WHITE PAPER

WHY PASSWORDS STINK

BEYOND IDENTITY

CONTENTS

01

INTRODUCTION

There are hundreds of billions of passwords in the world today, with more being created every day. In fact, the average business user maintains an astounding average of 191 passwords.[1] Unfortunately, these passwords represent a fundamentally weak link in most organizations because they will always be insecure.

This white paper examines why that is, investigates some alternative solutions, and introduces a new method of authentication using asymmetric keys and certificates to eliminate passwords altogether.

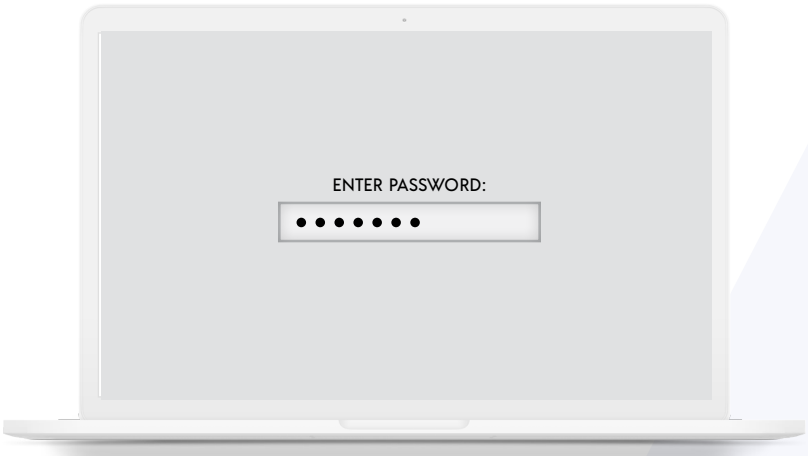
[1] https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

02 PASSWORDS ARE FUNDAMENTALLY INSECURE

Let's face it: Passwords stink! For employees and customers, they cause friction and frustration when logging in – Who can remember the 16-character combination of letters, symbols, and digits that are indicative of strong passwords, much less come up with them in the first place? When a password gets lost or stolen (and they invariably do), it places a burden on the help desk. In fact, 20-50% of help desk calls are for password resets, with the average call costing the organization $70.[2]

For CISOs, passwords represent corporate assets that can be targeted by bad actors. And that's a problem because they often transit networks in the clear, are stored in databases that can be and often are hacked, are shared among colleagues, and are reused across multiple apps – making them easy targets for malware, phishing attacks, and other credential-stealing schemes.

> Though widely used, passwords are fundamentally flawed and no longer an appropriate authentication method for any use case except those with minimal risk.
>
> – ANT ALLAN, VP ANALYST, **GARTNER**[3]



When passwords get hacked and stolen (either individually or as part of a database), they are usually shared online and offered for sale on the dark web. Threat actors buy these lists and use automated credential-stuffing attacks that run through username/password combinations until a match is found for the account. Passwords can be cracked through dictionary attacks, brute force attacks, lookup tables, reverse lookup tables, and rainbow tables.[4]

[2] https://searchenterprisedesktop.techtarget.com/tip/Resetting-passwords-in-the-enterprise-without-the-help-desk

[3] Ant Allan, Gartner "Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls" April 4, 2019.

[4] https://medium.com/@cmcorrales3/password-hashes-how-they-work-how-theyre-hacked-and-how-to-maximize-security-e04b15ed98d

DICTIONARY ATTACK

Systematically tests combinations of known words and other likely passwords.

BRUTE FORCE ATTACK

Systematically tests every combination of possible characters up to a certain length.

LOOKUP TABLE

A table of pre-computed hashes for passwords from a password dictionary are used to test hundreds of hashes per second.

REVERSE LOOKUP TABLE

A table that compares a table of password hashes from user accounts with a table of hashes of guessed passwords to find matches.

RAINBOW TABLE

Similar to a Reverse Lookup Table but uses a reduction function to reduce the amount of storage space needed.

This kind of computerized password cracking thrives on shorter passwords, which can be cracked in just a few seconds. As well, malicious actors can combine stolen databases with other datasets and run programs to generate different, potentially viable credential sets. Given that people often reuse these stolen passwords for far more sensitive corporate sites, even less sophisticated attacks can penetrate organizations.

Password insecurity leads to data breaches, account takeover, and worse. The 2019 Verizon Data Breach Investigations Report revealed that the use of stolen credentials is the second-largest cause of data breaches and billions of passwords have been compromised in just the last few years. In fact, an earlier version of the report claims that 81% of hacking-related breaches use either stolen and/or weak passwords, and the average data breach costs businesses $3.92 million, according to the Ponemon Institute.

> 81% of hacking-related breaches use either stolen or weak passwords.
>
> – VERIZON DATA BREACH INVESTIGATIONS REPORT

That's pretty challenging, since every CISO wants to provide effective security and protection for their organization, for a variety of reasons. First on the list is protecting company data, including financial information, customer data, intellectual property, and employees' personally identifiable information (PII), among other things. Companies need to demonstrate that they are in compliance with regulations such as GDPR and other data protection requirements such as the California Consumer Privacy Act. And, not only do companies not want to be breached, they also don't want to see themselves on the nightly news, have to explain to customers why their accounts were hacked, or tell the board the impact of the breach and what it's going to cost the organization. CISOs want to keep customer goodwill, a healthy stock price, and the company's public reputation. They also want to keep their jobs.

Good security also means protecting operational technology that connects your physical assets to the Internet, such as IoT devices and sensors, and to the IT network. If threat actors breach your IT network through weak or stolen passwords, they can move laterally into your OT network and vice versa, putting not just data but also the physical plant in jeopardy.

Poloniex's management confirms it sent an email to customers notifying them that a list of leaked emails and passwords could be used by malicious actors to gain access to their trading accounts. The crypto exchange says it is requiring affected users to modify their passwords.[5]

– CRYPTOCURRENCY EXCHANGE POLONIEX QUIETLY INFORMS USERS OF DATA BREACH

Password data and other personal information belonging to as many as 2.2 million users of two websites – one a cryptocurrency wallet service and the other a gaming bot provider – have been posted online.[6]

– PASSWORD DATA FOR ~2.2 MILLION USERS OF CURRENCY AND GAMING SITES DUMPED ONLINE

What if scammers could learn your password not from a massive cyberattack or taking control of your device, but from listening in as you type? That's the startling premise of a recent study by researchers at Cambridge University and Sweden's Linkoping University, who were able to glean passwords by deciphering the sound waves generated by fingers tapping on smartphone touch screens.[7]

– LISTEN FOR THE LOG-IN: HACKERS MAY GLEAN YOUR PASSWORD BY LISTENING TO HOW YOU TYPE ON YOUR PHONE

Facebook Inc. for years stored hundreds of millions of user passwords in a format that was accessible to its employees, in yet another privacy snafu for the social-media giant.[8]

– HUNDREDS OF MILLIONS OF USER PASSWORDS EXPOSED TO FACEBOOK EMPLOYEES

[5] Cryptocurrency Exchange Poloniex Quietly Informs Users of Data Breach

[6] Password data for ~2.2 million users of currency and gaming sites dumped online

[7] Listen for the log-in: Hackers may glean your password by listening to how you type on your phone

[8] https://www.wsj.com/articles/facebook-says-millions-of-users-passwords-were-improperly-stored-in-internal-systems-11553186974

03

THE PROBLEM WITH PASSWORDS IS THAT THEY ARE "SHARED SECRETS"

A shared secret is a piece of data, known only to the parties involved, in a "secure" communication. A password is a shared secret, as is a passphrase, a PIN, or a randomly chosen set of bytes. Other forms of identity, such as biometrics, can also be used as shared secrets when they are stored on servers. Anything shared means that there is an administrator who knows about it and that it is stored in a database that can be vulnerable to compromise. Although passwords are hashed for better security, bad actors have found a way around that as well. Salting them by adding extra information before hashing can help, but the same methods of password cracking can be applied.

04 CURRENT ALTERNATIVES AREN'T THE ANSWER

As a result, alternate methods of authentication have arisen, such as password managers, multi-factor authentication, and biometrics, but each of these methods has their pitfalls, and they don't solve the root "shared secret" problem.

PASSWORD MANAGERS solve the issue of password reuse by allowing you to more easily use unique passwords for each application without having to memorize them all. However, they do not solve the security issue posed by reliance on shared secrets. By storing all of your passwords locally and on the cloud, accessible via a master password, password managers can actually weaken your security posture – consolidating the risk in one place.

MULTI-FACTOR AUTHENTICATION (MFA) solutions appear at first glance to be a secure compliment to simply using passwords. The second factor improves the ability to correctly verify that the user requesting access is who they claim to be and since the authentication codes are one-time use they are not technically shared secrets.

Unfortunately, there are varying degrees of vulnerability with MFA, as the second factor of authentication is often sent via text or SMS, or other insecure channels, meaning that MFA can be compromised. Notably, Chinese state-sponsored group APT20 has found a way around 2FA through a stolen RSA SecurID software token. But even more simple methods include spoofing login pages to collect both the original password as well as the secondary authentication code, rendering the exercise vulnerable as a security method. Last, MFA increases user friction by requiring users to enter both a password and an authentication code, hindering organizational productivity.

SOME "PASSWORDLESS" EFFORTS such as biometrics are low friction and secure as long as the biometric data is stored in a protected hardware enclave. However, when used to access an external application, the biometric is still just sending a password on your behalf.

The alternative is for the biometrics to be stored on a server, but this introduces a new, more consequential target. The systems storing the fingerprints can be hacked, and if that happens, you can't change your fingerprint, retina, or face like you can a password. It is, in essence, just exchanging one type of shared secret (password) for another (fingerprint) that has far greater consequences if compromised.

Furthermore, biometrics as authenticators introduce potential new liabilities such as concerns about HIPAA compliance as well as usability challenges because the approach requires backup passwords or hardware fobs.

SINGLE SIGN-ON is a great first step to ease user friction caused by passwords, but it does not solve the underlying security issue. The session token that enables subsequent authentication can be hacked and used for nefarious access. And session tokens are often configured to remain live for a long time to keep friction low – increasing the window of compromise. Last, the passwords needed to access the SSO and for any applications that do not support identity management integrations (e.g., SAML) are often still stored on servers.

A SOLUTION TO THE PASSWORD ISSUE

Rather than half measures or Band-Aid solutions, it is necessary to achieve secure, 100% passwordless authentication. It's time for a world without passwords.

> Through the end of 2020, enterprises that invest in new authentication methods and compensating controls will experience 50% fewer identity-related security breaches than peers that do not.
>
> – ANT ALLAN, VP ANALYST, **GARTNER**[9]

Enterprises need an elegant solution that works with the apps they already use, integrates with their current IAM stack, and doesn't require third-party app vendors and SaaS providers to make it work. An ideal solution would solve all the issues caused by passwords and existing authentication methods, resulting in:

EFFORTLESS LOGIN EXPERIENCE FOR ALL AUDIENCES

No passwords to remember or for the organization to manage and secure.

SECURITY AND FULL AUDITABILITY

No central server storage means no more hacking of employee or customer passwords. Completely machine-verifiable audit trail.

RAPID TIME TO VALUE

Integrates with in-place IAM stack (SSO, MFA) and eliminates the need for MFA, thereby reducing costs.

STREAMLINED ONBOARDING

for employees, customers, and contractors – no IT required. User-executed device recovery and migration.

[9] Ant Allen, Gartner "Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls" April 4, 2019.

06

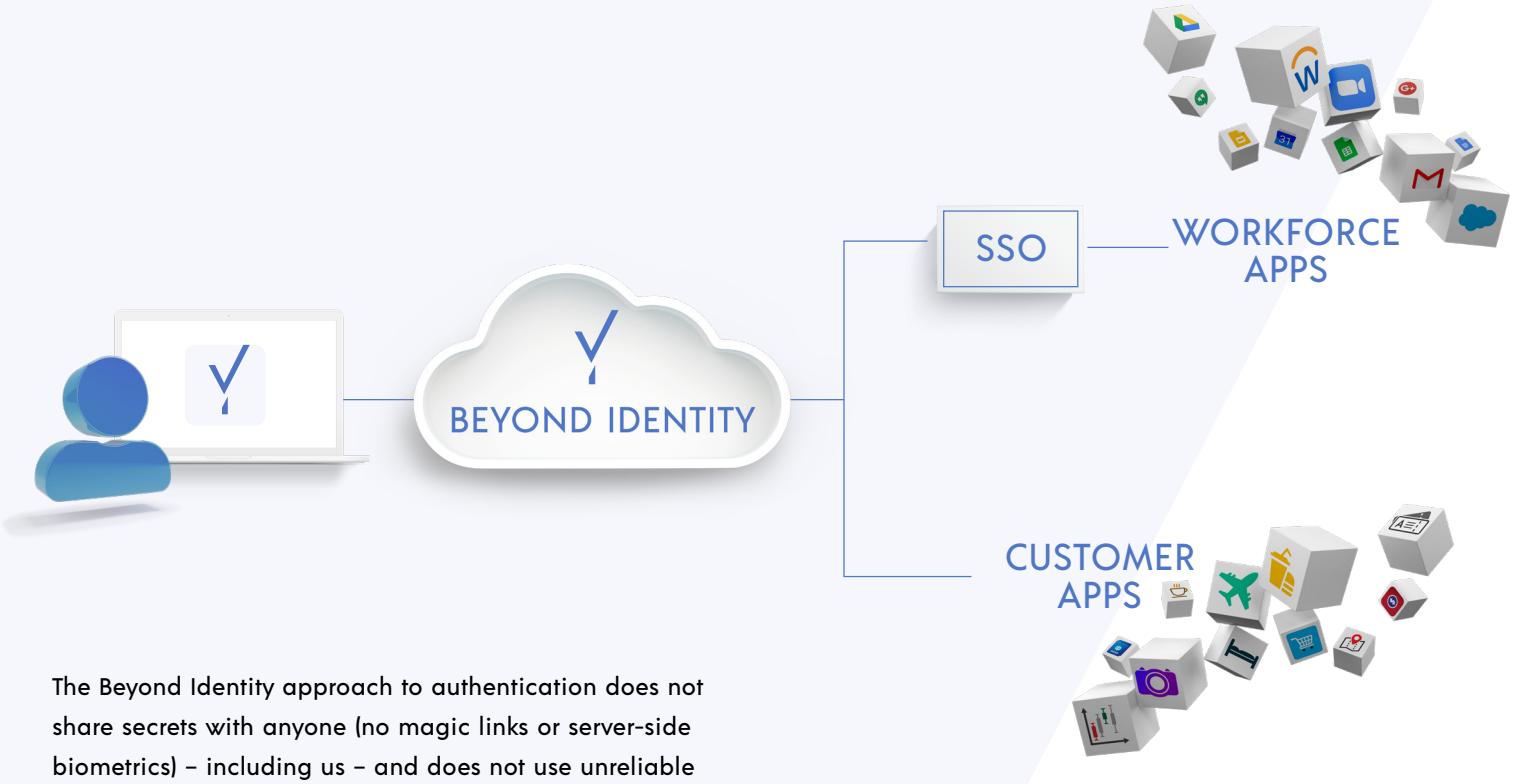
INTRODUCING

BEYOND IDENTITY

Beyond Identity is eliminating passwords and the friction and risk that come with them, using an elegantly simple concept, the personal certificate authority.

Our patented solution leverages secure, industry-standard asymmetric-key cryptography for authentication. Instead of a password, our solution employs self-signed X.509 certificates. Our cloud-native solution employs an app on endpoint devices to create and manage keys and fundamentally change the way users authenticate into networks and applications.

Beyond Identity integrates with existing SSO solutions with just a few lines of configuration code, enabling enterprise users to leverage established login patterns and eliminate both friction issues (password resets, need for strong passwords, etc.) as well as the multiple cybersecurity and compliance risks passwords present.



The Beyond Identity approach to authentication does not share secrets with anyone (no magic links or server-side biometrics) – including us – and does not use unreliable and insecure channels for authentication (no SMS, push notifications, or email links).

We're using industry-proven public key infrastructure (PKI), TLS, and hardware enclaves in a brand-new way to give enterprises the best of all worlds. A world that minimizes user friction and improves security.

BEYOND IDENTITY

07

CONCLUSION

Passwords, while ubiquitous, are also fundamentally insecure. Alternative solutions can help ease some of the challenges with passwords, such as user friction, but they cannot solve the problem of shared secrets. Any information that has to be stored in a database will never be secure. The only way to solve that problem is to eliminate it completely. No more password-fueled data breaches, no more costly password resets, no more user friction. Period.

NEXT STEPS

Visit our website: www.beyondidentity.com/technology
Request a demo: www.beyondidentity.com/demo

ABOUT BEYOND IDENTITY

Headquartered in New York City, Beyond Identity was founded by industry legends Jim Clark and Tom Jermoluk to eliminate passwords and radically change the way the world logs in, without requiring organizations to radically change their technology stack or processes.

Funded by leading investors, including New Enterprise Associates (NEA) and Koch Disruptive Technologies (KDT), Beyond Identity's mission is to empower the next generation of secure digital business by replacing passwords with fundamentally secure X.509-based certificates. This patents-pending approach creates an extended Chain of Trust™ that includes user and device identity and a real-time snapshot of the device's security posture for adaptive risk-based authentication and authorization. Beyond Identity's cloud-native solution enables customers to increase business velocity, implement new business models, reduce operating costs, and achieve complete passwordless identity management. Visit beyondidentity.com for more information.