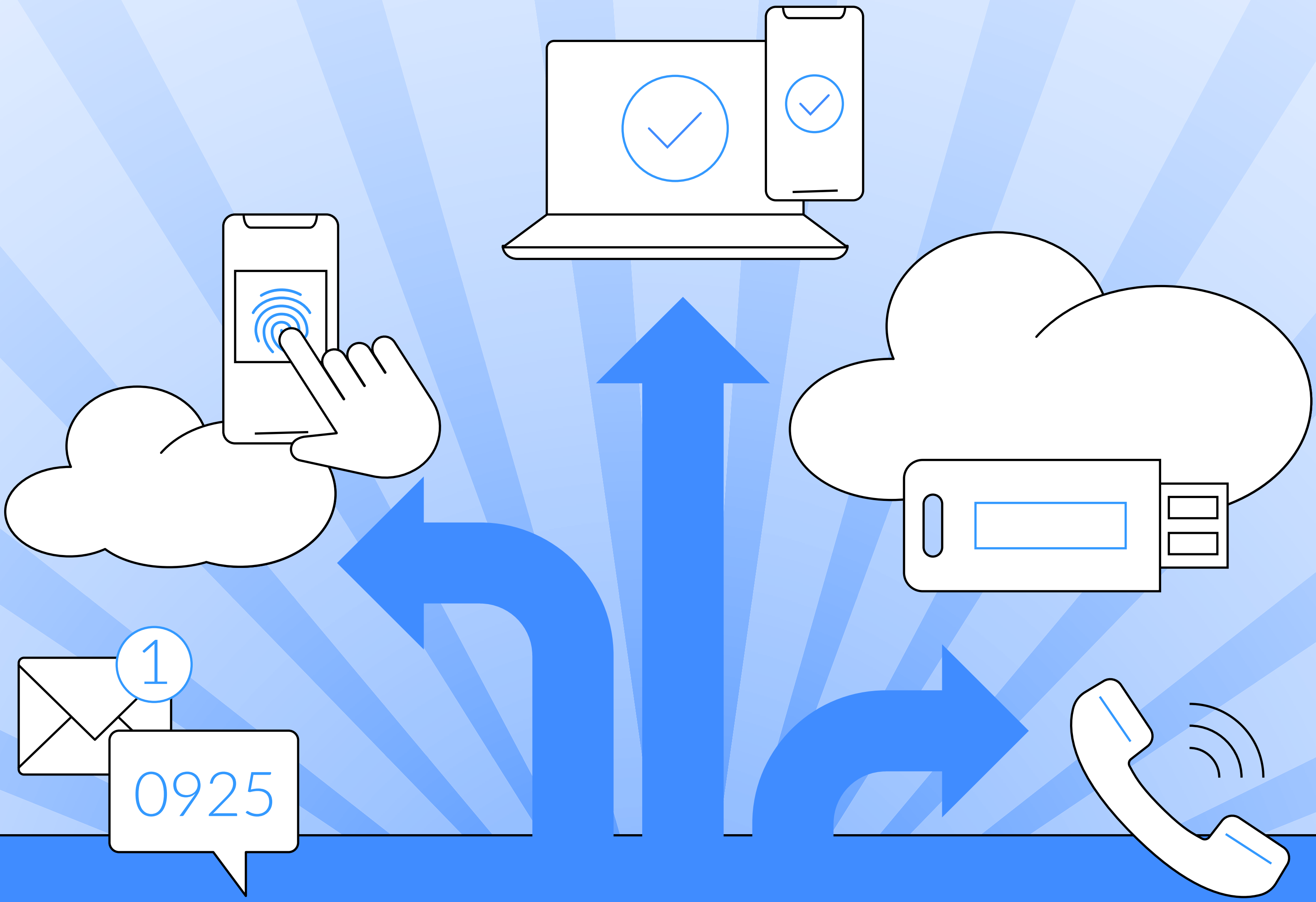
SECRET DOUBLE OCTOPUS
users are human

How to choose an Enterprise Authentication Solution

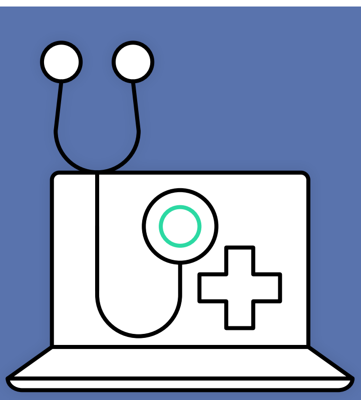


THE WHITEPAPER

Assessing enterprise authentication solutions

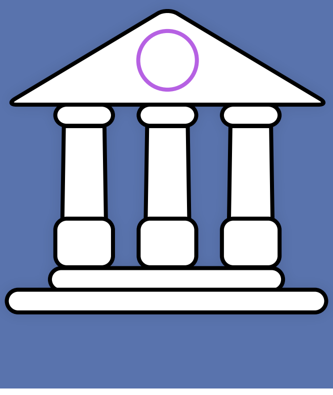
Find the solution that works for you

When evaluating enterprise authentication solutions, decision makers must consider several critical points. Starting with how well each solution addresses the real-world authentication needs of their users, and continuing to examine each solution's performance in terms of user experience, security and cost of ownership. Other important factors include its ability to work in harmony with existing infrastructure and applications, help the company comply with regulation, and prepare it for future business needs.



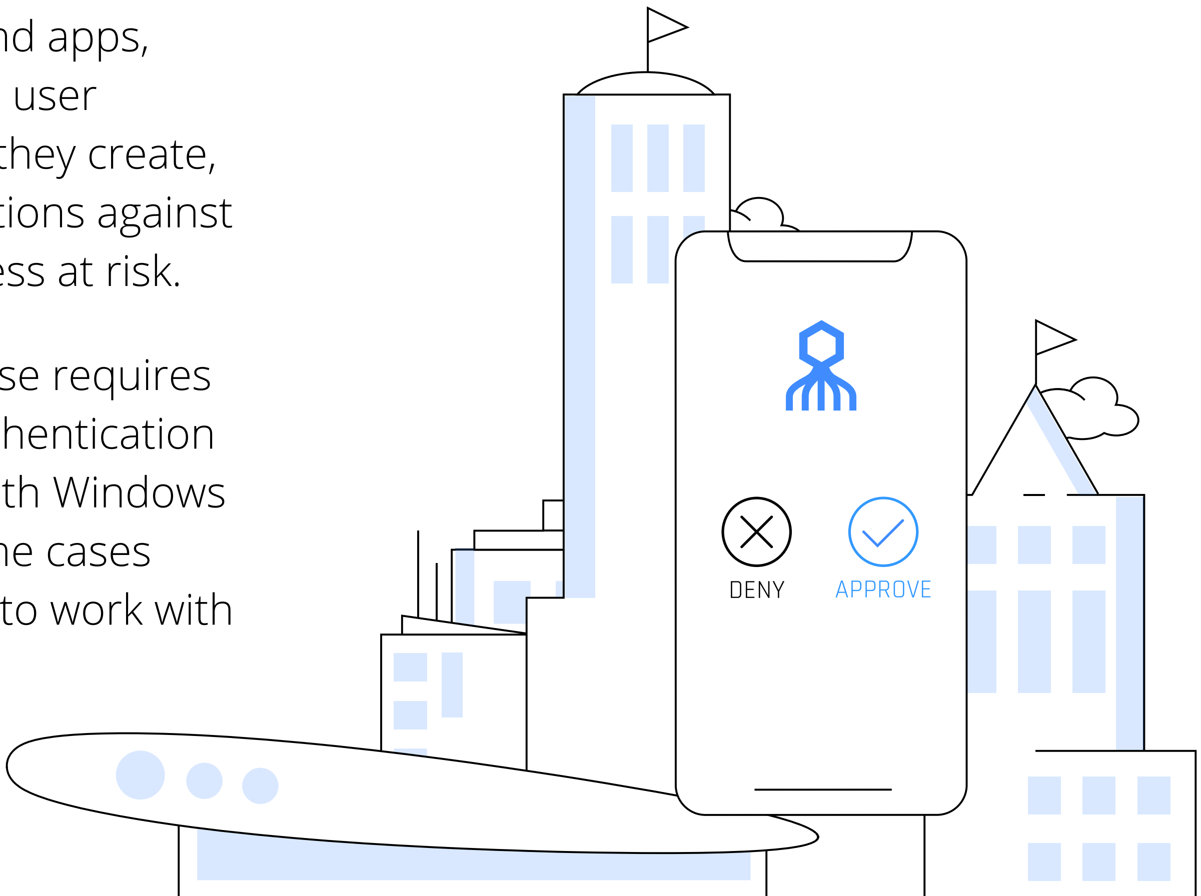
Some authentication solutions are built for specific industry verticals or use-cases. For example, authentication solutions in healthcare are highly optimized for authenticating caregivers on shared workstations. In these scenarios there's a crucial need for logon speed and smart session management, so precious caregivers' time is not wasted on typing usernames and passwords.

Another example is consumer authentication for financial services, where the goal is to provide a simple, cost effective authentication method that can be operated by people of all ages and levels of computer literacy, and also deliver meaningful protections against common attacks on financial services such as phishing and password spraying.



But for most real-world enterprise customers it is less about solving for one specific use-case and more about working with their heterogeneous IT environments. Enterprise authentication solutions need to work in harmony with a varied mix of existing investments in infra and apps, address the full breadth of the user authentication use-cases that they create, and deliver meaningful protections against the threats that put the business at risk.

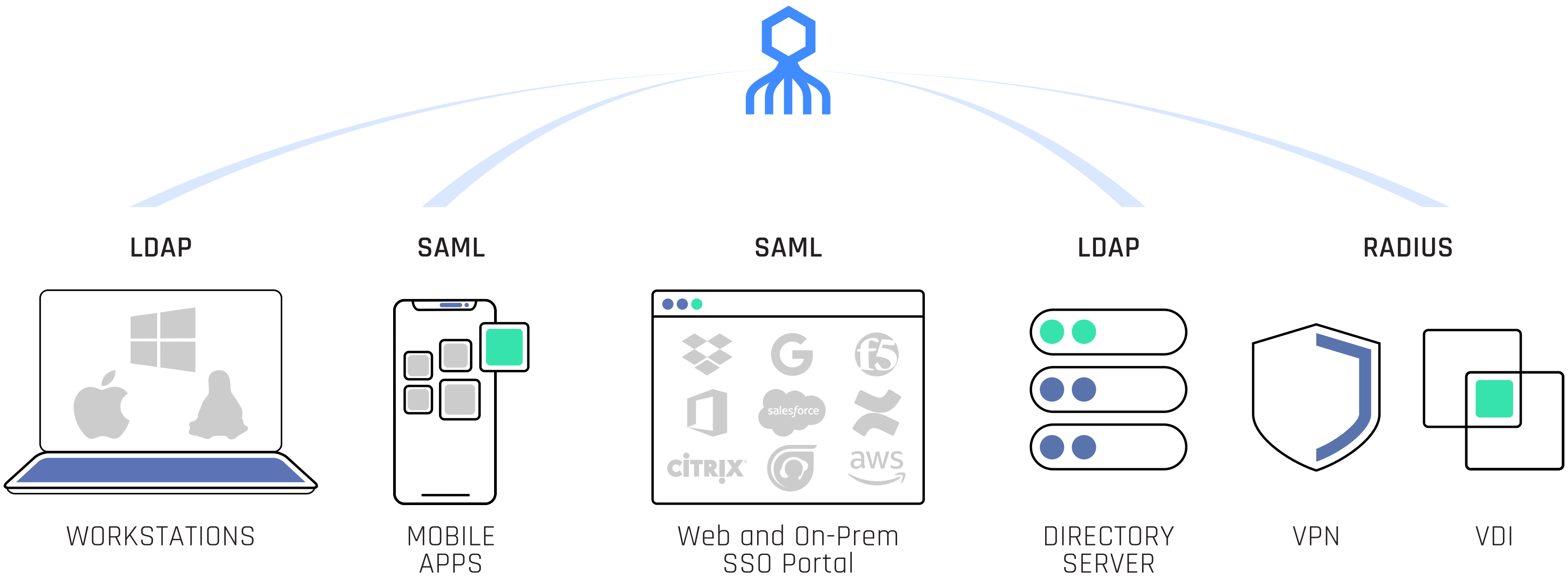
For example, a typical enterprise requires a workstation and network authentication solution that works not only with Windows hosts, but also Mac and in some cases also Linux hosts. It also needs to work with various remote access solutions (i.e. VPN, VDI, etc.), secure access to cloud apps, authenticate users to the enterprise SSO in-use, work with a secure printing system, enable access to a 20 year old HR system, and more.



Does it support the full scope of users' authentication needs?

The most fundamental question is whether an authentication solution supports the full breadth of use-cases encountered by users over the course of their workday. When specific use-cases are not supported, two options are available - leave in place an outdated authentication method or look for additional solutions.

Sticking with usernames and passwords for a single use-case defeats the purpose of investing in a better, more secure authentication solution **and** leaves the organization exposed. It's like building a fortified wall around your house but leaving a backdoor with just a padlock. Acquiring a second authentication solution that can handle the edge case, means that users will have to understand and handle more than one authentication flow. This means an extra expense, and perhaps more importantly, will also add friction and frustration for employees.



Common real-world enterprise authentication scenarios:

WORKSTATION LOGON

Windows, Mac and Linux machines require specific OS integrations domain management solutions.

REMOTE ACCESS VPN

Support of the Remote Authentication Dial-In User Service (RADIUS) protocol is an absolute requirement in most large organizations.

CLOUD APPLICATIONS ACCESS

Competing protocols and frequent revisions to existing standards makes cloud services support a moving target.

OFFLINE AUTHENTICATION

Guaranteeing secure access even when network connection is down or the authenticating server can't be reached has been the Achilles heel for many MFA solutions.

LOST AUTHENTICATOR

A huge pain for IT managers, especially when it's a hardware token that's been lost. Shipping a replacement costs time and money, not to mention employee downtime.

In summary, a modern enterprise authentication system has to deliver an all-around solution that will handle all use-cases and scenarios. Implementing several specialized solutions means extra time, expenses, training and support.

How does it perform?

Once it is established that an authentication solution supports the required use-cases, it can be assessed in terms of business outcomes - user experience, security and cost of ownership.

User experience

The success of any user authentication mechanism ultimately depends on whether it improves user experience and makes their lives easier. Users want a simple solution that works the same way across all systems and helps them get fast access to what they need. In other words, they want:

- One authenticator to access all systems and applications, on-premise and off, online and offline. There’s no reason for your users to keep carrying several authenticators, keys and tokens.

- Shorter time to authenticate. For users, authentication is a roadblock preventing them from getting their job done. The faster they can get past this roadblock, the happier, more productive they are.

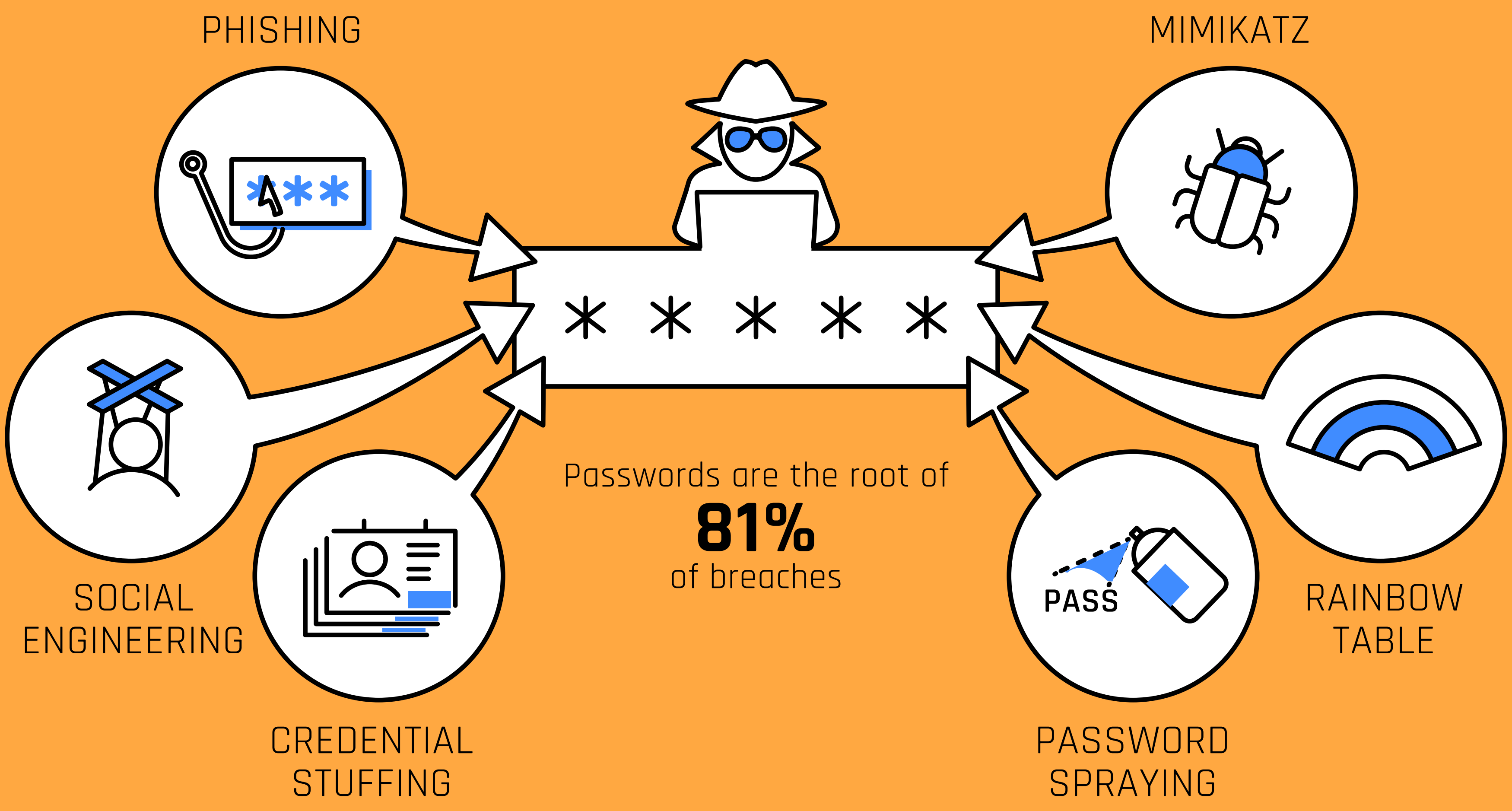
- Less downtime. One of the biggest problems with passwords and hardware tokens is that they often get forgotten or misplaced, leading to anxiety and frustration for users. Recovery often requires elaborate, expensive procedures and a lot of helpdesk support which in turn causes friction and negative sentiment between users and their IT staff.

...How does it perform?

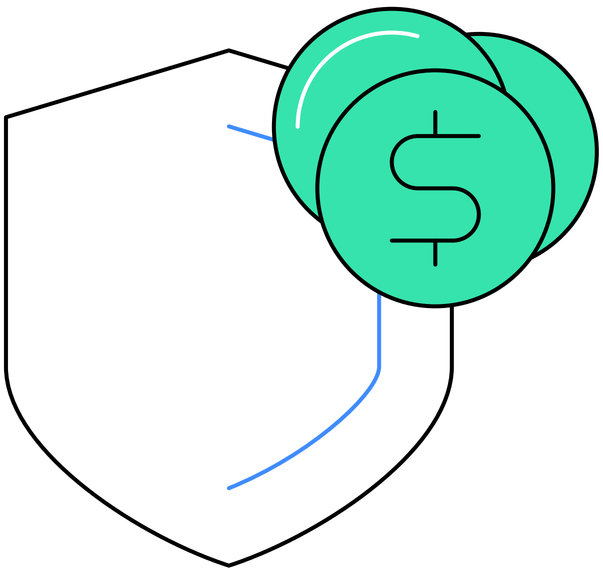
Security

Security is the reason businesses deploy authentication solutions in the first place. Without substantial gains in security, there's simply no point in making the investment. With an unbelievably broad spectrum of threats that is continuously evolving, there's no half measures when it comes to authentication security.

Over 80% of data breaches are associated with compromised passwords usually gained through credential theft attacks (most notably phishing) which are highly effective and therefore not likely to go away any time soon. Various forms of man-in-the-middle attacks are commonly used to specifically target authentication systems, not to mention common hacking tactics like stuffing, spraying and brute force attacks. To be seriously considered,any authentication system should provide robust protections against prevailing attacks and demonstrate high-assurance under any circumstances.



...How does it perform?



Cost of ownership

Decision makers want to understand the cost of ownership for any new technology acquisition, and rightfully so. Costs always need to be analyzed and weighed against the gained benefits in terms of security and productivity, and user authentication solutions are no exception.

In addition to the direct licensing and initial deployment costs, organizations need to consider the following operational costs:

HELPDESK LOAD

Poorly designed authentication solutions result in confused users requiring assistance. This, in turn, quickly translates into increased load on helpdesk and IT teams and associated expenses. With password-related issues causing anywhere between 20% to 50% of all help desk calls, this should be a major consideration when choosing the right authentication solution for your employees

PASSWORDS MANAGEMENT

Managing credentials across an entire enterprise requires substantial effort and resources. Enforcing and facilitating periodic password resets, helping employees when they forget passwords, and making sure systems comply with regulation can be a nightmare for IT teams and the employees they serve. Additional tools like phishing prevention systems are also commonly deployed, costing even more

EMPLOYEE DOWNTIME

Lost or forgotten tokens and credentials, whether they are simple passwords or sophisticated authenticators, means an immediate loss of time and productivity. With physical authenticators, recovery can take a long time and require a logistical effort, which makes things even worse

LOGIN TIME

Users are usually required to authenticate multiple times a day. While the few additional seconds required for authentication might seem insignificant, when you multiply them by the number of times an average user authenticates in a day, they add up to many frustrating minutes

Other considerations when evaluating an enterprise authentication solution include how well it works with existing investments in infrastructure and applications, whether it will help the Company comply with requirements from auditors and regulators, and its ability to adapt to the business's changing technology space and evolving needs.

Does it work with what I already have in place? Do I need to rip-and-replace systems?

The reality for most enterprises is that they have a varied mix of systems and applications purchased and built over the years. This is a challenge for any new authentication solution, which needs to work with everything that is already in place without lowering security or usability standards.

Unfortunately, not all modern authentication solutions are designed to support legacy systems and applications. That's why it's crucial to choose the technology that can easily integrate and interoperate with any existing IT infrastructure. Supporting Active Directory and other IdPs, working with customized legacy systems, and coexisting alongside other authentication solutions, are all necessary features and should not require additional integration projects.

Does the solution address requirements from auditors and regulators?

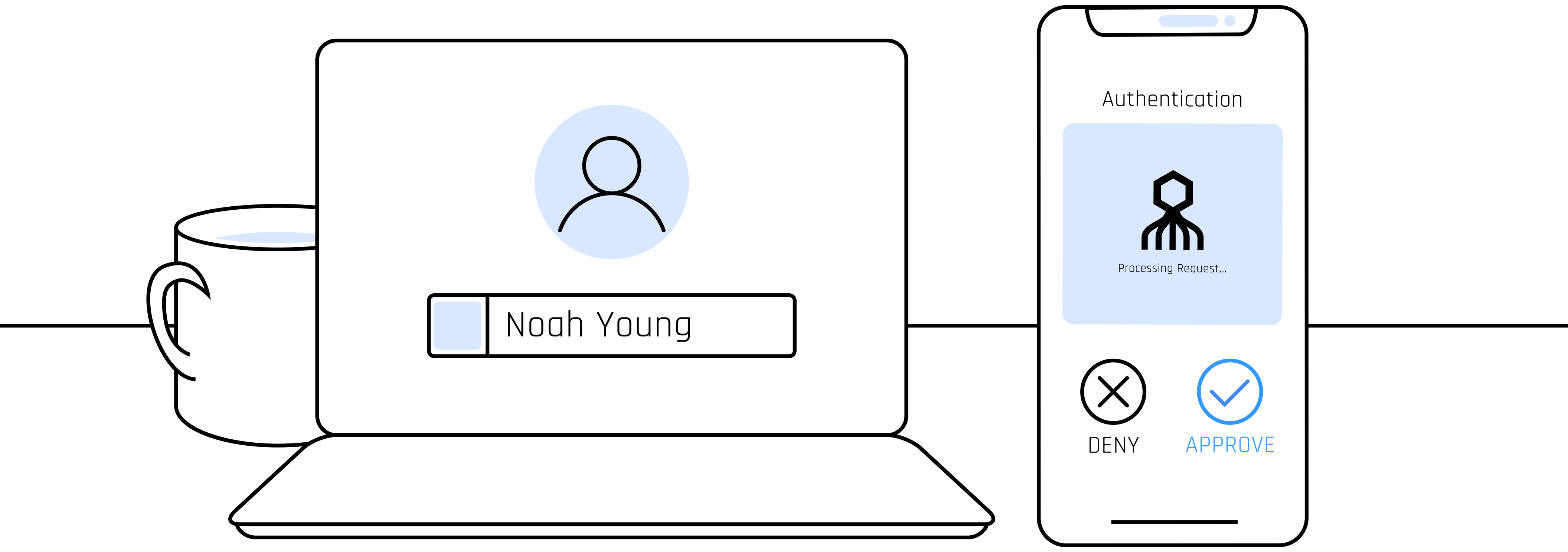
Most enterprises these days need to operate within regulatory environments that impose strict demands regarding data protection and user authentication. Compliance with regulations and industry standards like PCI DSS, DFARS, HIPAA, SOX/GLBA, PSD2, GDPR, and others is therefore a significant consideration and often the main driver for investing in a new user authentication solution.

Is it "future proof"?

The technology environment for most enterprises is in constant flux. It should therefore be assumed that any authentication solution deployed today will stick around for many years, and should evolve with the business reality, supporting new authentication needs and standards as those arise. An interesting technological change that is just around the corner for many enterprises is the adoption of Passwordless Authentication. This means that any authentication solution considered today should provide its users the option to easily migrate to Passwordless Authentication.

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