ENZOIC INTEGRATION WITH IAM SOLUTIONS

Responding to the Threat of Compromised Credentials

IAM

Enzoic for Active Directory combines real-time password policy enforcement with continuous password auditing and automated remediation to keep unsafe passwords out of Active Directory.

What distinguishes Enzoic is our unique approach to helping organizations prevent the #1 cause of a data breach while ensuring full, automated compliance with industry benchmarks like NIST and HITRUST. Our value proposition goes beyond defense; we're about maximizing resource efficiency, especially in IT and helpdesk, allowing organizations to redirect the saved time and financial resources to other critical areas.

Enhancing IAM with Enzoic

Real-Time Compromised Credential Monitoring

Enzoic's proprietary tools and threat research team continuously scan the Dark Web and other illicit sources for compromised credentials, providing real-time alerts when users' account details are compromised. An integration enables IAM solutions to promptly notify end users of compromised accounts, prompting immediate password changes and securing accounts before they can be exploited.

Automated Response and Remediation

Integrating Enzoic allows IAM solutions to automate responses to compromised credentials. This includes enforced password resets, account lockouts, and MFA enforcement, ensuring that compromised accounts are quickly secured. Such proactive measures significantly mitigate the risk of unauthorized access and data breaches.

Enhanced Risk Scoring

Enzoic's data empowers IAM solutions to enforce stronger, more dynamic security policies based on real-time threat intelligence in tandem with other variables such as unusual login patterns or high-risk geolocation. These policies can prohibit the use of known compromised passwords and enforce stricter authentication protocols. This proactive stance ensures that security measures evolve in tandem with emerging threats.

Proactive Threat Mitigation

End users benefit from immediate notifications and automated remediation actions when their credentials are compromised. This proactive threat mitigation reduces the window of opportunity for attackers, minimizing potential damage and ensuring continuous protection.

Automated Credential Expiry

Utilizing Enzoic's data, IAM solutions can automatically expire and prompt users to change credentials that have been compromised. This automated approach ensures that vulnerable credentials are updated, maintaining a higher standard of security and time savings versus outdated time-based password resets.

Adaptive Access Control

Enzoic's threat intelligence can inform adaptive access control policies, adjusting user permissions in real-time based on detected threats. For example, access to sensitive systems can be restricted if a user's credentials appear on a list of compromised accounts, limiting potential damage.

Enhanced Incident Response

Incorporating Enzoic's real-time data into incident response workflows enables quicker identification and mitigation of threats. Security teams can investigate incidents involving compromised credentials and take preemptive measures to protect affected accounts.

Policy Compliance and Auditing

Enzoic's data can support compliance with a wide array of security policies and regulatory requirements by providing verifiable evidence of proactive measures against compromised credentials. This integration streamlines auditing processes and demonstrates adherence to security best practices. To view all the compliance standards supported by Enzoic integration, please visit our compliance standards webpage.

YOUR COMPETITIVE ADVANTAGE

Contemporary compliance standards and industry research show the important role of compromised credentials in data breaches, making the integration of Enzoic's enhanced security features into IAM solutions increasingly necessary as organizations prioritize this area of risk. By addressing credential-based threats comprehensively, these solutions align with market demands for robust security measures, thereby driving higher sales and revenue for IAM providers. Additionally, incorporating Enzoic's Dark Web data helps providers stay competitive with other IAM solutions that are beginning to include this functionality.

IAM solutions can stay ahead of attackers by providing the best protection and peace of mind to their end users.