ENZOIC

QUESTIONS FOR EVALUATING PASSWORD MONITORING VENDORS

Organizations using Active Directory must update their password policies to block and detect compromised passwords but comparing vendors in this area can be challenging.

By asking the right questions, you can pick the right partner and avoid introducing new technical, security and compliance risks for your organization.

This document provides twenty questions to help find the right provider of password filtering and auditing tools for hardening domain passwords.

ADMINISTRATIVE OVERHEAD

1 Does the tool deploy a “Password Filter” object on the domain controller?	There are several ways to implement password screening. The Password Filter is how Microsoft supports password policy and change notification. It is the only method that works regardless of where the password is being changed.
2 Has your Password Filter been signed by Microsoft?	If a provider has not had the Password Filter reviewed and approved by Microsoft, it will fail under certain security hardening configurations.
3 Does the tool require custom dictionary entries to be updated on each individual domain controller?	Understanding how the product will be maintained across your multiple domain controllers can indicate how difficult it will be for your administrators to use.
4 Is there a graphical user interface for installation and configuration?	Products that provide user interface are generally easier to manage for more staff members and with less training time required.

ESSENTIAL FUNCTIONALITY

1 Does the tool differentiate between exposed passwords and exposed username and password pairs?	It's essential to prevent users from selecting passwords that are compromised, commonly used, or otherwise expected. However, a more comprehensive tool will also detect when the exact username and password pair is compromised. The username and password pair (also known as full credentials) is the complete key. An attacker can use this to log in immediately without any credential guessing effort whatsoever.
2 What are the automated remediation options available when a password is found to be compromised?	Automating the manual administrative tasks associated with password security can provide business value. However, not all tools offer sufficient automated remediation options. For illustration, if requiring a user password reset, can you add a window of time for this to be completed, so it doesn't result in the user being locked out. It's also necessary to have the option to align remediation with the severity of the attack. For example, detecting exposure of full credentials may necessitate a different response.
3 Does the tool only check passwords on a periodic basis? (daily, weekly, etc.)	Some tools are designed for auditing passwords only after they've been saved. This results in users creating passwords that are vulnerable (insecure) and then being forced to change them (frustrating) until they find a good password. NIST 800- 63B is explicit that the password shall be screened at the time they are being established.

ESSENTIAL FUNCTIONALITY

4 Does the tool only check when a password is being created or reset?	Most tools focus on checking only when the password is saved. However, a password that was previously safe may no longer be. The concept of continuous monitoring was not required when a good password could be determined by algorithmic complexity alone. Note that continuous monitoring requires a blacklist to be updated regularly.
5 Does the tool compare users' new and previous passwords to determine if they are substantially different?	Even good passwords are vulnerable to hacking if they are too similar to users' previous passwords. The FAQ from NIST 800- 63B indicates that the research shows that “select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password”
6 Can the tool exclude the name of your company and possible variations that may not have been previously compromised?	NIST is clear that the organization shall be able to prevent the use of context-specific words and have fuzzy matching to cover possible variations.
7 Can the tool support NIST recommendations for eliminating periodic password reset?	Substantial research has shown that password expiration policies don’t improve security. Therefore, NIST recommends NOT requiring passwords to be changed arbitrarily (e.g., periodically), but only if there are methods to immediately determine when a password is no longer safe. Many tools on the market can't detect when a saved password becomes vulnerable later.

BLACKLIST DEPTH & BREADTH

1 Does the password database also include data from actual cracking dictionaries?	NIST 800-63B is explicit that passwords shall be screened against dictionary words, including common substitutions, transformations, and patterns. This can be obtained by including cracking dictionaries actually used by hackers, but some providers only include passwords that have actually appeared in a data breach.
2 How frequently is the database of compromised password updated? (daily, monthly, quarterly, etc..)	Lists of compromised passwords will change every day as new data breaches occur. Attackers use the latest breach data, but many providers use blacklists that are rarely updated. They rely on free password sources rather than investing in keeping their data current.
3 Is your compromised password database in a flat file or format that I can see?	If a blacklist is maintained in a flat-file format, as the database becomes larger, you may find each check takes longer than you'd find acceptable.

SECURITY CONSIDERATIONS

1 Does the tool use clear text data for screening passwords?	There are a variety of techniques for password screening, including options that avoid the inherent legal risk and security vulnerability of dealing with clear text password data.
2 Does password checking always use a partial hash comparison?	Partial hash comparison (K-Anonymity) is an alternative to working with the clear text or hash of the full password and is essential to ensuring passwords cannot be reversed.
3 What client information is logged or stored at the provider?	Password screening should not require any client data to be stored by the provider.
4 Does the provider have a written Information Security Policy that adheres to known secure coding best practices and require third-party testing?	This type of software interacts with mission-critical systems that have the highest security implications.

VENDOR PARTNERSHIP

1 Does the provider specialize in compromised credentials or focus more on algorithmic rules for password complexity?	Current industry best practices put heavy emphasis on preventing compromised passwords and downplay algorithmic password policies that are the basis of older tools.
2 Do they have enough people to continue to operate in case of a support emergency?	Software from small companies can be risky if something unexpected happens.
3 Does the organization have Errors & Omissions insurance and the other forms of insurance that our company requires?	Insurance may be the only financial recourse if a major problem technical, legal or security incident were to occur

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.