IRON DEFENCE

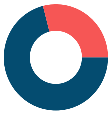
Be Security Vigilant!

ENABLING THE RIGHT PEOPLE WITH THE RIGHT ACCESS TO THE RIGHT RESOURCES

REGARDLESS OF DEVICE OR LOCATION

PASSWORDS FALL SHORT ON SECURITY

With your business becoming increasingly reliant on technology and the internet, the practice of a single level of security, like a password, is no longer enough to protect you from the risks of cyber threats. While passwords are not likely to disappear anytime soon, when it comes to security, they are extremely risky.



70%

Stolen or weak passwords are responsible for 70% of hacking-related breaches.[1]

51%

Nearly 51% of the data breaches in 2019 were caused by malicious attacks.[2]

MOVING BEYOND PASSWORDS

It can be difficult to control and enforce strong and secure password requirements across your organization. Often, users sacrifice security for convenience by using weak passwords or reusing passwords for multiple logins, resulting in increased risk of exposure or theft.

Even strong and complex passwords are not completely secure. Compromised credentials obtained as a result of phishing, keylogging, and third-party data breaches can be used to gain unauthorized access to your business.

YOU NEED IDENTITY AND ACCESS MANAGEMENT (IAM)

Enforcing user identity verification and blocking unauthorized access to your systems has become elemental to cybersecurity. But, how do you ensure the security of your business and critical data without compromising the convenience or flexibility of your workforce?

The right IAM solution will combine and integrate multiple security tools and systems into a single platform, enabling you to take control of your identity and access challenges, with minimal hassle to your business and your users.

[1] Verizon Data Breach Investigations Report 2019

[2] Passwordless Authentication: Bridging the Gap Between High-Security and Low-Friction Identity Management, IBM

COMPREHENSIVE SECURITY WITHOUT COMPROMISING CONVENIENCE, FLEXIBILITY OR PRODUCTIVITY

TWO-FACTOR OR MULTI-FACTOR AUTHENTICATION

Reinforce security by forcing users to validate their identity and access permissions with two or more unique factors and reduce or eliminate the risks related to exposed or stolen passwords.

Common authentication factors:

1. Something you know (e.g., password, PIN or security questions)
2. Something you have (e.g., mobile phone, USB device or email address)

SINGLE SIGN-ON

“Did you know the average employee logs into 10 applications each day?”

Single sign-on (SSO) functionality enables users to securely access multiple websites, applications, and cloud services they need for the day with a single login using just one set of credentials. SSO helps maintain strong password procedures while reducing password fatigue and virtually eliminating excessive tech support calls for password resets.

PASSWORD SERVER

Password Server helps store, organize, and manage the passwords your users have for accessing their accounts on different websites, applications, and cloud services. All your user passwords are securely stored in an encrypted format and can be securely accessed with a single master password.

With Password Server deployed, you can implement, enforce, and audit stricter password policies, such as requiring longer and more complex passwords and the prevention of reused or recycled passwords. You can streamline and automate all credential-related tasks, making security a priority.

CONTACT US TODAY TO ESTABLISH AN IDENTITY AND ACCESS MANAGEMENT PROGRAM FOR YOUR BUSINESS.

IRON DEFENCE™
Be Security Vigilant!