (e.g. a processor, acquirer, or payment gateway) that is responsible for the design, implementation, and on-going management and compliance of a specific P2PE solution. The provider seeks recognition from the PCI Security Council for the solution's integrity (otherwise referred to as a listing). Once listed, the provider can offer a managed P2PE solution for its customers.

The solution should include electronic inventory management and monitoring

Electronic inventory management and monitoring allows businesses to track and monitor PEDs remotely, providing realtime information that enables compliance. This way, any problems or suspicious activity can be quickly identified and corrected; and manual processes can be minimized, saving time and money. Solutions that include electronic inventory monitoring and remote updates help demonstrate compliance and allow businesses to benefit from seamless technology upgrades, such as contactless enhancements to support the introduction of mobile wallets.

The provider should make it possible to easily scale the solution

For large and growing businesses, it's important that the solution provider has the reliability and scale to support current and future needs. It's important that the provider has the capacity to support the business at trading peaks, and ensure outages don't occur.

Another option: develop your own solution in house

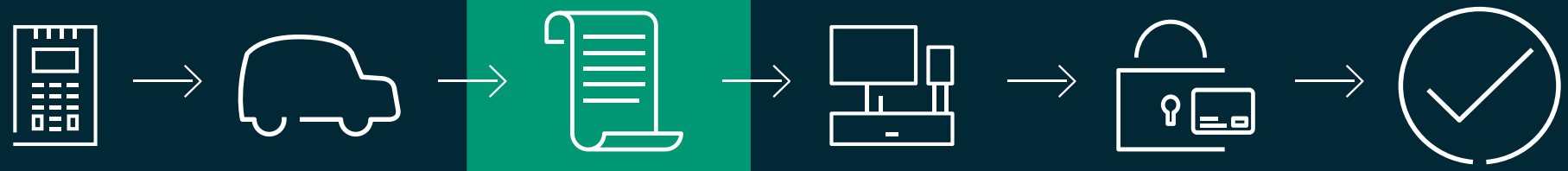
Although there are a number of established P2PE solution providers available, there is an option to assemble your own. This is called a Merchant Managed Solution (MMS). Before going this route, there are some factors to consider because establishing an MMS can present unexpected overheads.

The first is that a P2PE qualified QSA must be retained to assess the solution and ongoing compliance. Second, you'll incur the overhead of assembling certified components or building and managing your solution, including the ongoing maintenance. This is something your assessor will need to evaluate and approve as part of your compliance with PCI DSS. All responsibilities with a MMS rests with the business. Given the potential for large fines and the reputational risk at stake, it's a decision not to be taken lightly. A well implemented MMS P2PE solution could certainly benefit the largest organizations, but it could distract and prove to be highly expensive for others.

P2PE VISUALISED

Responsibility of solution provider

Responsibility of retailer



PED preparation and despatch

PEDs loaded with secure keys and inserted into tamper proof packaging.

Secure environment - PCI evaluated and approved.

Secure courier delivery

PEDs are despatched and tracked/traced.

P2P instruction manual (PIM)

The retailer carries out a series of implementation checks and documents when PEDs are received. There are ongoing checks that the retailer must undertake as part of the PIM.

Retailer needs to evidence compliance to their QSA

P2PE secure payment

Payment takes place within the retailer environment using PCI P2PE listed application and PCI PTS v3 certified PEDs.

Status monitored

Transactions securely decrypted

Transactions are decrypted once safely within the data center.

Status monitored

Transaction authorized

Authorizations requested in real time and passed for settlement.

Status monitored

HOW WORLDPAY CAN HELP

Worldpay from FIS (NYSE: FIS) is a leading payments technology company with unique capability to power global omni-commerce, processing 75 billion transactions annually around the globe. We lift economies and communities by advancing the way the world pays, banks and invests. With an integrated technology platform, Worldpay offers a comprehensive suite of products and services, delivered globally through a single provider. Our P2PE solutions help businesses build a safer future for commerce, by protecting card data, reducing risk, and simplifying PCI compliance.

Visit us at **www.worldpay.com**

DEFINITIONS

ICO
Information Commissioner's Office

P2PE
Point to Point Encryption, an industry standard recognised as contributing towards a business' PCI DSS compliance

PCI PTS
Payment Card Industry PIN Transaction Security, the standard for payment terminals in order to capture and validate data

PED
PIN Entry Device, typically a PIN pad or a card payment terminal

POI device
Point of interaction, typically a PIN pad or a card payment terminal, otherwise known as a PED

QSA
Qualified Security Assessor, an individual who is certified by the PCI Security Standards Council to audit businesses for PCI DSS compliance

SOURCES

[1] Ponemon: The 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses https://www.prnewswire.com/news-releases/ponemon-cyberattacks-on-smbs-rising-globally-becoming-more-targeted-and-sophisticated-300933394.html

[2] Risk Based Security, Data Breach QuickView Report, https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-repor

[3] Ponemon Institute, 2019 Cost of a Data Breach Report, https://www.ibm.com/security/data-breach

[4] LexisNexis Risk Solutions 2019 True Cost of Fraud, https://risk.lexisnexis.com/insights-resources/research/2019-true-cost-of-fraud-study-e-commerce-retail-edition

WFEN016 12.19