Channel Futures™
Leading **Channel Partners** Forward

TOP TIPS

6 Ways to Keep Authentication Secure

Keeping organizational data secure has become a major concern for IT departments of all sizes. Hackers are constantly working to find ways to compromise corporate data, and regulators are levying huge fines for organizations that don't keep IT security up to acceptable standards.

Securing the password layer is a cost-effective way to achieve far better security for your organization's data. Passwords are already in use in your environment, and you can secure them with a few simple tips.

Longer is Better

Requiring users to use longer passwords provides better protection against brute force attacks where hackers just try to guess the password over and over until they find one that works. Train users to think in terms of a 'passphrase' rather than a 'password'.

A good passphrase can be comprised of several unrelated words. Combining four words that can easily be remembered (horse, lawn, golf, tent) with a pattern of capital letters and special characters can create a very secure password that is easy to remember.

No Expiration

Research shows that when users are forced to change passwords too frequently, they often make incremental changes or follow other pattrerns easily guessed by hackers. In many situations (but not all, more on that later) forcing users to change their passwords will decrease your organization's overall security, not improve it. Also, eliminating expiration does require a method to detect when a good password becomes compromised.

Use Blacklists

The top password recommendation from the National Institute of Standards and Technology is not to use previously compromised passwords Users aren't security experts, and they cannot always be expected to know when a password is still OK to use. Employing a password blacklist is strongly recommended.

A blacklist is a list that contains values known to be commonly used or passwords that have previously been found to have been breached. Preventing users from choosing common or compromised passwords adds an invaluable layer of security to your environment.

Enable Lockout

One of the easiest and most effective methods in preventing brute-force hacking is employing a password lockout policy.

In this technique, the system locks the user out of their account after too many incorrect login attempts. The user is then prevented from logging in for a pre-set period, or until the system administrator unlocks the account. Since brute force attacks rely on high-volume guessing of commonly used words, a lockout policy efficiently thwarts this type of attack.

Sponsored by

ENZOIC

Continuous Monitoring

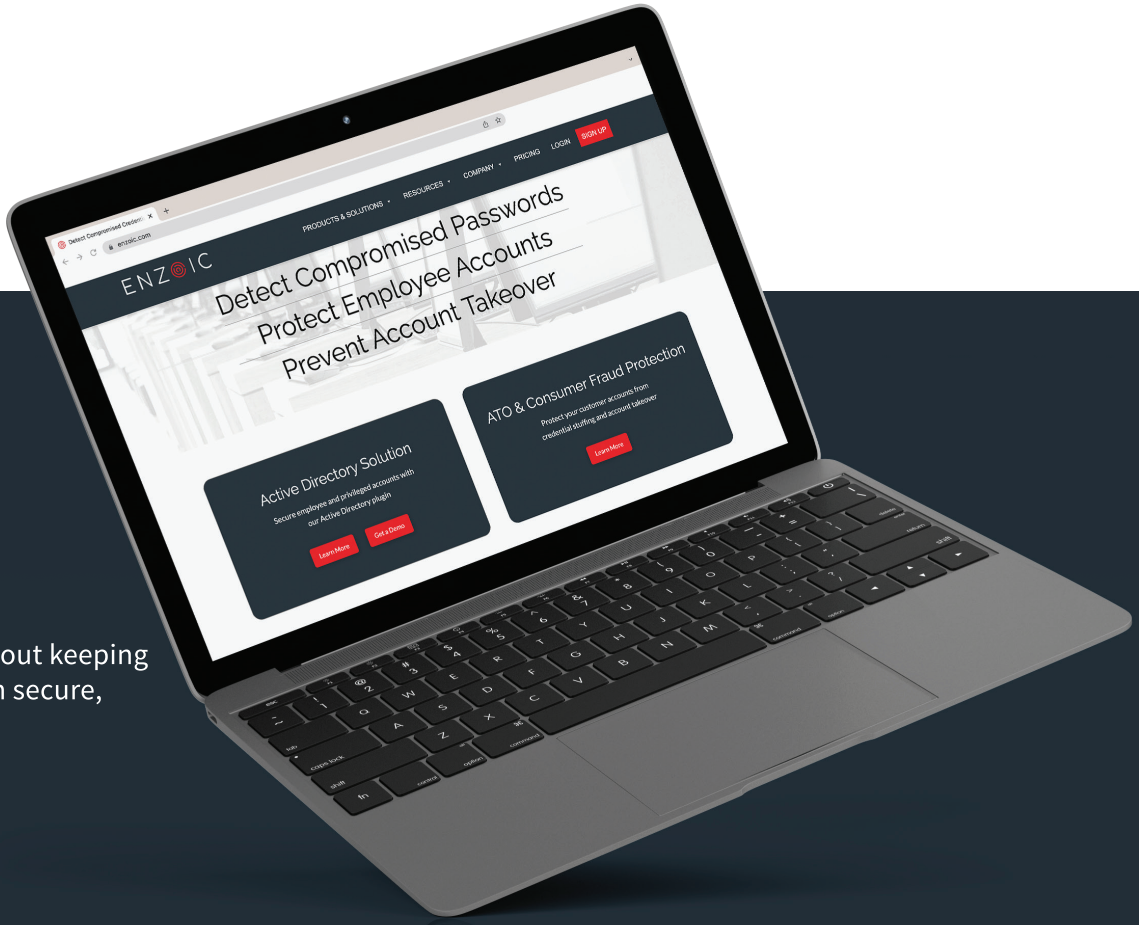
While security researchers recommend against forcing users to change passwords at frequent intervals, there are times when forcing a user to change their password is essential. For example, when a previously good password becomes compromised and would no longer pass the blacklist rule above.

Employing a password monitoring service can warn administrators when account and password pairs are found for sale. A good password monitoring system can even use that data to force a password reset when a specific user's account is found to be compromised, or they are currently using a password found in a database of breached passwords.

Add Layers

No single layer of authentication is enough to keep accounts secure anymore. When a there is just one layer standing between the bad guys and your organization's data, a security breach is bound to happen.

Multifactor authentication is a must, but not all multifactor authentication is the same. Using an authenticator app, or a hardware token with a rotating code is much more secure than a system that sends text messages or phone calls.



Detect Compromised Passwords
Protect Employee Accounts
Prevent Account Takeover

Active Directory Solution

Secure employee and privileged accounts with our Active Directory plugin

ATO & Consumer Fraud Protection

Protect your customer accounts from credential stuffing and account takeover

Find Out More

For more information about keeping password authentication secure, visit **www.enzoic.com**.

LEARN MORE

Sponsored by

ENZOIC