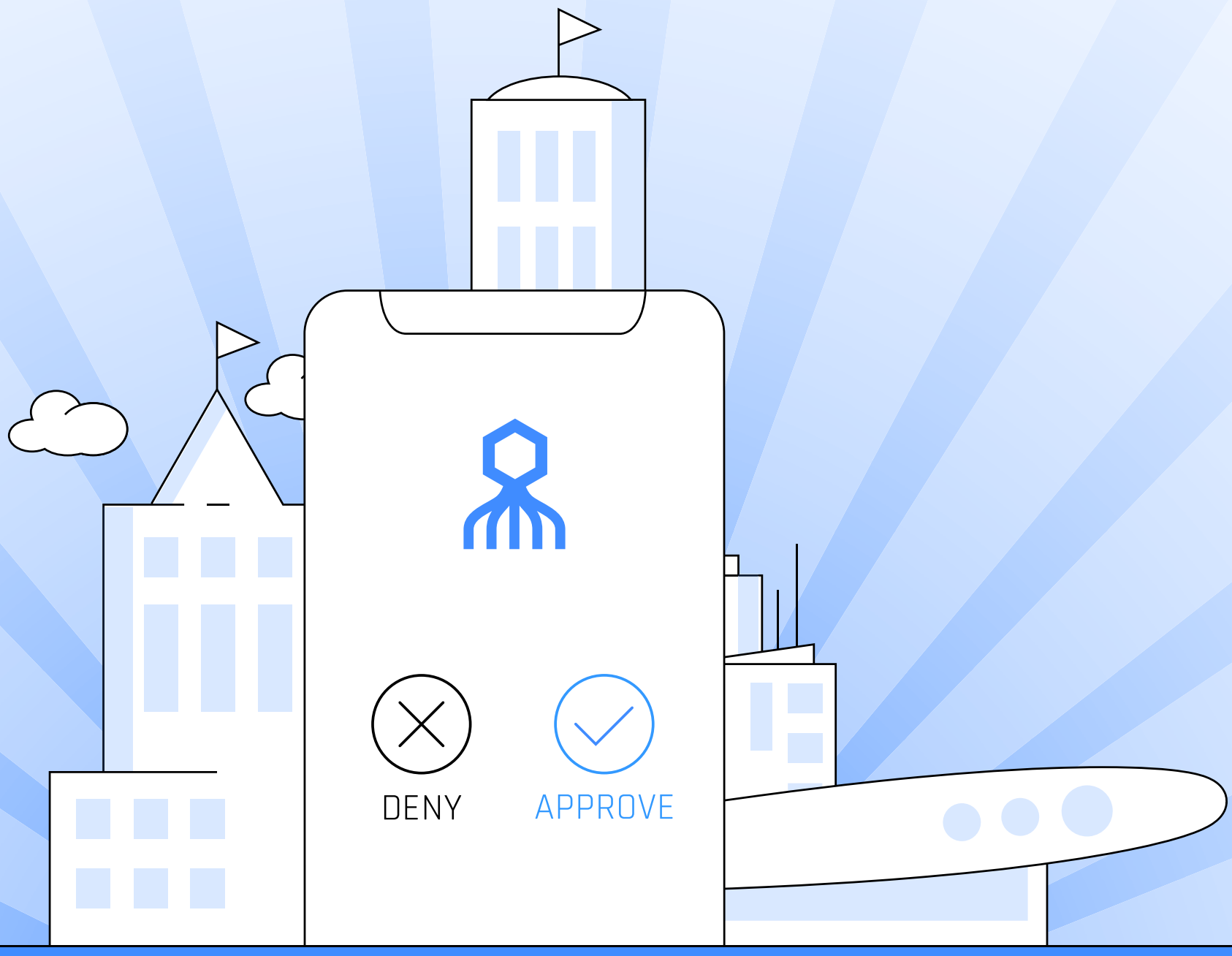
SECRET DOUBLE OCTOPUS
users are human

Passwords are a Vulnerability



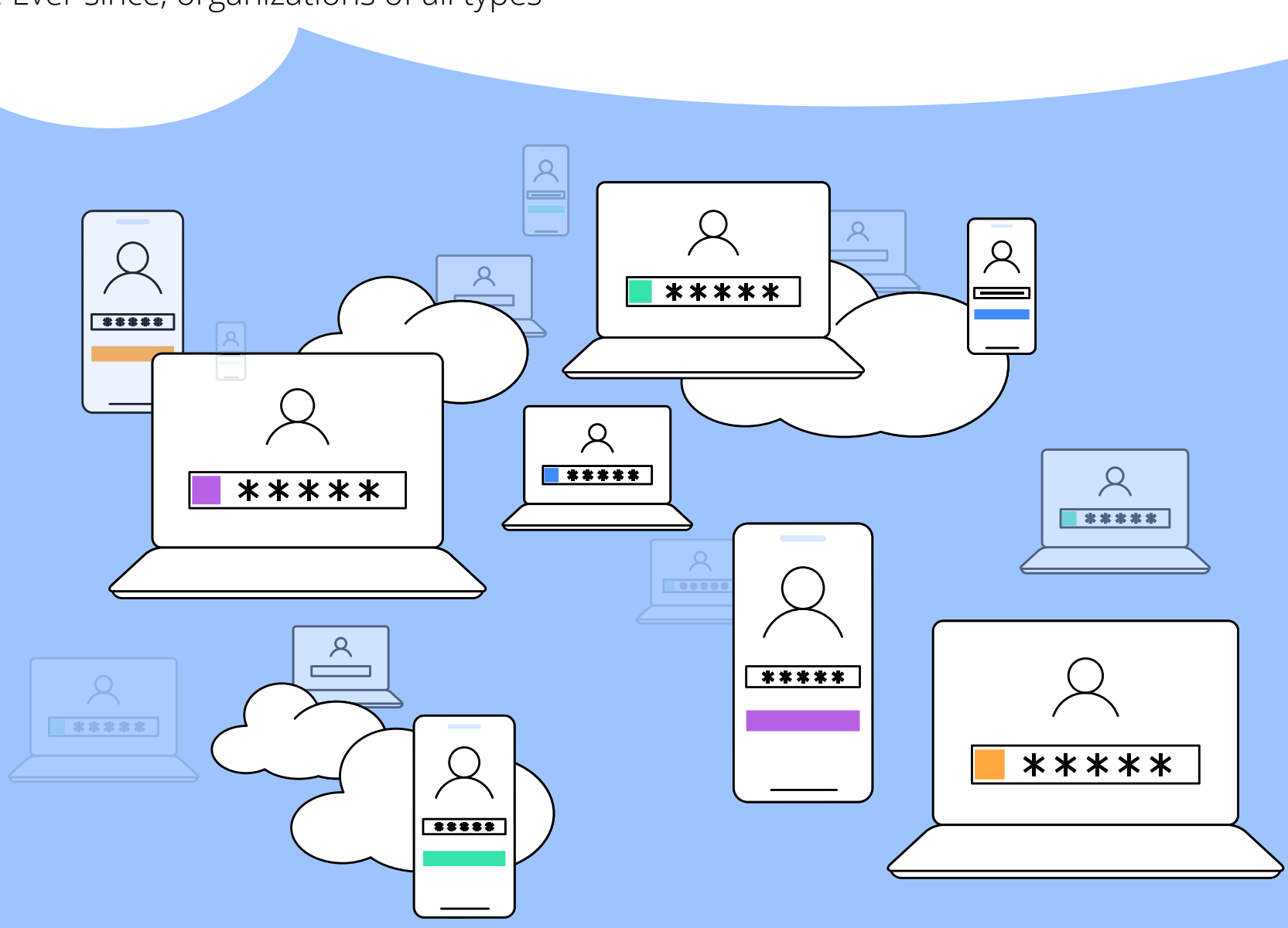
WHAT'S NEXT FOR AUTHENTICATION?

THE WHITEPAPER

Introduction

A History of Secrets

Passwords, in one way or another, have been used to confirm identities since the time Roman soldiers exchanged watchwords to distinguish friends from foes. Ever since, organizations of all types and sizes remain heavily dependent on the concept of a **memorized piece of information which immediately grants access to its holder**.



A couple millennia later, the age of computing brought new challenges to identity verification. The immeasurable amounts of sensitive data generated and stored today and the speed at which data can be stolen or destroyed, has long become a major concern for small businesses and large corporations alike, and the engine behind the multi-billion cyber security industry.

Dealing with this growing challenge demands constant adoption of new methods and tools, both technological and behavioral in nature, which together can guarantee a higher level of data protection for any enterprise. And while adding new defense layers is beneficial and even crucial sometimes, **there's a fundamental fact to face in the security world – relying on memorized passwords just doesn't cut it anymore**.

Passwords Are a Vulnerability

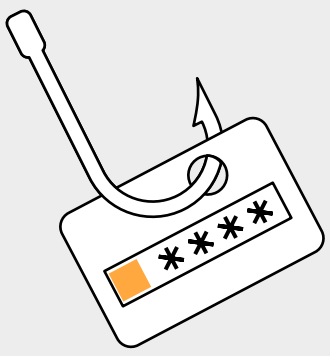
For years, the standard approach to dealing with the inherent security flaws of password was limited to three categories: enforcing increasingly harsher password policies, deploying a second (and sometimes a third) method of authentication on top of a password, and educating users about the dangers of social engineering and password misuse.

Yet, research shows that **these methods are not only insufficient, but commonly play into the hands of attackers**. Surprisingly as it may be for some, the most common password used in 2019 is still '12345'[1], followed by equally simple strings. In the business sector, where security policies prevent the use of such common strings, the problem is only slightly less dire. Recent research among IT security personnel showed 49% of responders admitting to sharing passwords with colleagues to access business accounts, while 59% reported that their organization relies only on memory to manage passwords and 42% say sticky notes are being used for that purpose[2].

81%

of hacking-related breaches leveraged either stolen and/or weak passwords[4]

The danger of passwords is clearly demonstrated by Verizon's 2019 Data Breach Investigations Report which associated 32% of breaches surveyed with phishing attacks and states that 29% involved the use of stolen credentials[3]. This comes as no surprise after the 2017 edition of the same report declared compromised credentials the direct cause of a staggering 81% of data breaches[4].



32%

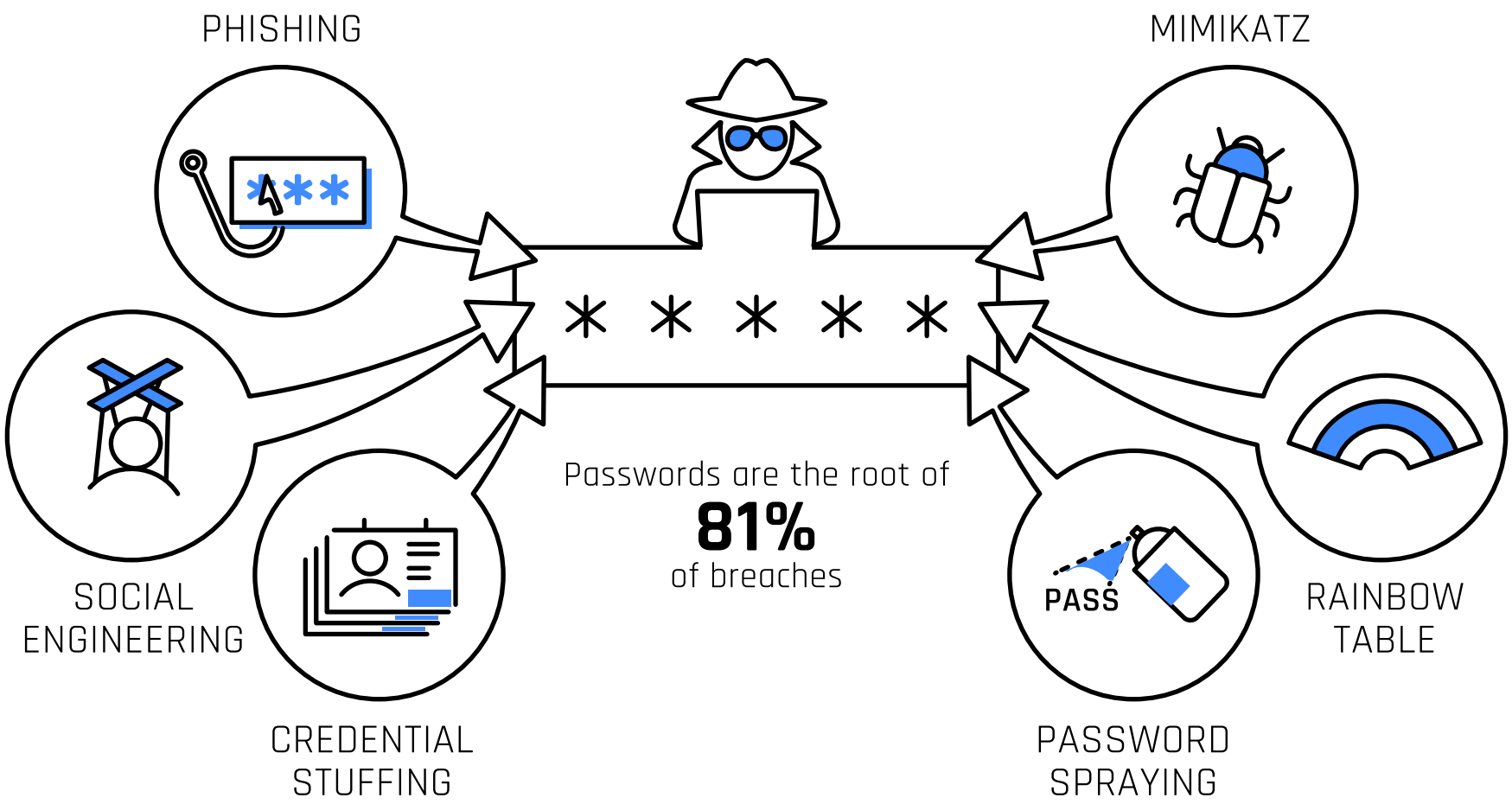
of breaches involved phishing

29%

of breaches involved use of stolen credentials

1 https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere
2 https://www.yubico.com/wp-content/uploads/2020/02/2020_ponemon_security_behaviors_report.pdf
3 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
4 https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

...Passwords Are a Vulnerability



With an average cost of $3.92M

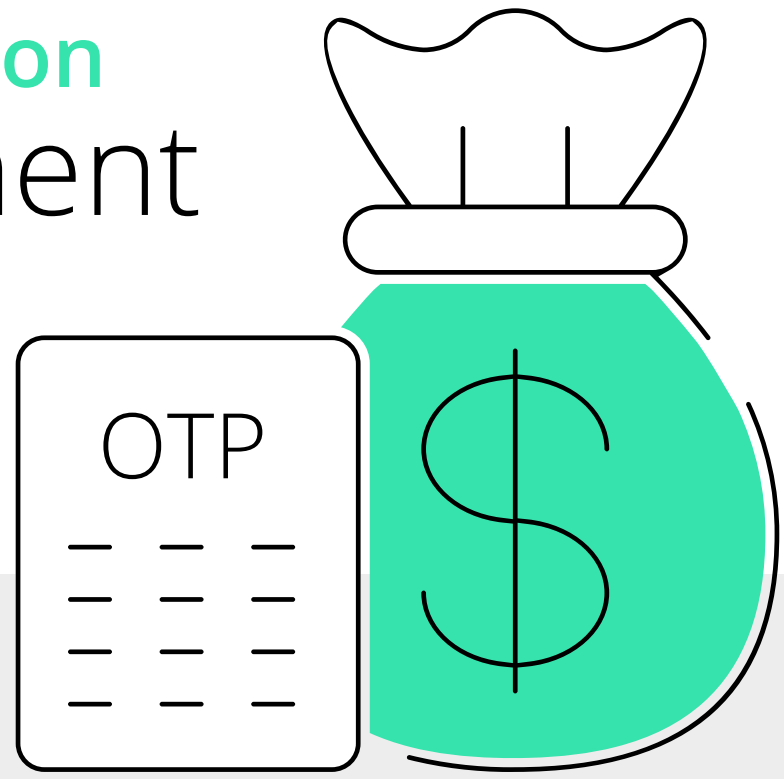
per corporate data breach according to a 2019 IBM report, preventing potentially devastating security incidents is more critical than ever before.

The financial implications of data breaches enabled by passwords are becoming more dire as well. With an average cost of $3.92 million per corporate data breach according to a 2019 IBM report[5], preventing potentially devastating security incidents is more critical than ever before.Confronted by this reality, IT departments and helpdesk teams have been trying to navigate the balance between enforcing adequate password policies and dealing with the heavy consequences of that same effort. Results however tend to be expensive and ineffective in providing better protection. Password complexity requirements, once thought to be critical in preventing hacks, have been determined useless and provide no defense against many common attacks. This approach is now regarded as an obstruction to both productivity and security[6][7]. Moreover, since up to 50% of all help desk calls are related to password resets according to Gartner. And with Forrester Research estimating an average cost of $70 per password reset[8], strict password policies are increasing operational costs dramatically.

5 https://www.ibm.com/downloads/cas/ZBZLY7KL
6 https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
7 https://pages.nist.gov/800-63-3/sp800-63b.html#policies
8 https://www.forrester.com/report/Best+Practices+Selecting+Deploying+And+Managing+Enterprise+Password+Managers/-/E-RES139333

Multi-Factor Authentication

Limited improvement at a great cost



In an effort to bolster password security and as a result of regulatory demands, many companies have Multi-Factor Authentication (MFA) solutions deployed for both employees and customers. MFA relies on the assumption that a combination of two or more distinct proofs of identity (something the user knows, something the user holds and something the user is) are enough to fully trust authentication under any circumstances.

But with the growing adoption of MFA, a slow realization is starting to emerge - Multi-Factor Authentication doesn't deliver sufficient security on its own. After several successful attacks on seemingly secure out-of-band authentication factors, regulators started adding restrictions on Multi-Factor Authentication methods. In a 2020 update to its digital identity guidelines, the US National Institute of Standards and Technology (NIST) states that authenticators leveraging phone calls and SMS messages to send unencrypted One-Time Passwords (OTPs), once considered a legitimate channel, are now labeled "restricted" and are subject to several limitations[9]. The use of biometrics as a standalone authentication factor is also limited by NIST for its probabilistic nature and susceptibility to spoofing[10].

To make matters worse, MFA solutions are expensive to deploy and manage and have a devastating effect on user experience and productivity. As a result, the use of MFA within enterprise environments and internal corporate networks remains sparse and is usually limited to corporate VPNs and remote services, according to the latest Mary Meeker Internet Trends Report[11].

In a 2020 update to its digital identity guidelines, the US National Institute of Standards and Technology (NIST) states that authenticators leveraging phone calls and SMS messages to send unencrypted One-Time Passwords (OTPs), once considered a legitimate channel, are now labeled "restricted"

In summary - not all Multi-Factor Authentication solutions are equal, with some offering higher protection than others. **But all MFA methods are inherently dependent on a vulnerable password and all add significant complexity and cost to both users and administrators**.

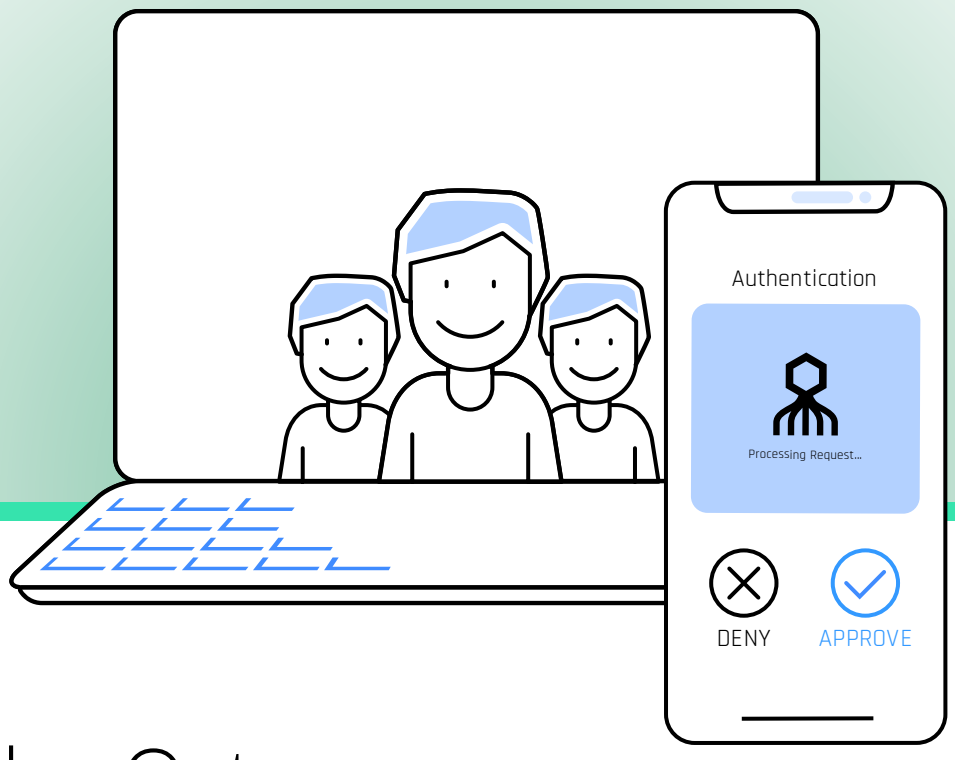
9 https://pages.nist.gov/800-63-FAQ/
10 https://pages.nist.gov/800-63-3/sp800-63b.html#biometric_use
11 https://www.bondcap.com/report/itr19/

A world without passwords is possible!

The passwordless solution

New technologies have been regularly introduced to reinforce IT security since the early days of computing. Nowadays, with the proliferation of fingerprint readers and image recognition technologies, the day-to-day security posture and convenience of most smartphone users has dramatically improved. Similarly, new standards such as Fast Identity Online (FIDO) and Web Authentication (WebAuthn) are becoming more prevalent, delivering businesses and individuals the benefits of easier, faster and more secure authentication.

But when it comes to corporate environments, where demands are more intricate and mistakes cost more, adoption is lagging. **Security teams are still struggling to manage and reset passwords, employees are still tempted to write down and share passwords and organizations still rely on extremely vulnerable password usage habits**.



In Comes the Octopus

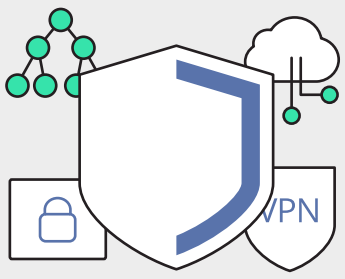
Now, with Secret Double Octopus' Passwordless Authentication, enterprise IT managers can eliminate password-related security threats and reduce their costs, with the added benefit of having a simpler and faster solution for their employees.

Secret Double Octopus' Passwordless Authentication technology is designed to address the diverse authentication needs of a real-world, working enterprise. It provides a universal user experience for accessing all enterprise resources, whether on-premise or in the cloud, online and offline.

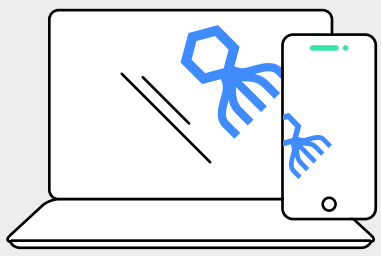
...In Comes the Octopus

Octopus Authentication replaces antiquated user-controlled passwords with a high-assurance, easy to use and universal passwordless authentication mechanism. Once enrolled, users never have to recall or change another password. Instead, a secure push notification is sent to the user's registered smartphone, and a PIN code or biometric signature is requested. **This built-in multi factor verification, relying on something you have and something you know/are, ensures stronger identity verification than any memorized password and standard MFA solutions**. It also means the end of password reset tickets or renewal policies to comply with.

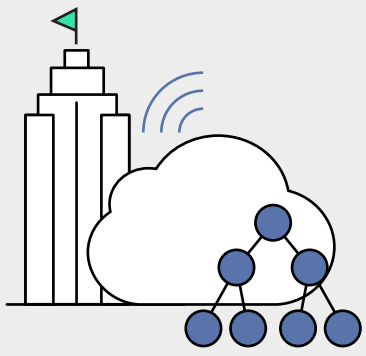
Enterprise-Ready Passwordless Technology



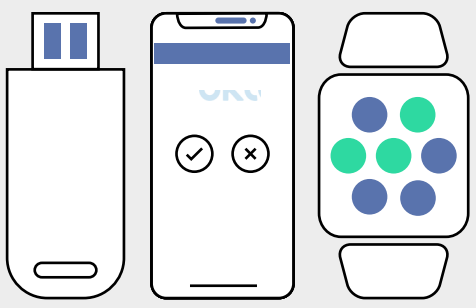
High-assurance authenticator using a multi-route secret sharing algorithm guarantees security even if one secret is stolen or captured en route.



Workstation passwordless authentication for Win & Mac, that work even when computer and authenticator are offline.



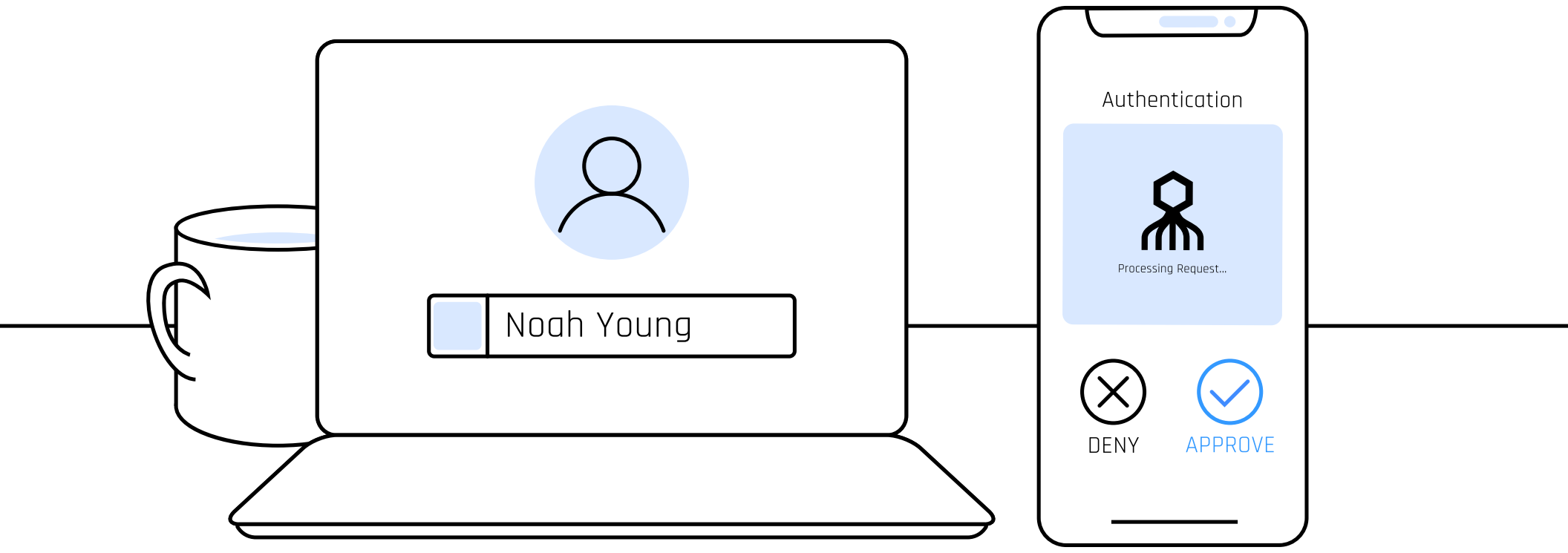
Deployed across all enterprise services and systems, on-premise or in the cloud, including all legacy applications.



Built to work in any scenario – online and offline, with or without a smartphone and with the broadest range of FIDO compliant authenticators.

About Secret Double Octopus

Secret Double Octopus enables real-world, working enterprises to adopt passwordless authentication using its high-assurance passwordless mobile authenticator app or any FIDO-compliant authenticator. Our Passwordless Authentication solution can be deployed on any modern infrastructure and supports on-prem applications and cloud services, as well as legacy systems that require passwords. Octopus Authentication works across a broad range of business use-cases, delivering outstanding protection and allowing compliance with cybersecurity requirements and regulations. From being named a Gartner “Cool Vendor” in 2016, our 3rd generation platform is now serving mid-sized to Fortune 500 customers around the globe.



SCHEDULE A DEMO

GET OUR SOLUTION OVERVIEW

SECRET DOUBLE OCTOPUS

contact@doubleoctopus.com
sales@doubleoctopus.com