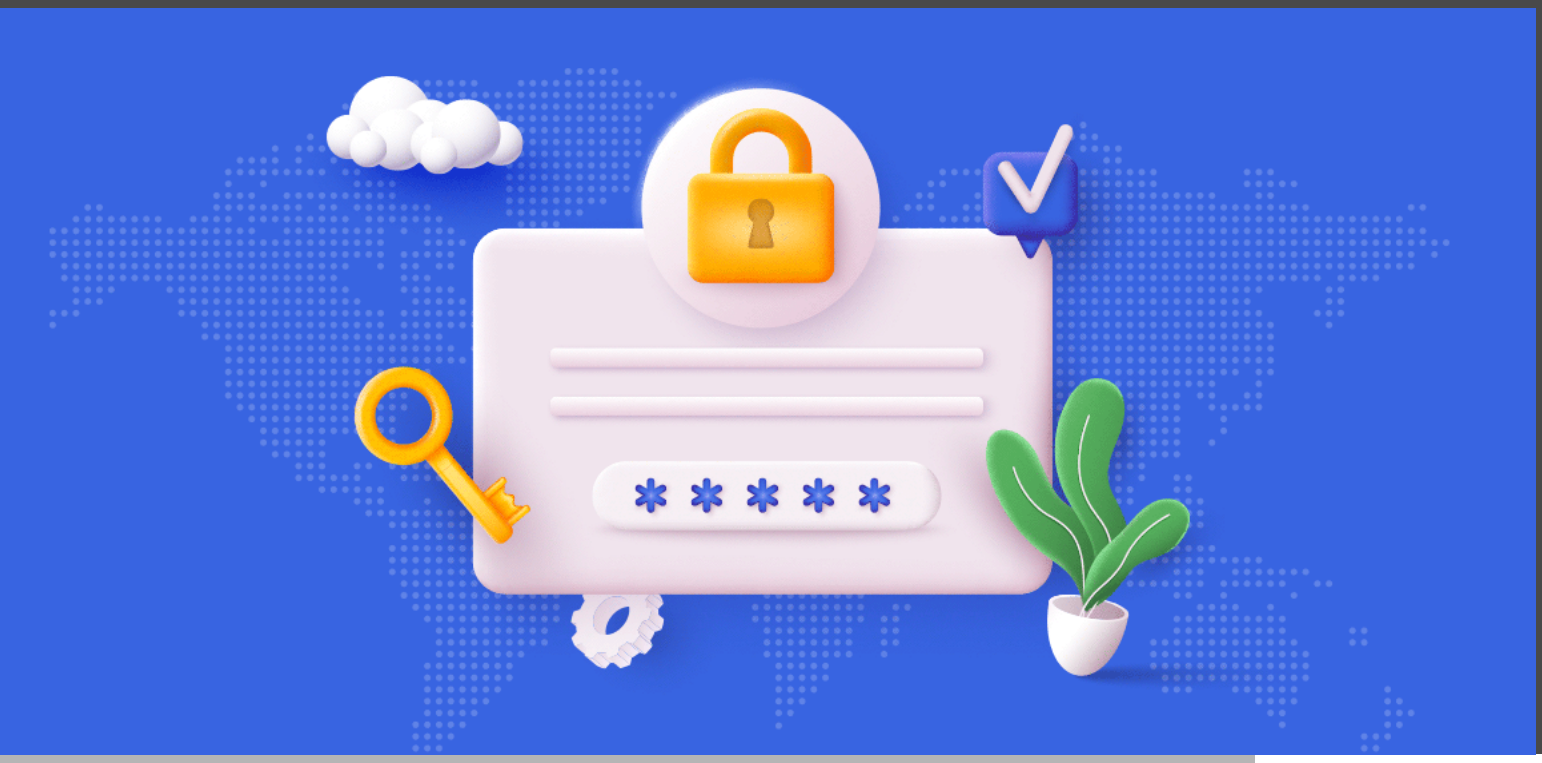
# World Password Day 2022: Things Are Getting Better...and Worse!



## ARE ORGANIZATIONS AND THEIR END USERS GETTING BETTER AT PASSWORD MANAGEMENT, OR ARE THEY GETTING WORSE?

Back in 2005, Security Researcher Mark Burnett wrote a book called Perfect Passwords, in which he advised people to select one day a year to examine and change their passwords. Intel liked the idea of having a special day when people focused on overall password awareness and hygiene (and not just on rotating passwords), and on May 2, 2013 the tech giant launched the inaugural World Password Day. Since then, it has been held on the first Thursday in May.

As we mark the ninth annual World Password Day in 2022, we ask: are organizations and their end users getting better at password management, or are they getting worse? It turns out that the answer is both! Let us start with the positive trends and practices.

## 2FA and Password Managers Are on the Rise

According to Bitwarden's 2022 Password Decisions Survey, **88% of IT decision-makers worldwide are using two-factor authentication** (2FA). Granted, 2FA is not bulletproof. Yet, it is an essential component of good password management. The survey also found that **86% are using password managers, which is a 9% increase from the year before.**

However, while the increasing reliance on password managers is good news, this statistic is not necessarily applicable to all types of organizations. The Devolutions State of Cybersecurity in SMBs in 2021-2022 survey found that **71% of SMBs used a password manager, which was down 10% from the year before.**

What might explain this drop? The most likely reason is that, despite ample evidence to the contrary, some SMBs continue to hold the **mistaken belief that they are not as vulnerable as large organizations and enterprises.** Basically, these SMBs think: "we have not been hacked yet, therefore the methods that we are using to store and share passwords must be safe". This perception is patently wrong, but as the old saying goes: old habits die hard (both good AND bad ones!).

## Password Managers: Cloud vs. On-Premises?

In a moment, we will look at some other troubling password management trends revealed by the survey. But first, let us take a deeper dive into password managers and examine a critical — and for some, complex and confusing — aspect: cloud vs. on-premises.

Basically, this decision should be about an organization's specific password management needs, which vary according to multiple factors such as (but not limited to):

- User location and roles
- Availability requirements
- IT environment size and complexity
- Value of data to protect
- Compliance and security requirements

In some cases, it is wiser to implement hybrid deployments that combine elements of both cloud and on-premises solutions. In addition, a single solution could be deployed multiple times in order to enforce policies such as segregation of duties (SoD).

Regardless of what password management solution an organization chooses — on-premises, cloud, free, or paid — it is critical to clearly define all needs (current and anticipated) before shopping for technology.

## Storing, Selecting and Sharing Passwords Remains a Problem

We mentioned a moment ago that some password management trends are problematic instead of positive. Here are the grizzly details: according to the aforementioned Bitwarden survey, **53% of respondents said that they store passwords in spreadsheets and other documents, 42% rely on their memory, and 29% use pen and paper.**

And the story gets worse: **53% of IT decision-makers are sharing passwords through email, which is 14% higher than last year.** Doubtlessly, the rapid expansion of remote work is behind this trend. Plus, despite numerous high-profile cyberattacks and growing vulnerabilities caused by remote work, **92% of respondents admitted that they re-use the same passwords on multiple accounts, 41% share passwords over chat, and 31% share passwords in conversation.**

## Is Eliminating Passwords the Answer?

In theory, the vulnerabilities associated with passwords could be addressed by eliminating them. Unfortunately, in practice, this — at least for now — is not a viable solution for most organizations (and virtually all SMBs) that cannot practically or affordably implement an entirely passwordless infrastructure. What's more, despite their inherent drawbacks, passwords are highly versatile and can be used on any device, at any time, and from any location.

Since it is impractical to eliminate passwords, the next best option is to close the gap by taking a hybrid approach. Such a hybrid approach **uses an account tied to an Identity Provider (IdP) to authenticate to a Privileged Access Management (PAM) solution.** As a result, end-users only need a single password to connect to accounts for standalone non-federated assets (e.g., printers, network equipment, specialized machines, etc.), while the PAM solution facilitates connection to all other accounts. More advanced PAM solutions also allow organizations to add greater control through functions like secure credential injection, access request requirements, and time-based usage.

## Looking Ahead

A whopping 81% of hacking-related breaches involve stolen or weak passwords, and the average cost of a single data breach has skyrocketed to $4.24 million USD per incident — which is the highest amount ever.

Properly managing, storing, and sharing passwords (which includes monitoring their use) is something that all organizations MUST do to fortify their defenses and minimize their exposure. This World Password Day, we strongly encourage all organizations to make this a top priority. The risks and stakes are higher than ever, and good password management practices are not just important. They are critical.