perinova IT-Management GmbH

Securing your data password less

perinova

IT-Management GmbH

Perinova
IT-Management GmbH

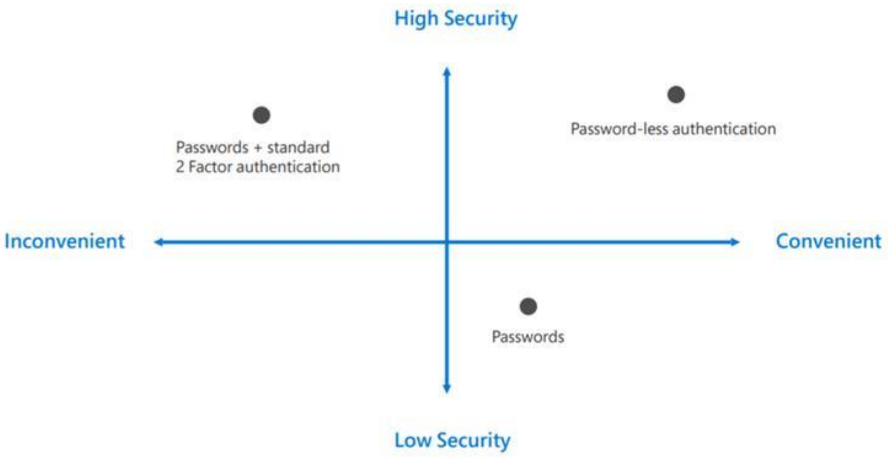
Secured without Passwords

Challenges

- Complex passwords are needed but painful to manage and remember.
- Memorizable passwords (usability) vs. complex passwords (security).
- Keep your passwords secure. Hacked Password databases are common.
- For enterprise IT departments, nothing costs more than password support and maintenance.
- It’s common practice for IT to attempt lessening password risk by employing stronger password complexity and demanding more frequent password changes. However, these tactics drive up IT help desk costs while leading to poor user experiences related to password reset requirements. Most importantly, this approach isn’t enough for current cybersecurity threats and doesn’t deliver on organizational information security needs.

Ideal Solution

- Easy user driven solution to create a highly secured login without passwords.
- Easy to manage.
- Cost and administrative reductions,
- Single Sign on to all services and apps.



Desired Outcomes

- No passwords for windows sign in and for internal services and trusted partners.
- Login with FIDO 2 Security key and second factor (facial recognition, fingerprint, pin, smart card).
- Simple to deploy and easy to use.
- Overall lower attack vector.
- High security and yet high user satisfaction.

perinova IT-Management GmbH – Passwordless Authentication

Passwordless Authentication

Passwordless Login

- Use a Fido 2 stick to sign up,
- No need to remember any passwords,
- Take the Fido Stick with you when you leave your workplace and lock workstation automatically.

Multifactor

- Use a second factor for authentication like facial recognition, fingerprint or a simple PIN.
- Theft of first factor does not lead to a security breach.

Single Sign On

- Ensure Single Sign On capability of apps and services.
- Replace old legacy applications with incompatible authentication requests.
- Use a single authentication provider like Active Directory or Azure Active Directory with Kerberos, oAuth and openID.

Password Safe

- In case there are passwords for third party services, which can not be eliminated, us password safe accessable by MFA.

All requirements of security officers and requirements of DSGVO regarding logins are completely met.

Microsoft + HID + perinova

The perfect security match: Microsoft Software + HID Hardware + perinova Services

Solution Alignment

Microsoft

Azure Active Directory as authentication provider with Kerberos, oAuth and openID.

Windows Hello with facial recognition (or other biometric and PIN).

HID

FIDO 2 Security keys (or other hardware implementations like smart cards, rfid or nfc)

perinova

Professional services based on best practices.

Focused on the secure modern workplace.

Strong eat your own dog food policy.