

# DETECT COMPROMISED CREDENTIALS PREVENT ATO & FRAUD



ENZOIC

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.

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

Billions of username and password combinations are circulating on the Internet and Dark Web from a record number of 3rd party data breaches.

Since most people reuse passwords across multiple websites, cybercriminals can obtain credentials that can be used to gain unauthorized access to your corporate network or customer accounts.

### Protect Your Customers

Account takeover (ATO) attacks drain loyal customers' accounts of value and personal information resulting in billions of dollars in fraud and damage to brand reputation.

### Protect Your Employees and Organization

Attackers can gain access and use social engineering or other vulnerabilities to escalate privileges and penetrate corporate networks.

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

- 🔒 21% of consumers have had an online account compromised *CSID*
- 🔒 73% of people reuse passwords across accounts *Telesign*
- 🔒 81% of hacking-related breaches leveraged stolen or weak passwords *Verizon 2017 DBIR*
- 🔒 100% of the cases we investigate can be traced to stolen credentials *Mandiant*
- 🔒 NIST now requires screening for compromised passwords *NIST SP 800-63B*
- 🔒 \$3.62 million is the global average cost of a data breach *Ponemon*
- 🔒 \$184 million to \$332 million is the average loss to the value of a brand from a data breach *Experian*

---

“The password is by far the weakest link in cybersecurity today.”

*Michael Chertoff, Former Head Homeland Security CNBC.com*

---

# How Does It Work?

Enzoic's solutions draw from a massive 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 the new NIST 800-63B.



## 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 accounts from hijacking
- 🔒 Detect logins from 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

Unlike threat intel feeds of usernames, Enzoic confirms current username and password combinations are actually compromised, reducing unnecessary alerts and user frustration.

## 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 or even hashes pass in either direction.

