



# TRUSTING PASSWORDS

## BEST PRACTICES FOR THREAT-PROOFING CREDENTIALS

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) eBook

Written by Steve Brasen

May 2020

Sponsored by:

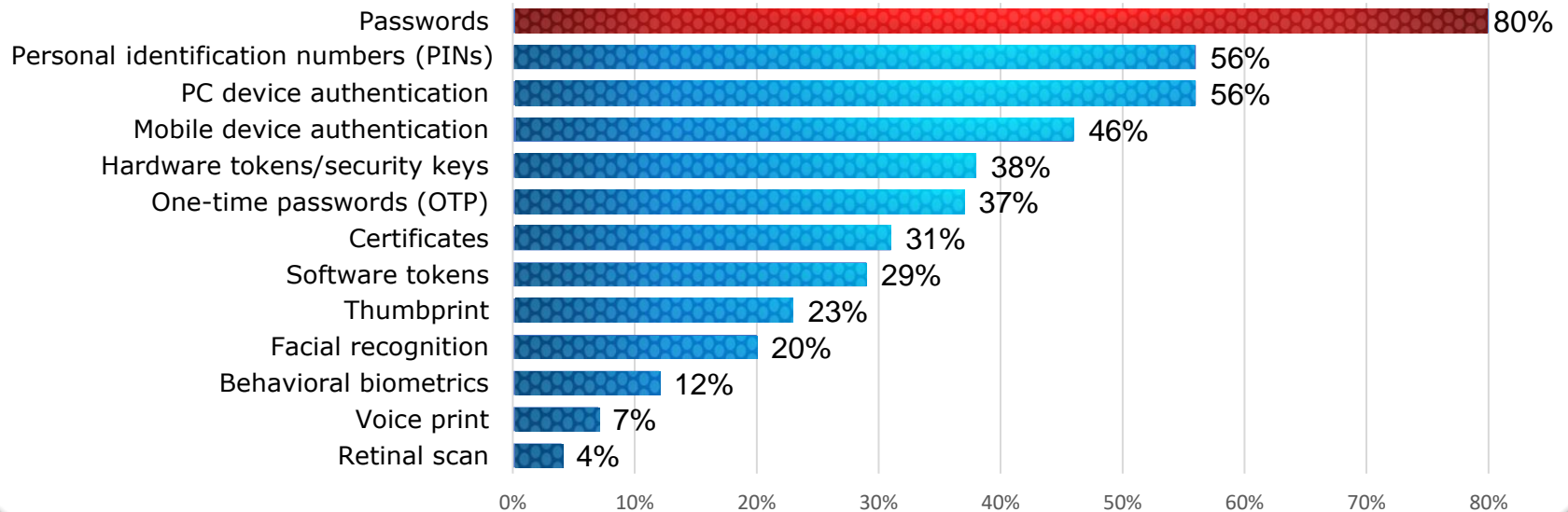
ENZ  IC



IT & DATA MANAGEMENT RESEARCH  
INDUSTRY ANALYSIS • CONSULTING

# Password Reliance

[According to EMA primary research](#), passwords continue to be employed as the dominant method of authentication for accessing business IT resources, including applications, data, and other IT services. Building on a legacy that dates back to the early days of computing, passwords are ubiquitous across all types and sizes of organizations and are a key instrument for empowering workforces with responsible access to the information and resources they need to drive business success. Today, there is a wide-variety of alternative types of authenticators available. However, these are principally adopted to supplement, rather than completely replace, password-based access controls. Even though technologies, such as single sign-on (SSO) and password vaulting, have been broadly adopted to simplify authentication processes, they are still reliant on basic passwords as the principle method of identifying users.



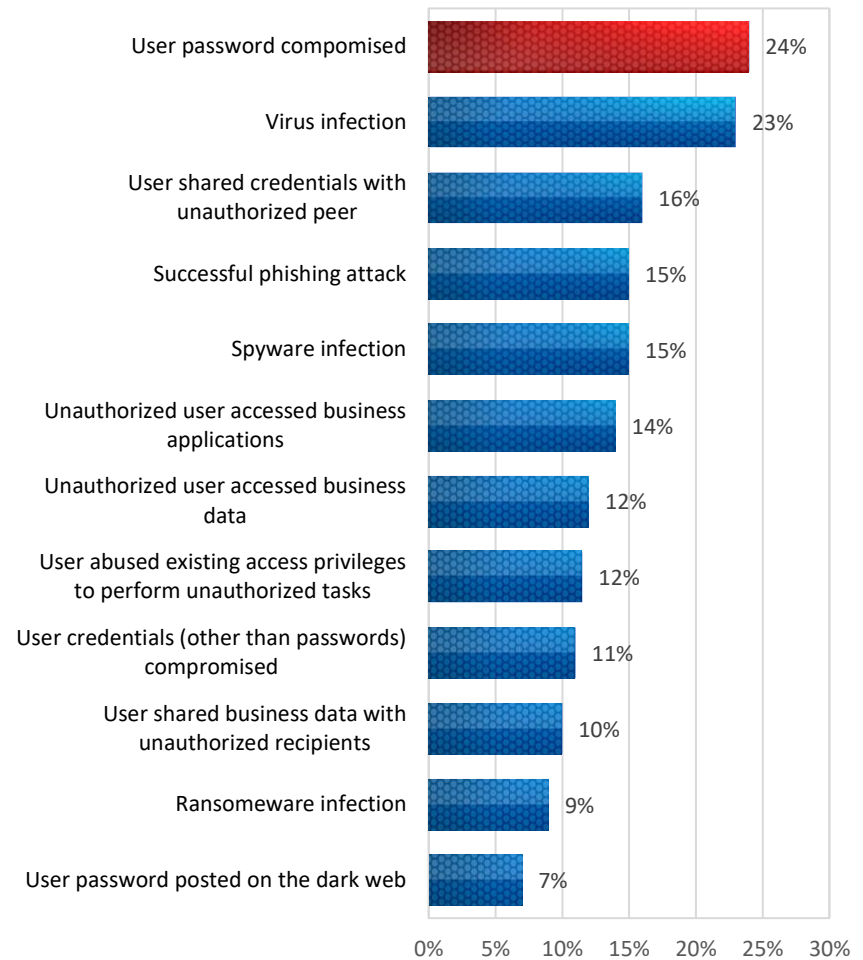
**Percentage of EMA survey respondents indicating types of authenticators commonly used in their organization to enable access to business devices, applications, and data**

# The Weakest Link in Enterprise Security

More than 60% of organizations experience a security breach each year, according to [EMA research results](#). Roughly one quarter of survey respondents indicated that a password in their organization had been compromised in the preceding 12 months.

Reported incidents of password violations only represent breach incidents that have actually been detected. The high rate of other security infractions strongly suggests a much higher rate of undetected password failures resulting in business-impacting attacks, including malware infections, unauthorized data access, and a misuse of IT investments. In order to truly enable security effectiveness, organizations must introduce solutions that protect against both known and unknown attack vectors.

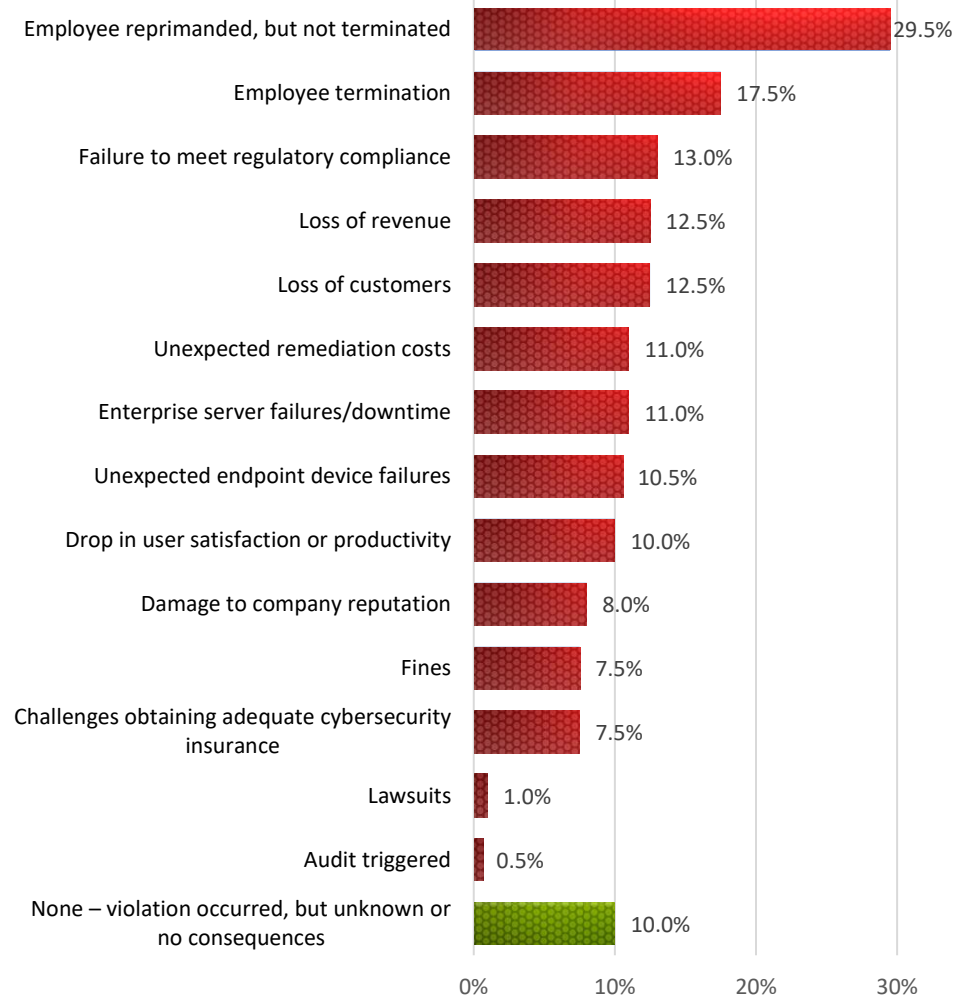
Traditional methods of password management are the weakest link in enterprise security because they fail to ensure credentials currently in use have not been compromised.



Percentage of survey respondents indicating security breaches that have occurred in their organization in the preceding year



# The Consequences of Security Breaches



**Percentage of survey respondents indicating security breaches that have occurred in their organization in the preceding year**

[EMA survey results](#) confirm that 90% of organizations that have experienced a security breach suffered significant business consequences as a result.

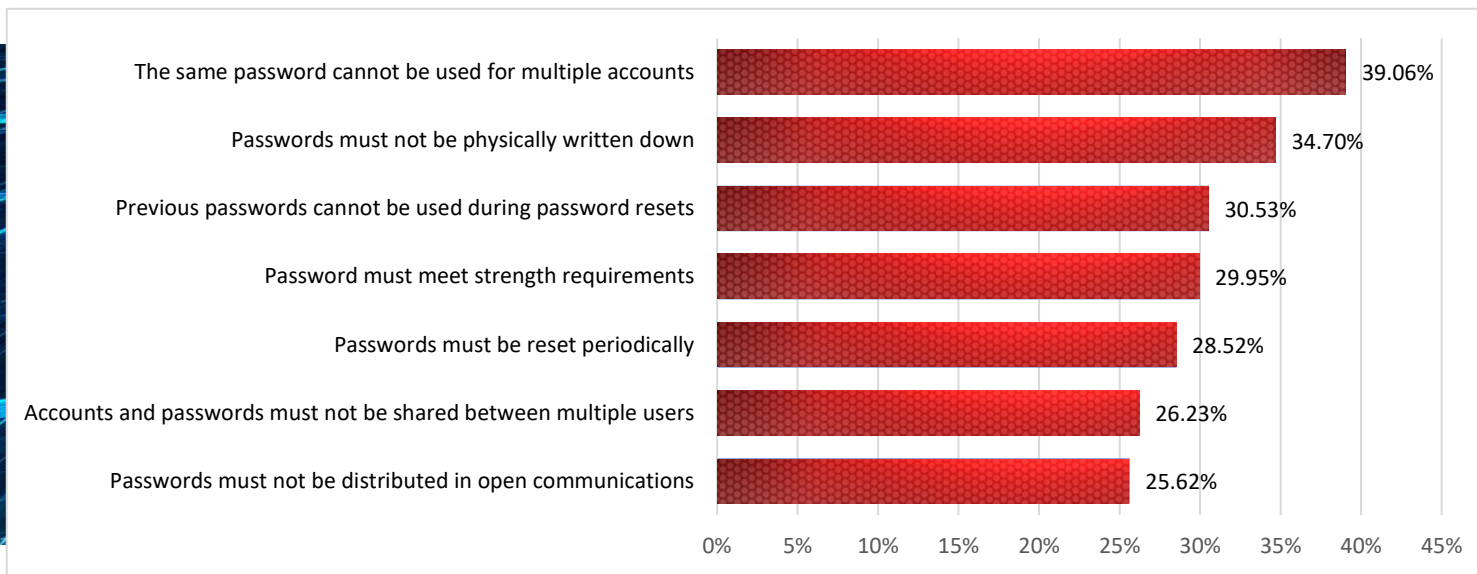
Breach incidents resulting in severe business consequences (including “failure to meet regulatory compliance,” “loss of revenue,” “loss of customers,” and “damage to company reputations” were collectively reported by 31% of survey respondents. This indicates a one in three chance of severe financial impacts to the business when a breach occurs that could have dire ramifications for business performance and continuance.

The most common cause of security breaches is the inability to enforce proper password management practices. In fact, [EMA has determined](#) that more than 90% of organizations experience significant password policy violations each year.

## 3 | Trusting Passwords: Best Practices for Threat-Proofing Credentials

# Password Policy Violations

Password policy violations most frequently occur when users bypass established policies in order to access business IT services more quickly with little regard to enterprise security. Weak password enforcement controls expose organizations to a whole host of opportunities for exploitation by nefarious actors.



Brute force attacks can be used to systematically identify password strings, keystroke logging can capture the moment when users enter their passwords, and phishing schemes can trick users into sharing their passwords.

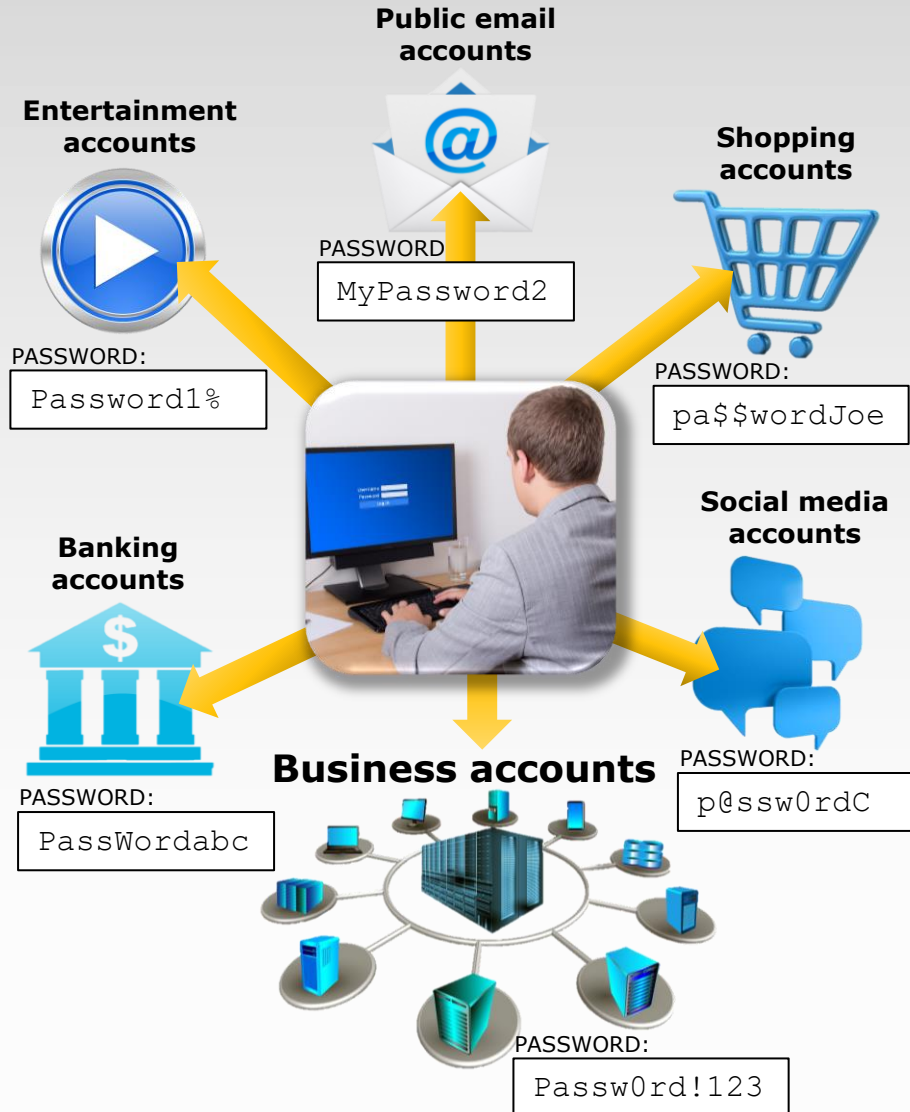
# Password Reuse is the Greatest Challenge

The use of identical passwords to support multiple accounts is the password policy violation most frequently experienced by organizations. It's an unfortunate fact that human brains are not proficient at memorizing multiple, constantly-changing, and complex strings of characters. People often compensate for this deficiency by utilizing the same or similar passwords for multiple accounts.

Password reuse is particularly difficult because it is impossible to prevent using traditional password management processes. Even the most stringently secure environment can only enforce unique passwords on the IT services and systems that are part of their support stacks. Passwords created for non-business-related services—such as a user's social media or public email accounts—are not protected by enterprise password management systems. When these public resources are breached, captured passwords are sold and distributed across the dark web, which can then be used to attack business resources that support common users.



# Traditional Password Practices Are Not Secure



Traditional password security approaches rely on algorithmic complexity, requiring a mixture of characters in the password string (e.g., uppercase letters, lowercase letters, numbers, and symbols) and enforcing periodic password changes. However, complex strings of characters that are frequently changed are very difficult for users to memorize and recall.

To make passwords easier to remember, users typically generate passwords that are easy to crack. Users often employ common words and predictably replace letters with numbers or symbols in order to meet minimum password strength requirements (for example "Passw0rd!"). Cracking tools utilized by hackers quickly and easily check for obvious character substitutions across a library of common words and known passwords that have been exposed in past data breaches.

It is also often common for users to employ a common root word for multiple passwords. The root word is appended with additional characters to make it appear slightly different in multiple accounts or during password resets. While this approach meets commonly adopted requirements for password uniqueness, they are easily broken by today's more sophisticated attack methods.



# NIST Password Guidelines

[Digital Identity Guidelines](#) published by the National Institute of Standards and Technology (NIST) recommend eliminating requirements for algorithmic complexity and periodic password changes. Instead, NIST recommends systematic credential verification checks to ensure passwords have not been compromised or are easy to guess.

## Section 5.1.1.2: Memorized Secret Verifiers

When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list MAY include, but is not limited to:

- Passwords obtained from previous breach corpuses.
- Dictionary words.
- Repetitive or sequential characters (e.g., 'aaaaaa', '1234abcd').
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

# NIST



Additionally, NIST recommends users only be required to reset passwords in the event that credentials have been detected as compromised.



# Establishing Password Trust

The key to establishing effective passwords is enabling the real-time detection of unsecure credentials. When a user initially selects a password string, it should be evaluated to ensure it does not appear in common cracking dictionaries or otherwise includes common root words and predictable character substitutions. The use of “fuzzy password matching” will most effectively identify passwords that may be similar to previously used or compromised credentials.

Dark web websites that publish and sell captured credentials must be frequently and continuously monitored to rapidly identify any compromised passwords currently in use or prevent them from being created. Upon detection of a compromised credential, alerts should be sent to IT managers and breached user accounts should be disabled until they can be reset to a trusted password. In this way, users are only required to reset passwords when a breach has been detected.

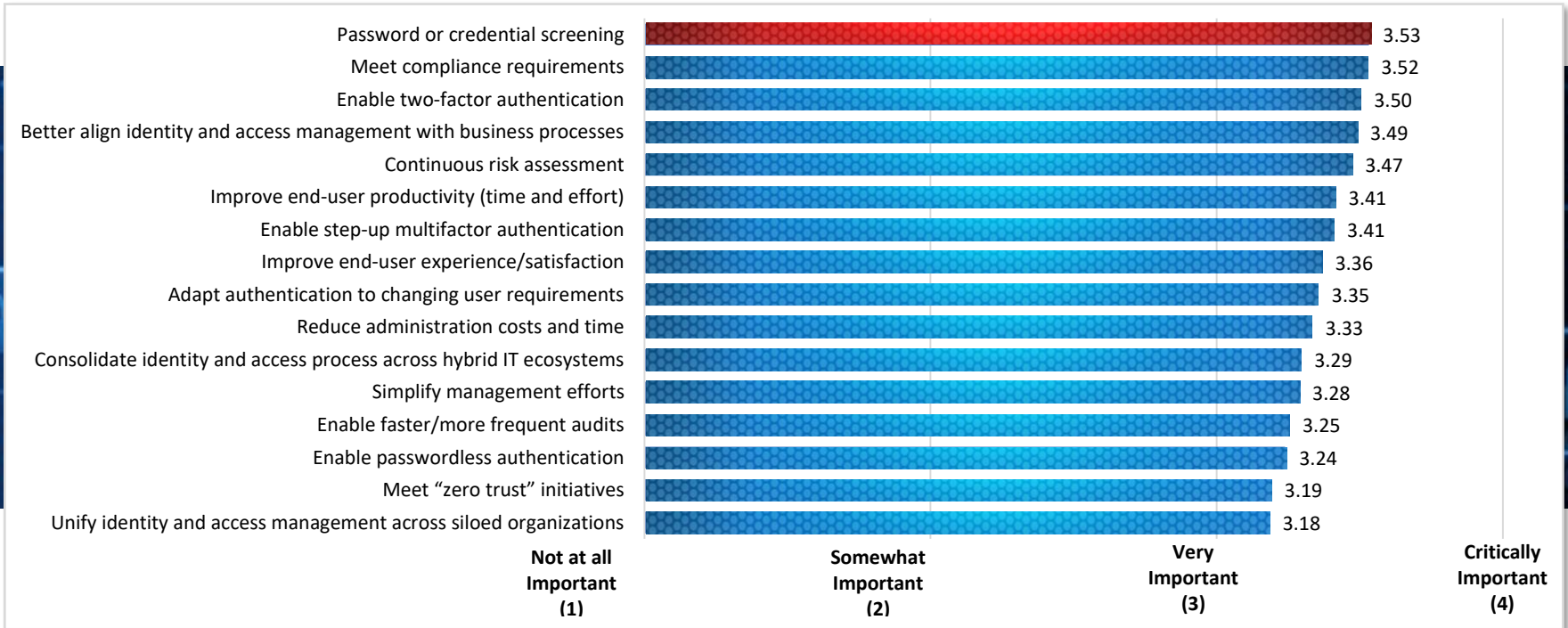
PASSWORD:

\* \* \* \* \*

ALERT:  
PASSWORD INSECURE

# Selecting a Password Management Platform

According to [EMA survey](#) respondents who are responsible for purchasing identity and access management solutions, the most important platform feature today is the ability to perform credential screening. In total, 90% of respondents indicated related capabilities are very or critically important to their business operations.



**Average responses of surveyed IAM purchasers indicating level of importance of specific features and capabilities**

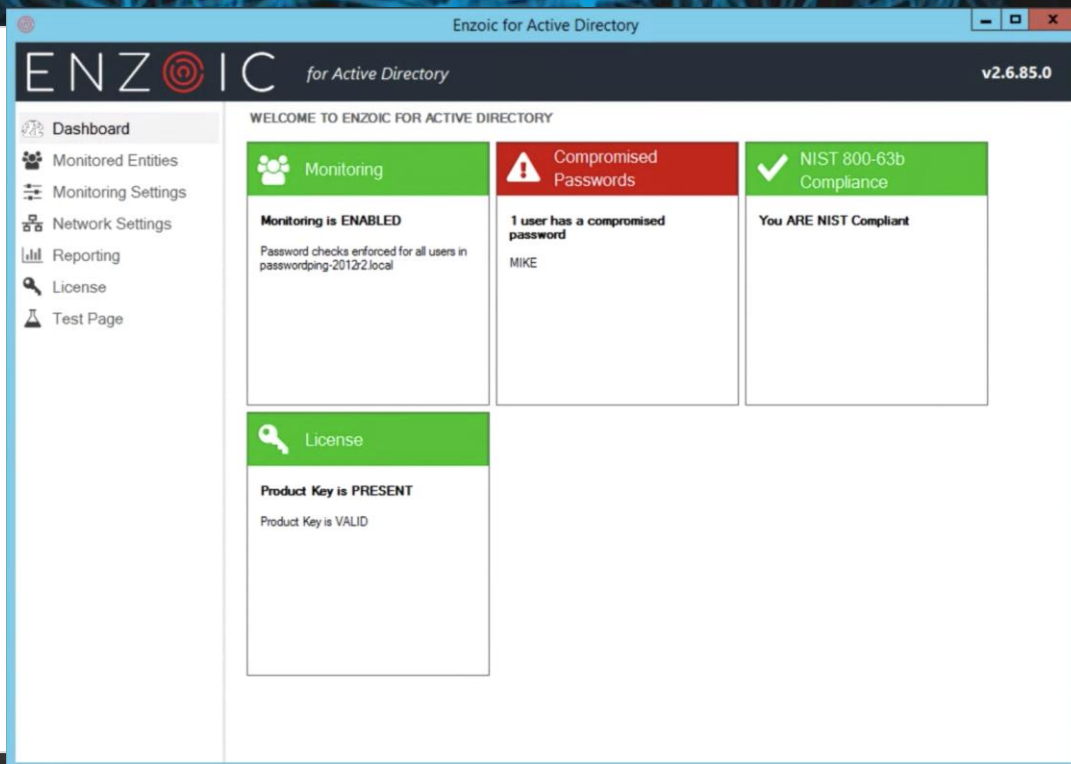
Unfortunately, most password management solutions on the market today lack the ability to effectively identify compromised passwords. For instance, while many organizations have adopted Microsoft Azure Active Directory to manage passwords, the solution was never designed to natively detect if passwords have been posted on the dark web and, instead, relies on a password validation algorithm and a vendor-maintained list of banned passwords.

## 9 | Trusting Passwords: Best Practices for Threat-Proofing Credentials

# Effective Password Protection with Enzoic

Enzoic for Active Directory was purpose-built to provide continuous credential protection by enforcing policies that ensure real-time blocking of unsafe credentials. The platform is installed as a plug-in to Microsoft Active Directory on each domain controller, either manually or via group policies (GPOs).

Passwords are checked for vulnerabilities at the time they are created and every day after to determine whether they have been compromised. Enzoic's database of compromised passwords is updated several times each day to ensure every password is continuously assessed against the most current security information and dark web posting.



The screenshot displays the Enzoic for Active Directory dashboard. The interface includes a navigation menu on the left with options: Dashboard, Monitored Entities, Monitoring Settings, Network Settings, Reporting, License, and Test Page. The main content area is titled 'WELCOME TO ENZOIC FOR ACTIVE DIRECTORY' and features three primary status cards: 'Monitoring' (green) indicating 'Monitoring is ENABLED' with a note that checks are enforced for all users in 'passwordping-20122.local'; 'Compromised Passwords' (red) showing '1 user has a compromised password' with the name 'MIKE'; and 'NIST 800-63b Compliance' (green) stating 'You ARE NIST Compliant'. A 'License' card (green) at the bottom confirms 'Product Key is PRESENT' and 'Product Key is VALID'. The top right corner of the window shows the version 'v2.6.85.0'.

**Enzoic for Active Directory meets all the password requirements established in NIST's Digital Identity Guidelines.**



# Key Conclusions

Traditional methods of password management reliant on algorithmic complexity are no longer sustainable.

An inability to ensure passwords have not been compromised is a primary cause of security breach events and may result in significant impacts to business performance.

Addressing modern challenges to credential security requires the adoption on solutions that accurately and continuously evaluate the effectiveness of passwords.

EMA recommends all organizations reliant of password-based access controls adopt a responsible password evaluation solution, such as Enzoic for Active Directory, to establish confidence in the security of their IT environments.

Username or email

●●●●●●●●

login





Enzoic is a cybersecurity company committed to protecting accounts in Active Directory through compromised password detection. Organizations use the Enzoic for Active Directory tool to automate password policy enforcement & to comply with NIST password guidelines. The plugin also includes continuous exposed password monitoring, which detects if a password is compromised when it is created and on a daily basis thereafter.

**For more information on Enzoic for Active Directory and optimal solutions for password protection, go to:**

**[www.enzoic.com/active-directory](http://www.enzoic.com/active-directory)**

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at [www.enterprisemanagement.com](http://www.enterprisemanagement.com) or [blogs.enterprisemanagement.com](http://blogs.enterprisemanagement.com). You can also follow EMA on Twitter, Facebook or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2020 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

### Corporate Headquarters:

1995 North 57th Court, Suite 120  
Boulder, CO 80301  
Phone: +1 303.543.9500  
[www.enterprisemanagement.com](http://www.enterprisemanagement.com)  
3974.05042020

