imperva
a Thales company

5 Essential Steps to PCI DSS 4.0 Compliance

PCI DSS 4.0 isn't just about checking boxes—it's about securing your business against modern threats while staying compliant. This new framework shifts the focus from rigid controls to outcome-based security, giving organizations more flexibility in protecting sensitive payment data.

5 Ways to Comply with PCI DSS 4.0

01 SECURE YOUR APIS: DISCOVER, DEFEND, AND PATCH

PCI DSS 4.0 requires a complete software inventory. Unpatched vulnerabilities = open doors for hackers. API Security tools help you **identify and fix flaws fast, block unauthorized access, and secure your software supply** chain with an SBOM.

02 BLOCK FRAUD BEFORE IT STARTS WITH ADVANCED BOT MANAGEMENT

Bots fuel fraud. PCI DSS 4.0 demands **stronger fraud prevention**. Advanced Bot Protection stops **credential stuffing, fake transactions, and account takeovers** before they happen.

03 LOCK DOWN YOUR PAYMENT PAGES WITH CLIENT-SIDE PROTECTION

Attackers inject malicious scripts to **steal customer payment data**. Client-Side Protection ensures **real-time monitoring, script authorization, and airtight content security policies** to stop data theft.

04 PREVENT DOWNTIME WITH DDOS PROTECTION

DDoS attacks can **take your business offline**. Keep your payment services up and running with **malicious traffic filtering, rate limiting, and strong network defenses**.

05 DEPLOY A WEB APPLICATION FIREWALL (WAF) FOR ALWAYS-ON PROTECTION

Public-facing apps? You **need a WAF.** It inspects all incoming traffic, blocking **SQL injections, XSS, and other web-based threats** before they compromise your system.

Ready to secure your business?

PCI DSS 4.0 Compliance Made Simple

Our industry-leading security solutions help you achieve and maintain PCI DSS 4.0 compliance.