

Sieťový perimeter je mŕtvy, je treba uplatňovať princíp Zero Trust

#MFA #IAM #OTP #FIDO #PKI #Biometrics

Petr Kunstát, Thales CEE

www.thalesgroup.com



State of MFA in 2022

1

43.2% of companies do not use Multi-Factor Authentication (MFA)

2

11.4% of companies do not plan to acquire MFA within the next 12 months

3

31.8% of companies plan to get an MFA solution within a year

4

7% more companies use MFA than last year

Source: 2022 Cyberthreat Defense Report

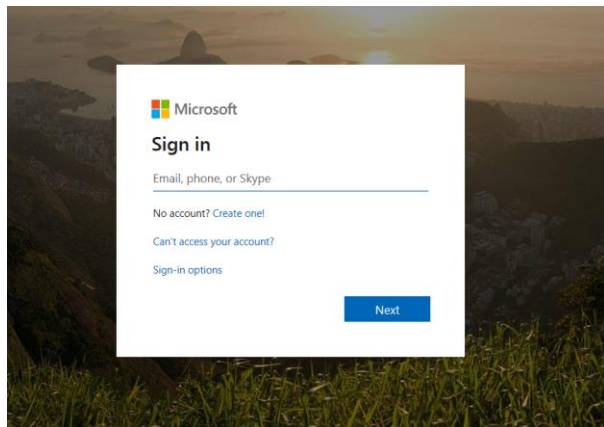
According to Microsoft, “**99.9% of cyberattacks can be prevented by using Multi-Factor Authentication.**” Yet many organizations are slow to adopt this prevention technique.

80%
of breach incidents came from identity theft

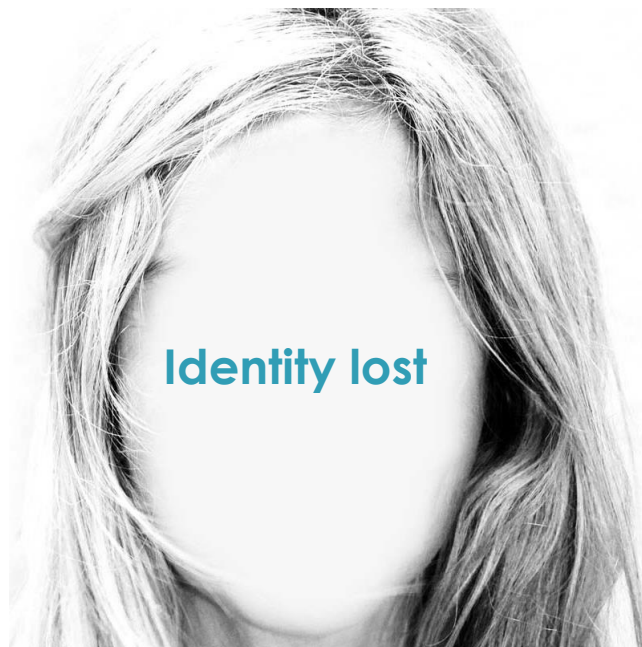


Typické vektory útoku na naše identity

- Social engineering
- Phishing / Smishing
- Credential Stuffing
- Lazy Phi\$hing



- Deepfake
- Malware-initiated fraud



Deepfake

■ A portmanteau of "**deep** learning" and "**fake**" is a technique for human image synthesis based on **artificial** intelligence.



Xi Jinping

President of China



Justin Trudeau

Prime minister of Canada

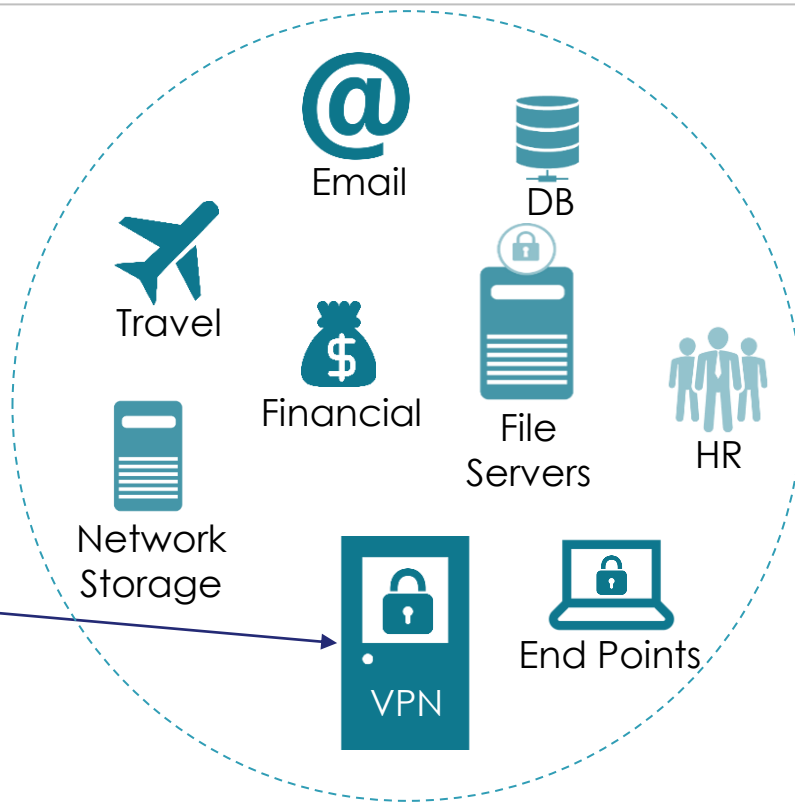
UK-based energy firm was duped out of \$243,000 through a sophisticated deepfake voice scam

Jak to vypadá u nás

With perimeter defense, there is only one access point – the VPN



Password

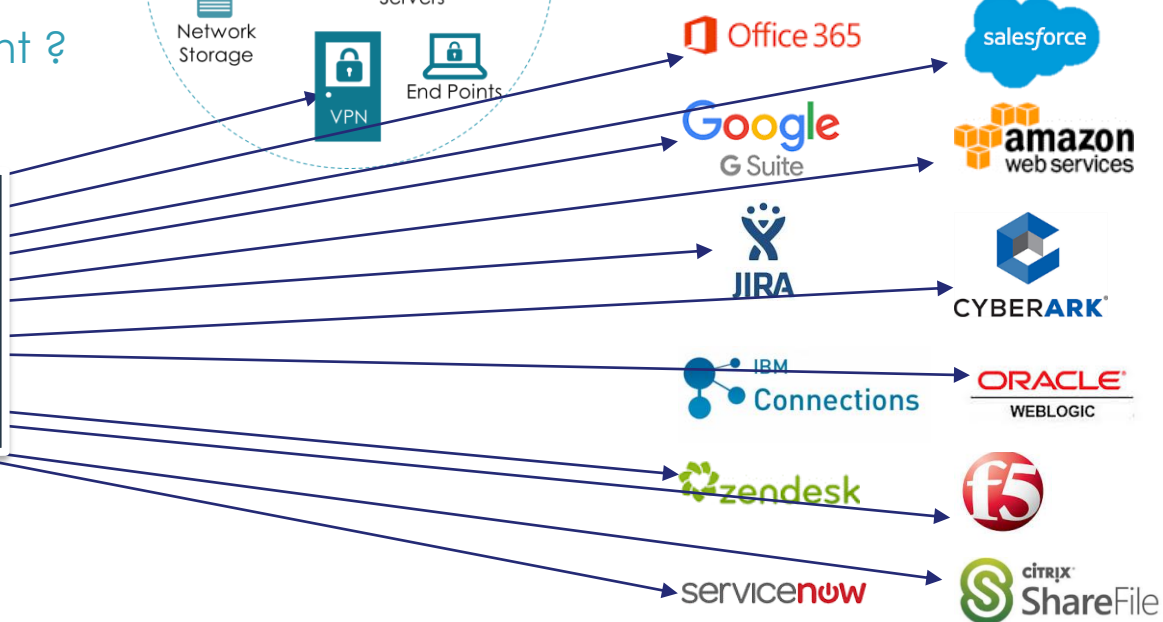
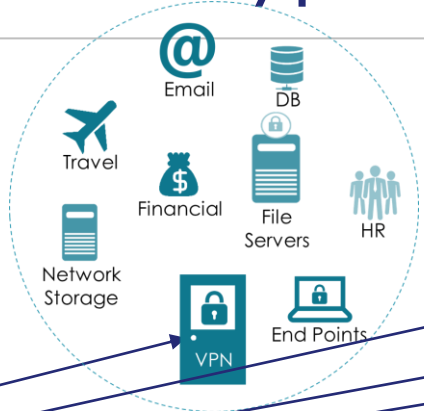


Uživatelé jsou dnes tím hlavním security perimetrem

How is protected your account ?



Theb3stP@ssword
Heslo123
Hesloheslo
Mojeheslo
Theb3stP@ssword
Password1



Uživatelé jsou dnes tím hlavním security perimetrem

Applying the **right level of security** for the **right users** at the **app level**



Strong MFA
Smart SSO
Access Policies



Office 365



Google
G Suite



JIRA



IBM
Connections



zendesk



servicenow



SafeNet Trusted Access

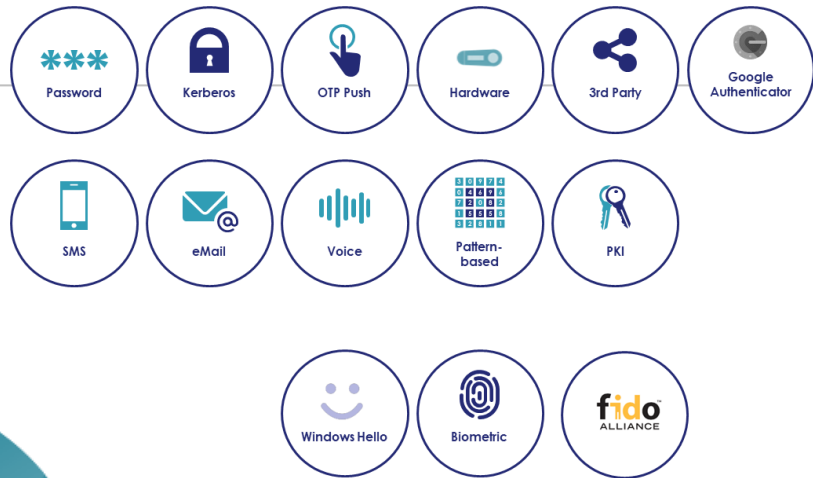
SaaS / IaaS

On-prem Apps



3
APPLY
Apply appropriate access controls, with smart single sign on

1
IDENTIFY
Validate user's identity

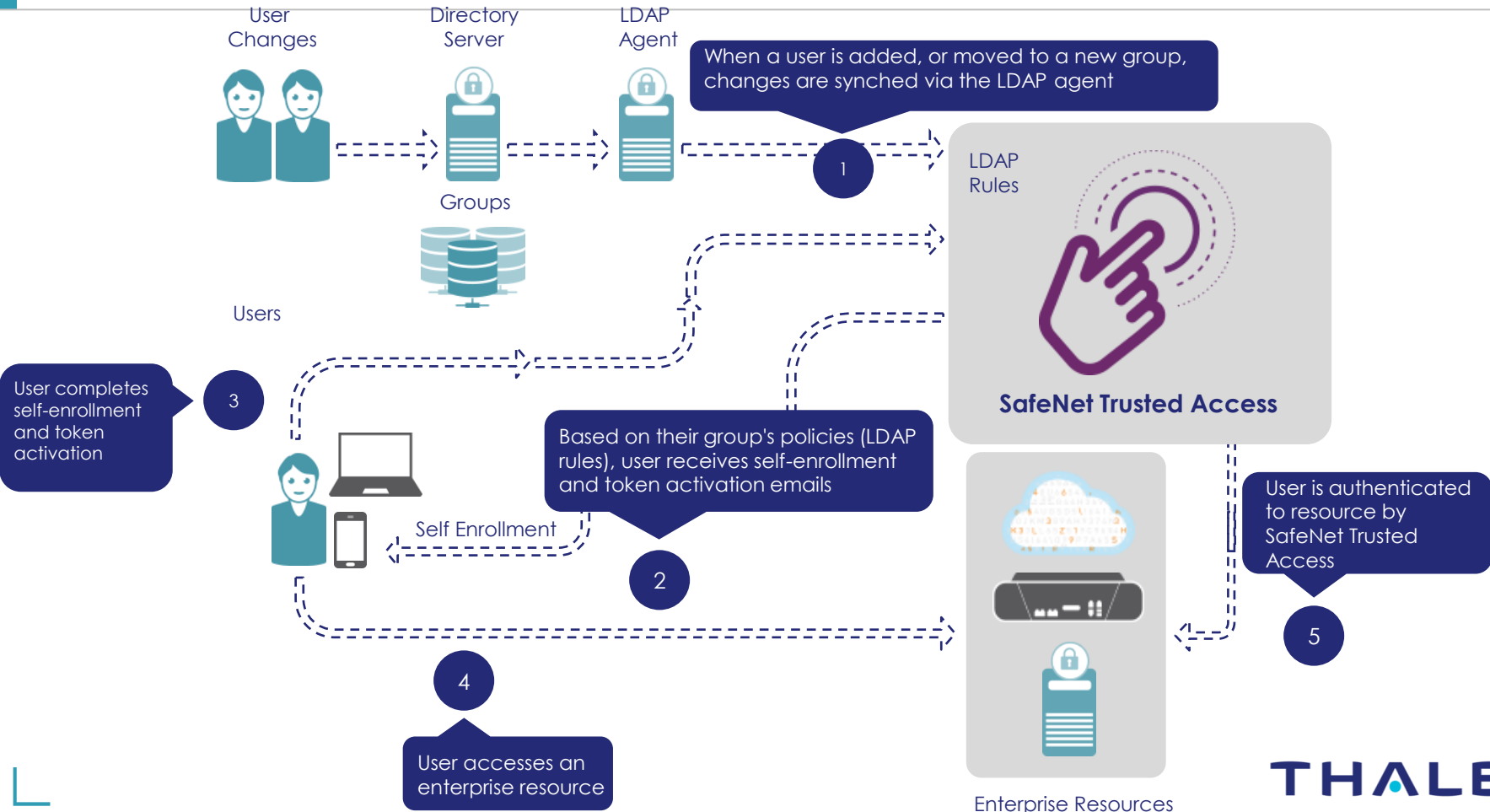


2
ASSESS
Assess which access policy should be applied



SafeNet Trusted Access allows organizations to manage access to cloud applications by validating identities, determining levels of trust and applying appropriate access controls each time the user accesses a cloud service.

Automated Workflows Triggered by User Store Changes



STA Authenticator Provisioning and Self-Service


STA has several different options for **authenticator provisioning**:


- **Admin-provisioning:** Administrators can send out enrollment links via email
- **Self-provisioning:** Users can set up their preferred authenticator during first time login

User Self-provisioning

Available for MobilePASS+ and FIDO

Log in to access **Acme Access Portal**

 **leia**
Leia Organa
[Switch User](#)



Protect Your Account

Your account needs an additional layer of security.

To comply, you need to add an authenticator to one of your devices or your computer.


[Add Authenticator](#)

[Cancel](#)

Service powered by **THALES**

Add Authenticator

Confirm Your Identity



Hello **leia!** First we need to confirm your identity to add a new authenticator.

Password

[Cancel](#) [Submit](#)

Add Authenticator

Select Authenticator Type

Select a type of authenticator to add to your account:

Authenticator App
Set up the SafeNet MobilePASS+ app on your mobile device or computer

Security Key or Windows Hello
Register your security key or Windows Hello as an authenticator

Grid Pattern
Set up a pattern for your GridSure authenticator

[Cancel](#) [Submit](#)

MobilePASS+ for Apple Watch

Users can now approve login requests without ever touching their phone

- Users will feel a **tap** on their wrist whenever a login request is sent via MobilePASS+
- With Watch biometrics enabled, users can approve push authentication requests with a simple tap
- Generate passcodes from the MobilePASS+ Apple Watch app

Technical details

- MobilePASS+ for Apple watch is a companion app for watchOS v6.0 and above
- Uses Apple Watch's wrist detection as second biometric authentication factor
- Approve/Deny push authentications directly from the notification on watch



Pattern-based Authentication

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

1 User is presented with grid

			3 RD	4 TH
		1 ST	2 ND	

2 User selects their PIP

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

5582

3 User enters their PIP, producing an OTP

1	5	9	6	6
7	7	8	9	4
2	3	3	8	2
0	5	0	1	2
1	4	5	0	3

1	5	9	6	6
7	7	8	9	4
2	3	3	8	2
0	5	0	1	2
1	4	5	0	3

0182

4 In the next logon, the same PIP will produce a new OTP

Proč MFA od Thalesu

- Thales se zaměřuje pouze na IT Security
- Mobile Pass+ nelze klonovat
- HW tokeny – HOTP/TOTP
- Pattern based token
- Podpora PKI a FIDO
- Multitenant prostředí
- Cloud, On-prem nebo Hybrid



Zero Trust -> Adaptive authentication

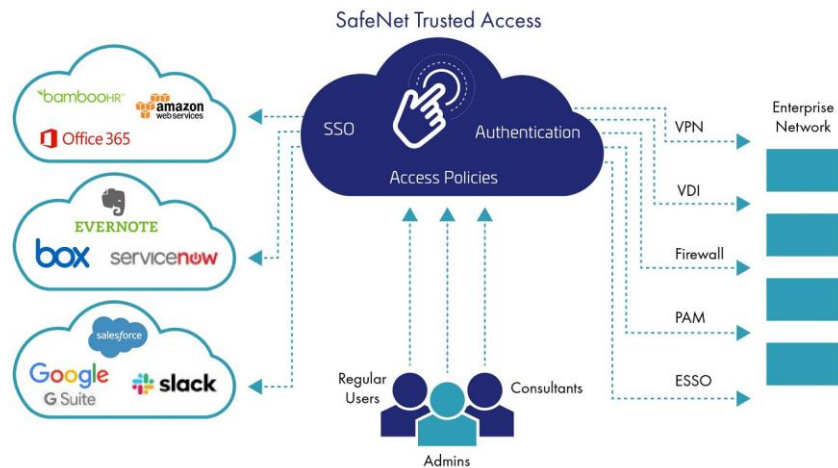
- Organizations should **not automatically trust** anything inside or outside their perimeters.
- Enterprises should leverage flexible security applied at the **app level** based on **users**
- Rather than trusting the network to any extent, a zero-trust model puts all of its effort behind **protecting applications**, and the **data** they access.

Passwordless -> FIDO2

- More Secure - **Eliminate phishing**, credential stuffing & other passwords related attacks
- Less Friction - **No** need to **remember** multiple passwords. Faster & seamless login.
- Lower TCO - **Reduce** IT operations **costs** & support costs

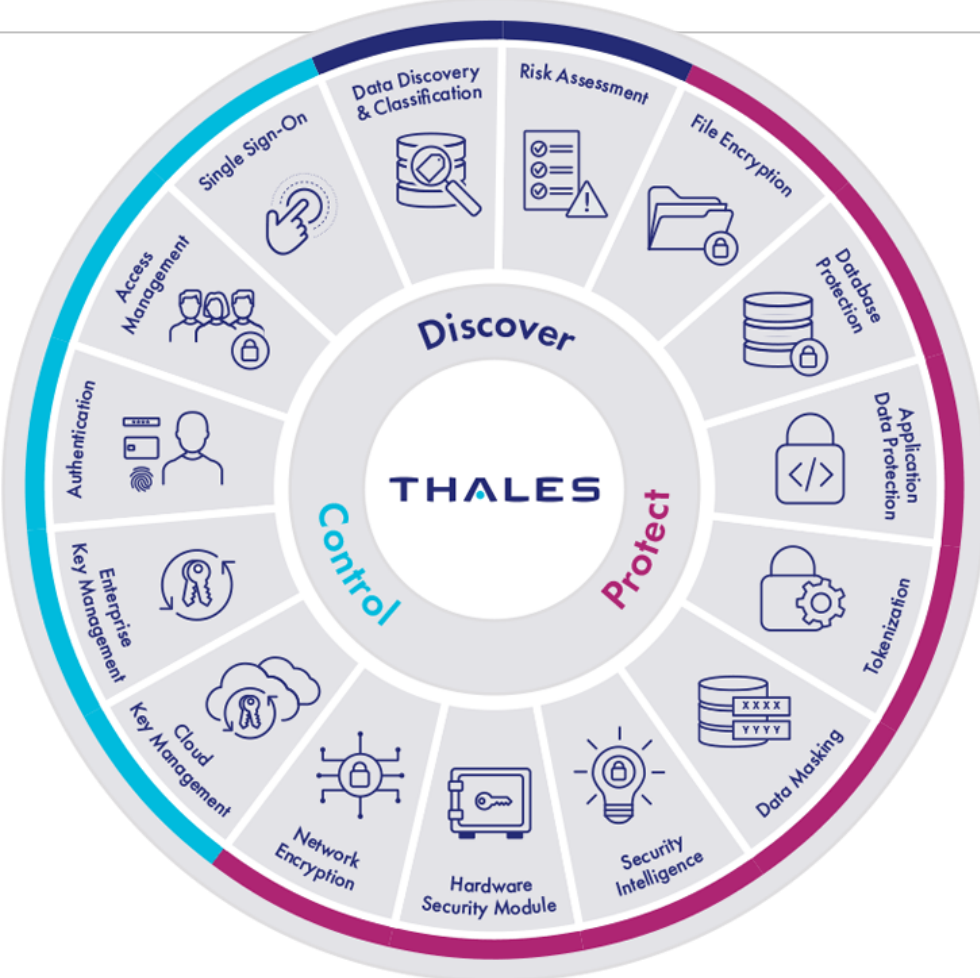
Možnosti nasazení MFA

- Cloud IAM
- Onprem IAM
- Hybrid IAM



- PKI – certifikát na kartě
- Virtuální PKI - certifikát v HSM + IAM
- FIDO – není třeba CA





Enjoy the event

petr.kunstat@thalesgroup.com



www.thalesgroup.com

