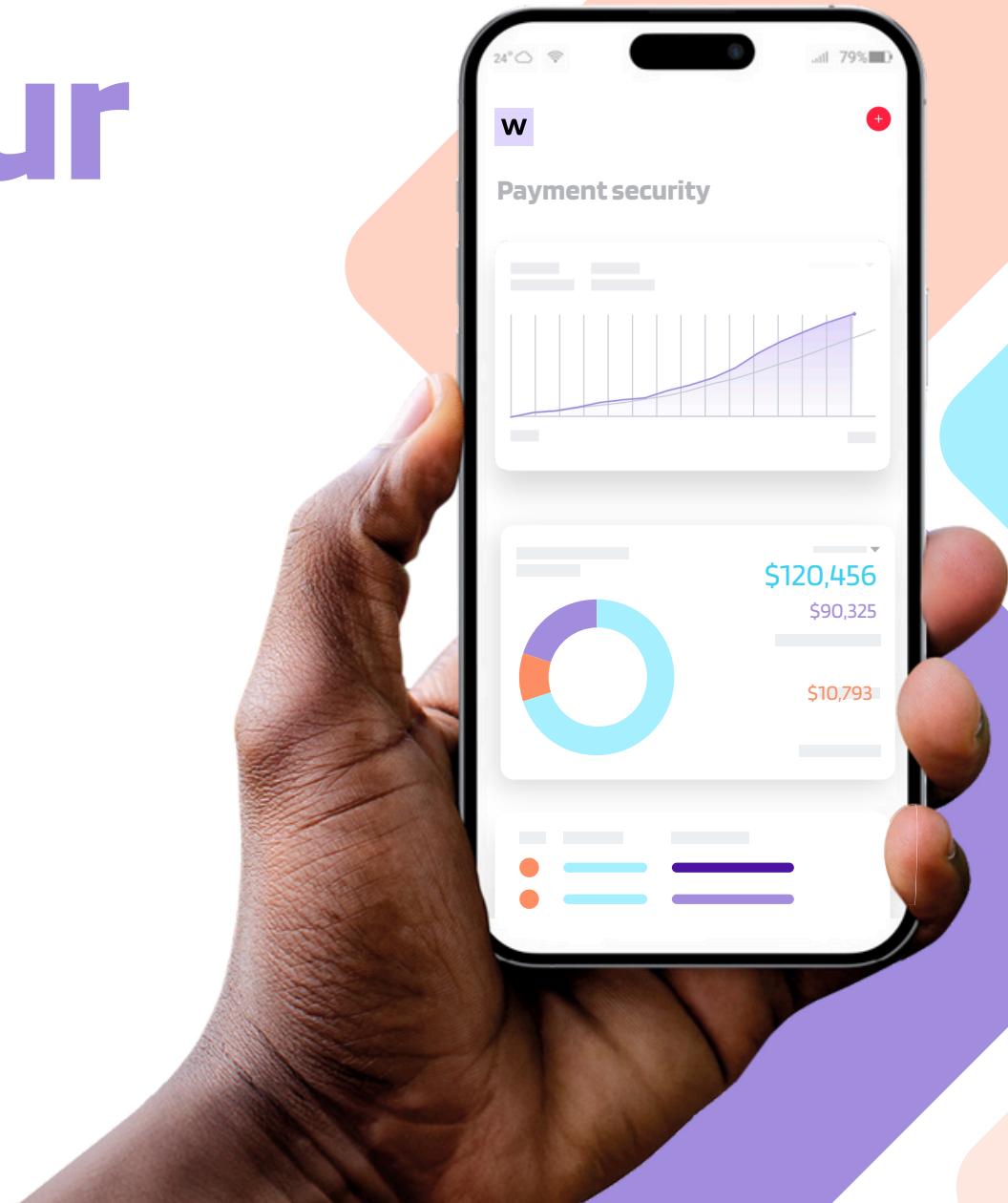
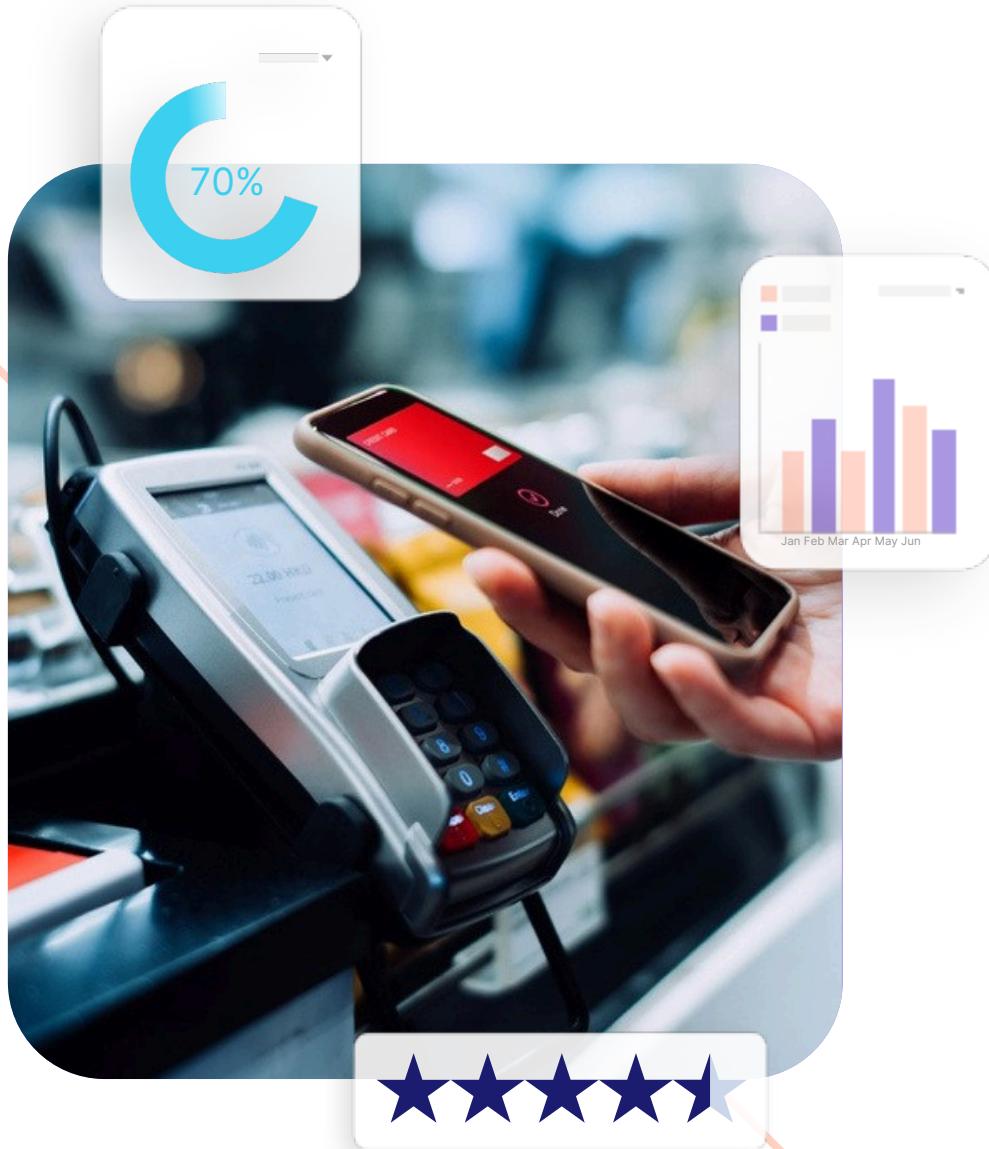


PCI COMPLIANCE

# Unlock your platform's security potential





Protecting cardholder data isn't just good business – it's essential. Let's cut through the complexity and show you how PCI compliance keeps your platform secure and your customers happy.



# Understanding PCI compliance

The Payment Card Industry Data Security Standard (PCI DSS) is the global standard that all businesses, including software companies, handling credit card payments must follow.

## In short

PCI DSS is fundamental to your success. Most software companies don't have an in-house PCI expert — that's where we come in.

PCI compliance isn't just about regulatory requirements. It's your key to safeguarding cardholder data and maintaining a secure software business.

## PCI helps you:

Identify and fix vulnerabilities before they compromise your security

Build trust with customers and partners by demonstrating your commitment to protecting their data

Establish credibility in your industry and differentiate your services



TRAX



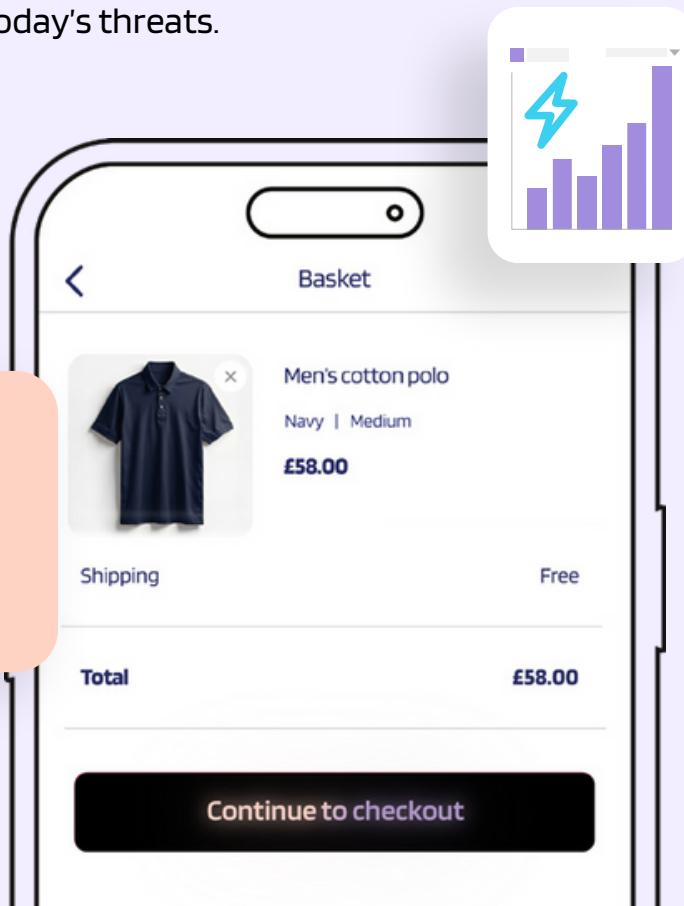
# PCI 4.0: Security for the digital age

Remember when fraud means someone skimming your card at the ATM? Those days are gone.

Today's fraudsters have their sights set on eCommerce, where the payoffs are bigger and the attacks more sophisticated. That's why PCI DSS 4.0 exists — it's your comprehensive security shield for today's threats.

## In short

PCI 4.0 isn't just a compliance checkbox — it's essential for your business.



PCI 4.0 arms your platform with over 60 new protections including:

### Phishing shields

Keeping credential thieves at bay

### Multi-factor authentication

Now mandatory (and for good reason)

### eCommerce skimming protection

Stopping invisible thieves at checkout

### Regular vulnerability scans

Finding weaknesses before attackers do

### IP address security

Locking down your digital front door

# The role of platforms in PCI compliance

In the payment card ecosystem, security requires coordination across multiple stakeholders. Processors, software platforms, and merchants each have unique responsibilities but must work in unison to ensure PCI compliance and protect customer information. This represents a shared responsibility model.

Software companies, particularly those serving SMBs (small and medium-sized businesses), play a crucial role in this

framework. Consider that 46% of all cyber breaches target businesses with fewer than 1,000 employees, with incidents potentially costing up to \$650,000 per breach.

With such significant risks, it's essential for software companies to partner with a payments processor that prioritises PCI compliance. Through effective collaboration, you can safeguard your user base and the 420 million U.S. cardholders they serve.

## Payments processors

Powering the sophisticated behind-the-scenes infrastructure

## Merchants

Conducting business with system confidence

## Software platforms

Building reliable performance with ironclad security

## Cardholders

Trusting the system with their financial data

# Data security fundamentals

PCI compliance goes beyond payments — it's about building a security culture where even tiny details matter enormously.

Did you know 81% of company data breaches start with weak passwords? It's true. A seven-character password can be cracked in about four seconds, while an 18-character password would take roughly 480,000 years.

These fundamental security practices aren't just technical requirements — they're the foundation of customer trust and business longevity.

» We need to start thinking about the payments flow as a relay race. Your software customers are depending on you to make sure that you play your part in that because they need protection. And more importantly, their customers (the cardholders) need protection too.

Head of Partner Activation  
Worldpay for Platforms

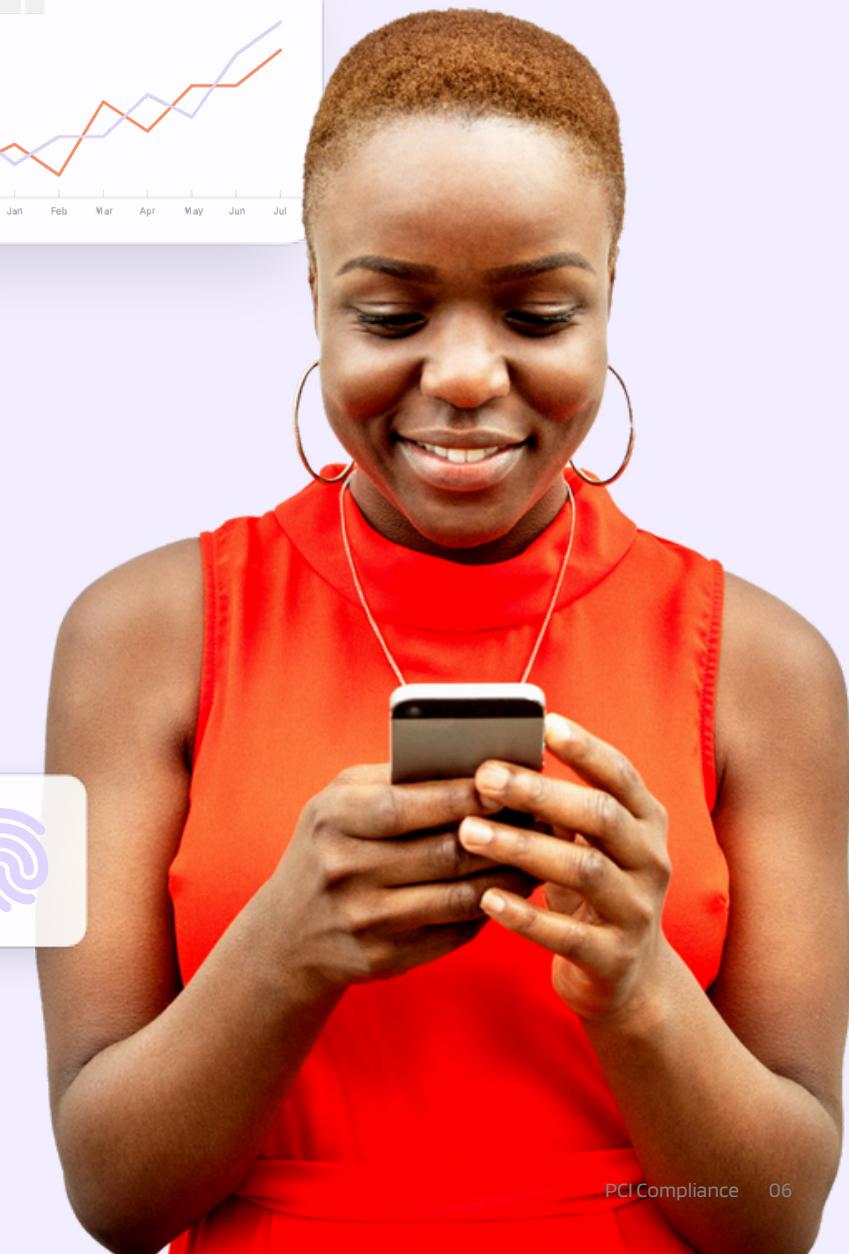
# Trust

## Your most valuable asset

Strong security isn't just about preventing breaches — it's about building unshakeable customer confidence.

When your platform demonstrates solid security, you're not just protecting data; you're creating peace of mind that builds lasting relationships.

The good news? You don't have to do this alone. Strategic partnerships, especially with payment processors who understand security inside and out, can provide the expertise you need.



# Finding your perfect security partner

The ideal payment processor serves as your compliance partner, providing guidance that you can confidently share with your customers. This approach builds trust and positions you as an authority in payments compliance.

## Ask potential payment partners

3

How will they help you build customer confidence? Is breach assurance extended to them too?

1

Do they offer breach assurance? What PCI reporting tools do they provide?

2

Can they back up their claims?

5

Do they provide a clear responsibility matrix showing who handles what?

4

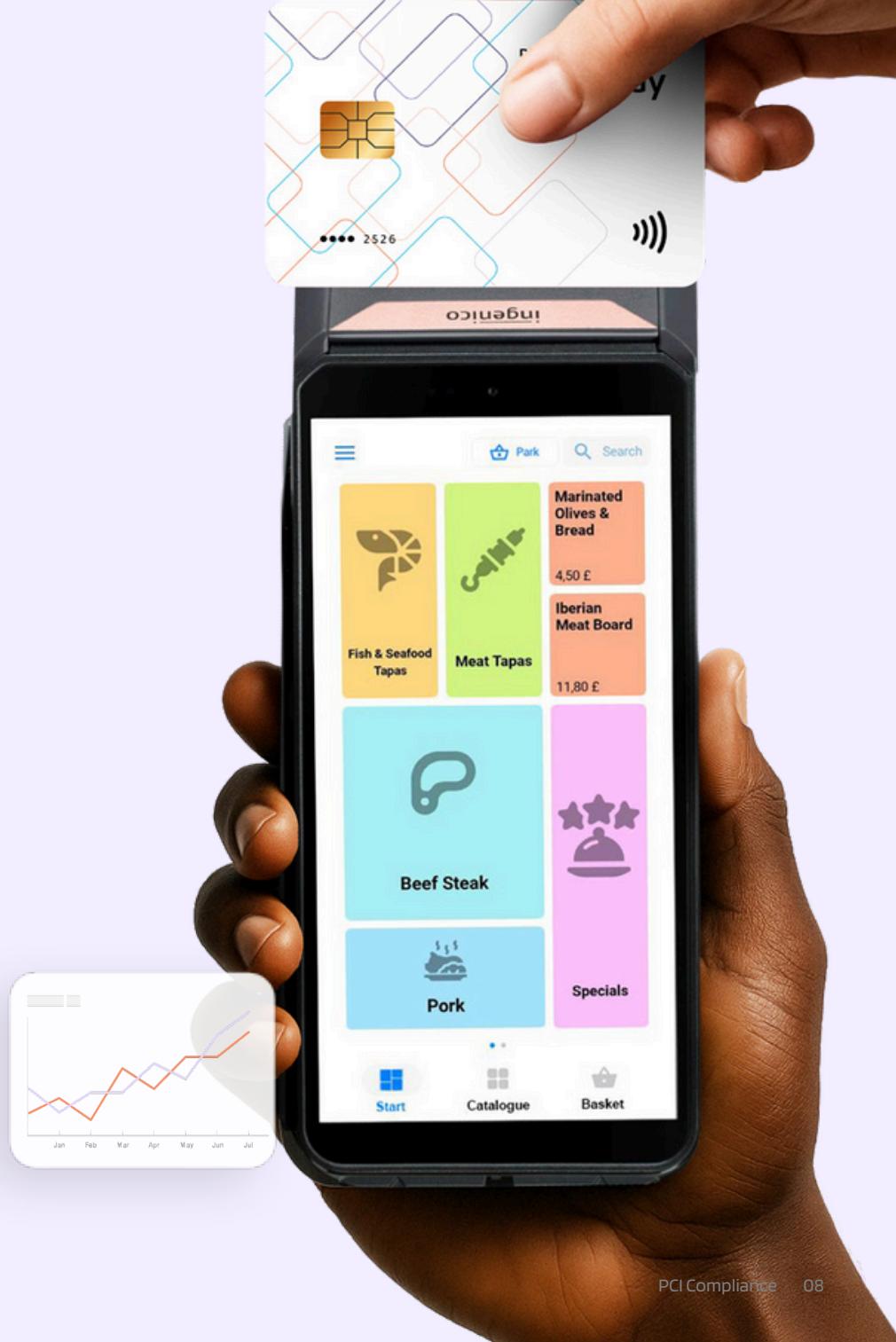
Will they guide you through each integration's specific PCI requirements?

# Next steps

Ready to strengthen your security strategy?

Partner with a payments provider that makes PCI compliance straightforward.

As your trusted advisor, we provide the tools, expertise, and support to keep your platform secure and compliant, letting you focus on growth while we handle the technical details.



## **Make payments your source of strength, not vulnerability**

Ready to turn payment security into your competitive edge?  
Book a demo with us and discover tokenisation solutions that  
deliver both optimal security and efficiency for your business.

[Book a demo](#)

