DETECT COMPROMISED CREDENTIALS
PREVENT ATO & FRAUD

ENZOIC

Helping Organizations Achieve PCI-DSS Compliance

Enzoic directly strengthens employee account authentication in Active Directory by blocking weak/compromised passwords at change/reset and continuously detecting compromised passwords, tightening PCI DSS v4.0.1 alignment for Requirements 8.3.6 and 8.3.9.

PCI password requirements in scope

Requirement 8.3.6 mandates password/passphrase complexity: "minimum length of 12 characters (or... eight)" and "contain both numeric and alphabetic characters." PCI guidance also calls out comparing proposed passwords to a "bad password list."

Requirement 8.3.9 (single-factor password-only) requires **either**: **(a)** change at least every 90 days, or **(b)** "security posture... dynamically analyzed" with real-time access automatically determined. Guidance describes posture inputs such as device integrity, location, access times, and resources accessed.

What Enzoic enforces

Enzoic installs a Microsoft-standard password filter that gates password changes/resets and checks candidate passwords against a continuously updated compromised-password database using a partial-hash lookup; compromised passwords are rejected.

Policy controls include minimum length, required number, and required alphabetic (upper/lowercase) checks, plus screening admin-performed resets (help desk resets included).

Continuous monitoring detects password compromise on a daily 24-hour cadence and can automatically remediate by forcing change at next logon or disabling the account (immediate or delayed).

Privacy-by-design: monitoring can send only the first 10 characters of a hash and compare full matches locally.

Other PCI mappings

Requirement 8.3.8 (user guidance): authentication policies/procedures must be communicated (including strong-factor guidance and instructions on compromised passwords). Enzoic Client surfaces password requirements and rejection reasons on the Windows change-password UX with real-time feedback, reducing "policy ambiguity."

Requirement 10.2.1.5 (audit logging): audit logs must capture "all changes to identification and authentication credentials." Enzoic produces SIEM-ingestable JSON events for password changes, rejections, compromise detections, and remediation actions.

PCI Security Standards Council®

Evidence to show auditors

Screenshots of Enzoic Monitoring Policies showing: min length, number requirement, screen password changes, screen admin resets, monitoring + remediation action.

Test Page results demonstrating rejection of a known compromised password and policy enforcement. Exported Enzoic JSON logs / SIEM records for PasswordChangeRejected and compromise/remediation events. Remediation records (tickets/exports) tying detections to forced change/disable with timestamps