IDENTITY-FIRST THREAT INTELLIGENCE

HARNESSING DARK WEB SIGNALS TO STRENGTHEN IAM AND AD SECURITY

ENZOIC

Identity Is the New Perimeter (and Attackers Know It)

For decades, enterprise security was built around the concept of keeping threats outside the network. Firewalls, VPNs, and perimeter defenses protected corporate infrastructure, and everything inside was trusted.

The model is long gone.

Today, attackers don't need to breach the perimeter. They log in with legitimate credentials that have been stolen, purchased, or harvested, then move laterally through your environment as trusted users.

Recent breach data validates this:

Stolen credentials remain the top action in Basic Web Application Attacks, appearing in 52% of breaches in that category

Exploitation of public-facing applications surged 44% year-over-year, accounting for 40% of incidents observed in 2025, even as attackers expanded credential harvesting operations through AI chatbot ecosystems and infostealer campaigns

Credential abuse appears across 39% of all breaches, making it the single most pervasive technique across the full attack chain

The Shift to Identity

When attackers are logging in with valid credentials rather than exploiting vulnerabilities or deploying malware, perimeter defenses have nothing to detect. The threat is already inside.

For teams managing Active Directory, identity providers, and authentication workflows, this has immediate consequences. Every credential in the environment is a potential entry point. And unlike a firewall rule or a patch, a compromised credential looks like a legitimate login.

eBook TLDR

This paper explores why a different approach that integrates Dark Web threat intelligence is required. It covers:

1. **How the infostealer economy has industrialized credential theft**
2. **Why password reuse turns any consumer breach into an enterprise risk**
3. **Where traditional IAM and AD tools fall short**
4. **What identity-first threat intelligence looks like**
5. **How to operationalize continuous monitoring across Active Directory and application environments**

The Infostealer Economy: How Compromised Credentials Reach the Dark Web

Credential theft is no longer a manual, opportunistic exercise. It's an industrialized operation powered by Malware-as-a-Service (MaaS) platforms that make sophisticated harvesting accessible to any threat actor willing to pay for it.

The Infostealer Problem

The scale of the issue is staggering. In 2025 alone:

1.95B

1.95 billion malware-sourced credential exposures were detected

276M

276 million of those credentials included active session cookies, enabling attackers to bypass MFA entirely

2.86B

2.86 billion compromised credentials were identified, with business cloud and authentication services accounting for more than 30% of all exposed data

87

The average compromised device yielded 87 stolen credentials, spanning corporate applications, personal accounts, and cloud services accessed from the same machine

How the Model Works

Infostealers like Lumma, Raccoon, and Vidar operate as turnkey criminal products. An attacker doesn't need technical sophistication. They subscribe to a MaaS platform, deploy the malware via phishing emails or malicious downloads, and the stealer does the rest, silently harvesting:

- Saved passwords from browsers and password managers
- Session cookies and authentication tokens
- Browser fingerprints and device information
- Autofill data, including passwords, email addresses, and usernames

That data is packaged into logs and sold on Dark Web marketplaces and Telegram channels, often within hours of exfiltration.

This happens quickly:

53%

of stolen credentials were indexed within one week of theft, and 36% within 24 hours.

The Enterprise Exposure Risk

What makes this so dangerous for organizations is that infostealers now target corporate identity infrastructure.

Enterprise exposure more than doubled, rising from approximately **6% of infections in early 2024 to nearly 14% by late 2025**

Microsoft Entra ID appeared in **79% of enterprise identity logs,** making it the most impacted identity provider

Over **2 million infostealer logs exposed enterprise identity credentials**, providing attackers with potential access to corporate email, cloud infrastructure, SaaS platforms, and internal systems

In 18% of cases, one infected device exposed credentials for multiple identity providers (e.g., both Entra ID and Okta), giving attackers several entry points from one compromise

Infostealer malware also led to more than 300,000 ChatGPT credentials ending up on the Dark Web, signaling that AI platforms now carry the same credential risk as core enterprise SaaS

Why Periodic Checks Fail

The volume and velocity of attacks render traditional password screening obsolete. A credential that was safe at creation can be compromised hours later through an infostealer infection on an employee's personal device. And of course, infostealers are not the only path to compromise; other tactics include phishing, brute force, credential stuffing, password spraying, keyloggers, third-party breaches, hardcoded credentials in code repositories, misconfigured cloud storage, and SIM swapping.

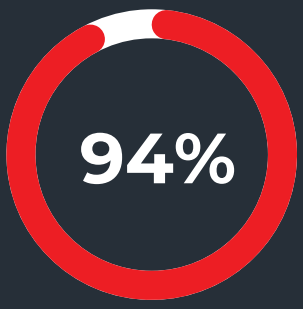
The rate of theft is increasing, with 50% more credentials exposed in the second half of 2025 than the first, and 90% more in Q4 than Q1. As a result, the risk is compounding.

Security teams need to shift their focus from whether credentials in their environment have been exposed to how quickly they can detect and respond when they are.

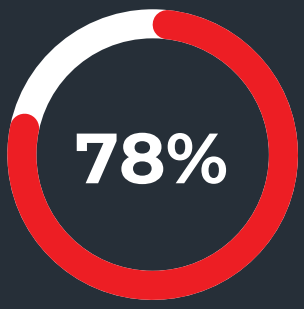
Why Consumer Breaches and Enterprise Risk Collide

The Reuse Reality

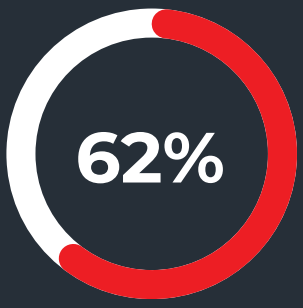
Password reuse is one of the most well-understood risks in cybersecurity, as it turns every consumer data breach into a potential corporate compromise. Despite decades of evidence around the risks, the practice continues as people sacrifice security for convenience to avoid the frustration of being locked out of accounts and having to reset passwords.



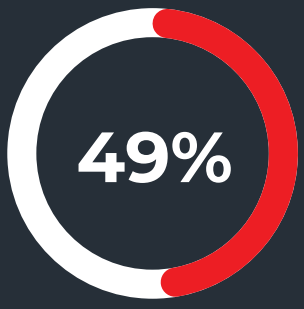
A study of over 19 billion leaked passwords found that 94% were reused or duplicated



78% of people use the same password for more than one account, with 52% reusing it across at least three



62% of workers reuse passwords or rely on close variations across professional accounts



Verizon's analysis of infostealer logs found that in the median case, only 49% of a user's passwords across different services were distinct

The Reuse Attack Vector

An employee uses their work email to sign up for a personal shopping site or a free SaaS tool. That site gets breached. The exposed credential, the same one protecting their corporate accounts, is now circulating on the Dark Web.

The attacker doesn't target the organization directly. They test the stolen credential against corporate login portals. If the password matches, and statistically it often does, they walk straight in. No exploit required. Just a valid login.

This plays out at scale. Verizon found that credential stuffing accounts for 19% of all daily authentication attempts against single sign-on (SSO) providers, blending into normal traffic and rarely triggering lockout protections.

73% of ransomware victims in the 2026 DBIR had an associated infostealer infection or credential leak event in the year preceding the attack. And half of those experienced it within 95 days of the ransomware strike. The credentials were already circulating, and the ransomware was the outcome.

Where Visibility Breaks Down

More than 56% of respondents in a 2025 Osterman Research study said they could not immediately detect when employees' credentials appeared on Dark Web forums, and only 19% reported complete visibility into active identity threats such as the sale of compromised passwords.

That visibility gap shows up operationally inside IAM and Active Directory environments. Compromised password mitigation represented 16% of Enzoic's partner effort in 2025, with exposure detected during login and password reset or additional remediation triggered according to each organization's policy. Enzoic's Active Directory data analysis also identified nearly 10,000 password-sharing incidents among users.

A single reused password, exposed in a breach the organization had nothing to do with, is all it takes.

Why Traditional IAM Falls Short

Conventional IAM tools and native Active Directory protections were designed to enforce password policy, not to detect stolen credentials.

Built for Policy, Not for Threats

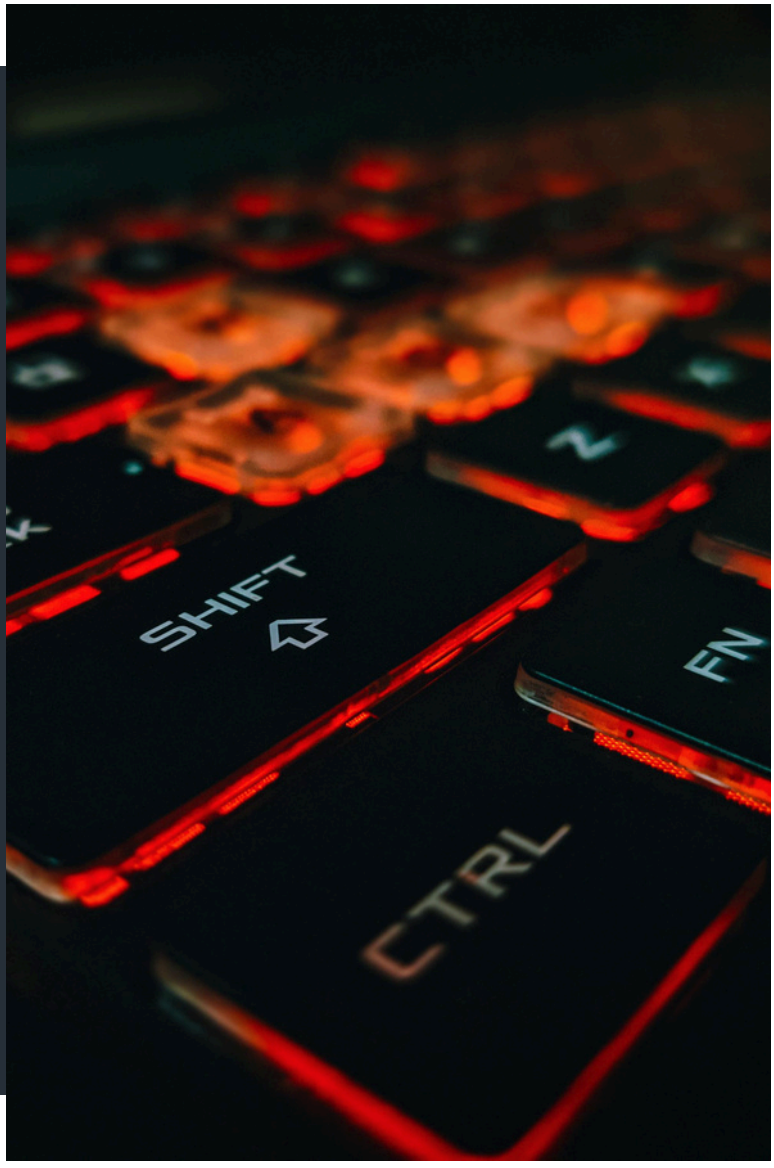
Microsoft Entra ID Password Protection, the most widely deployed native defense, screens passwords at creation and reset. Between those events, there is no monitoring. A credential can be exposed, traded, and exploited without generating a single alert.

Entra ID has additional weaknesses:

Limited intelligence: Passwords exposed in breaches, infostealer logs, or Dark Web datasets may still pass if they are not captured by Microsoft's limited banned-password evaluation or are exposed after the password is set.

Policy focus, not credential exposure focus: It is designed to block weak, common, and predictable password choices rather than serve as a breached-credential monitoring layer.

No credential pair checking: Entra Password Protection evaluates password choices, not exposed username/password combinations.



What This Means in Practice

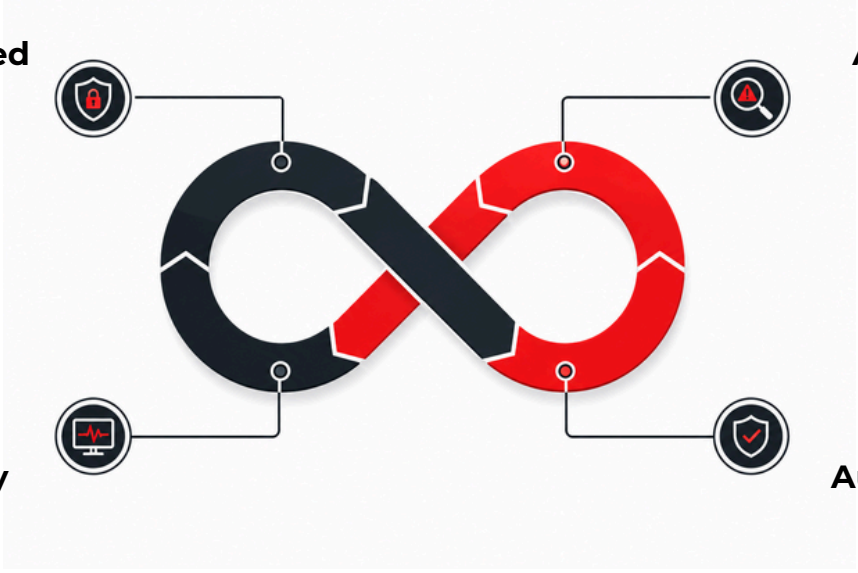
An employee sets a strong password in April. In July, that same credential appears in a third-party breach or infostealer log, but the next scheduled change isn't until October. For three months, that compromised credential is the key to Active Directory and every application connected to it. As the password met the policy requirements when it was set, there is no flag. It simply stopped being safe.

The Case for Identity Threat Detection

These issues have driven the emergence of Identity Threat Detection and Response (ITDR). Traditional IAM enforces policy. ITDR adds detection and response at the identity layer, closing the window between compromise and action.

But most organizations still lack this capability, and those that have it rarely connect it to Dark Web intelligence. Without that signal, teams cannot identify which credentials are already in the hands of attackers.

Continuous Monitoring for Compromised Credentials



Identity-First Threat Intelligence:

Continuous Monitoring for Compromised Credentials

Some companies attempt their own threat intelligence and/or curate blacklists of passwords that are known to be weak or previously compromised. But these efforts simply can't keep pace with the rate of credential exposure, which is where Enzoic comes in.

The company vets password and username combinations against its dynamic database of billions of exposed credentials. Maintained using a combination of proprietary automated processes and research from Enzoic's threat intelligence team, the platform is updated multiple times per day. This allows organizations to proactively spot and block compromised credentials before threat actors can utilize them.

In Active Directory environments, this means enforcing safer passwords from the start and rechecking them on an ongoing basis against live threat intelligence. Enzoic's AD plugin uses secure partial-hash comparisons so companies can identify exposure without revealing them in plaintext, which helps preserve privacy while eliminating credentials as a threat vector. Should a previously safe password become compromised, organizations can automatically activate a remediation plan with a variety of actions based upon the threat's severity.

The same intelligence can extend beyond AD through APIs that plug into IAM platforms, authentication services, and security tools. Enzoic supplies credential risk signals that help organizations determine whether to allow access, require additional authentication mechanisms, or force a password reset.

We'll explore these capabilities further in the following sections, beginning with Enzoic for Active Directory.

Strengthening Active Directory

Active Directory remains the backbone of enterprise authentication, which makes it a high-value target. Research estimates that approximately **90% of modern cyberattacks involve AD** at some point in the attack lifecycle. While it's impossible to eliminate all of these threats, hardening the environment can significantly enhance protection.

Enzoic for Active Directory

Enzoic for Active Directory screens newly created credentials against configurable password policies, custom dictionaries, username derivatives, common substitutions, and live exposure data. This allows companies to block terms specific to their business or industry and prevent users from selecting a weak, reused, or compromised password at the outset. As stated, however, credentials are only as secure as the latest breach data. Enzoic brings this threat intelligence into enterprise environments, continuously monitoring username and password pairs against its active exposure database.

The solution is the only AD product to provide this level of compromised credential protection. Enzoic also ensures **compliance with NIST 800-63B guidelines,** which require that all new or changed passwords be vetted against a list of those that are commonly used, expected, or compromised.

Because it is fully automated, Enzoic for Active Directory provides enhanced security peace of mind without requiring additional IT resources. The solution is easy to deploy, with some customers fully implementing it in just 15 minutes. What's more, Enzoic frees security teams to focus on other priorities by eliminating the work associated with periodic password changes and helpdesk reset requests.

The screening happens in the background, with users only becoming aware should a compromise be detected. Companies can then automatically activate a remediation plan with a range of customizable actions, including the immediate disabling of the compromised account. Enzoic for Active Directory also enables organizations to set specific password rules and remediation actions by Container, Group, or account. This allows them to have more aggressive monitoring and response as needed—for example, with accounts related to finance or IT.

Security Integrations

Active Directory protection is strongest when credential risk signals feed into the broader security ecosystem. Enzoic for Active Directory offers integrations with tools such as CrowdStrike Falcon NG-SIEM and Duo, ensuring this intelligence appears in the same place as other security telemetry. This makes it easier to correlate suspicious authentication behavior with endpoint, network, or cloud activity, and have visibility over remediation actions. The result is a more resilient AD posture with less manual intervention.

Extending Protection Across the Identity Stack: API-Driven Intelligence

Active Directory may be a ubiquitous enterprise product, but protecting it alone is not enough. Companies also authenticate employees, customers, partners, contractors, or other third-parties across multiple systems, and compromised credentials can enter through any of them. Enzoic offers a series of hosted REST APIs to keep exposed passwords out of these environments without rearchitecting existing identity infrastructure.

The APIs support password screening, credential checks, breach and identity monitoring, and domain-level alerting, making them ideal for IAM platforms, fraud prevention workflows, and compliance automation. That means a customer-facing website, partner portal, or a privileged-access workflow can all evaluate identity risk using the same threat intelligence that underpins Enzoic for Active Directory. The flexible architecture makes it easy to embed the APIs into existing systems or new applications. In addition, Enzoic offers language-specific SDKs to further reduce integration friction.

Rather than forcing a complete identity overhaul, API-based credential intelligence lets teams add risk checks at points where they already make access decisions. In practice, that can mean blocking a compromised password at reset, requiring step-up authentication for a risky login, or triggering compliance workflows when exposure is detected.

Building an Identity-First Security Strategy: A Practical Framework

Building an identity-first security strategy starts with recognizing that the threat is already inside. Compromised credentials are a welcome mat for attackers, and they won't leave on their own.

A practical first step is to align with NIST password guidance by focusing on credential compromise, rather than routine password expiration.

From there, companies should audit their Active Directory password health, including whether credential screening is implemented and if custom policy controls are being enforced. It's important to determine where password checks remain periodic or manual, as these are the gaps most likely to be exploited.

Extending credential intelligence into IAM platforms, customer authentication, and other systems where users login or reset passwords is the next consideration.

Deploying a solution that supports automated remediation is also critical, ensuring risky accounts can be challenged, reset, or disabled without waiting for human intervention.

With new credentials being exposed in real-time, identity security is not just about stronger passwords; faster detection and response are essential. Continuously monitoring for compromise allows companies to act before threat actors can. What's more, the approach reduces manual overhead and creates a more resilient authentication environment across the organization.

Bringing Identity Intelligence to Action

Enzoic is a leading provider of **compromised credential detection and account takeover prevention solutions.** As infostealer malware continues to surge, Enzoic protects organizations by monitoring for credentials and PII exposed through data breaches, malware campaigns, and dark web sources. With seamless integration into Active Directory and authentication workflows, Enzoic enables organizations to identify and block stolen credentials in real-time, stopping attacks before they succeed. Organizations worldwide trust Enzoic to mitigate credential-based risk and strengthen identity security. Learn more about Enzoic here and connect on Twitter and LinkedIn.