Responsible Password Protection

Securing Credentials Hosted in Active Directory

AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) WHITE PAPER
PREPARED FOR ENZOIC
BY STEVE BRASEN
SEPTEMBER 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

EVOLVING REQUIREMENTS FOR PASSWORD PROTECTION

There is a certain irony in the fact that passwords are commonly relied on as the first line of defense for protecting enterprise applications, data, and IT services, yet they are also broadly recognized as the weakest link in enterprise security. Concerns about the effectiveness of password-based controls are not unwarranted. Hackers are increasingly inventing new and nefarious methods of breaking passwords, such as by employing a cracking dictionary, brute-force attacks, keystroke logging, and phishing schemes. Once acquired, passwords are sold or distributed across the dark web to bad actors who are prepared to use them to perform criminal and vandalistic activities. With attack vectors around password exploitation rapidly increasing, it is no wonder one out of every four American citizens was a victim of a cybercrime in 2018.[1]

At the heart of the problem is the fact that end users commonly employ very poor practices when it comes to password security. According to EMA primary research, 90% of organizations support users who utilize the same password for multiple accounts.[2] The same research findings also concluded that 40% of organizations do not place any restrictions on the passwords selected by users, and 93% of organizations are not confident that their existing security controls are able to detect and prevent compromised user credentials. It also doesn't help that, while one-third of all businesses rely on Active Directory as their primary repository for passwords, most fail to monitor Active Directory vulnerabilities to adequately prevent threats.

[1] https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx
[2] https://www.enterprisemanagement.com/research/asset.php/3576/Pragmatic-Identity-and-Access-Management

BEST PRACTICES FOR PREVENTING PASSWORD VULNERABILITIES

A responsible approach to password security establishes and enforces reasonable guidelines to ensure passwords are not compromised or easily guessable. Key controls should be introduced at the time end users create passwords. 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 words or predictable character strings. Hackers are certainly aware that users often rely on names and words that are easy to remember, often appending them with a simple number. Brute-force attacks can rapidly break these passwords, breaching an organization's primary access controls. By proactively reviewing passwords at the time they are created, organizations can immediately prompt users to adopt unguessable password strings that will better protect enterprise IT investments.

A responsible approach to password security establishes and enforces reasonable guidelines to ensure passwords are not compromised or easily guessable.

It is also essential to continuously monitor credentials to ensure they have not been compromised and are available on the dark web. Ideally, this compromise screening will also occur at the time a password is created so nefarious actors never have an opportunity to exploit the compromised information. Dark web monitoring of established passwords should also be continuously and indefinitely performed to ensure credentials do not become unexpectedly compromised. On detection of a compromised password, alerts should be sent to IT managers and/or breached accounts should be disabled until they can be reset by properly authenticated users. This will help organizations achieve continuous compliance with access policies while also establishing confidence in adopted security controls.

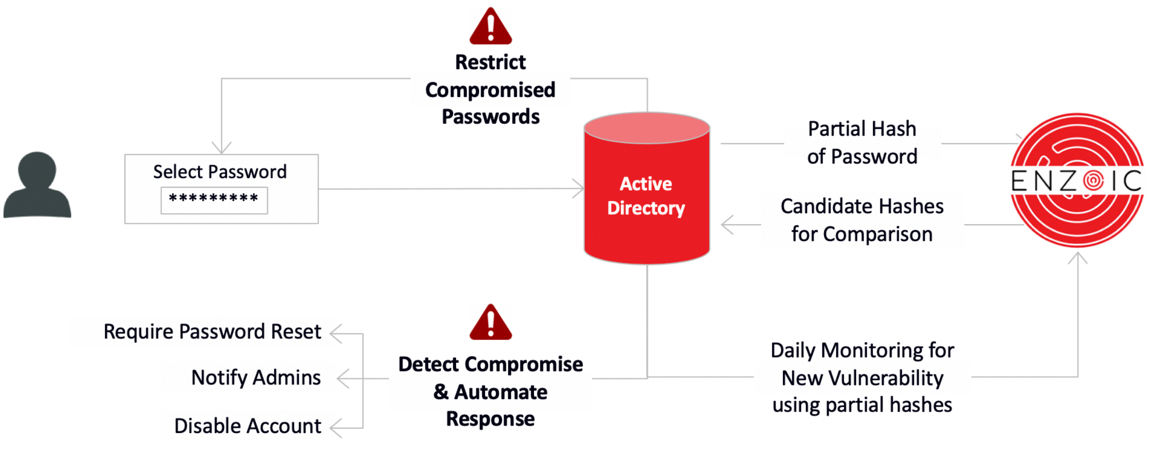
As an additional benefit, the reliable detection of compromised passwords eliminates the need to force periodic password resets. This value derives from the logic that if that if there is certainty a credential has not been compromised, there is no need to change it. This can have a dramatic effect on reducing end-user efforts, boosting their productivity and overall work experiences. When users do not have to "jump through hoops" to access business resources—such as by having to perform periodic and cumbersome password resets—they are much more likely to use approved access controls, rather than bypassing security by utilizing risky public services (such as public email and data sharing systems). In fact, EMA primary research determined that reducing end-user access efforts directly increases overall security effectiveness.

ENABLING RESPONSIBLE PASSWORD SECURITY

Evaluating credential viability during password creation and consistently confirming password effectiveness with systematic reviews is only sustainable with the use of automated credential monitoring and management resources. Adopted technologies should adapt to support existing credential policies in order to proactively prevent the use of poor or compromised passwords. Solutions should also have the flexibility to adjust to changing requirements in real time. For instance, as new threats are discovered and new cracking dictionaries are published, the credential evaluation solutions should automatically update to ensure credentials are promptly checked to confirm they have not been compromised. Any delay in updating the platform could expose the business to risks during any time period when the solution is out of date.

As an example of a responsible password security solution, Enzoic for Active Directory was purpose-built to provide continuous credential protection while minimizing end-user and administration efforts. Enzoic's proprietary research is powered by a combination of human and automated intelligence. Their database is updated several times each day to ensure every password is continuously assessed against the most current security information. The platform is installed as a plug-in to Microsoft Active Directory on each domain controller, either manually or via GPO policies. Alternatively, Azure Active Directory deployments may be supported in a hybrid mode. The platform is managed from an easy-to-use, centralized console application that enables organizations to integrate existing and newly implemented policies. Enzoic for Active Directory was designed to provide continuous password protections by enforcing enhanced policies to ensure real-time blocking of unsafe credentials. Passwords are checked for vulnerabilities at the time they are created and every day after to determine whether they have been compromised. To ensure the checks themselves cannot be breached, only partial hashes are evaluated, guaranteeing exact passwords or even complete hashes of passwords, never leave the protected environment. The effective password controls offered by Enzoic for Active Directory meet all the requirements established in NIST's digital identity guidelines (NIST 800-63).

> Enzoic for Active Directory was designed to provide continuous password protections by enforcing enhanced policies to ensure real-time blocking of unsafe credentials.


Restrict Compromised Passwords
Select Password
****
Active Directory
Partial Hash of Password
Candidate Hashes for Comparison
ENZOIC
Require Password Reset
Notify Admins
Disable Account
Detect Compromise & Automate Response
Daily Monitoring for New Vulnerability using partial hashes

Enzoic for Active Directory Architectural Diagram

EMA PERSPECTIVE

The most dangerous security threats are the ones that are completely invisible to the business. Known threats can be prevented or mitigated, but unknown threats are only resolved after a security breach has occurred. This is why the most valuable tool for achieving security assuredness is enabling the rapid identification of vulnerabilities so that proactive measures can be taken to eliminate risks. However, any vulnerability detection solution is only effective if it is performed continuously. Infrequent security reviews (i.e., performed monthly or quarterly) leave the business vulnerable during the stretches of time between audits.

Enabling consistent visibility is particularly essential in support of identity management processes since these provide the first line of defense in the protection of enterprise IT investments and intellectual property. Ensuring the strength of identity controls requires continuous assurance of the safeguarding of user credentials from the time of their creation through their final deactivation. EMA recommends all organizations reliant on password-based access controls adopt a responsible credential evaluation solution, such as Enzoic for Active Directory, to certify sustained confidence in the security of their IT environments.

ABOUT ENZOIC

Enzoic is an enterprise-focused cybersecurity company committed to preventing account takeover and fraud through compromised credential detection. Organizations can use Enzoic solutions to screen customer and employee accounts for exposed username and password combinations to identity accounts at risk and mitigate unauthorized access. Enzoic is a profitable, privately held company in Colorado. For more information on Enzoic for Active Directory, go to https://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 or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3888.092019