A BIO-key® Solution.

PortalGuard's Password Management Buyers Guide

When looking into integrating a password management program it is important to do your homework to fully understand the platform and what you are buying into. Make sure to review the products features, benefits and also think forward to options you may not be prospecting currently, but may need in the future.

Below we have identified the top five things to look for in a Password Management Program

1.) Required Password Quality

Having an intricate password is a key component to securing your company's information. It is very important to define what your corporate requirements are and identify that the product you are considering follows your policy.

Strong passwords consist of a number of requirements for complexity. Things to consider when creating a policy and picking a program are password length, character requirements, and capitalization requirements. Enforcing the requirements and choosing the correct program will ensure that your company truly is "hassling the hackers".

2.) Innovative Two-Factor Authentication

Employing an innovative and flexible Two-Factor Authentication process that is user friendly is a great way to reduce your company's vulnerability. The best way to exercise this is through a One-Time Password (OTP).

Another thing to consider while researching is that many solutions blanket Two-Factor Authentication across your organization enforcing stronger authentication unnecessarily. Every employee may have different scenarios, which would require different needs and ways to retrieve their Two-Factor code.

For example, you can enforce Two-Factor Authentication when a user accesses a payroll application but require only a password when accessing the email system. Furthermore, some companies charge individually for their OTP methods. It is best to purchase a solution set that includes all of the delivery options available for one price.

Secure methods for OTP:

- **SMS (Text Messaging):** These gateways deliver SMS messages directly to identified cell phones or smartphones and can be delivered through multiple service providers

- **Printed**: When the user is unable to receive an OTP via SMS or phone call, the user has the option of generating and printing a batch of OTPs. These values are still OTPs in that they can only be used for a single authentication.
- **Voice**: It is also possible for OTP's to be retrieved via a user's landline or mobile phone with a hosted text-to-speech service or with the SIP protocol to leverage your existing phone infrastructure.
- **Hardware**: Another option to consider is the YubiKey. This is a small USB-key which is inserted into the user's machine. By touching the hardware button YubiKey creates and sends a time-variant OTP by simulating keystrokes on the keyboard.
- **PassiveKeyTM**: This option validates both the user -AND- the device they're using. PassiveKeyTM automatically generates a Time-based One-time Password (TOTP) on a configurable interval and sets the value as a session-based cookie. This cookie is created for only specific websites and is encrypted using public-key cryptography to ensure only the correct server can decrypt it.
- **Email**: An OTP can be sent to the user's enrolled email account.
- **Mobile Authenticator**: The OTP can be read from an enrolled Mobile Authenticator App installed on a smart phone.
- **Help Desk**: The OTP can be given to the user over the phone from the Help Desk Administrator.

3.) Flexible Password Expiration Settings

Setting standards and enforcing a policy for your password resets is very important. Perhaps your company has highly sensitive data and needs a short password reset timeframe. Maybe your company may have certain employees that have access to proprietary information and you need to keep these highly classified documents safe.

No matter your company's situation, being able to set your own password expiration date is a great feature to have. A stale, out of date or static password can be a huge vulnerability.

4.) Self-Service Password Reset or Account Unlock

Locking yourself out of an account is an awful experience and usually happens at the worst possible time. This can lead to a help desk call to either reset the password or unlock their account.

Deploying a Self-Service Password Reset or account unlock method, may not avoid your end user forgetting their password. But, it will avoid the pain of having to rely on a help desk to unlock the account which will surely reduce help desk calls.

With this solution, typically users who have forgotten their password launch a Self-Service application from an extension to their workstation login prompt, using their own or another user's web browser, or through a telephone call. Users establish their identity, by answering a series of registered personal questions, using a hardware authentication token, responding to a password notification e-mail or, less often, by providing a biometric sample.

5.) Three Strike Lockout Policy

When the end user or hacker is attempting to log in to an account it is important to enforce a “Three Strike Policy”. This policy will ensure that the person sitting at the keyboard has only three attempts to enter the correct password before the account is locked out.

When incorporated with a self-service password reset, this layer of authentication is most effective.

Why PortalGuard

Founded in 1999, PistolStar is a pioneer in user authentication and credential management solutions, technology and services. PistolStar developed PortalGuard Complete User Authentication for Client-facing Applications as a complete, end-to-end platform to enable organizations to safely and effectively provide the information and application access their users need by enhancing security, usability, audit-readiness, and regulatory compliance—all while educing demands on your development timeline.

PortalGuard is a proven solution from an established vendor you can trust. Our solutions are designed to be highly customizable and scalable to adapt to your current and future processes while leveraging and augmenting your technology investments with additional critical functionality.

This gives you the peace of mind that comes from knowing you're deploying a solution that will greatly reduce security risks while improving end-user satisfaction.

In addition, PortalGuard will help you:

1. **Better focus your in-house development efforts on the core functionality of your application** - resulting in a more robust application with greater usability and user satisfaction.
2. **Reduce development costs and deliver application development projects on budget** - while accelerating your time-to-market by meeting critical application development project deadlines.
3. **Simplify your development process** - by sourcing all the User Authentication methods you need from a single, highly-experienced and trusted provider.
4. **Avoid development headaches and enable higher customer user satisfaction** - with fewer problems or Help Desk calls.

You design your solutions to have a meaningful and measurable impact on the success of your business. PortalGuard can help you more quickly and cost-effectively build, offer, deploy and manage secure client-facing applications to enhance security, usability, audit-readiness and regulatory compliance to support new business innovation.

To find out more: visit our website www.bio-key.com/portalguard

Email us at info@bio-key.com

Call us at 603-547-1200