ENZOIC

MSP and MSSP

How to Solve the Password Problem

A detailed overview of the password problems that the market faces and how Enzoic solves the issues

2022

www.enzoic.com

Introduction

The range of services offered by Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) has evolved significantly since the industry's inception in the early 2000s. While the former are still focused primarily on supporting IT infrastructure and operations, security has become an increasingly important consideration for MSPs as well. Case in point, one survey found that 99% of MSPs are offering some form of security services in response to the rise in ransomware and other emerging threats.

Today's complex threat landscape also means that MSSPs have evolved their services to help companies better address and mitigate these vulnerabilities. Availing of AI, machine learning, automation, and other technologies is one way in which MSSPs are protecting the growing attack surface. These capabilities have made MSPs and MSSPs a popular option for companies of various sizes and sectors. However, as reliance on MSPs/MSSPs has increased so has their profile among the cybercriminal community and they are now a prime target of threat actors.

As a result of this uptick in attacks, the US. Cybersecurity and Infrastructure Agency (CISA), NSA and the FBI recently issued a warning to help MSPs protect against the threats facing them and their customers. Among the recommendations was that organizations adhere to best practices for password and permission management to prevent against brute force, password spraying, and other password-based attacks.

This might seem like common sense, but the number of breaches that result from poor password practices every year underscores that companies continue to ignore their password vulnerabilities. This is particularly dangerous for MSPs and MSSPs, as a breach in one company's network can easily lead to subsequent attacks on its customer base. For many organizations, the financial, reputational, and logistical damages of this situation is too much to withstand.

As such, it's imperative that the MSP and MSSP community prioritizes password security. After all, what's the point in investing in the latest AI-driven cybersecurity innovation if hackers can still access the network via a weak or compromised password?

Read on for more about the password problem and what MSPs and MSSPs can do to protect themselves and—most critically—their customers.

Passwords: The Good, The Bad and The Ugly

Passwords have been around for decades and despite claims of their imminent demise, organizations rely on them for identity and access management. They remain the most common means of authentication as they can be a low-cost, simple and effective tool for safeguarding information assets. Many users object to the friction caused by multi-factor authentication and rely solely on passwords. However, due to poor and ineffective password policies and users’ practices, they are often the Achilles' heel of many security postures. And when a password is compromised, it provides an easy enterprise entry point.As a result, compromised passwords have become the leading driver of data breaches.

The Data Breach Plague

Data breaches remain a constant threat as cybercriminals strive to exploit any weakness. No organization is immune from the risks; these breaches continue to spread seemingly unchecked from Fortune 500 companies to startups to countries. In recent years, there has been a surge in cyber incidents spanning ransomware, criminal hacking, phishing, and other malware attacks. And when you look under the hood, the most frequent source of these attacks is the password.

Password Deep Dive

The 2022 Verizon Data Breach Investigations Report (DBIR) highlighted the growing threat from breaches and the leading role of stolen credentials in fueling these attacks.

Out of all the security incidents, there 5,212 were confirmed data breach compared to 1,935 in 2017.

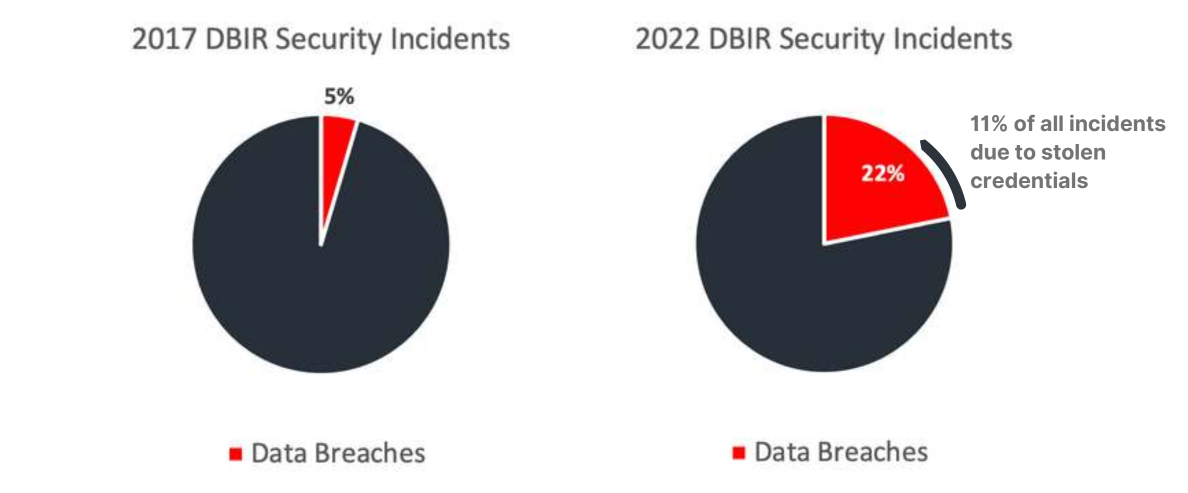


Figure 1: Number of Breaches (source: Verizon DBIR)

In 2021, the use of stolen credentials remained by far the most common entry point, occurring in nearly 50% of incidents with data breaches.

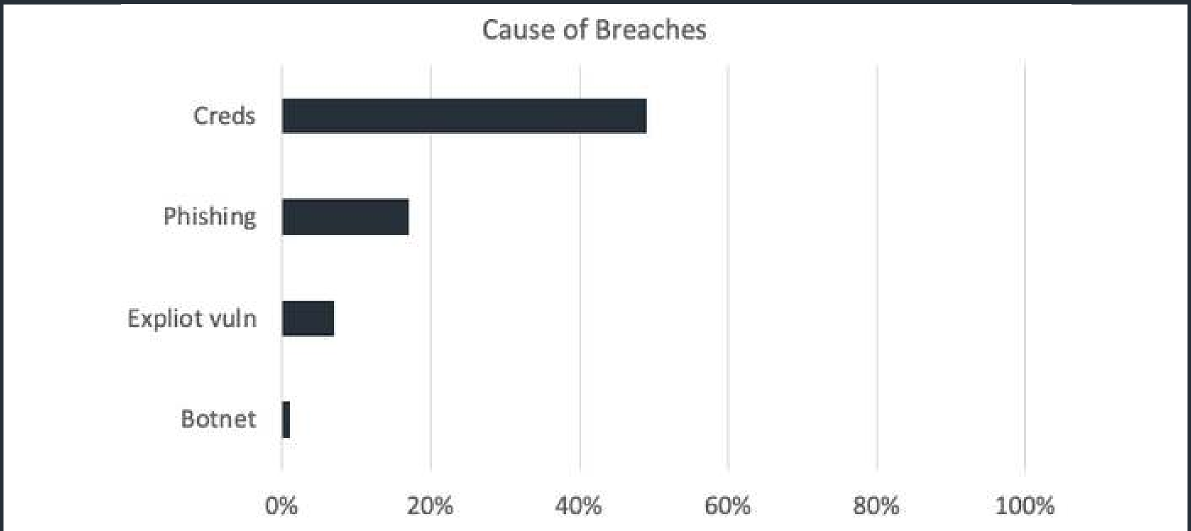
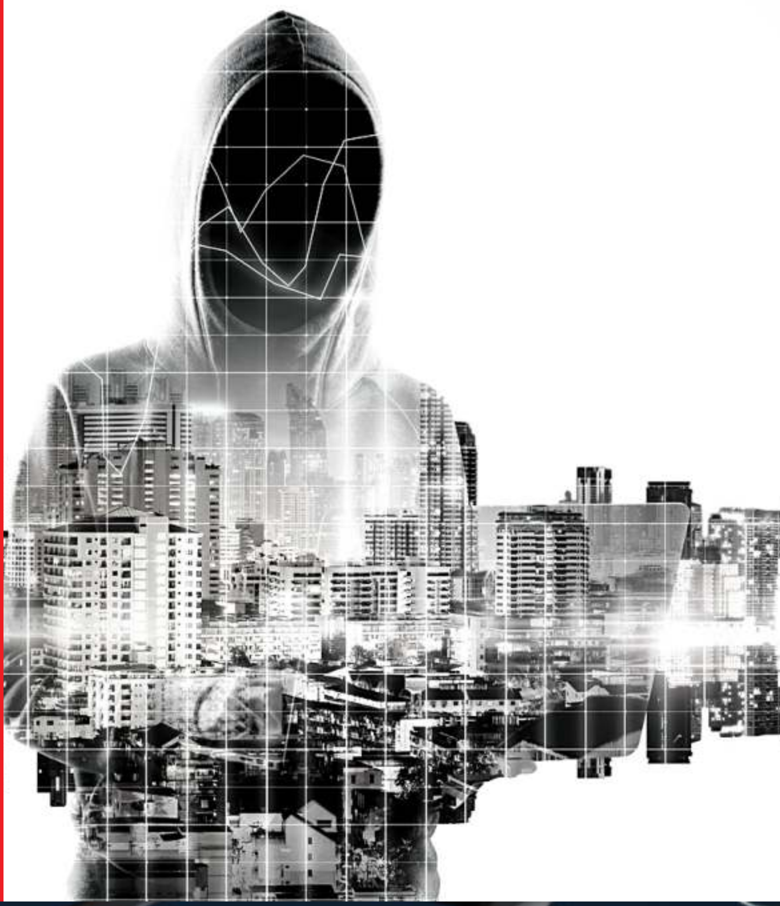


Figure 2: Initial Access Vectors (Source: Verizon DBIR)

As a result of the pervasiveness of data breaches and cybersecurity incidents, the volume of stolen credentials available on the Dark Web and the internet continues to grow exponentially. Once acquired, passwords are sold or distributed across the Dark Web to bad actors who are prepared to use them for various purposes, including financial gain, revenge and political agendas to name a few. The organization that has the data breach is vulnerable to nefarious activity; however, the problem worsens because so many people reuse passwords. As a result, bad actors can fraudulently access other accounts using the same username and password combination. The DBIR found cybercriminals, hackers and even nation-states are tapping into stolen credentials to power various cyber attacks.



Using Stolen Password for Cyber Attacks

There are multiple ways that stolen passwords are used to facilitate successful cyber attacks. Here are three of the most popular ones:

01 Brute Force Attacks

This automated attack is a high-volume guessing strategy reliant on trial and error to crack passwords to access individual accounts or an organization's systems. Cybercriminals use automated software to attempt as many guesses as possible to eventually find the right combination and gain access to an account. Brute force attacks rely on cracking dictionaries which include lists of common and compromised passwords, and it's a relatively simple yet effective tactic to gain unauthorized access.

02 Password Spraying

This approach relies on trying a few commonly used passwords against a large number of accounts. Its success assumes that there is likely to be a percentage of the population using a common and compromised password within any large group of people. This method is slower than a brute force attack but allows hackers to attempt to gain access without getting locked out.

03 Credential Stuffing

This method exploits the reuse of passwords by users across multiple sites and uses full credentials exposed in prior data breaches. Cybercriminals use a bot with a list of stolen credentials against many other sites to try and gain access. When the bot is successful, it's logged, and the hacker can either access the account directly or sell the account data to other bad actors.

These password attack methods have the same end goal of account takeover and fraud. It's up to organizations to take steps to shore up their password hygiene to prevent themselves from being easy targets.

The Password Problem

The core weakness with passwords comes down to people. Passwords put the onus on users to remember numerous complex character strings. Out of a desire for convenience and ease of use, people typically reuse passwords across their work and personal accounts or only slightly modify a root password. And, when access requirements become too complicated and time-consuming, users often find ways to bypass security controls. Despite years of training, it has failed to effectively change human behavior; therefore, enterprises must take steps to address the password problem and reduce the risk of compromised credentials being utilized.

Sharing is Not Caring

The pervasive problem of password reuse is why these password-based attacks are successful. The chart below outlines the sheer magnitude of the problem.

65% of people **reuse passwords** across **multiple**, if not all, sites*
*Google

72% of individuals **reuse passwords** in their **personal life***
*Hypr

The **average person reuses each password** as many as **14 times.**
*LastPass

76% of **millennials recycle** their **passwords**
*Security.org

The issue with reuse is that if one account suffers a breach, then every other site or service associated with the exposed password is also at risk. Therefore, an organization is as vulnerable as the third party site or service with the weakest link.

In addition, even if the password isn't directly reused, employees often utilize the same root password with obvious, easy-to-guess evolutions and deploy it across personal accounts, oftentimes on lower security services. And it's this weakness that bad actors and nation-states exploit through various automated attacks, including credential stuffing.

With new breaches occurring daily, this threat is continuously growing. For example, in the first half of 2022 Enzoic updated its database with an average of several millions of compromised credentials per day!

Legacy Password Policies

Eliminate Periodic Resets

In addition to password reuse, archaic policies such as time-based forced resets contribute to the problem. Organizations have historically addressed the threat from compromised passwords by enforcing periodic password resets. However, this is ineffective as there is no scheduled period that will be short enough to close the vulnerability. It also doesn’t ensure that the new password hasn’t already been exposed. Typically when a user knows they need to reset a password every quarter, they follow a predictable pattern such as simply changing one character on a reused password. Periodic resets can also increase operational costs and negatively impact employee and user productivity.

Replace Complexity

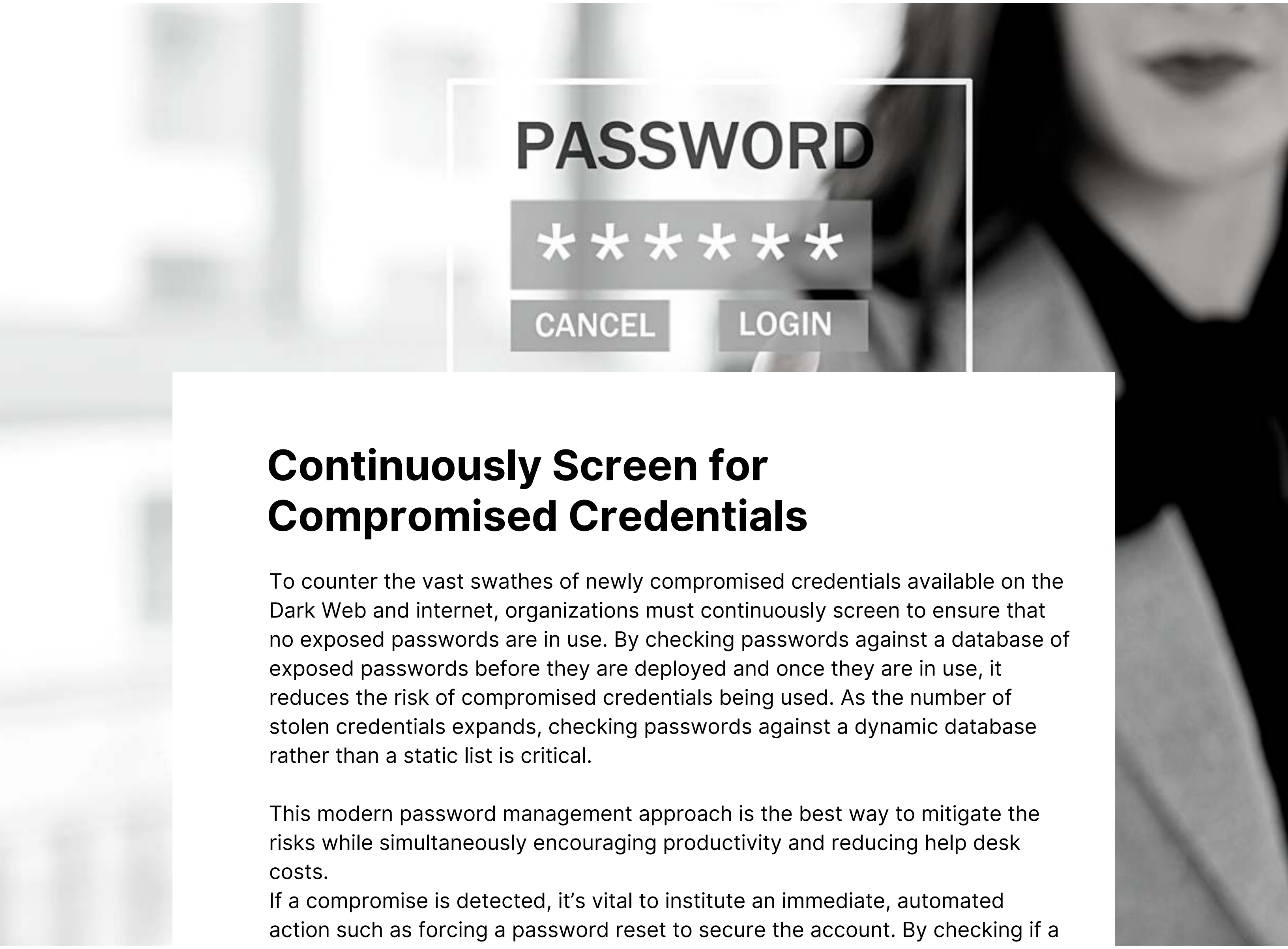
Another weakness is the belief that a complex password improves security. One of the key reasons it doesn't is that human behavior often leads users to follow predictable patterns when selecting a password that aligns to specific complexity requirements. For example, a basic phrase such as "P@ssword1!" might check all the boxes from a compliance perspective. However, it's clearly a weak password guaranteed to exist on a list of stolen credentials. Extensive research has shown that enforcing rules around a mix of character types encourages even more predictable behavioral patterns that hackers can leverage. Instead of complexity, companies should focus on making sure the password is not a compromised password. The National Institute of Standards and Technology (NIST) recommends passwords not be common, easy-to-guess or previously compromised. This presents new challenges for organizations establishing policies because they will need to be able to check against an evolving blacklist rather than evaluate character complexity.

Solving the Password Problem

Organizations must modernize their password policy and future-proof themselves from the risks associated with outdated and ineffectual password strategies. As the number of breaches continues to grow, so does the risk that credentials could be compromised. This requires following the NIST guidelines that every password is checked against a blacklist that includes dictionary words, repetitive or sequential strings, passwords taken in prior security breaches, variations on the site name, commonly used passphrases, or other words and patterns that cybercriminals are likely to guess. And unless companies secure the password layer, they risk offering cybercriminals easy access to the network.

NIST Guidelines

With hackers increasingly targeting credentials to breach the next organization, companies must modernize their approach to password management. NIST recommends that companies now verify that passwords are not compromised before being activated and monitor those passwords on an ongoing basis.



Continuously Screen for Compromised Credentials

To counter the vast swathes of newly compromised credentials available on the Dark Web and internet, organizations must continuously screen to ensure that no exposed passwords are in use. By checking passwords against a database of exposed passwords before they are deployed and once they are in use, it reduces the risk of compromised credentials being used. As the number of stolen credentials expands, checking passwords against a dynamic database rather than a static list is critical.

This modern password management approach is the best way to mitigate the risks while simultaneously encouraging productivity and reducing help desk costs.
If a compromise is detected, it’s vital to institute an immediate, automated action such as forcing a password reset to secure the account. By checking if a password is compromised at creation and continuously monitoring for credentials that become exposed, it stops systems from being an easy target for password-based attacks. This dual approach is the key to mitigating the risk.

Prevent Account Takeover

Account takeover schemes are costing businesses billions of dollars each year. Threat actors carry out these automated attacks using stolen passwords at a mind-boggling scale and pace. By screening and preventing the use of compromised credentials, businesses reduce the risk of being a victim of an account takeover attack.

Password Strategies

Password Security in the Modern Age

As mentioned earlier, legacy approaches to password security actually resulted in weaker passwords. Yet, as we've also discussed, people are often their own worst enemy when it comes to password security. That's why organizations should assume the responsibility for ensuring credential security and implement strategies for their continued protection.

The trick is in finding the right approach that balances credential security with minimal user friction.

Password Hardening

The first step in securing passwords is introducing some form of password hardening–in other words, deploying a technique or technology that makes it more difficult for the password to be guessed and exploited by bad actors.

Instituting some form of compromised password checking is an important component of a modern approach to password hardening. Companies can obtain static black lists of exposed credential data online, and some organizations even curate their own. However, given the time associated with managing this in house and the rate at which new breaches occur, a better approach is relying on an external provider for credential screening. There are a variety of elements companies should consider when evaluating vendors, including how–and from where–the vulnerable password data is sourced.

Multifactor Authentication

Multifactor authentication requires users to present two or more pieces of evidence in addition to their password when attempting to login. MFA provides another security layer but it introduces a fair amount of friction and, when given the choice, many people choose not to implement it. For example, Google has stated that less than 10% of its users have opted to turn on MFA. In addition, while adding new security layers is beneficial from a security standpoint it doesn't eliminate the need to harden each layer– which brings us back to the importance of password security.

Adaptive Authentication

Adaptive authentication cross-references IP address, geolocation, device reputation, and other behaviors to assign a risk score to an inbound login and step-up factors accordingly. Because these systems are generally tuned aggressively to increase their efficacy, they often add additional authentication steps in situations that don't warrant them. As a result, users are typically frustrated by adaptive authentication.

Biometric Authentication

Biometrics have been touted as the answer to many credential security woes, but there is a significant difference between this vision and biometrics in reality. For one thing, deploying biometrics as a singular authentication strategy is impractical as many devices and technologies are not currently equipped with biometric capabilities. There are also biometric-specific security concerns, particularly as deep-fake technology matures and hackers are able to spoof people's physical attributes. Finally, most biometric systems still rely on a fallback password-based authentication mechanism when the biometric fails or becomes unavailable.

Complex Threat Environment Demands a Layered Approach

Companies’ best defense in today’s heightened threat landscape is to adopt a layered approach to credential security–and ensure that each layer is effectively hardened. As the above underscores, passwords will remain a primary authentication mechanism for the foreseeable future. So, what should organizations do to ensure their security?

The Password Screening Imperative

The most critical step is to implement credential screening to keep unsafe passwords out of the IT environment.

NIST recommends that companies screen new passwords against those known to be commonly-used, expected, or compromised because this approach matches the methods employed by bad actors in modern brute force attacks. People have demonstrated that they follow very simple patterns in password selection—even with a written password policy in place. As a result, hackers have lists of common passwords and patterns obtained via previous breaches that they use to narrow down the universe of passwords attempted in their attacks.

Research from Virginia Tech University found that over 70% of users employed a compromised password for other accounts up to a year after it was first exposed, with 40% reusing passwords which were leaked over three years ago. In addition to this long-tail effect, the staggering rate at which new breaches occur means that threat actors have an ever-growing repository of new credential data to mine.

Along with checking the integrity of newly created passwords organizations also must continually assess their security in order to stay a step ahead of hackers. After all, a password could pass a security check at its creation, but easily become compromised down the road.

Enzoic Solutions

Eliminating Passwords as a Threat Vector

Enzoic provides companies with an automated approach to these two critical use cases. The company uses a combination of human and automated threat research to collect credentials from data breaches, turning hackers' ammunition into a defense tool for organizations of all industries and sizes.

The company offers two products, Enzoic for Active Directory and Enzoic APIs, that provide enterprises with unparalleled password protection.

Complete Password Protection

Enzoic for Active Directory screens passwords at their creation to prevent users from selecting weak or previously exposed credentials. In addition, Enzoic continuously monitors both these passwords and the usernames affiliated with them to ensure they do not subsequently become compromised. The solution is the only Active Directory product to provide this level of comprehensive protection against compromised credentials.

Enzoic for Active Directory works by plugging into a company's Active Directory environment and screening credentials against its proprietary dynamic database of billions of exposed username and password combinations. As we've discussed, some companies attempt to screen credentials via static blacklists either obtained online or built in-house. However, these fail to account for the rapidly evolving threat landscape. Enzoic maintains its database using a combination of proprietary automated processes, submitted contributions and research from its threat intelligence team. In addition, the database is automatically updated multiple times per day, ensuring that companies' password security reflects the latest breach data.

Easing the Security Burden on IT and Employees

Along with providing this enhanced level of security, Enzoic also ensures that it comes without adding any additional burden on IT. Enzoic for Active Directory is easy to deploy, with some customers having the solution fully implemented in as little as 15 minutes. And because the screening happens automatically, IT resources are freed to be deployed to other strategic areas with the assurance that password security is covered.

If a compromise is detected, companies can automatically activate a remediation plan. These offer a range of actions based on the severity of the threat, up to and including the immediate disabling of the compromised account. Enzoic for Active Directory also allows companies to set specific password rules and remediation actions by Container, Group, OU, or account. This enables them to have a more aggressive monitoring and response for sensitive accounts—those related to IT or finance, for example.

Unlike other approaches to password security that have historically frustrated employees, Enzoic for Active Directory offers a relatively friction-free experience. Users with uncompromised passwords gain access without adding additional steps or device requirements and employees only become aware that the screening has occurred in the event of a compromise. Should this happen, companies can automate the process of facilitating safe access to the account or system.

Enzoic APIs

Enzoic also allows companies to extend this unparalleled protection to other sites and systems. Through a series of simple, hosted REST APIs, organizations have direct access to Enzoic's dynamic database for any use case or integration. By harnessing the power of Enzoic's compromised credential database, enterprises can be more proactive in their defense against account takeover and other types of fraud. Enzoic APIs include:

☑ Passwords API

A typical use case might involve integration into account signup and password change forms to determine if the proposed password exists in Enzoic's database

☑ Credentials API

Companies could vet credentials against this API when users log into a website or application and, if a compromise is detected, block the login and redirect into a password reset flow

☑ Exposures API

This enables organizations to conduct periodic scans of their user base and determine if any have been involved in new exposures

Case Study

Network Intrusion Spurs City of Prescott, Ariz. To Confront the Password Problem

Prescott, Arizona has a rich history as a frontier mining town, and today is the county seat of Yavapai County and home to over 45,800 residents. Its IT team is a full-service government organization, overseeing the city's police, fire, airport, library, water monitoring, and golf businesses, among other responsibilities. Each of these entities has different requirements and needs, necessitating that Prescott's IT department juggle competing priorities.

This can be challenging at the best of times, and these challenges were exacerbated in 2020. The first COVID-19 lockdowns had just occurred, and the city was scrambling to support the shift to remote work and also cover employees who were sick or unable to work due to quarantine. In addition, the IT team was busy with budget season, in the midst of an ISP migration, and navigating the after-effects of a flood in its office.

It was in the midst of this chaos that a network engineer noticed a suspicious login on his computer. He notified his superiors and immediately changed his password, but the damage had already been done. Prescott was soon contacted by the FBI, warning about a post on the Dark Web that claimed to have access to an Arizona government network. The Bureau believed the poster planned to either use the access to extort the city or sell it to other threat actors for use in a ransomware campaign.

After investigating the incident, Prescott's IT Director, Nate Keegan, determined hackers had exploited a weak password to a legacy remote access system to gain entry to the network. While the ISP migration would have phased out this remote access system, Keegan had seen first-hand the damages that can result from poor password hygiene.

He selected Enzoic for Active Directory to address this vulnerability. After the initial deployment, Prescott found that 35% to 45% of the passwords in use were either already compromised, the same or very similar to other employees', or simple and easy to crack. Armed with the information, Keegan implemented a rule requiring that employees create new credentials that complied with NIST's recommendations. And because Enzoic for Active Directory continually checks their integrity, Prescott is confident that any new compromise will be detected.

In addition to this enhanced security, Enzoic's automated solution also enables Keegan to allocate valuable IT resources to other projects. This is a significant benefit, particularly when contrasted with the manpower associated with creating and maintaining a blacklist in-house.

As Keegan puts it, "It's insane not to address the threat of weak or compromised passwords in your environment. Studies have repeatedly shown that the majority of breaches are the result of a compromised password—a reality with which we're all too familiar now. Deploying Enzoic ensures that Prescott does not fall victim to this type of attack. I sleep better every night knowing that my passwords are secure."

Why a Passwordless Future is an Illusion

With the surge in password-based attacks, the vision of passwordless authentication has been gathering steam. Biometrics, one-time pin codes and other invisible security strategies are touted as the answer to the password problem. However, while this sounds appealing, the challenge is that passwords are still involved in the authentication process.

This happens in two primary ways:

Passwordless Solutions Rely on Passwords

If you have an Apple device, chances are you've encountered an issue with Touch ID at some point. There are numerous reasons why Touch ID authentication might fail—debris on the button, users' finger positioning, or issues with system configuration. When a problem occurs, the system defaults to asking you to enter a password. This means that if Touch ID is enabled, the security of those accounts is determined by the password.

Given the current maturity of biometric technology, an additional authentication method will be required for the foreseeable future. And when you consider that this is generally a password, the promise of passwordless is a mirage.

Credentials are Required on the Backend

The other core issue is that credentials are still required to authenticate the system at some point in the security chain. For example, if you gain access to an office via a fingerprint scanner, it defaults to your unique access code if/when the biometric proves unreliable. However, the IT admin who logs into the system to analyze the data uses a password, so the system's security is still reliant upon the password security.

In addition to the two core issues, there are additional authentication concerns with biometrics and other invisible security strategies, including device limitation, user issues and, of course, the fact that biometric identifiers can't be reset.

Despite the hype around passwordless, organizations must continue to prioritize password security in tandem with other emerging forms of authentication.

Adopt a Layered Approach Today

Year after year, Verizon's DBIR and other studies document the growing threat of stolen credentials, yet companies continually fall victim to these attacks. Simply put, organizations can no longer afford to ignore the problem. It's clear that companies must act now to modernize their password policy.

As in other areas of security, a layered approach offers the best defense. From a password perspective, it's unrealistic to expect human behavior to change. People will continue to select relatively weak passwords and reuse them across various sites and systems. Implementing credential screening eliminates the inherent vulnerabilities in this behavior and removes the friction associated with legacy approaches to password management. However, this peace of mind is only assured if passwords are screened via a dynamically updated database, as static blacklists simply cannot address the evolving threat landscape.

Enzoic offers the industry's only comprehensive credential screening solution. With Enzoic for Active Directory, companies can check password integrity at creation and on an ongoing basis—ensuring that the IT environment is free of unsafe passwords. Enzoic APIs extend this assurance into other websites and applications. Detection and remediation are automatic with both products, meaning that the screening happens passively and only impacts the users' experience if the need to protect them arises.

Protect Your Customers by Eliminating Credentials as a Threat Vector

As mentioned above, whether you're an MSP or an MSSP companies are increasingly turning to you for some form of security. That's why it's more critical than ever to ensure that you have taken all the right steps to reduce the threat of compromised credentials within your own environment.

Deploying Enzoic's credential screening solution enables you to do exactly that, and also comply with both NIST guidelines and the recent joint CISA, NSA and FBI warning. What's more, it allows you to demonstrate your commitment to cybersecurity to existing customers and when competing against other MSPs/MSSPs for new business.

It's clear that now is the time to act when it comes to hardening the password layer.

RUN OUR FREE PASSWORD AUDIT

Check your Active Directory for any password-related vulnerabilities and begin improving your clients security posture and permanently eliminating credentials as a threat vector.