RESOURCE CENTER

Why Enterprises Need a Password Manager

Enterprises investing in cybersecurity can't afford to ignore password management. Read on to learn why.

Get the full interactive view at https://bitwarden.com/sv-se/resources/why-enterprises-need-a-password-manager/

bitwarden

Introduction

Smart cybersecurity superheroes need the right tools for the job. Building a comprehensive security stack with password management is critical for success. Here are 5 reasons why.

Because stolen passwords have negative impacts

- The average cost of a data breach is $9.24 million, and stolen or compromised credentials are often to blame.
- Data records containing usernames and passwords are often root causes for perpetrating new breaches - two billion such records were compromised in 2021, an increase of 35 percent over 2020.
- Over half of all records breached were a result of unauthorized access where bad actors gained entry to an organization with passwords that were weak, shared, or previously exposed. (Source: Forgerock Identity Breach Report)
- 81 percent of hacking-related breaches succeeded through stolen passwords or weak passwords (Source: Verizon Breach Report)

Because most companies suffer from unauthorized access via weak or stolen passwords

- A Ticketmaster employee hacked into a competitor's accounts with login credentials stolen from a previous employer
- DailyQuiz suffered a breach where attackers stole account information from 8.3 million users, including passwords stored in plaintext, and sold it on the dark web
- A weak password may have allowed the infiltration of cybersecurity firm, SolarWinds, resulting in the hacking of several U.S. government departments
- An attack on Microsoft Exchange email servers, at least partially due to stolen passwords, impacted businesses and government agencies across the U.S.
- Attackers gained access to GoDaddy servers with a compromised password, exposing email addresses and customer details of 1.2 million WordPress users.
- Throughout the pandemic as companies went virtual, Zoom had been the target of cybercriminals who were amassing stolen login credentials and trying to sell them on underground forums.

Because your employees need tools to help them practice better password habits

- In a recent survey of 400 independent IT decision-makers across various industries, Bitwarden found that 92 percent of respondents reuse their passwords across at least 1-5 sites.
- The average person has created dozens of password-protected profiles to access business systems, websites, and smartphone applications.
- It's natural for employees to take shortcuts to minimize frustration and password fatigue, like reusing passwords across business and personal accounts and sharing passwords with coworkers.
- A password manager is a great way to enhance a security culture throughout your organization. Not only is it easy to deploy, it's accessible and easy to use by everyone. This, in turn, empowers employees to be more aware of their online routines

Because password managers are the front lines of defense critical to your overall security stack

"Why do we need a password manager if we have SSO?"

- While Single Sign On (SSO) is a popular way for businesses to centralize access control for critical applications, services, and tools, SSO isn't necessarily enough to protect employee credentials and accounts.
- Not all SaaS applications support SSO, which means organizations still have to manage access control through individual logins.
- A password manager enables secure sharing across teams and functions.
- The only way to ensure all your credentials are secured is to use SSO with a password manager.

"Why do we need a password manager if we have firewalls?"

- Firewalls are critical to network security, often sitting at an organization's network perimeter to prevent external threats, or within the network to guard against internal threats.
- Firewalls inspect internet traffic coming in and out an organization's network and looks for malicious traffic.
- Because a significant portion of data breaches involve issues with password and credential safety, password management is probably the most important network security safeguard.
- Firewalls block malware by filtering data coming in and out of your system.
- Password managers, on the other hand, can be integrated at every level of your architecture, not just at the perimeter.

"Why do we need a password manager if we have email security?"

- Email is a top choice among attackers to launch phishing and ransomware.
- Email security solutions include a blend of techniques to prevent attacks such as URL analysis, source verification and authentication, fraud protection, malware detection in email attachments, and more.
- Email security cannot protect against unauthorized access to an organization's accounts and applications if a cybercriminal has access to login credentials.
- A locked door is useless if a criminal has the key.
- A password manager stores and secures these 'keys' (login credentials) using end-to-end encryption.
- A password manager provides additional phishing protection by retaining known and confirmed URLs. It can show you whether a site visited is stored within the password manager by showing an icon in the browser bar. If an employee accidentally lands on a malicious site, the known login icon would not appear.

Because a password manager is critical to staying safe online

- Widespread use of passwords without the proper tools causes weak password choices, password reuse, and insecure sharing of credentials.
- Within organizations, the needs for centralized and shared resources can be resolved with a password manager.

- Cyberattacks can be minimized or prevented by proper password management use.
- Phishing attacks, for example, can be prevented with a password manager - a phishing scam might trick an employee into clicking on a malicious link, but it can't trick a password manager.
- A password manager is the only way for your employees to secure sensitive information with an end-to-end encrypted vault.
- A password manager makes it easy for employees to generate and store unique passwords for all their work (and personal) accounts.
- A password manager can show your IT security team whether there are weak and reused passwords that could be compromised.
- A cybersecurity strategy that includes password management can minimize organizational risk for data theft, ransomware attacks, and other cyber threats with substantial financial and reputation repercussions.

Password manager market landscape

- Globally, password management is a $1.38 billion business, and with an ever-evolving and expanding cybersecurity risk landscape, it is expected to reach $5.86 billion over the next decade.
- Worldwide, the market experienced a compound annual growth rate (CAGR) of 11.8% from 2016-2020, intensified by increased remote work and personal online activities during pandemic lockdowns.
- With ongoing hybrid work models, a global reliance on website logins across industries, and continued growth of mobile apps and software-as-a-service (SaaS) platforms, the market expects a CAGR of 14.2% through 2031.