Cybersecurity INSIDERS

SOLUTION REVIEW

Enzoic for Active Directory 3.6

Continuous Password Risk Management



WHY NATIVE AD PASSWORD CONTROLS FALL SHORT

Most enterprises run their identity perimeter on Active Directory, and most rely on AD's built-in password controls to keep that perimeter trustworthy. Those controls have not kept pace with how credential risk actually unfolds today. The traditional setup is familiar: minimum length, character composition rules, scheduled expiration, and account lockout thresholds. AD checks a password when the user creates it, then assumes that judgment holds until the next scheduled reset. For most of AD's history, that was a reasonable assumption. It no longer is.

A password that satisfies every AD policy at creation can show up in stolen credential data a week later. Employees reuse credentials across personal and corporate accounts, often without realizing the corporate account is exposed. Service accounts get shared informally between teams that have lost track of who actually holds the password. Dormant accounts keep their valid credentials for months. Passwords configured never to expire, often set years ago to avoid breaking a service or a printer, slowly become exposed as new breaches accumulate.

None of this is visible from the standard AD administrative view. Security teams typically piece the picture together through scripts, periodic audits, and adjacent tooling, and the work rarely produces a complete view of where the actual exposure sits.

The 2025 Verizon Data Breach Investigations Report (DBIR) puts numbers on the risk pattern. Among ransomware victims the DBIR team analyzed through infostealer logs and underground marketplace data, 54% had their domains appear in credential dumps before disclosure. The largest spike of those exposures appeared about two days before disclosure. That is a tight window, and organizations without continuous credential monitoring rarely catch the exposure in time to act on it.

Enzoic for Active Directory closes that gap. Version 3.6 brings identity-first threat intelligence, granular policy enforcement, account-risk reporting, and security operations workflow integration into existing AD environments, with the goal of catching exposed credentials before they become account takeover paths.

ENZOIC THREAT INTELLIGENCE AT A GLANCE



1,112 **breached credentials recovered per second by Enzoic**

Credential intelligence refreshed multiple times daily across breaches of all sizes, infostealer logs, honeypot networks, and proprietary collection.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

HOW ENZOIC WORKS INSIDE ACTIVE DIRECTORY

Closing the gap between a static password policy and a moving credential exposure surface requires more than tighter rules at the moment of password creation. Enzoic for Active Directory operates as a closed-loop system that runs across three connected stages: identify, monitor, and remediate. Each stage feeds the next.



IDENTIFY

Screen passwords against current credential exposure intelligence at every meaningful checkpoint, and separate confirmed exposure from internal noncompliance.

- Compare new and existing AD passwords against billions of compromised credentials from breach data, dark web sources, infostealer logs, honeypot networks, and proprietary research
- Screen username-and-password pairs as a separate, higher-confidence risk class beyond password-only matches
- Distinguish compromised credentials from out-of-policy passwords with explicit labels in the dashboard and reporting layer



MONITOR

Continuously check credentials between password changes, so a password safe yesterday gets flagged the moment it surfaces in a new breach.

- Run detection at password creation, on a continuous monitoring cadence, and on demand from the administrative console
- Apply granular policy controls across the directory: length rules, character requirements, custom dictionaries, fuzzy matching, similar-password detection, and username-derivative blocking
- Surface password and account hygiene conditions that quietly accumulate in AD: shared passwords, accounts with no password set, never-expiring passwords, and stale accounts



REMEDIATE

Carry the response forward through users, administrators, and the SOC, closing the loop with audit-ready evidence.

- Notify affected users, force a password change at next login, and document remediation directly from the Enzoic console
- Push compromised and out-of-policy events to the SOC through CrowdStrike Falcon NG-SIEM or any standard SIEM via JSON event logs
- Guide the user reset with real-time policy feedback that reduces helpdesk volume and reset-cycle confusion

Account takeover prevention through continuous credential exposure monitoring

PRIVACY-PRESERVING CREDENTIAL CHECKS

Enzoic uses a partial-hash comparison model for cloud lookups and performs likely-match analysis locally, so sensitive credential material never leaves the customer environment. Security and compliance teams can validate compromised-password checks without creating a new credential exposure path.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

KEY CAPABILITIES IN VERSION 3.6

The three-stage operating model shows up as six product capabilities, each tied to one or more stages. Together they turn AD password risk into something teams can identify, monitor, and remediate inside the directory they already run.

1

Identity-First Threat Intelligence (Identify)

Underpinning the solution is Enzoic's identity-first threat intelligence, focused on credential, PII, and identity attribute exposure rather than generic indicators. Sources include human-led research, proprietary collection, dark web monitoring, honeypot networks, and infostealer log ingestion. Beyond single-password screening, Enzoic monitors username-and-password pairs as a higher-confidence risk class. Without this intelligence layer, the five capabilities that follow are mechanical features. With it, they form a continuous credential exposure system.

2

Granular Policy Enforcement (Monitor)

Administrators can define precise password policy controls and apply them differently across the directory. Length rules, character class requirements, custom dictionaries, username-derivative blocking, fuzzy matching, and similar-password detection give policy designers significantly more precision than native AD alone, with compromised credential screening in the same workflow. The point is policy precision, not policy complexity.

3

Compromised vs. Out-of-Policy Distinction (Identify)

The administrative dashboard treats compromised credentials and out-of-policy passwords as separate categories with explicit labels in the UI and reporting layer. A compromised credential indicates known breach exposure; an out-of-policy password indicates internal noncompliance. Separating the two gives security and IT teams a clearer view of severity, so confirmed exposure does not get buried under routine policy alerts.

4

Account Hygiene Reporting (Identify, Monitor)

Reporting in 3.6 surfaces the password and account conditions that quietly accumulate in AD: compromised and out-of-policy users, shared passwords, accounts with no password set, never-expiring passwords, and stale accounts. Centralizing the views moves administrators from reactive enforcement to proactive risk discovery, with the option to refresh against live data and trigger remediation from the dashboard.

5

CrowdStrike Falcon NG-SIEM Integration (Remediate)

Enzoic exports JSON event logs that integrate with any SIEM, with CrowdStrike Falcon Next-Gen SIEM as one of the prebuilt integrations. Password-risk alerts push directly into Falcon, where compromised and out-of-policy events appear alongside broader telemetry. Routing Enzoic events into the SOC workflow gives analysts credential context where they already investigate suspicious activity. Custom SMTP support also lets administrators send Enzoic notifications from their own domain.

6

Real-Time Password Feedback for End Users (Remediate)

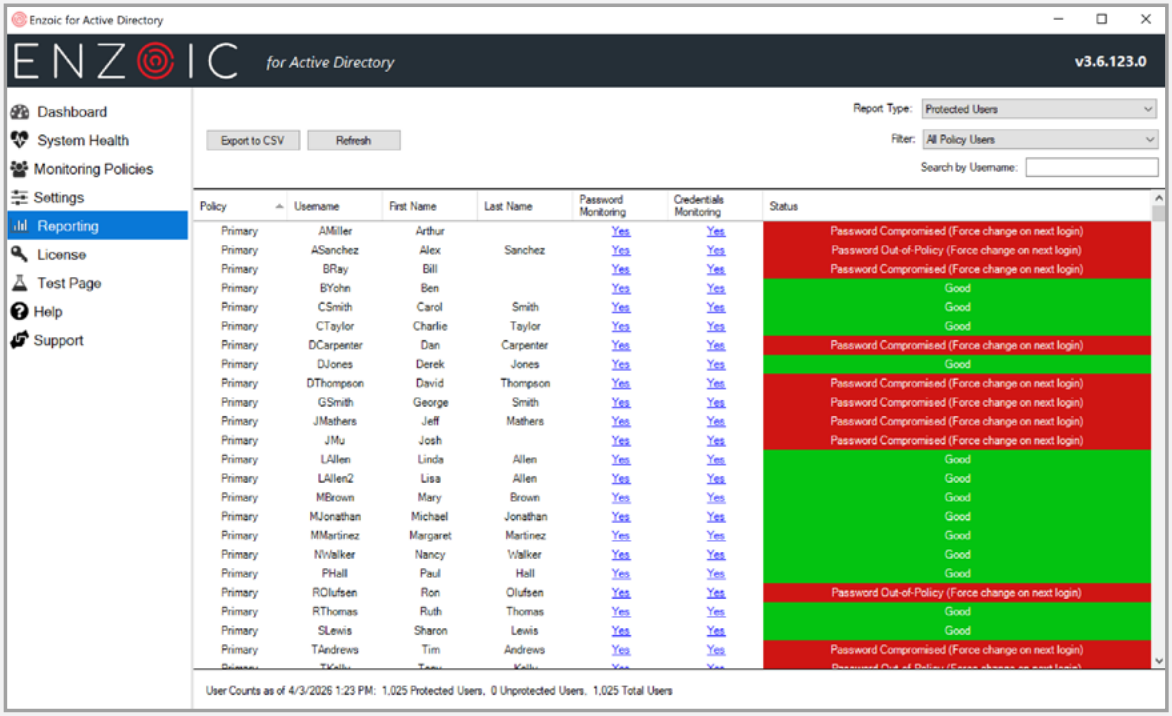
The Windows client provides live policy guidance directly on the standard Windows password-change screen. As the user types, length, character rules, custom dictionary terms, and compromised-password checks all show their status in real time, and a previously breached password is flagged as compromised rather than just rejected. The result is a guided remediation experience that reduces helpdesk volume.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

THE WORKFLOW IN PRACTICE

Capabilities translate into workflow once they reach the dashboard. A security engineer opens Enzoic during a routine review. The dashboard separates users with compromised credentials from users whose passwords are out of policy, and the compromised set takes priority because it represents known exposure.

The engineer refreshes the report against current credential intelligence and checks related AD hygiene reports for never-expiring passwords, stale accounts, shared passwords, and other risk conditions. Enzoic events flow into the dashboard or SIEM, where SOC analysts can correlate credential exposure with other suspicious activity in the same investigation surface.



The Reporting view shows per-user password and credentials monitoring status across the entire directory, with compromised, out-of-policy, and good states clearly distinguished and ready for one-click remediation.

Enzoic continuously monitors AD credentials for confirmed exposure and can automatically remediate risks based on configured policy, giving teams a set-it-and-forget option for exposed passwords. Findings are also surfaced immediately in the dashboard, where admins can review affected users and manually trigger remediation or force password changes when they want direct control. Users complete the reset with real-time feedback that shows which requirements have been met. The workflow closes the loop: identify exposure, monitor continuously, remediate fast, and document the outcome. It runs inside one console, against existing AD infrastructure, without replacing the identity layer organizations already depend on.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

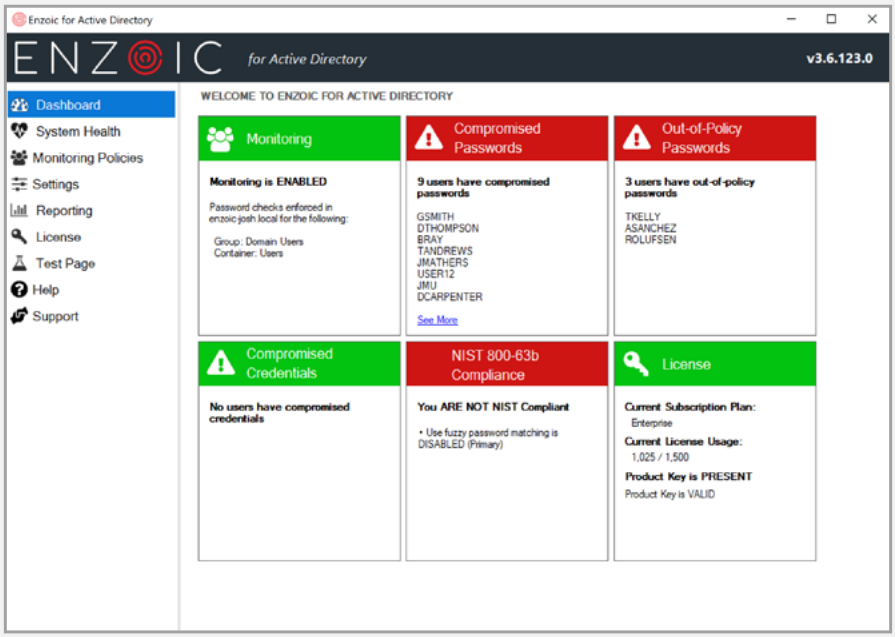
"After deploying Enzoic for Active Directory, Hylan was able to follow NIST standards and eliminate all compromised passwords from our Active Directory environment. The installation process took only one hour across our eight domain controllers. This project allowed us to improve enterprise security and reduce helpdesk resources dedicated to passwords by 90%."

Ramon Diaz, Director of IT, Hylan

OPERATIONAL AND COMPLIANCE VALUE

For security and IT teams, Enzoic closes the gap between what password policy says and what the directory actually contains. Risky accounts surface faster, teams spend less time stitching together directory evidence, users get clearer guidance during password changes, and password-risk events flow into the tools analysts already use.

For compliance and audit teams, Enzoic produces the evidence trail. It supports alignment with password security requirements tied to NIST 800-63B, NIST IA-5, HITRUST, and internal security policies. Its NIST-oriented configuration helps organizations align with core guidance for password length, compromised-password screening, and evidence-based remediation. For organizations that also need to satisfy internal or legacy complexity rules, Enzoic provides additional controls for character classes, custom dictionaries, username derivatives, and similar-password detection.



Dashboard showing NIST password-guideline compliance

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

Where Enzoic Extends Native Microsoft Password Controls

Many organizations rely on native Microsoft password controls as part of their identity security program. In most AD environments, security teams need deeper compromised credential intelligence, continuous post-creation monitoring, and richer account-risk reporting than native controls provide on their own. Enzoic adds that layer directly into Active Directory.

Native Microsoft Password Protection	Enzoic Extends With
EXPOSURE INTELLIGENCE	
Microsoft Entra Password Protection uses a limited global banned-password list built from Microsoft Entra security telemetry. Microsoft states the global list is not based on external third-party compromised-password lists.	Identity-first intelligence refreshed multiple times daily across breach data, infostealer logs, and proprietary collection. Enzoic's compromised credential intelligence delivers the broadest coverage of exposed passwords and credentials, enabling earlier detection of risk.
POST-CREATION MONITORING	
Entra Password Protection only evaluates passwords at change or reset.	Continuous monitoring with automated remediation when a previously safe password becomes compromised.
CREDENTIAL SCREENING SCOPE	
No credential screening available.	Username-and-password pair monitoring, with paired exposures treated as a higher-confidence risk class.
NIST 800-63B ALIGNMENT	
Lacks the controls needed to support NIST SP 800-63B alignment.	One-click NIST 800-63B compliance configuration with continuous monitoring against breach data.
ACCOUNT HYGIENE REPORTING	
No native reporting on shared passwords, no-password accounts, never-expiring passwords, or stale accounts.	Centralized hygiene reports on compromised users, shared passwords, blank passwords, never-expiring passwords, and stale accounts, with on-demand refresh and one-click remediation.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

How Enzoic Deploys

Enzoic for Active Directory deploys as a software plugin that integrates with existing AD Domain Controllers through a password DLL filter. It enforces controls centrally, without requiring a broad workstation agent rollout for core protection. Most environments install and configure in 15 minutes or less. Optional Windows endpoint agents enable the real-time as-you-type feedback experience during password resets. The product runs on a subscription model scaled to the number of protected accounts, with a free Startup tier covering up to 20 users, paid Business and Premium tiers, and a custom Enterprise tier.

The Bottom Line

Enzoic for Active Directory gives AD teams a continuous way to detect, prioritize, and resolve password risk. It turns exposed-credential intelligence into enforceable directory action, separates confirmed exposure from policy noise, and documents remediation as it happens.

The fit is clearest for organizations running Active Directory at the identity layer, working toward NIST 800-63B or other regulatory alignment, and looking to retire periodic password resets without losing audit evidence. The free Startup tier covers up to 20 users and can validate the model in under an hour.

The free Enzoic for Active Directory Lite Auditor scans an existing AD environment and quantifies password exposure before any commitment.

ENZOIC

ABOUT ENZOIC

Enzoic is an enterprise-focused cybersecurity company committed to preventing account takeover and credential-based fraud through identity-first threat intelligence monitoring. Organizations use Enzoic solutions to screen customer and employee accounts for exposed passwords, credentials, and PII, identifying accounts at risk and mitigating unauthorized access.

CUSTOMERS INCLUDE: Motion Picture Association, Backblaze, OneLogin, and LogMeIn. Protecting Active Directory environments across healthcare, financial services, government, education, and the public sector.

Learn more about Enzoic at: **www.enzoic.com | info@enzoic.com**

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved