BeyondTrust

Supporting PCI DSS 4.0.1 compliance with BeyondTrust Identity Security Insights®

The compliance challenge

PCI DSS 4.0.1 puts identity at the center of protecting the cardholder data environment (CDE). Requirements 7, 8, and 10 demand least privilege, unique identification, strong multifactor authentication, disciplined control of application and system accounts, and continuous monitoring of access. Yet most CDEs are surrounded by unmanaged accounts, excessive standing privilege, and non-human identities (NHIs) that legacy tooling can't adequately see or assess. No single product makes an organization PCI compliant—but clear, provable visibility into identity risk makes the path far shorter.

How BeyondTrust Can help

BeyondTrust Identity Security Insights delivers the visibility, intelligence, and protection that PCI DSS 4.0.1 assumes, but rarely finds in place. Our solution discovers all identities—human, NHI, and agentic AI—across cloud and on-prem systems without agents, calculates True Privilege™ to reveal who can actually reach the CDE, and continuously detects the identity threats and control gaps auditors ask about. Identity Security Insights transforms identity from an audit liability into evidence you can present.

Requirement-to-capability mapping

PCI DSS 4.0.1 Requirement	How Identity Security Insights Helps	Evidence or Outcome
Req 2: Secure configurations for system components	Identifies identity-related configuration risks such as shared, dormant, orphaned, and over-privileged accounts.	Evidence of identity-related configuration risks requiring review or remediation.
Req 7: Access by need to know and least privilege	Surfaces excessive standing privilege and over-entitled accounts through True Privilege™ and Paths to Privilege™ analysis.	Prioritized view of who can reach the CDE, so access can be right-sized.
Req 8.2: Unique identification for all users	Discovers shared, generic, orphaned, and dormant accounts across the estate.	Inventory of accounts that break unique-ID expectations, ready for remediation.
Req 8.3 to 8.5: Strong authentication and MFA	Detects privileged accounts and access paths that lack MFA or strong authentication.	Gap list of unprotected privileged access to target for MFA enforcement.
Req 8.6: Application and system accounts	Identifies non-human identities, service accounts, and secrets sprawl, including hardcoded credentials.	Visibility into machine identities and secrets that fall outside manual review.
Req 10: Log and monitor all access	Continuously monitors identity behavior and detects identity threats mapped to MITRE ATT&CK.	Ongoing detection and alerting that supports access monitoring obligations.
Req 12.3: Targeted risk analyses	The Identity Security Risk Assessment (ISRA) delivers a repeatable, evidence-based identity risk review.	Documented, periodic assessment of identity risk to the CDE.

Key capabilities

- Agentless discovery of all human and non-human identities across cloud and on-premises environments
- True Privilege to reveal effective access to the cardholder data environment
- Paths to Privilege to visualize and prioritize identity attack paths into the CDE
- NHI and secrets sprawl detection for application and system accounts
- Continuous identity threat detection, with prioritized, contextual recommendations

From assessment to assurance

Start with an Identity Security Risk Assessment to baseline identity risk to your cardholder data environment, then use Identity Security Insights for continuous monitoring. Where remediation is needed, Identity Security Insights informs the BeyondTrust Pathfinder Platform's privilege-centric identity security portfolio, including Password Safe®, Endpoint Privilege Management, Privileged Remote Access, and Entitle, to enforce least privilege and secure credentials.