Go Passwordless

Reduce your risk exposure with password alternatives

Nicola Ferrini

Microsoft MVP – Cloud and Datacenter Management

NicolaFerrini.it

nicolaferrini

Who Am I ?

NICOLA FERRINI

Microsoft Certified Trainer — Microsoft MCT — Trainer — 2020 - 2021

Microsoft Certified Professional — Microsoft MCSE — Productivity — Earned 2016

Microsoft Certified Professional — Microsoft MCSE — Cloud Platform and Infrastructure — Earned 2016

Microsoft Regional Director

MVP — Microsoft® Most Valuable Professional

VEEAM CERTIFIED ENGINEER V9

vmware 2X CERTIFIED PROFESSIONAL — DCV & DESKTOP MOBILITY — MILESTONE

Microsoft CERTIFIED — AZURE ADMINISTRATOR — ASSOCIATE

Microsoft CERTIFIED — AZURE SECURITY ENGINEER — ASSOCIATE

Microsoft 365 CERTIFIED — MESSAGING ADMINISTRATOR — ASSOCIATE

Microsoft 365 CERTIFIED — TEAMS ADMINISTRATOR — ASSOCIATE

Microsoft 365 CERTIFIED — SECURITY ADMINISTRATOR — ASSOCIATE

Microsoft 365 CERTIFIED — MODERN DESKTOP ADMINISTRATOR — ASSOCIATE

Microsoft CERTIFIED — AZURE SOLUTIONS ARCHITECT — EXPERT

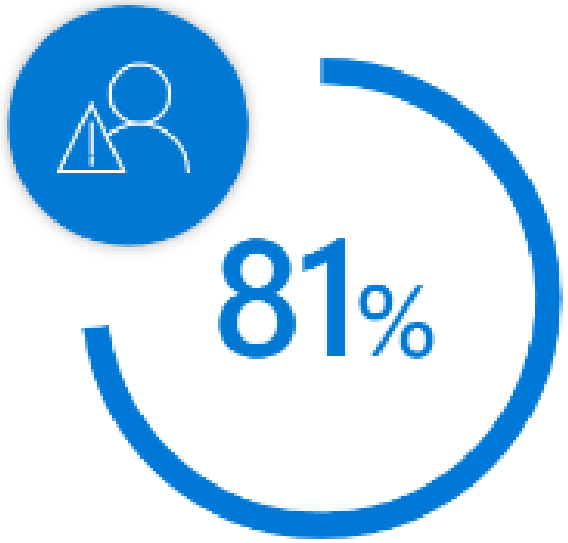
Microsoft 365 CERTIFIED — ENTERPRISE ADMINISTRATOR — EXPERT

Evolution of Identity technology

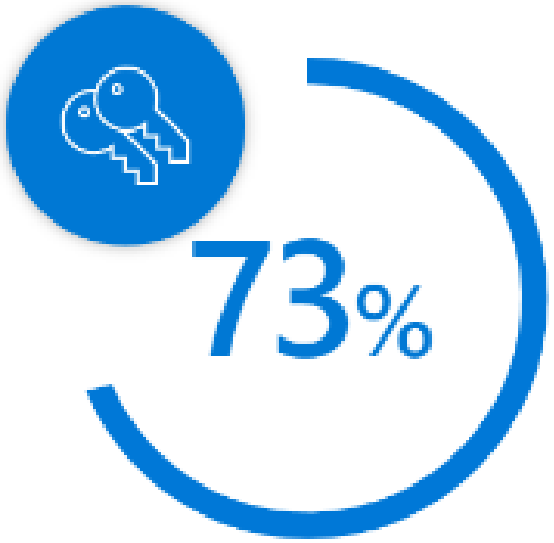
Evolution of IT, threats, and Microsoft Identity security

MICROSOFT IDENTITY APPROACH	Windows NT Domains	+ Enterprise Active Directory + Smartcard Authentication	+ Azure Active Directory + Passwordless Authentication + Hardware Credential Isolation
IDENTITY AND ACCESS TRENDS	Local Identities	Enterprise Single Sign On + 2 factor authentication	Hybrid and Federated Cloud Identity
INFORMATION TECHNOLOGY	 Mainframes + PCs	 + Datacenters + Mobile Devices	 + Cloud + Internet of Things (IoT)

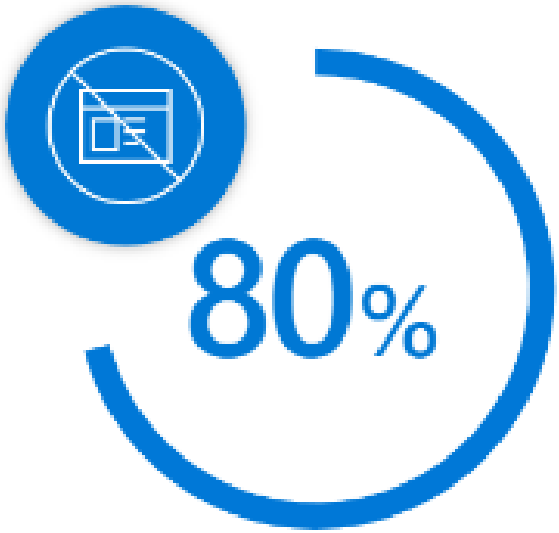
Identity challenges



of breaches are caused by credential theft

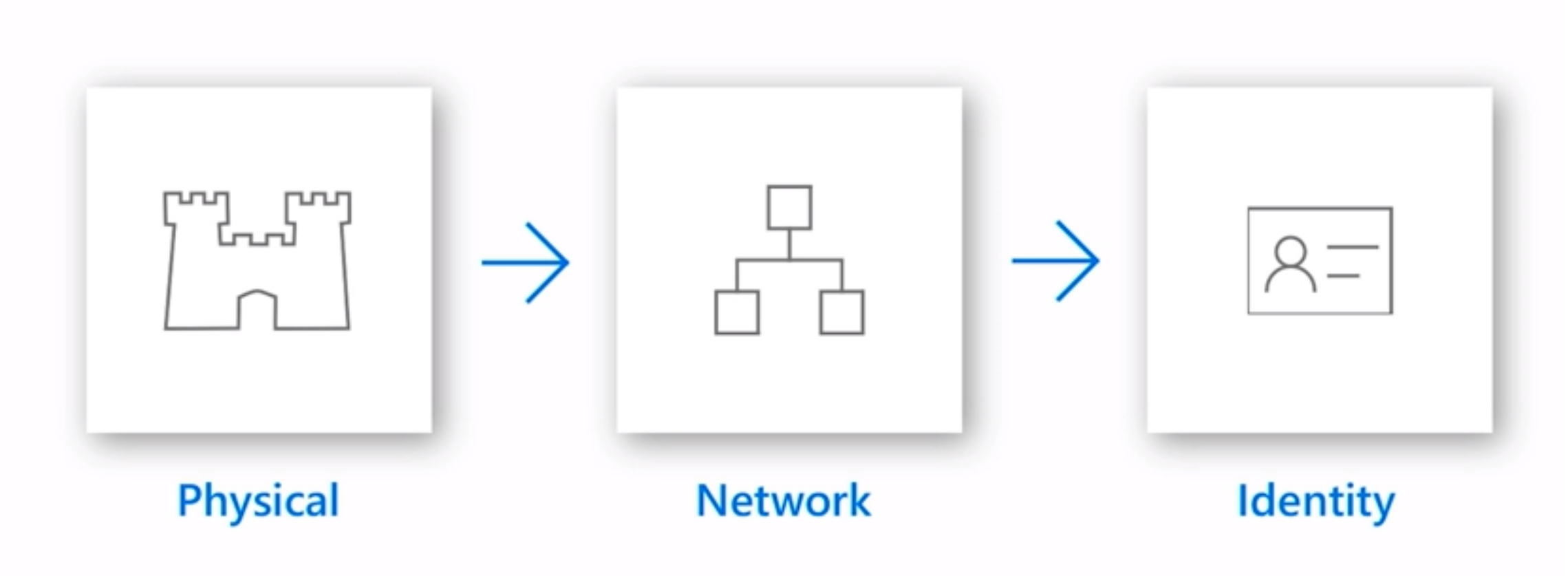


of passwords are duplicates



of employees use non-approved apps for work

Identity is the new perimeter



Passwords are no longer enough

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.

Why Passwords are Bad

Passwords are problematic

Passwords are increasingly being

- Cracked
- Stolen
- Intercepted
- Eavesdropped
- Peeked
- Phished
- Reused

Passwords are in the way

Your colleagues forget their passwords

Password resets cost loads of money

81% of all digital incidents are related to weak or leaked passwords

20% of IT costs for organizations are made to help end users with lost passwords

How Easy It Is To Crack Your Password

https://youtu.be/K-96JmC2AkE

Complicating Factors

Cloud

Cloud services offer signing in, based on

- Username and password
- Username, password and multi-factor
- Certificates
- Federation

End-users

Your colleagues use their business e-mail addresses for personal services

2017 had 1579 data leaks in the US, a 45% increase compared to 2016

In 2016, 1 in 14 phishing attacks was successful

GDPR

Now, when your credentials leak, everything you have can be easily gathered and/or forgotten

Why eliminate passwords?

Multi-factor authentication (MFA) - for instance, a PIN and password, or biometrics - has presented a more secure method for organizations.

However, depending on the implementation, MFA can also lead to increasing complexity regarding the user experience.

It's imperative for IT teams to deliver a seamless user experience while balancing security risk.

One upon a time…

Many years ago, we started multi-factor authentication with *smart-cards* to secure the identity of our employees.

Initially, we used physical smart-cards to secure, but it didn't give people a smooth user experience.

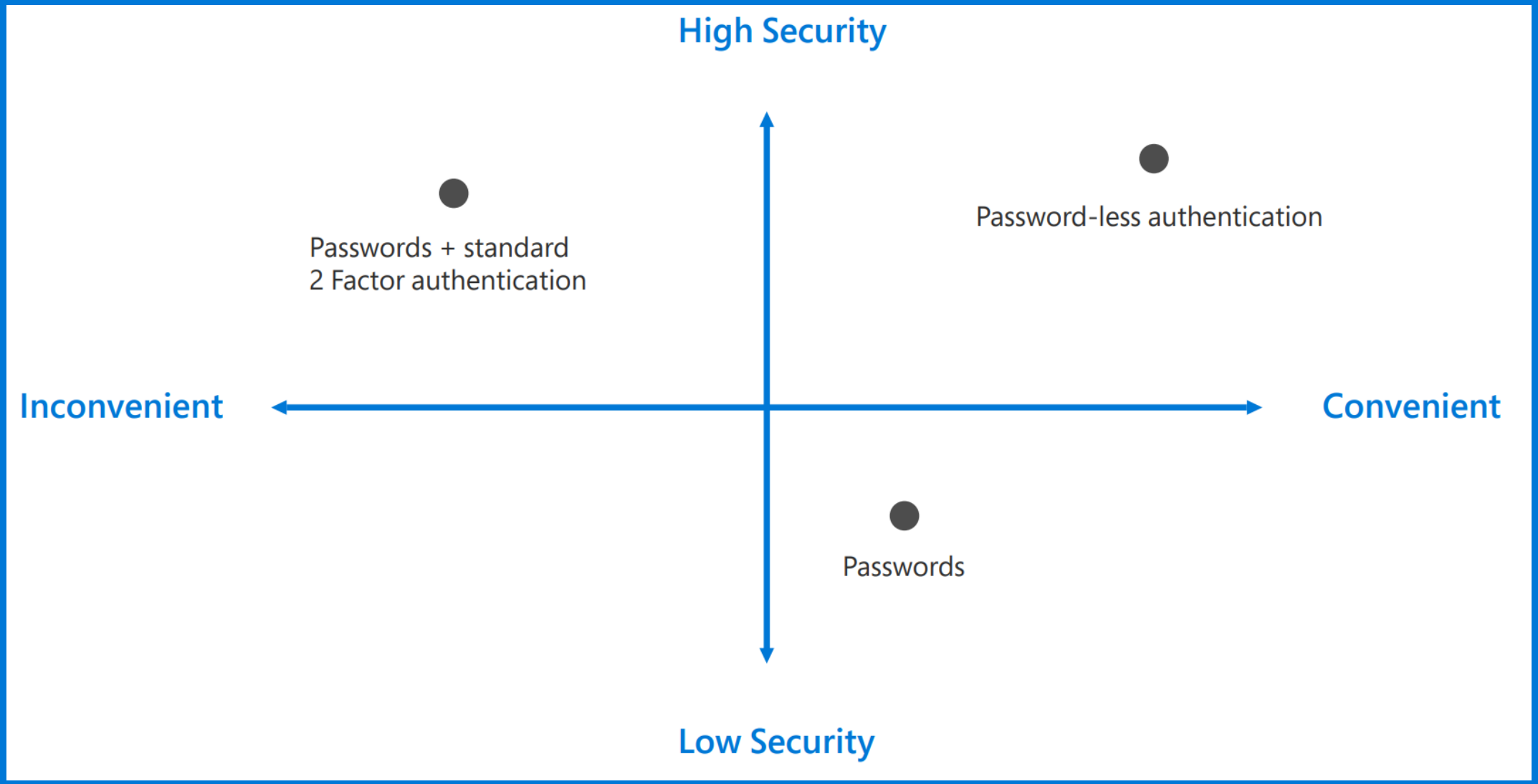
Additionally, this also requires a card reader in each hardware device which can be challenging to implement and also smart-cards are prone to be lost or forgotten.

Today

IT security are moving toward **passwordless** authentication using advanced technologies like biometrics, PIN, and public/private key cryptography.

Plus, new standards like Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2) are enabling passwordless authentication across platforms.

These standards are designed to replace passwords with biometrics and devices that people in your organization already use, such as security keys, smartphones, fingerprint scanners, or webcams.


High Security
Passwords + standard
2 Factor authentication
Password-less authentication
Inconvenient
Convenient
Passwords
Low Security

Introduction to password replacement technology

What do we mean by password-less authentication?

Password-less authentication is a form of multi-factor authentication that replaces the password with a secure alternative.

This type of authentication requires *two or more verification factors* to sign in that are secured with a cryptographic key pair.

Choosing the right technology

With biometrics on mobile phones and computers becoming more ubiquitous, the number of password replacement technologies has increased.

Introduced by Microsoft in Windows 10, **Windows Hello** uses *biometric* sensors or a PIN to verify a user's identity.

The **Microsoft Authenticator app** is a software token that allows users to verify their identity with a built-in biometric or a PIN when signing into their work or personal accounts from a mobile phone.

With **biometrics** on **mobile phones** and **computers** becoming more ubiquitous, the number of password replacement technologies has increased.

You can now use portable **FIDO2 hardware devices** to log into a work machine or cloud services on supported devices and browsers.

Microsoft Authenticator app

The Microsoft Authenticator app enables users to verify their identity and authenticate to their work or personal account.

Microsoft Authenticator can be used to augment a password with a one-time passcode or push notification.

Windows Hello for Business

Windows Hello for Business replaces passwords with strong multi-factor authentication on Windows 10 platforms, including PCs and mobile devices.

This authentication consists of a new type of user credential that's linked to a device and uses a biometric or PIN.

It lets you sign in with your face, iris scan, fingerprint, or a PIN, and enables you to authenticate to enterprise applications, content, and resources without a password being stored on your device or in a network at all.

The biometric data is only used locally and never leaves the device.

FIDO2 security keys

FIDO2 standard is intended to solve multiple user scenarios including strong first factor (password-less) and multi-factor authentication.

Devices and tokens that adhere to FIDO2, WebAuthN, and CTAP protocols bring about a cross-platform solution of strong authentication without using passwords.

Passwordless login Demo

Some useful links

Passwordless login al Microsoft Account con Windows Hello e con Yubikey

Abilitare il passwordless sign-in per Azure AD e per Microsoft 365 / Office 365 utilizzando una security key FIDO2

Utilizzare Azure Multi-factor Authentication con token hardware Yubikey

ICT POWER.IT

https://aka.ms/gopasswordless

Products to get started

Windows Hello for Business

Increase login convenience with a biometric. Replace passwords with strong MFA on Windows 10 PCs.

LEARN MORE >

Microsoft Authenticator

Authenticate with a mobile device. Get a push notification and verify identity with a biometric or PIN.

LEARN MORE >

Microsoft-compatible security key

Replace passwords with a security key using MFA with the standards-based protocols on a mobile device.

LEARN MORE >

Microsoft Edge

Authenticate from a browser. Microsoft Edge supports the broadest set of passwordless authenticators.

LEARN MORE >

Grazie

Nicola Ferrini
MVP Cloud and Datacenter Management

/nicolaferrini.it
@nicolaferrini