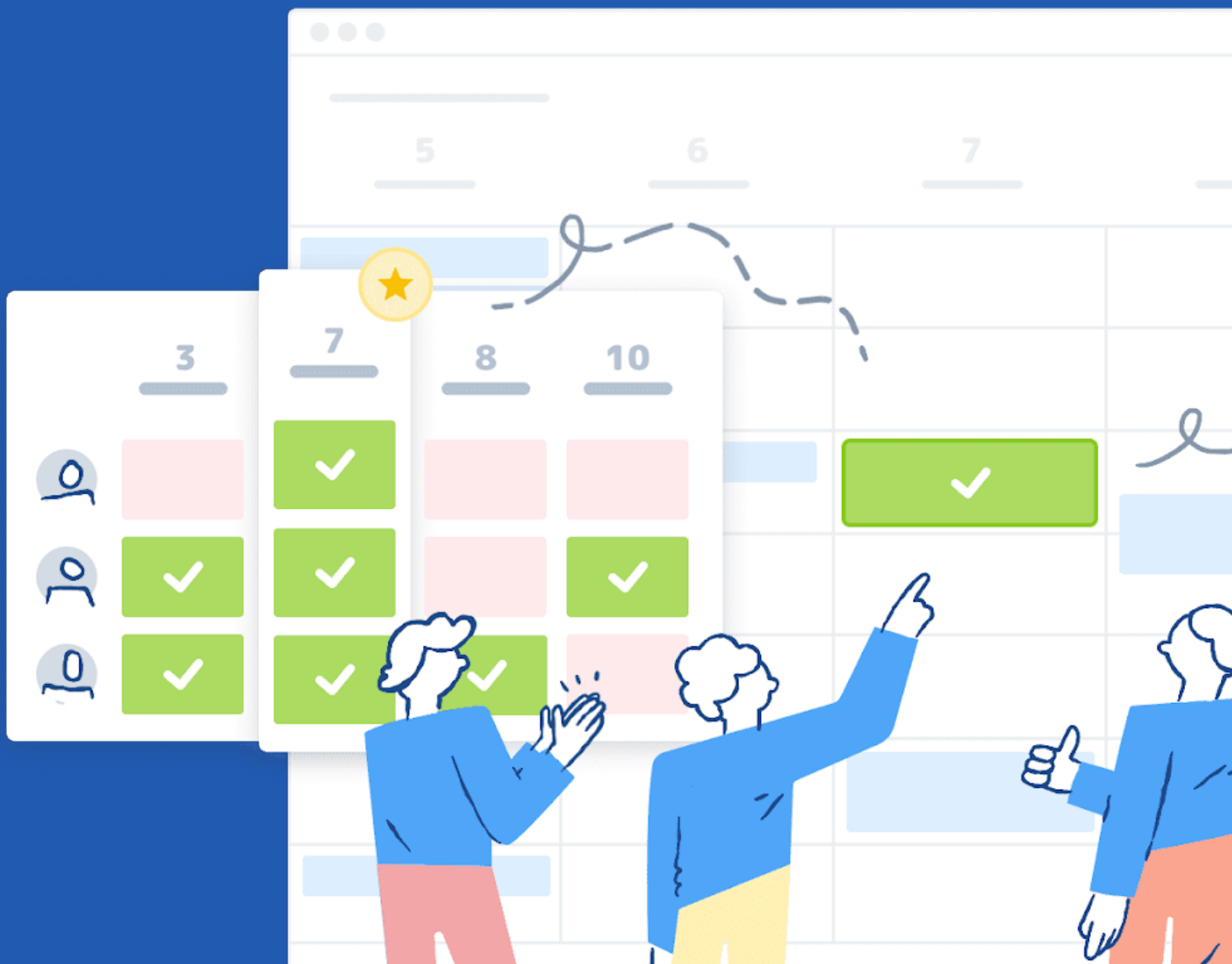


Doodle

CORPORATE RISK AND SINGLE SIGN-ON

**Does your organization need
a Single Sign-On Solution?**



Contents

Introduction	3
What Benefits Does Single Sign-On Offer?	5
Why Passwords Are a Problem?	6
Case Study: Equifax	8
Is Single Sign-On Right For You?	10
What Else Should I Know	11
Comparison	12



INTRODUCTION

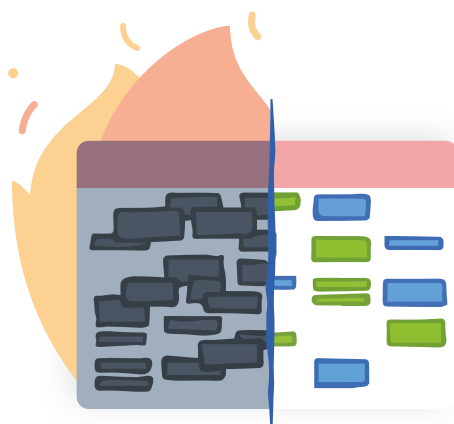
IT leaders operate in a sector that is marked by constant change. New technologies bring both opportunities and risks, and stretch the capabilities of corporate IT departments at every turn. Staying on top of these shifts should be paramount for every tech leader: with hackers constantly searching for fresh vulnerabilities to exploit, making the right decisions around the security of your tech stack is paramount for both your company's future, and your own.

The complexity of a modern-day IT stack would have been unimaginable to a CTO just a few years ago: in 2000, the average business used just 4 or 5 enterprise software solutions — all of which were maintained on the company's own servers. In 2019, according to the *Wall Street Journal*, the average large company deployed some [129 apps](#) — an increase of 68% in just four years —

while smaller firms deploy around 73 different tech solutions. And the majority of those apps are cloud-based SaaS solutions, greatly increasing both the complexity and security of the stack.

In 2019, according to the Wall Street Journal, the average large company deployed some 129 apps — an increase of 68% in just four years.

Against this background, it is no surprise that many companies have begun to explore Single Sign-On (SSO) as a potential solution for increased security. Read on to learn more about why SSO should be part of your organization's IT security protocols.



What Is Single Sign-On?

Single Sign-On (SSO) is a secure, web-based, authentication mechanism. It shares identities between organizations and applications and has the potential to eliminate the need for individuals to remember separate login information for each of the apps and services

they use on a daily basis. Instead, users log into their company's enterprise environment and are automatically logged in to any app within the company's tech stack that the IT administrator has provided them access to.



WHY PASSWORDS ARE A PROBLEM

While good security hygiene practices recommend using a unique username and password for every application or service, a 2019 TechRepublic article noted that the average employee switches between an average of 35 different applications more than [1000 times](#) per day. This proliferation of non-standardized usernames and passwords makes it almost impossible for employees to practice effective security hygiene: many resort to non-recommended practices such as writing

down login details, or simply repeating credentials across different services.

In addition, this proliferation of passwords also causes user frustration and leads to productivity issues — both within the IT function, which must deal with the surge in password assistance and reset requests, and across the company as a whole, as employees also lose valuable time dealing with password management.



WHAT BENEFITS DOES SSO OFFER?

Major benefits to SSO include improved security and productivity and cost savings across your organization.

Improved Security

In recent years, a number of high-profile hacks of major corporations have exposed sensitive data for millions of customers. These breaches cost companies time, reputation, and billions of dollars in fines, compensation and lost revenue. (For one example, see Equifax Case Study below.)

While SSO won't prevent hackers from seeking vulnerabilities to exploit, it can tighten up the most common source of hacking-related breaches. According to Verizon's 2019 Data Breach Investigations Report, attacks where credentials had been hacked or phished were the most common source of data breach, accounting for 52% of all breaches.

However, while major firms such as Capital One and Equifax may make the headlines, smaller businesses are also at risk. As Verizon's report indicates, 43% of breaches involve small business victims.

Cost Savings & Productivity Gains

According to the Gartner Group, up to 50% of a company's help desk calls are for password resets — a direct cost that affects almost every company, not to mention a source of friction that weighs down productivity for individual workers and the help desk as a whole.

As discussed above, the more apps an employee has to sign into, the greater the risk of them reusing passwords (creating a security risk), or forgetting their credentials, resulting in a help desk call and precious minutes and hours wasted.

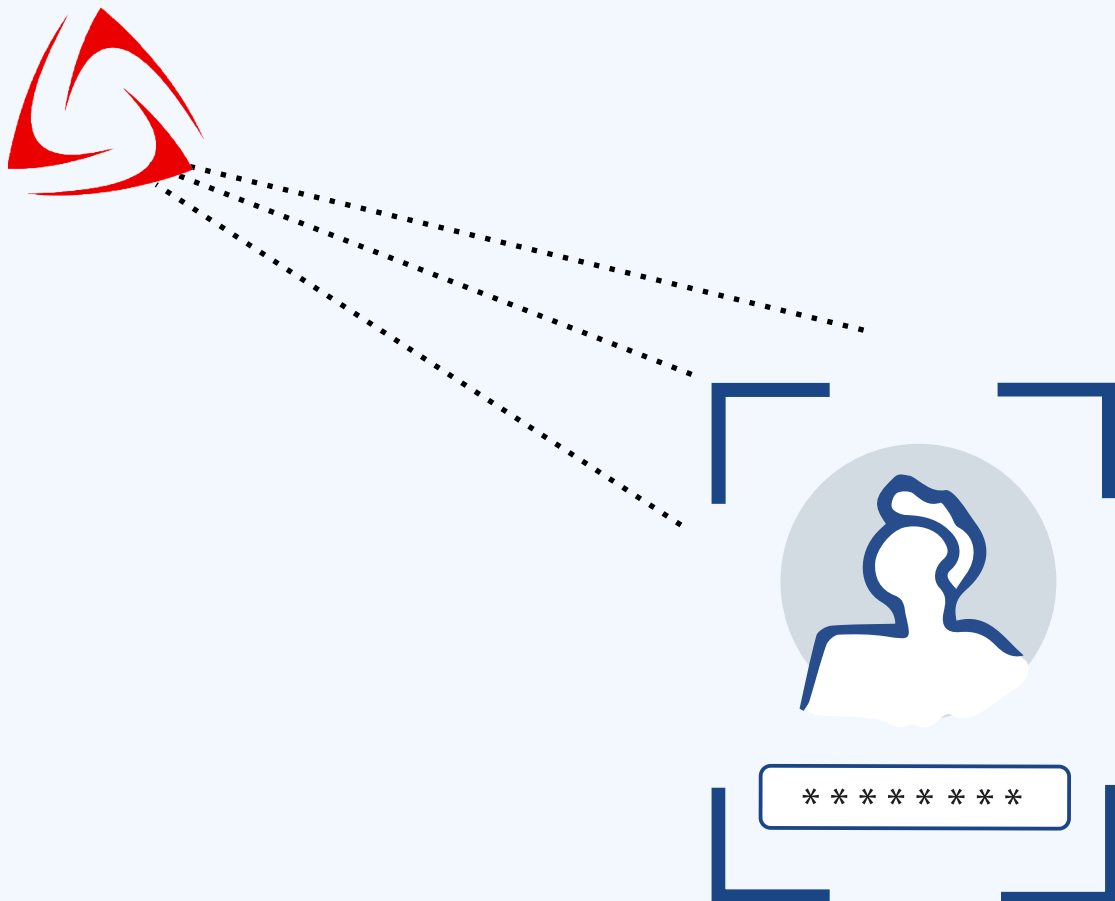
In addition to helping to reduce these financial and productivity costs on a day-to-day basis, SSO also offers IT managers the opportunity to grant or revoke access to multiple applications simultaneously. This can help to improve the efficiency of your company's onboarding processes for new hires, control access for remote employees and contractors, and also increase security when an employee leaves the organization.

What Is SAML?

For SSO to work, the parties involved need to be able to authenticate each other and authorize access. Currently, the two main standards are SAML 2.0 (Security Assertion Markup Language) and OpenID Connect.

Doodle uses SAML 2.0 for authentication and

authorization. The key benefit of SAML 2.0 is that, during sign-in, it stores a user's authentication details as a secure XML signature. This signature can then be passed along between trusted providers, allowing a user access to any apps that accept the credentials without having to sign in again.



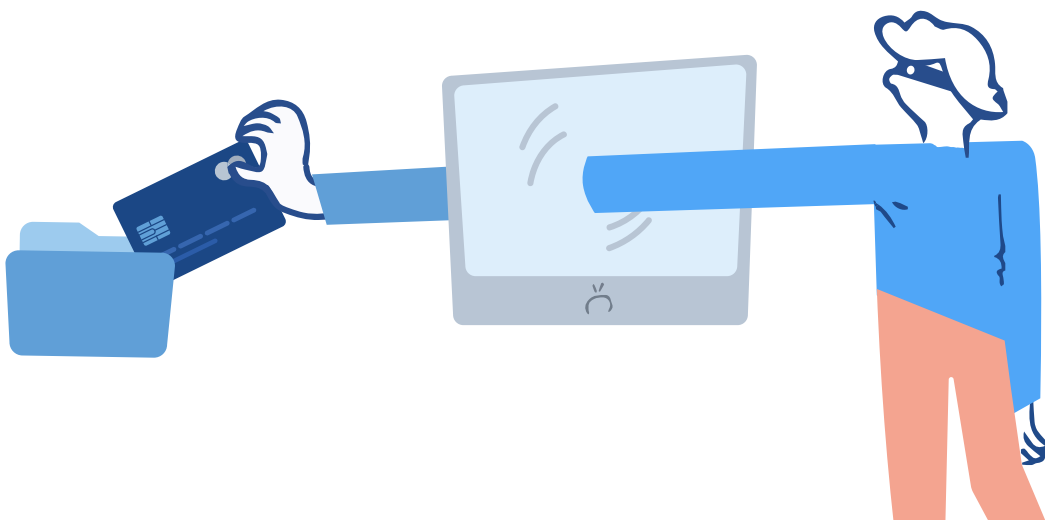
CASE STUDY: **EQUIFAX**

In 2017, Equifax, one of the largest credit monitoring agencies in the world, was hacked by a group that stole the personal information of 147.7 million Americans — more than half of the adult population of the US.

According to a 2018 Government Accountability Office (GAO) [report](#), hackers discovered a known vulnerability in Equifax's online dispute portal, and exploited it in a number of ways, including to discover "unencrypted usernames and passwords that could provide the attackers access to several other Equifax databases. According to Equifax's interim Chief Security Officer, the attackers were able to leverage these credentials to expand their access beyond the 3 databases associated with the online dispute portal, to include an additional 48 unrelated databases."

The hack had severe consequences for both Equifax as a corporation and the employees who had been tasked with Equifax's security. In September 2017, a week after Equifax made the hack public, both its CIO and Chief Security Officer retired. Meanwhile, at least two other senior employees have spent time in jail for insider trading related to the hack: both sold company stock after the hack became known internally, but before it had been announced to the public.

In July 2019, Equifax reached a settlement with the FTC to pay between \$575 million and \$700 million in fines and to provide compensation and free credit monitoring for people affected in the hack. Had Equifax had a robust SSO implementation in place, it may well have been able to avoid the fines, loss of trust and reputation, and other costs it incurred as a direct result of the hack.



How Do Passwords Get Exposed?

There are many ways that hackers can gain access to a password. Here are a few of the most common methods:



Hacking

As seen in the Equifax case, hacking involves an unauthorized user gaining access to one or more registries of user IDs and passwords, typically by exploiting security weaknesses.



Phishing

Phishing scams typically involve a hacker sending an email that directs an unsuspecting user to a convincing, fake login page that has been set up to capture login credentials.



Keystroke Logging

Keystroke logging involves a piece of malware — either downloaded unwittingly by the user or implanted by a third party — that reads the user's keystrokes and stores them for a hacker to access.



Cracking

Many users — particularly for business applications — tend to use predictable passwords. Cracking involves the use of software to rapidly iterate through multiple variations of the most common passwords in an attempt to find a match.

IS SINGLE SIGN-ON RIGHT FOR YOU?

There's no question that SSO eliminates many of the risks and weak spots for organizations with complex tech stacks. The ability to eliminate poor password hygiene as a risk factor greatly reduces exposure to all but the most dedicated, sophisticated hacking attacks. And, by reducing the number of weak spots in the organization's security infrastructure, tech leaders can shift from reactive mode (fixing vulnerabilities as they become exposed) to directing resources towards proactive monitoring and testing of their organization's security.

Recognizing its benefits for security, productivity and convenience, many of the best-known corporate SaaS solutions offer SSO integration as part of their service. As such, integrating SSO into your organization's IT strategy is likely the way to go if you find yourself dealing with any of the following criteria:

- Multiple SAAS applications
- Distributed teams
- Remote employees
- Contractors
- Employees bringing their own devices to work
- Limited help desk capabilities
- A significant volume of password reset requests from employees

Of course, no single solution can ever completely eliminate risk, and it's important to be aware that SSO may not be appropriate in all scenarios. For example, in organizations where many users share or can access the same devices or terminal, there is a higher risk of unauthorized users gaining access to another user's apps and data.



WHAT ELSE SHOULD I KNOW?

While the chances of being hacked are significantly lower with SSO, a successful hack of a single user would give the hacker unlimited access to all of the data stored in any of the apps that the user

had access to. As such, leaders who do opt for SSO as a solution can further reduce their risk by adopting the following protocols:



Educate users throughout the organization on the importance of password and login hygiene



Set time limits for login credentials across the organization — both for individual sessions and the lifetime of an individual password



Set strong permission protocols; users should only have access to the data and apps they regularly use






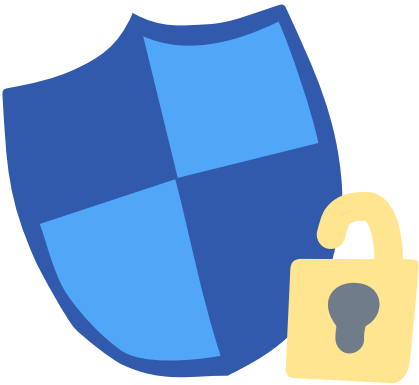
Limit access for vendors and freelance users; regularly review access and employment status for these users



Consider adding a password manager for employees to your stack

COMPARISON

	AWS hosted + ISO 27001 certification	Cloudflare for DDoS Protection	SSO
Doodle	✓	✓	✓
 calendly	✓	✗	✗
 Acuity Scheduling	✗	✗	✗
 you can book me	✗	✗	✗



ABOUT DOODLE

Doodle is the simplest way to schedule meetings with clients, colleagues, or teams. Find the best time for one-to-ones, team meetings, and more with our suite of user-friendly calendar tools.

The world's leader in online scheduling, Doodle is used by over 30 million people every month. Doodle AG is

headquartered in Zurich, and has offices in Belgrade, Berlin, and New York City. Doodle is part of the Swiss media group Tamedia.

Visit www.doodle.com or email sales@doodle.com to learn more about how Doodle can help you take control of scheduling.

Thousands of teams worldwide rely on Doodle everyday



Google

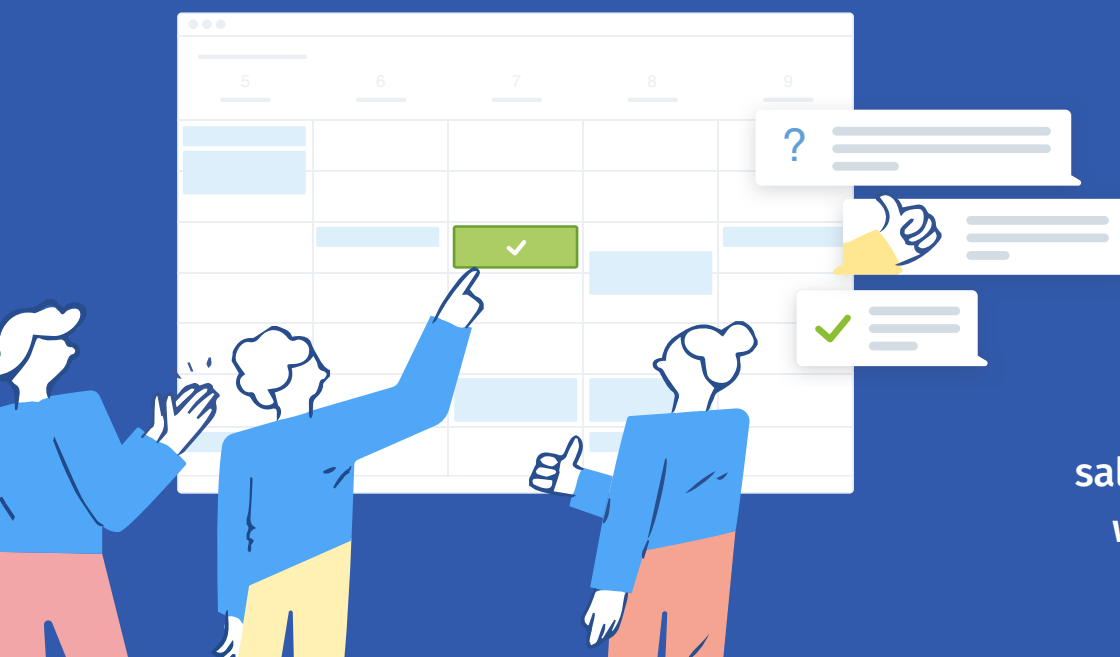


amazon

LinkedIn



Microsoft



sales@doodle.com
www.doodle.com