REDSCAN

# UNDERSTANDING THE PCI DSS

How to protect sensitive cardholder data

✉ info@redscan.com ☎ 0800 107 6098 🖱 redscan.com

# Meeting the latest payment card industry standards

If your business accepts electronic payments, protecting sensitive cardholder data should be a high priority.

The Payment Card Industry Data Security Standard is a minimum set of technical and operational requirements designed to help organisations avoid damaging data breaches and reduce fraud.

Organisations that fall short of the PCI standard, and/or those not working towards achieving compliance, are liable to incur significant penalties. These include fines, increased transaction fees and, in some instances, withdrawal of banking services.

## How Redscan can help

Without a high level of cyber security knowledge and awareness, achieving PCI compliance can be a long, complex and expensive process. All organisations that accept or process credit card payments are required to undertake an annual audit to assess their security posture. This covers data retention, encryption, physical security, authentication and access management.

As an award-winning provider of managed security services, Redscan can help your organisation to understand and address the latest PCI requirements by:

Identifying and assessing security risks

Scoping compliance projects

Improving resilience against cyber attacks

Enhancing threat detection and response

## FAQs

### To whom does the PCI DSS apply?

The PCI DSS applies to organisations, such as merchants and service providers, that store, process and transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

### Who is the standard enforced by?

PCI DSS is administered and managed by the Payment Card Industry Security Standards Council (PCI SSC). Enforcement of the standard is, however, the responsibility of payment brands such as Amex, Mastercard and Visa, as well as all acquiring banks.

### Which requirements apply to my business?

The minimum PCI requirements applicable to your business is dependent upon its merchant classification level. This is based on the annual volume of card data transacted, with more stringent requirements placed on organisations that process millions of payments per year.

### What is CHD and SAD data?

Cardholder data includes Primary Account Number, Cardholder Name, Expiration Date and Service Code. Sensitive authentication data includes Full Track Data (magnetic stripe data or equivalent on a chip) and CAV, CVC, CVV and CID numbers, PINS and PIN blocks.

# A faster route to compliance

The road to PCI compliance can be full of pitfalls. These include a failure to fully understand the requirements of the standard, a belief that investment in technology alone represents a fast track to compliance, and viewing adherence as a one-off exercise rather than a continuous programme of improvement.

By helping you to continuously identify and address weaknesses in your organisation's security, as well as proactively detect and remediate breaches, Redscan's cost-effective services support ongoing PCI compliance.

## PCI DSS 3.2 requirements

✓ **Build and maintain a secure network**

1. Install and maintain a firewall
2. Avoid use of default credentials

✓ **Protect cardholder data**

3. Protect stored cardholder data
4. Encrypt card data during transmission

✓ **Maintain a vulnerability management program**

5. Use and update antivirus software
6. Develop and maintain secure systems

✓ **Implement strong access control measures**

7. Restrict access to cardholder data
8. Authenticate access to system
9. Restrict physical access to data

✓ **Regularly monitor and test networks**

10. Track and monitor access to data
11. Regularly test systems and processes

✓ **Maintain an information security policy**

12. Maintain employee & contractor policies

| Supporting service | How we help |
|---|---|
| Virtual CISO | By supplying a qualified security expert on-demand, Redscan's vCISO service can help assess risks, devise and enforce security good security practices and processes, and raise employee cyber awareness. |
| ThreatDetect™ Network MDR | Our 24/7 Managed Detection and Response service combines experienced cybersecurity professionals, aggregated threat intelligence and the latest security technologies to provide deep visibility of, and help eliminate, threats that target your business. ThreatDetect offers:<br>- Log aggregation, analysis, and correlation<br>- Resource tracking and monitoring<br>- Intrusion detection<br>- Continuous user authentication monitoring<br>- Risk classification and compliance reporting |
| ThreatDetect™ Endpoint EDR | Protecting systems against malware is a fundamental PCI requirement. Our ThreatDetect EDR service provides an extra line of defence, supplying next-gen endpoint technology and CSOC experts to enhance threat discovery and incident response. |
| Managed Vulnerability Scanning | Internal and external network vulnerability scanning, performed by our qualified experts, helps to identify, classify and remediate common exposures such as weak user credentials, unsafe privileges and unpatched or out-of-date systems and applications. |
| Penetration Testing | Utilising real-life hacking techniques, a pen test is designed to identify hidden risks and provide the guidance needed to address them. Internal and external penetration testing must be performed on an organisation's complete cardholder data environment and include any systems which may impact its security. |
| Red Team Operations | A Redscan simulated cyber-attack comprehensively challenges organisations' detection and response capabilities, including the effectiveness of technology, personnel and processes. |

# Flexible solutions for all PCI DSS needs

### Virtual CISO

By acting as an extension of in-house resources and fully understanding business needs, a Redscan vCISO can help to assess data security risks plus develop and implement the policies, procedures and controls needed to strengthen defences and achieve compliance standards.

### Cyber Essentials

Designed to mitigate common security threats such as malware infections and social engineering attacks, CE is an annual assessment of key security controls that can help organisations to defend against common attack vectors that target enterprise-level and corporate IT systems.

### ThreatDetect™ MDR & EDR

Supplying leading security professionals, advanced threat detection technologies, and latest industry intelligence, this award-winning service monitors network infrastructure and endpoints to hunt for threats and provides the early notification and remediation advice necessary to respond swiftly and effectively.

### Managed vulnerability scanning

Leveraging specialist scanning tools, Redscan's offensive security professionals help to define, identify, classify and address weaknesses across on-premise, cloud and hybrid network environments.

### Penetration Testing

Redscan's CREST certified ethical hackers use multi-layered evaluations to identify security risks across networks, websites and applications, plus provide the support needed to help address them.

### Red Team Operations

An extensive Red Team engagement replicates modern adversarial techniques to fully test an organisation's resilience and capacity to detect and respond to a sophisticated cyber-attack targeting physical and virtual defences.

### About Redscan

Redscan is an award-winning provider of managed security services, specialising in threat detection and integrated incident response.

Possessing a deep knowledge of offensive security, Redscan's experts are among the most qualified in the industry, working as an extension of clients' in-house resources to expose and address vulnerabilities plus swiftly identify and shut down breaches.

Services offered include: CREST accredited Penetration Testing, Red Team Operations and Managed Detection & Response.

CREST.

SC 2018 awards EUROPE Winner Best Customer Service

2018 Computing Security Awards WINNER Pen Testing Solution of the Year

## Talk to our data security experts

**EMAIL US**
✉ info@redscan.com

**CALL US**
☎ 0800 107 6098

**ONLINE**
redscan.com

REDSCAN