DETECT AND BLOCK
COMPROMISED CREDENTIALS

Compromised credentials from data breaches have become the new attack vector. They undermine the integrity of an essential security layer and leave your workforce and consumer accounts open to penetration, fraud and PII loss.

ENZOIC

Even if your site hasn't been breached, it is at risk of account takeover due to password reuse.

Billions of username and password pairs have been exposed due to an unprecedented volume of third-party data breaches, which are now readily accessible on the Internet and the Dark Web. As password reuse across multiple platforms is a common practice, this exposes a significant security risk; cybercriminals can leverage these credentials to infiltrate your corporate network or hijack customer accounts, posing a grave threat to personal and organizational security.

Protect Your Customers

The ramifications of such breaches extend beyond immediate unauthorized access. Protect your customers: Account takeover (ATO) attacks not only strip loyal customers of their account's value and personal data but also cost businesses billions in fraudulent activities, all while inflicting long-lasting damage to a company's hard-earned reputation. Moreover, this erosion of trust can have a ripple effect, deterring potential customers and shaking the confidence of existing ones.

Protect Your Organization

In terms of internal security, the stakes are equally high. Protect your employees and your organization: Attackers who initially gain foothold through compromised credentials can exploit further vulnerabilities or use social engineering tactics to escalate privileges. This allows them to delve deeper into corporate networks, potentially accessing sensitive data, disrupting operations, or laying the groundwork for more insidious threats such as ransomware. It is essential to recognize that a single compromised credential can be the linchpin for a broader security catastrophe.

Enzoic makes it easy to identify exposed credentials, harden the password layer, and block account takeover attempts.

- ATO attacks increased **354%** year-over-year in 2023
  Sift
- Compromised credentials are the **#1** cause of a data breach
  2023 Verizon DBIR Report
- **88%** of users admit to reusing passwords
  LastPass Psychology of Passwords 2022
- **34%** of North American companies suffered a data breach that cost between $1 million and $20 million in the past three years
  2023 PwC Global Digital Trust Insights Report
- **$4.45** million is the global average cost of a data breach
  IBM
- NIST compliance requires screening for compromised passwords.
  NIST SP 800-63B and IA-5

"The password is by far the weakest link in cybersecurity today."
Michael Chertoff, Former Head Homeland Security CNBC.com

How Does It Work?

ENZOIC

Enzoic's solutions draw from a continually updated proprietary cloud database of exposed login credentials collected from the Internet and Dark Web. Enzoic clients leverage APIs built for the largest consumer scale environments to securely access the database and detect compromised credentials for their users, customers, or employees.

Harden Passwords

Check passwords against cracking dictionaries and compromised passwords upon set up, login or password reset. This protects against easy-to-guess passwords and hardens the directory against offline cracking. This practice is explicitly recommended in NIST 800-63B, NIST IA-5, and HITRUST frameworks.

Prevent Account Takeover

Check username and password combinations against known compromised credentials. This protects against "password reuse" threats and online credential stuffing attacks with no false positive and false negative alerts of rules-based detection.

Detect Credential Exposure

Monitor domain accounts to see if they have been compromised and receive alerts on data breach exposures to help you mitigate the risk associated with those accounts.

How do you better protect your customers and your organization?

- Protect your environment from account takeover
- Detect compromised credentials in real-time
- Screen to prevent commonly used and known passwords
- Monitor by domain accounts

Why Enzoic?

Specialized Research
Our analysts are entirely focused on aggregating credentials from the public Internet and Dark Web using manual research and extensive data normalization efforts.

Reduced Attack Window
Immediately begin blocking attackers as soon as credentials are indexed, substantially reducing the time your environment is at risk.

No False Positives
Enzoic confirms current username and password combinations are actually compromised, reducing unnecessary alerts.

Hardening the Password Layer
Restrict commonly used or compromised passwords, assuring uniqueness that substantially reduces the effectiveness of cybercriminal guessing or cracking attempts.

Zero Impact on User Experience
Unlike authentication solutions that add steps or devices, Enzoic works seamlessly and flags a definitive risk in the password layer.

Secure Data Exchange
Neither credential data nor hashes pass in either direction.