

THE THREAT IS REAL:

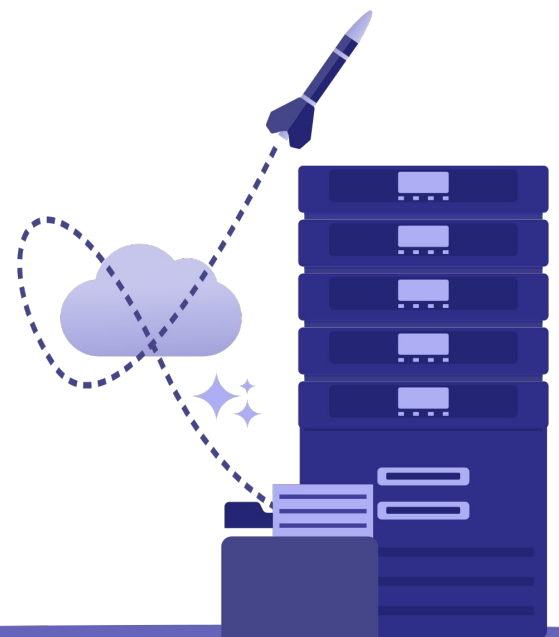
# Avoiding Catastrophic Business Failure by Using Breached Password Detection to Secure User Accounts, Applications, and Assets



# Table of Contents



- 1** Introduction
- 2** Severity of the Problem
- 4** Breached Password Detection is the Most Valuable Solution
- 8** Breached Password Solutions for 2020 and Beyond
- 10** Safeguard Both Your Users and Your Organization
- 13** Enable Breached Password Detection for Your Organization Today



# Introduction

Attackers have an infinite number of ways into your systems. In a perfect world, organizations could mitigate the risk of unauthorized access if users practiced proper password etiquette. Unfortunately, getting users to adopt good password hygiene across the board is a losing battle.

The stakes are high, as breaches can lead to lawsuits that run into the millions or billions<sup>1</sup> and harm corporate reputations. However, the real cost of breached passwords extends far beyond the initial breach, as compromised credentials can then be used to breach user accounts on your system. No matter how resilient your security posture, if credentials are reused across systems, your user accounts are vulnerable through no fault of your own. Expensive and time-consuming account recovery efforts and chargebacks are ultimately on the line.

The most viable solution to this growing challenge is breached password detection, which has the distinction of being a strategic and highly successful workaround for problematic user behaviors. Breached password detection can notify users in real time when their credentials have been leaked by a third-party data breach. It can also proactively secure your organization's applications, systems, and other assets, keeping bad actors at bay.

We'll describe breached password detection in greater depth and share best practices for implementation of a solution that meets both organizational needs and user expectations. To help set the stage, we'll begin by describing why so many organizations are choosing breached password protection as a critical line of defense in identity and access management.



<sup>1</sup> For example, the 2017 Equifax breach resulted in multibillion-dollar lawsuits and a [payout of at least \\$425 million](#).

# SEVERITY OF THE PROBLEM



Account takeover attacks result in billions of dollars of fraud. Here, we'll highlight the risks and costs associated with this growing problem.

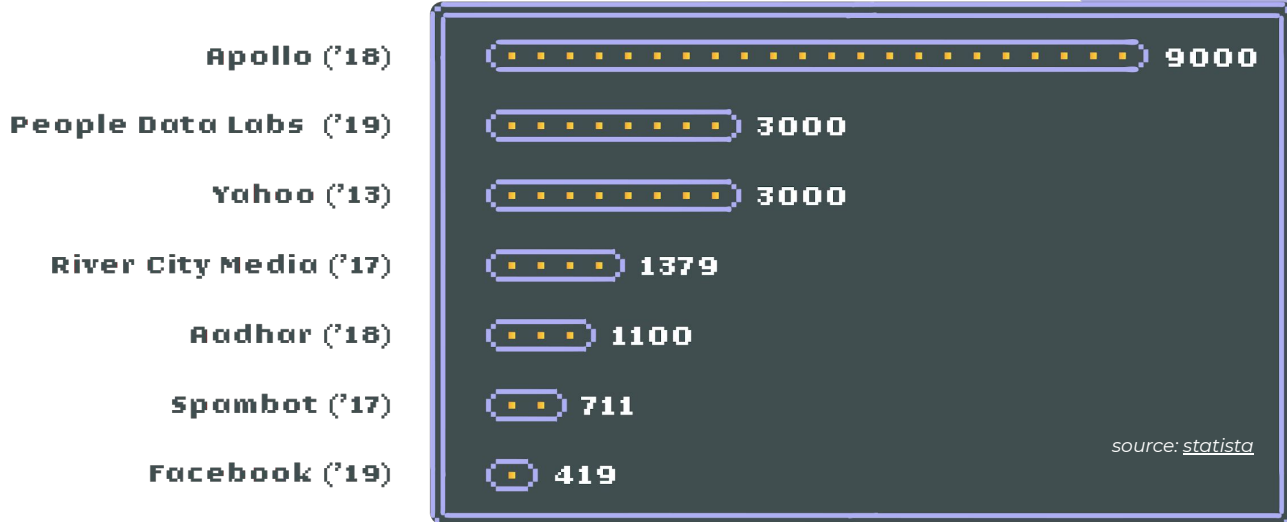
## Password Leaks Cause Monumental Damage

Recent data breaches include Yahoo (all 3 billion accounts hacked) and millions of accounts at Equifax, eBay, LinkedIn, Dropbox, Target, Twitter, and Canva.<sup>2</sup> The damage can be so devastating that it's nearly impossible for some companies to recover.

That damage doesn't stop with the breach, of course. **Breaches open endless criminal possibilities for hackers, who trade**

**passwords amongst themselves and use the passwords to target and compromise bank accounts, e-commerce accounts, mobile payment services, social media accounts, shop loyalty schemes, cryptocurrency wallets, and email accounts.**

These account takeovers are a form of online identity theft in which a cybercriminal gains illegal access to a victim's account, usually through credential stuffing or credential cracking attacks,<sup>3</sup> where bots test millions of email and password combinations to attempt to compromise on a range of login pages. The victim's account either holds funds or access to products,



**Number of compromised data records in selected data breaches as of April 2020 (In Millions)**

<sup>2</sup> See which companies you recognize from David McCandless' [data breach word cloud](#), last updated in May 2020.

<sup>3</sup> *Credential stuffing is an automated web injection attack where hackers use credential information sourced from data breaches to gain access to the victim's other accounts. Credential cracking is a brute force attack where hackers use dictionary lists or common usernames and passwords to guess their way into an account.*

services, or other stored value. Once the cybercriminal gains access to the account, they make online purchases, liquidate funds, use loyalty points, apply for loans, demand ransoms from the account owner, or use the information they find to commit additional acts of online fraud.

Hackers are sitting on billions of passwords that enable them to breach individual user accounts. Due to the rising number of attack vectors, account takeover attacks are a lucrative business for cybercriminals. More to the point, they're a major threat to consumers and the online accounts they create at businesses worldwide.

## The Real Costs of Account Takeovers

The IBM Security Cost of a Data Breach Report records the global average total cost of a data breach as \$3.86 million in 2020. In the United States, the average total cost of a data breach in 2020 is a whopping \$8.64 million. The average time to identify and contain a breach is 280 days.

The breaches are difficult to identify, and their eventual containment can cost billions. What's less obvious is the cost of the fallout that occurs when compromised passwords

are later used to access non-breached sites. Businesses incur exorbitant customer service and chargeback costs as a result of fraudulent transactions and account takeovers. For example, **a new study from Juniper Research has found that businesses across the globe and across all industries will cumulatively lose more than \$200 billion to fraudulent online transactions between 2020 and 2024.**

## Bad Password Practices are Difficult to Correct

Users tend to choose weak passwords, reuse passwords across applications and services, and not use a password manager or two-factor authentication. The most logical solution to this problem is to force users to choose better, more secure passwords. Indeed, today's complex password policies have evolved in response to users' bad habits. First, organizations made users change passwords frequently. Users still chose bad passwords, so organizations made them use longer passwords and add numbers and special characters.

Yet user accounts are still breached. As it turns out, the most logical solution has also proven to be the solution least possible to successfully implement.

**As just one example, in January 2019 773 million email address and password combinations were publicly posted on a popular hacking forum known as Collection #1. Afterward, only one in three affected users changed their passwords. These new passwords were often weaker than their previous passwords and were similar to passwords they used on other accounts.**

This data may seem shocking. However, this highly risky behavior is the norm. To be fair, trying to remember numerous passwords

### HIGH COST OF BREACHES

Globally	2020	2019
Avg global cost of breach	\$3.86M	\$3.9M
Avg US cost of breach	\$8.64M	\$8.19M
Time to identify and contain	280 days	279 days
Security automation deployed	59% of orgs	62% of orgs
Costliest industry	Healthcare	Healthcare

Source : IBM Security Cost of a Data Breach Report

<sup>4</sup> A dedicated password manager generates random strings that are harder to crack and make it easier to avoid password reuse.

<sup>5</sup> Safeguarding company data with an additional layer of protection may decrease the odds that a hacker will steal user data. Two-factor authentication (2FA) typically requires a user to provide a string provided to them via SMS, a Time-based One-time Password (TOTP) application or other source, as well as the password. However, attackers can easily subvert insecure authentication challenges, and 2FA also may require users to install and manage a TOTP application.

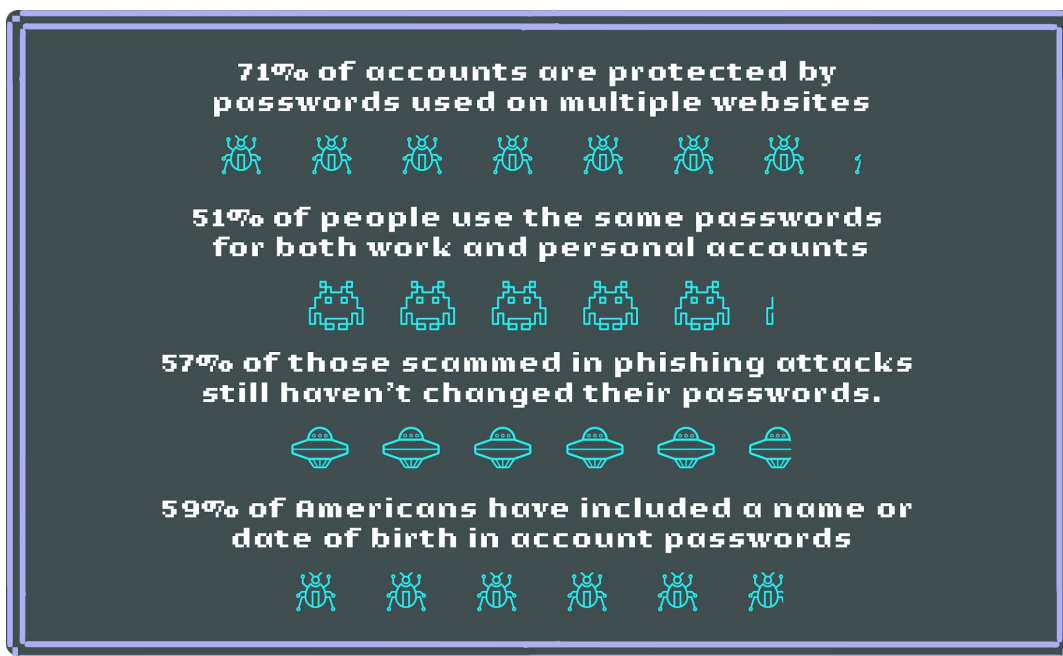
(each with its own set of convoluted requirements) for dozens of online accounts is difficult. Users often have to reset their login details for one reason or another, and this inconvenience alone leads many users to weigh the risks and choose to reuse passwords despite the high costs incurred if their accounts are compromised.

Most passwords are short, simple, and easy to crack because humans are predictable. More than half of internet users reuse passcodes for both their personal and business accounts. According to DataProt.net:

- 71% of accounts are protected by passwords used on multiple websites.
- 51% of people use the same passwords for both work and personal accounts.
- 57% of those scammed in phishing attacks still haven't changed their passwords.
- 59% of Americans have included a name or date of birth in online account passwords.
- The password "123456" is still used by 23 million account holders.

Industrial-scale password-breaking software like HashCat can make up to 300,000 guesses at a password per second. In a study of 10 million passwords, security analyst Mark Burnett found that hackers could leverage a known list of breached passwords to identify 16 out of 1,000 passwords using only the top 10 list of passwords.


Consider this: a hacker could use HashCat to comb through your organization's high-value user accounts and compromise one or more of those accounts in seconds.



<sup>6</sup> As a rule of thumb, passwords found on *Security Magazine's* list of most used passwords should not be used.

<sup>7</sup> The problem is exacerbated by the fact that people often create passwords on mobile devices that make characters like symbols and capital letters much harder to select than they are when using a keyboard.





# BREACHED PASSWORD DETECTION IS THE MOST VIABLE SOLUTION

Existing password policies aren't making organizations more secure or contributing to real-world password management solutions. Convoluted password policies are a nuisance to users and security professionals alike. According to the National Institutes of Science and Technology (NIST) Digital Identity Guidelines, the frustration users face in meeting password requirements that differ from business to business may "cause them to focus on minimally satisfying the requirements rather than devising a memorable but complex [password]."

Organizations that do not want to get into the complex business of managing user credentials would do well to choose a solution that will handle authentication and credential management for them. Breached password detection works precisely because it provides a strategic, highly effective workaround for users' bad password hygiene practices.

## Identity and Access Management for a New Day and Age

Breached password detection is a simple solution that can help keep user accounts safe from account takeovers by preventing hackers from gaining access to your services. It can also notify your users when their credentials have been leaked by a third-party data breach or compromised in any way.

Breached password detection can not only secure user accounts quickly and easily but also do so without negatively affecting the

user experience or causing significant user pushback. Enabling detection does not attempt to change user behavior. Instead, it expands the universe of acceptable passwords, which may now include long passphrases without any special characters (e.g., a string of unique words or an easily remembered, slightly modified quote).

## The Real Costs of Account Takeovers

Every time a user logs in, that user's credentials are compared with a database of millions of known leaked credentials. If a match is found, the system notifies the user. Organizations can optionally prevent access to those accounts until compromised passwords have been reset. Anytime a trigger occurs, any administrator viewing the user details will also see a warning and information about when the breach was found.

### BREACHED PASSWORD DETECTION DOES THE FOLLOWING:

- ✓ Finds datasets of compromised passwords and either builds or uses a system to download, process, manage, and store these datasets.
- ✓ Configures a system to check passwords when authentication, registration, and password events occur.
- ✓ Takes action when a user's password is found in a breached dataset.

NIST recommends that breached password detection systems check user-provided passwords against a variety of sources, including the following:

- Passwords obtained from previous breaches
- Dictionary words
- Repetitive or sequential characters (e.g., aaaaaa and 1234abcd)
- Context-specific words, such as user names and derivatives thereof.

### NIST RECOMMENDS CHECKING PASSWORDS AGAINST:

- Passwords obtained from previous breaches
- Dictionary words
- Repetitive or sequential characters
- Context-specific words, such as user names

If the user's password is determined to be compromised, NIST recommends that the user should be forced to select a different

password and told why the password was rejected.

When searching for a compromised password, a breached password detection system needs to determine how to match accounts in the current system with compromised accounts. There are a number of options for doing so. For instance, the system could match on the password alone or on the password and the username. The match will check for a compromised credential anytime a user's password is created or modified. The provided password will be checked against a large and ever-growing database of compromised credentials.

**Informing a user that their account has been compromised provides a valuable service to that user. Compromised password detection is a safety measure that can protect your users by helping them identify other accounts that may share the same password. It can also help your organization prevent unauthorized access to your systems without requiring any user action—at least until a password leak or insecure password is found.**





# BREACHED PASSWORD SOLUTIONS FOR 2020 AND BEYOND



What traditional password hygiene practices have in common is that they require users to act. Breached password detection offers an alternative that takes into account the realities of user behavior. Organizations need breached password detection to secure user accounts because behavioral changes are impossible to implement and enforce.

Some organizations choose to create their own data ingestion system and breached password detection API. The benefits of creating and managing a custom solution include the ability to build custom dictionaries and gain more control over the system's design and capabilities. Common drawbacks of custom APIs include high development and maintenance costs, design and usability issues, variable response times and other performance problems, possible security holes, and lack of dedicated, in-house cybersecurity expertise.

If you choose to implement an in-house solution, here are some things to consider. Since you'll be shipping your users' passwords to and from the API, make sure you use TLS for all traffic. You also may want to encrypt the payload so passwords sent to the service will remain secure if your certificate is hijacked or if a TLS vulnerability occurs. Since credentials are extremely sensitive, assess your security posture and make sure that you've considered how to mitigate vulnerabilities quickly.

Third-party APIs offer fewer opportunities for customization but greater reliability, security, and ease of use. They provide both a source of breached credentials and an easy way to check compromised passwords. Organizations gain a simple solution with few moving parts.

**Using a third-party API is usually a better solution than custom building an API. However, not all third-party APIs are created equal. Choose your third-party API wisely to ensure it does not negatively affect your application's performance (latency), reliability, and ability to authenticate. If your application or service is degraded, then the user experience is degraded as well.**



# BREACHED PASSWORD DETECTION BEST PRACTICES

Breached password detection may be the wave of the future, but some third-party solutions are better than others. Performance, flexibility, ease of use, user experience, and value can vary greatly. Keep these best practices in mind when choosing the solution that is right for your organization.



## Prioritize Ease of Setup, Implementation, and Use

Choose a scalable product that simplifies identity authentication and management. Make sure the solution requires minimal developer integration time, making it ideal for organizations that want to integrate an identity access and management solution into their business for immediate use.

You should be able to enable breached password detection and then choose the options and rules that make the most sense for your business. If you need varied configurations for different applications, use a multi-tenant feature to create separate tenants and configure them individually. You should also be able to specify password settings.



## Prioritize User Experience

Choose a solution with out-of-the-box features that enable real-time detection and mitigation and accommodate the ever-evolving breached password landscape. **The flexibility and performance of the solution should be matched by the strength of the user experience the solution provides.**

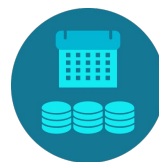
Companies tend to implement complex password policies, requiring users to follow convoluted password rules. The user experience suffers. And these policies don't suffice, as users work around them in ways that are harmful to system security. The goal should be to meet users where they currently are, not where we want them to be. User experience, including minimal user interference unless a problem is detected, should be a top priority.



## Implement an Extra Layer of Security

The solution should offer features that include anomaly detection. Security features should be able to differentiate between different types of attacks, identify which API calls are reliable, and recognize user access anomalies immediately. Breached password protection should work in context with other features, such as limiting the number of failed logins, blocking login attempts made from suspicious or malicious IP addresses, and blocking attackers from brute-force entry into user accounts.

In addition, make sure these credentials remain secure as they are being examined. They should never be stored on disk. They should always be encrypted in transit.

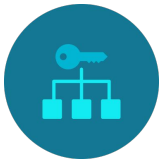


## Keep Your Datasets Up to Date

**To secure your systems, your solution provider will need to research and catalog**

lists of plaintext passwords. They may start with Have I Been Pwned, the Hasso-Plattner-Institute site, DeHashed, GhostProject, or other sources that include billions of compromised credentials and accounts and provide secure hash algorithms (SHAs). Make sure your datasets include additional common words and character sequences even if they are not present in any public data breach.

New breaches happen daily. Make sure your provider researches new datasets early and often to keep those datasets up to date.



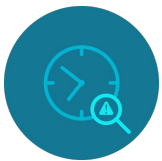
### Prevent All Known Compromised Credentials from Entering Your System

Configure your authentication system to check for breached passwords anytime a user registers, a user logs in, or a user's password is changed (by the user or an administrator). If any user provides a publicly known password, the system should reject the operations they are attempting immediately.



### Keep Unencrypted Passwords Safe

Some providers analyze passwords asynchronously to determine if they have been breached. Asynchronous password checks require providers to store the password somewhere, usually in a database and often in plaintext. Passwords also might be stored in memory for long periods of time. Avoid this huge security hole at all costs. Consult with your provider to ensure they are never storing plaintext passwords in a database or in memory for extended periods of time.



### Detect and Mitigate Breaches in Real Time

Only 43% of users who had accounts on breached domains changed their passwords.

One study concludes, “[P]assword breach notifications are failing dramatically, both at causing users to take action and at causing users to take constructive action.”

Suppose a user signs up on Example.com with a great password. Next, they sign up on your site with the same great password. Then Example.com is breached. Example.com may send out a notice, but your user may not receive it or may not change their password in response.

Make sure your solution immediately checks if a password has been breached when a user logs in. Most systems check passwords latently. Make sure all password-based login attempts can be checked in real time, matches can be blocked in real time, and users can be instantly alerted and forced to change their passwords.



### Create Breached Password Detection Protocols Based on Possible Impacts

Set up your authentication system to check for and prevent the use (or reuse) of breached passwords. Doing so allows users to pick the unique password they want while still keeping their accounts secure.

The million-dollar question: what, if any, action should you take upon user login? One option is to not check for compromised passwords during login. Choose this option only if login performance is of the utmost importance or if you don't protect any data but instead use authentication for reporting.

**If you check for compromise only when passwords are created at registration or modified by users, you'll end up with users who have credentials leaked by breaches external to your system after account creation. As a result, your system will be exposed to the possibility of unauthorized access. Make sure that the performance win is worth the possible security consequences.**

When you find a user with a breached password, the next step should depend on the level of harm unauthorized access could cause. In increasing order of user impact, you could:

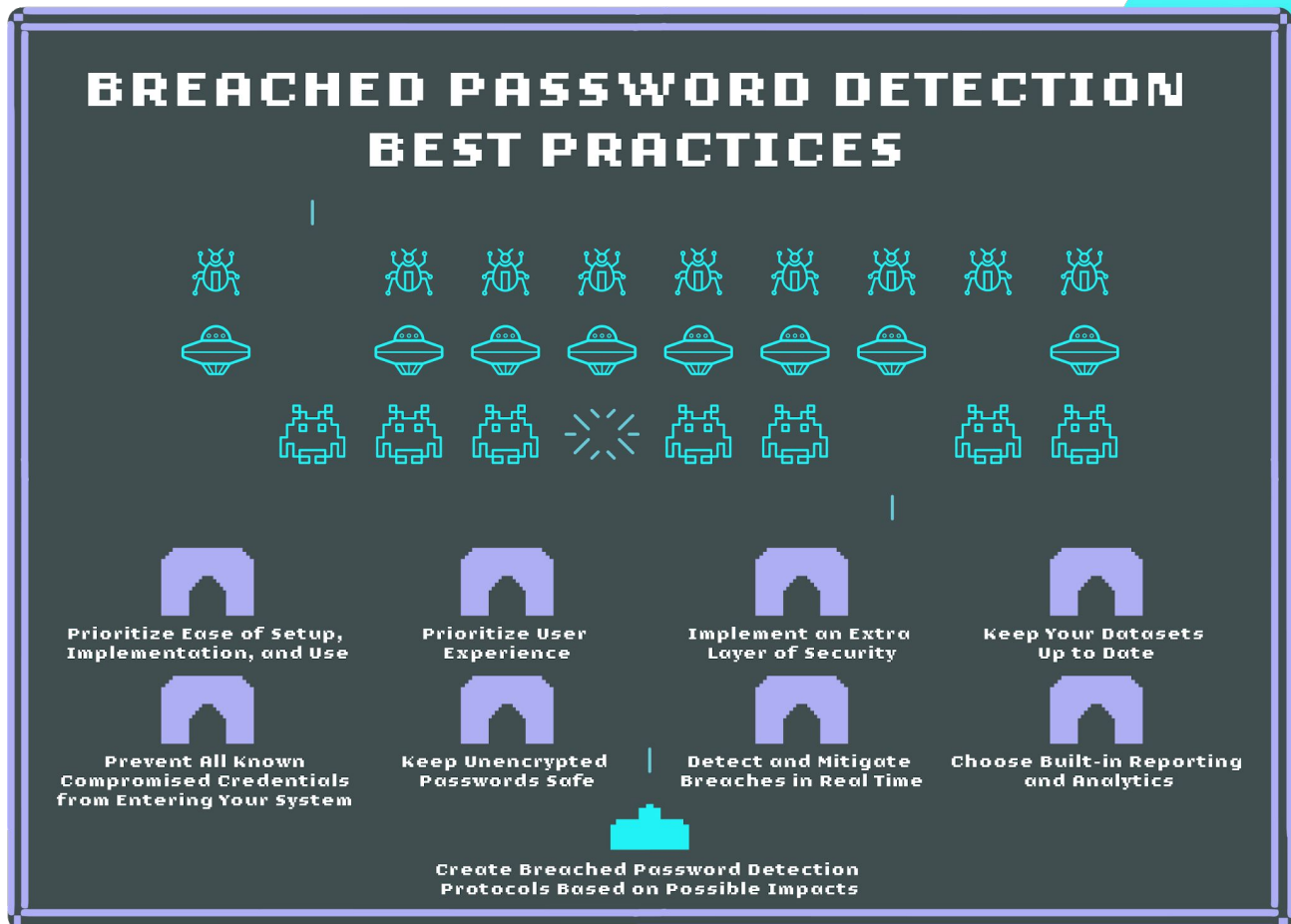
- Record the result, which will update statistics (and optionally fire an event to a webhook, allowing other systems to take action).
- Email the user to tell them their password has been compromised.
- Force the user to change the password before their authentication can be completed.
- Lock the account and prohibit use until the password has been changed.
- Reset the password and confirm unauthorized access did not occur.



### Choose Built-in Reporting and Analytics

The administrative user interface of your identity system or your breached password solution provider should make it easy to search for users who have compromised credentials, lock accounts, and reach out to your customers. On a customer-by-customer basis you should also be able to see how many of your users have had breached passwords and ensure your authentication system can notify external systems of critical events.

You need to be able to run reports and analytics to determine if compromised passwords have any patterns and to know how many of your users have been affected. All configurable actions taken when a vulnerability is detected should be logged for reporting and analysis.



# SAFEGUARD BOTH YOUR USERS AND YOUR ORGANIZATION



Threat detection is only half the equation. Today, organizations need automated detection and management for smart, real-time incident response. Organizations need to be able to manage critical security issues by quickly identifying breach password attacks, correlating alerts against threat intelligence, and taking appropriate action.

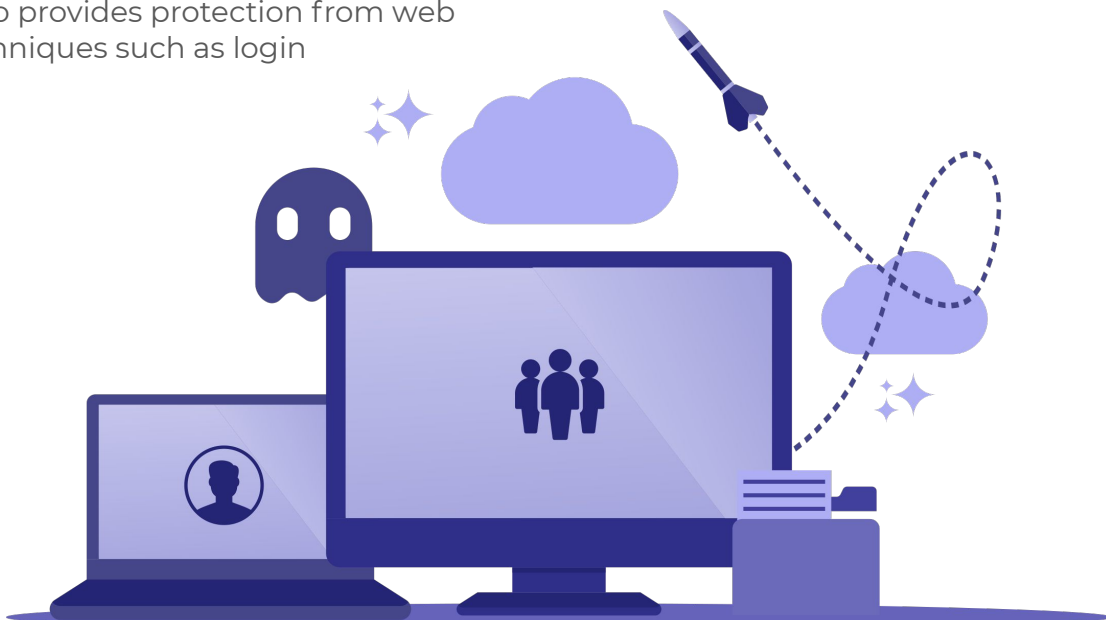
**Breached password protection is a strategic solution that anticipates user behaviors and automates the rapid discovery and remedy of breached password risks in order to keep your applications secure while also protecting your customers' assets.**

**FusionAuth Reactor** is a powerful suite of features that includes breached password detection. To support our clients' identity and access needs, we collect, continuously update, and check against hundreds of millions of compromised usernames and passwords from numerous breached databases to keep your users' accounts safe from external threats. Our platform also provides protection from web hacking techniques such as login

sniffing, password stuffing, DNS spoofing, and SQL injection. Comprehensive documentation, a community forum, and 24/7 phone, email, and website support make our solution even faster to implement and easier to use.

FusionAuth breached password detection makes your applications and services as secure as possible with less user interference, which minimizes your business risks and reinforces customer trust.

FusionAuth's high-value, high-performing breached password detection solution is user-friendly, flexible, scalable, and secure. It can help protect users' data and your assets in real time. You can choose how you want to respond and how you want to check passwords during the user authentication experience. You can include additional security with none of the frustrating password rules that often stymie user registration.





# ENABLE BREACHED PASSWORD DETECTION FOR YOUR ORGANIZATION TODAY

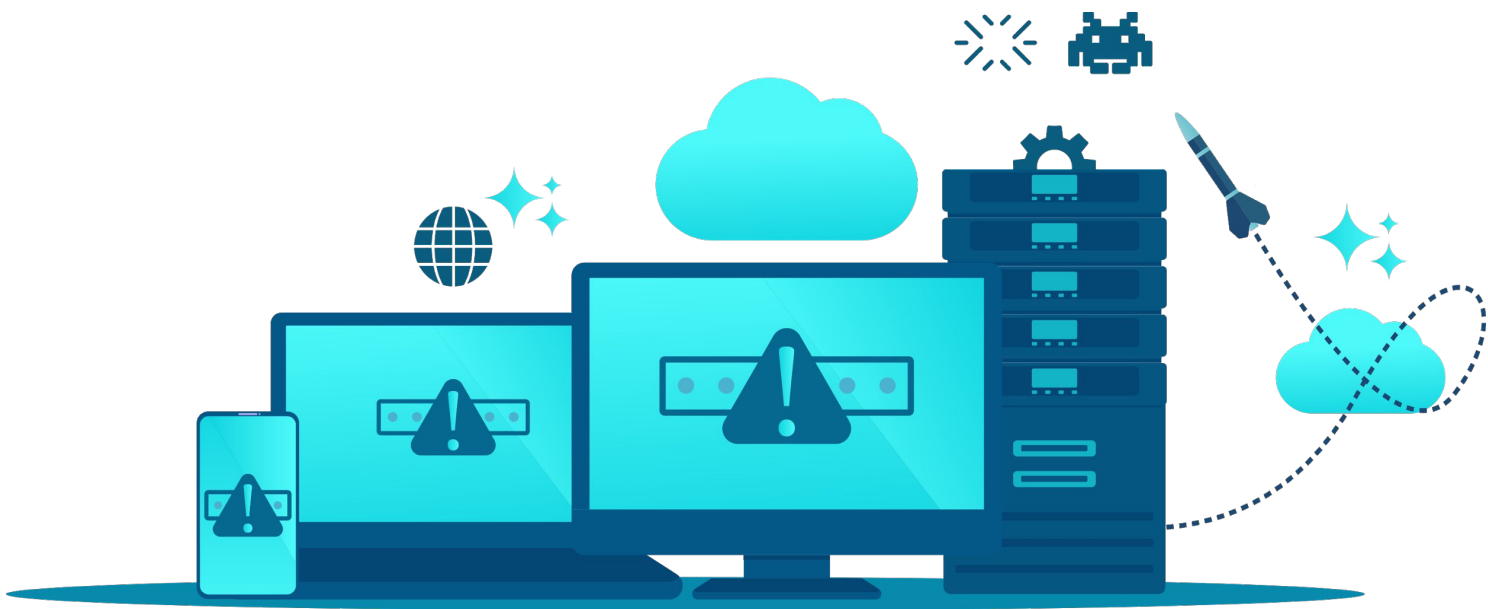
Stop trying to change user behavior. Instead, adopt a breached password detection solution, which is the simplest, most strategic way to address the growing problem of breached passwords.

Taking action on the front end can greatly reduce user and organizational risk. Preventing users from using publicly available passwords, compromised passwords, and other exposed credentials will improve your system security. Now is the time to clean up password practices to avoid unauthorized account access by following the principles of defense in depth.

**Breached password detection protects your applications and systems from breaches that occur elsewhere with no effort on your part. In fact, enabling breached password detection actually**

**empowers your users. Rather than enforcing random sets of password characters and expectations, you are disallowing problematic passwords while keeping an eye on growing lists of breached passwords at all times. Best of all, breached password detection only impacts users who have compromised passwords, leaving other users unencumbered.**

FusionAuth offers authentication, authorization, and user management capabilities for any app: deploy anywhere, integrate with anything, in minutes. Learn more about how you can enable breached password detection features that take the stress of data protection off your plate without impacting user experience. Sign up for a free trial today or reach out to learn more.



FusionAuth is a complete identity and access management tool that saves your team time and resources. Implement complex standards like OAuth, OpenID Connect, and SAML and build out additional login features to meet compliance requirements. It's built for devs to deploy anywhere and integrate in minutes. Go build something awesome!