QUICK REFERENCE GUIDE
REDUCE PCI DSS V4.0 AUDIT SCOPE

Protection of Cardholder Data

- **WHAT?** Requirement 3 – Protect Stored Account Data
- **WHY?** Disk-level encryption is no longer sufficient with PCI DSS v4.0. Organizations managing sensitive financial information must adhere to new PCI mandates to ensure robust protection over cardholder data and sensitive authentication data at-rest against evolving cyber threats.
- **HOW?** Pseudonymization technologies like tokenization and format-preserving encryption enhance the protection of cardholder and sensitive payment data by obfuscating it. In a security breach, these tokens and hashes render the data useless to unauthorized parties.

Auditing

- **WHAT?** Requirement 10 – Log and Monitor All Access to System Components and Cardholder Data
- **WHY?** PCI DSS v4.0 aims to ensure that organizations can effectively monitor, analyze, and respond unauthorized access attempts as part of larger efforts to enhance accountability, traceability, and detection of security incidents.
- **HOW?** Data security platforms can be configured to log new accounts, event details, privilege escalations, and changes to user accounts. These logs can be sent to dedicated logging servers or security incident and event management (SIEM) tools.

PCI Scope Measurement

- **WHAT?** Requirement 12 – Support Information Security with Organizational Policies and Programs
- **WHY?** Organizations must enhance their scope measurement processes as PCI DSS v4.0 pushes to facilitate more accurate risk assessments, effective security controls, and compliance verification across the payment system with cardholder data.
- **HOW?** Data security platforms identify and continuously locate known and unknown instances of cardholder data. This simplifies scoping processes and provides insights into cardholder data environments, while also supporting other regulatory requirements and PCI mandates for targeted risk analysis and secure access to payment systems.

CHANGES TO KEY REQUIREMENTS
PCI DSS V4.0 AUDIT SCOPE

comforte

PCI Requirement	Description	Technologies Commonly Used
Requirement 2	Apply Secure Configurations to All System Components	Configuration Management Tools | Vulnerability Management Tools | Endpoint Security Tools | Patch Management Systems | Firewall and Network Security Solutions | Security Information and Event Management (SIEM) | Cloud Security Posture Management (CSPM)
Requirement 3	Protect Stored Account Data	**Format-Preserving Encryption (FPE) | Format-Preserving Data Tokenization (FPT) | Data Masking** | Data Hashing | File Encryption | Transparent Data Encryption | Secure Network-Attached Storage (Secure NAS) | Key Management Systems (KMS) | Hardware Security Modules (HSM)
Requirement 7	Restrict Access to System Components and Cardholder Data by Business Need to Know	**Format-Preserving Data Tokenization (FPT) | Data Masking** | Data Hashing | Identity and Access Management (IAM) Systems | Key Management Solutions (KMS) | Certificate Management Systems | TLS/SSL | IPsec | VPNs | SFTP and SFTP Gateway | FTPS | Secure Email Gateways | Web Application Firewall (WAF) | Network Intrusion Detection (IDS/IPS)
Requirement 8	Identify Users and Authenticate Access to System Components	**Format-Preserving Data Tokenization (FPT) | Data Discovery and Classification** | Identity and Access Management (IAM) Systems | Multi-Factor Authentication (MFA) | Role-Based Access Control (RBAC) | Privileged Access Management (PAM) Systems | Access Control Systems (ACLs) | Intrusion Detection and Prevention Systems (IDPS) | Security Information and Event Management (SIEM)
Requirement 10	Log and Monitor All Access to System Components and Cardholder Data	**Format-Preserving Data Tokenization (FPT) | Data Masking | Data Discovery and Classification** | Data Access Control Systems | Policy Management Systems | Risk Management Tools | Compliance Management Systems | Governance, Risk, and Compliance (GRC) Platforms | Security and Event Management (SIEM) | Intrusion Detection Systems (IDS) | Intrusion Prevention Systems (IPS) | Incident Management and Ticketing Systems | Data Loss Prevention (DLP) Solutions | Vulnerability Scanning Tools
Requirement 12	Support Information Security with Organizational Policies and Programs	**Data Discovery and Classification** | Risk Assessment Platforms | Threat Intelligence Services | Security Information and Event Management (SIEM) | Vulnerability Assessment Tools | Governance, Risk, and Compliance (GRC) Platforms | Penetration Testing Tools | Endpoint Detection and Response (EDR) Solutions | Automated Risk Analysis Tools | Cloud Security Posture Management (CSPM)