

Data jsou ropou 21. století Chraňte si je !

Tomáš Jilík, Petr Kunstat
Thales CEE

Pardubice
2019

Vitajte!
Welcome

Karşılama! 歡迎 добро пожаловать

ברוך הבא ;Bienvenido! Vítejte! Benvenuto!

Fogadtatás! Iarguralcome! ようこそ

Velkommen! Välkommen!

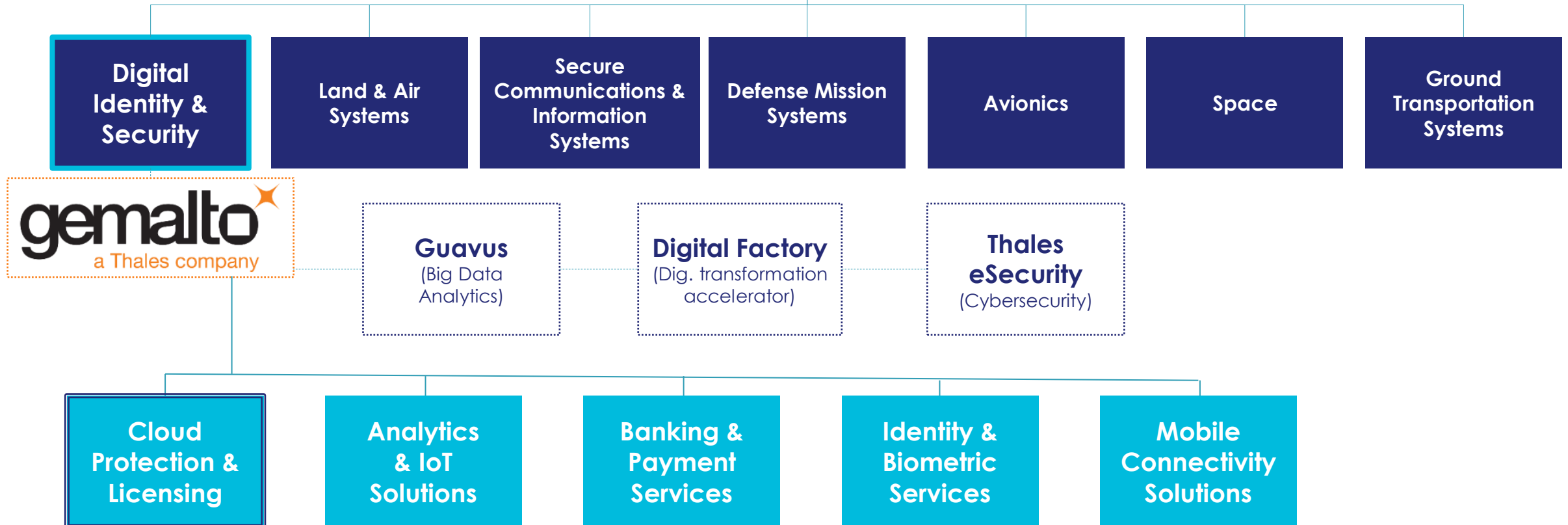
الدهسو.الهأ! Willkommen! 환영

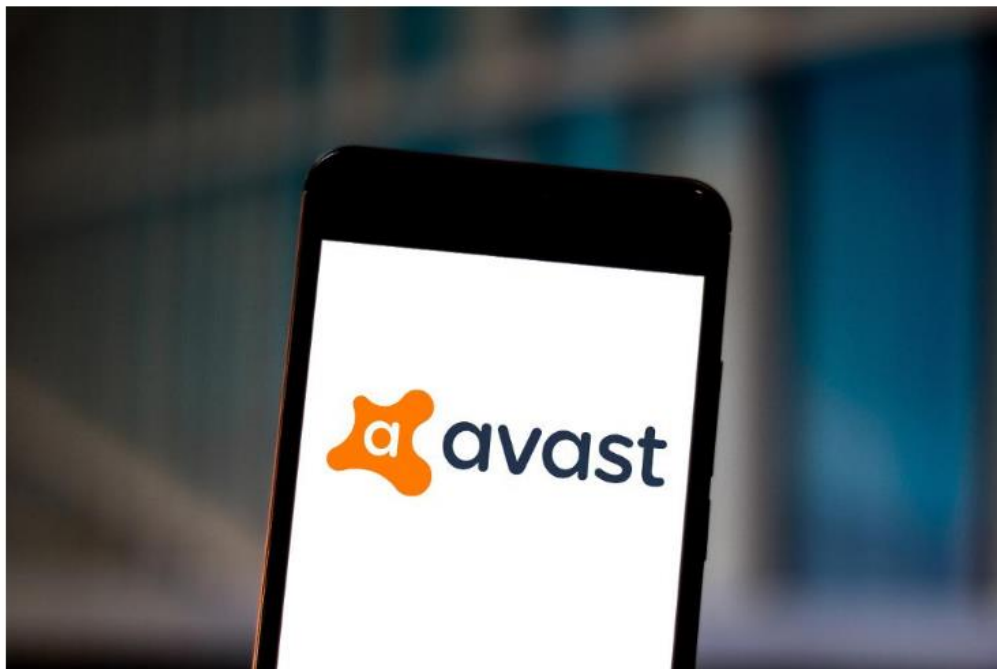
Bienvenue
Tervetuloa! ; Bem vindo!

Thales' new Digital Identity & Security



€19b revenue
80,000 employees
68 countries
€1b R&D investment





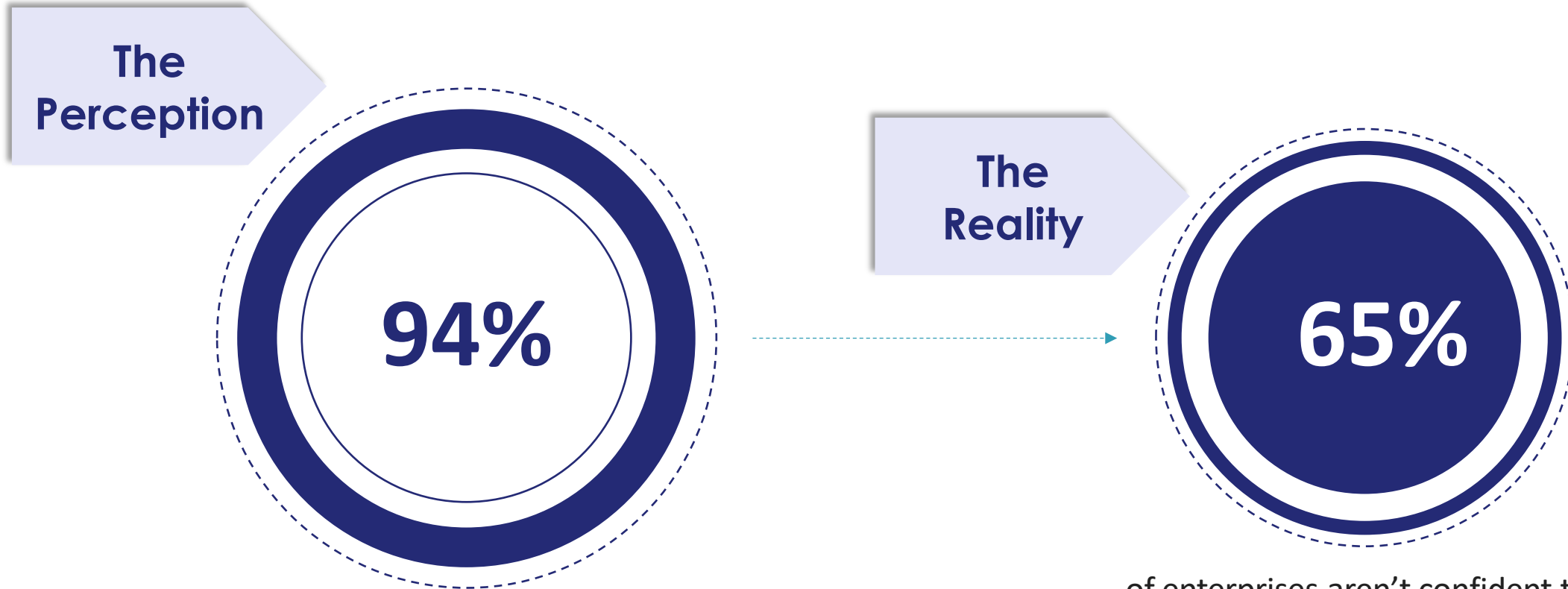
Avast has suffered a breach of its internal IT network thanks to what it calls a sophisticated hack. PHOTO ILLUSTRATION BY RAFAEL HENRIQUE/SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Avast has become the victim of a cyberespionage campaign that saw hackers gain deep access to its network. But the Czech company, which has more than 400 million customers for its various antivirus and cybersecurity products, claims the damage is limited.

Co se stalo ?

V pondělním ranním oznámení společnost Avast uvedla, že její vnitřní síť byla narušena pomocí uživatelského jména a hesla pro VPN dočasný účet. Účet byl omylem ponechán otevřený a nevyžadoval druhý faktor autentizace, což poskytuje snadný přístup k počítačům Avastu.

Would your data be secure after a breach?



of enterprises say their perimeter security technology is quite effective at keeping unauthorized users out of their networks.

of enterprises aren't confident their data would be secure after a breach.

Move security beyond the perimeter to defend what's really under attack

ENCRYPT SENSITIVE DATA

- Secure data at rest and data in motion
- Secure data across cloud, virtual, and on-premises environments

OWN & SECURE ENCRYPTION KEYS

- Manage key lifecycle
- Store keys securely
- Manage cryptographic resources

CONTROL ACCESS

- Manage and ensure appropriate access to resources across enterprise environments
- Provide strong multi-factor authentication to corporate resources



The main causes of cyber threats

Main cause of attacks

IDENTITY THEFT

69%
of breach incidents
came from
identity theft



Main cause of damages

UNENCRYPTED DATA



95%
of breaches involved
unencrypted data

Dance
like no one
is watching

Encrypt like
everyone is



Some quotes from Werner:

*We need to make sure that all the pieces we are building are also **individually protected***

Encryption is the one and only tool you have to make sure you are the only one who has access to your data.

Over 116 different services within AWS with encryption enabled, 52 of them you can **bring your own keys**.

We urged you to **bring your own master keys**. Because if you do that you are the only one who decide who has access. **Not AWS**, not any foreign entity. It is you who controls access to your systems.

Dr Werner Vogels – CTO AWS

AWS Summit Berlin 2019 Keynote - February 27

<https://www.youtube.com/watch?v=loilscPHiiA>

THALES

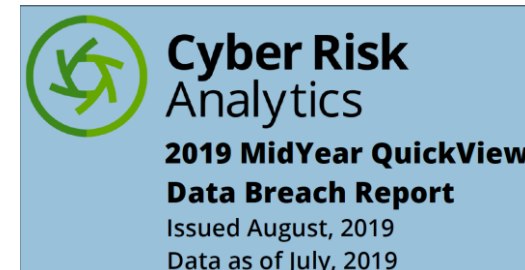


Ochrana Identit a kontrola přístupu k datům

www.thalesgroup.com



Nejčastějším cílem útoku jsou uživatelská ID a hesla



What Did Breaches Look Like So Far in 2019?

The breach trends observed in the first quarter continued and remained strong as we moved through the midway point of the year. The disclosure rate for publicly reported breaches continued its breakneck pace, jumping to over 3,800 breaches in the first six months. This represents a 50% or more increase over each of the prior four years, begging the question: why?

The interest in user credentials is the key. Troves of username and password combinations continue to become available on forums and file sharing sites while phishing for access credentials - a perennially popular method for gaining access to systems and services - has surged in recent months, proving once again that tried and true social engineering techniques still produce results for attackers.

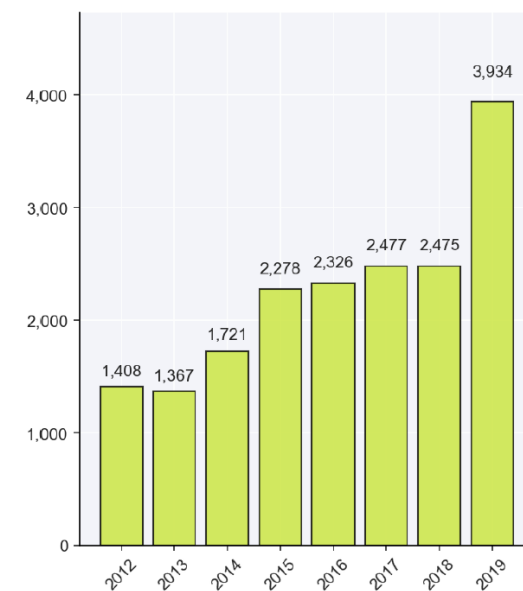


Figure 1: The number of breaches (in millions) added by Q2 in the past 8 years.

New threat example – Artificial Intelligence

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



Xi Jinping



Justin Trudeau

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

MFA

- Increase security
- Reduce Risk of Data Breach
- User Inconvenience
- Have to have Token – hw, sw, sms

SSO

- No additional security
- Risk to gain access to sensitive data
- User Convenience
- Not need to login twice

Safenet Trusted Access

- The best of both combining **SMART** SSO and MFA

SafeNet Trusted Access



1

IDENTIFY

Validate user's identity



SMS



Biometric



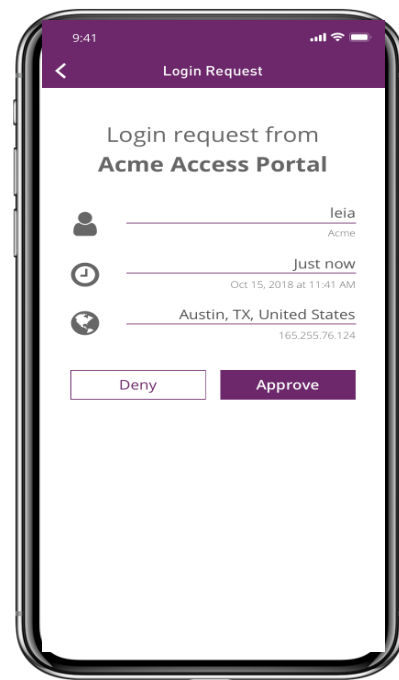
OTP Push



Hardware



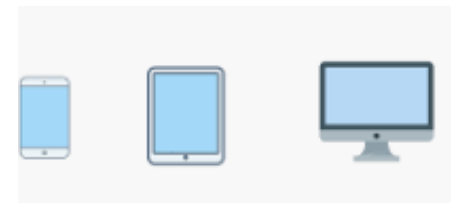
PKI



2

ASSESS

Assess which access policy should be applied



3

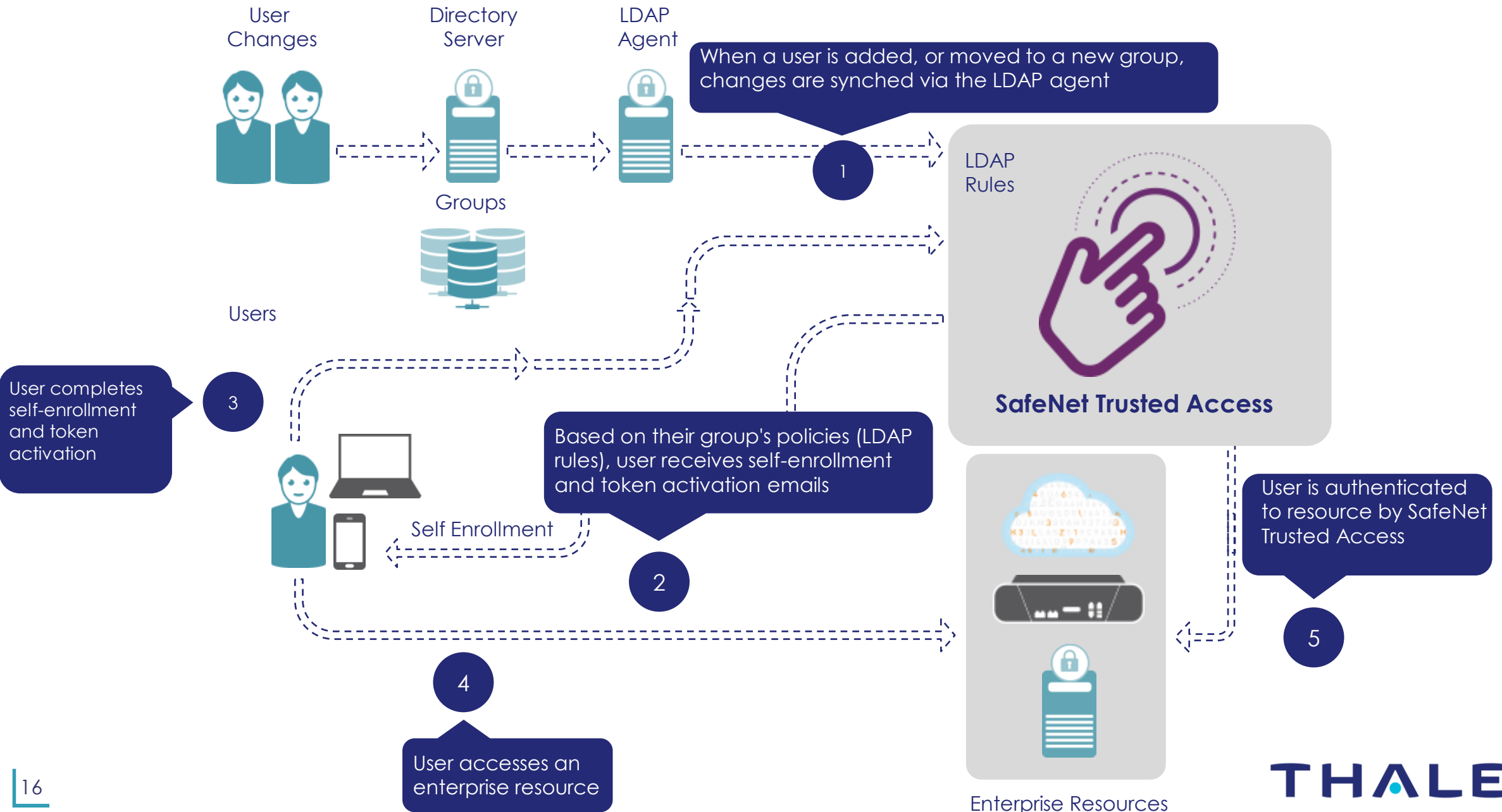
APPLY

Apply appropriate access controls, with smart single sign on

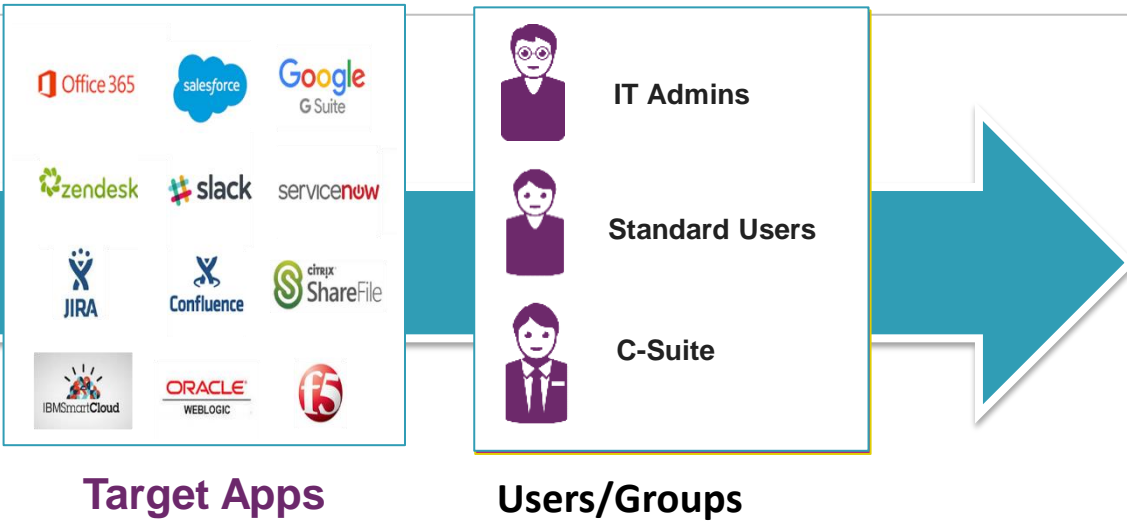


SafeNet Trusted Access allows organizations to manage access to cloud applications by validating identities, determining levels of trust and applying appropriate access controls each time the user accesses a cloud service.

Automated Workflows Triggered by User Store Changes



MFA – multifaktová autentizace s kontextem



Policy Scope

Users

All Users Any of these User Groups:

C-Suite

Applications

All Applications Any of these Applications:

Zendesk X Google G Suite X Salesforce2 X

Default Requirements

When an access attempt occurs, then access is

Granted
 Denied

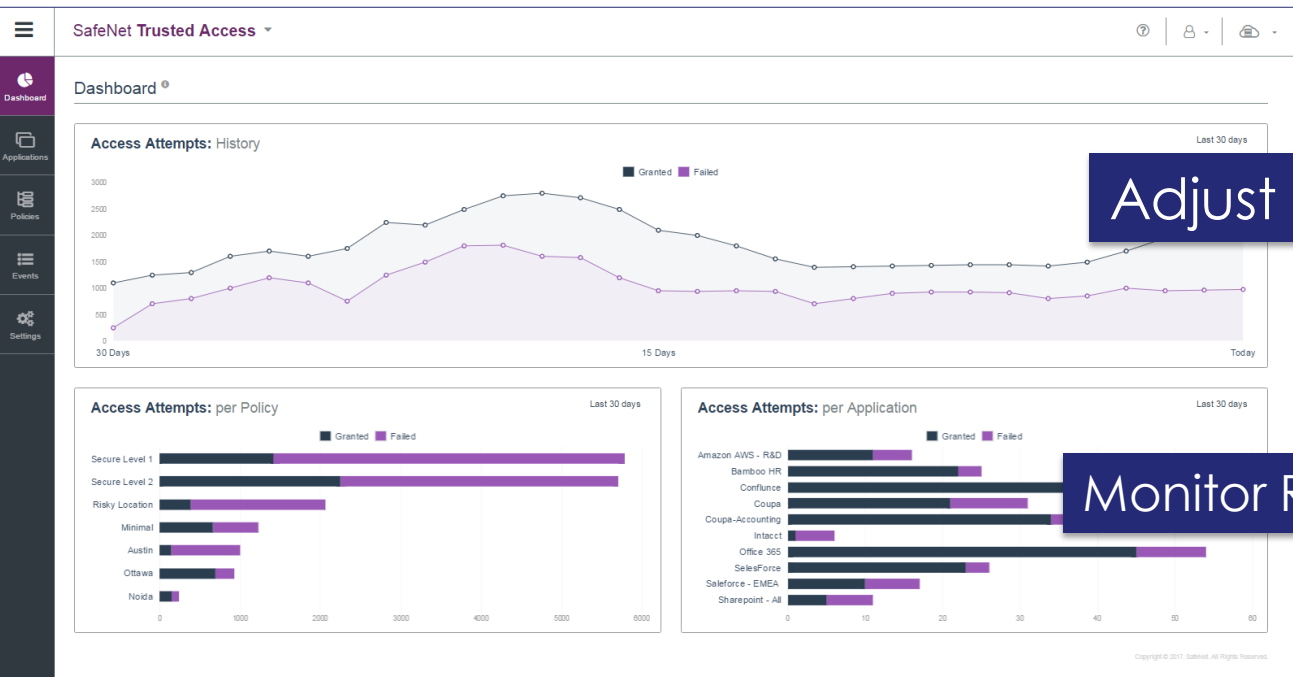
After authenticating using the factors

Password

Once per session
 Every access attempt

Token Based Authentication (OTP)

Once per session
 Every access attempt



Adjust

Monitor Risk

Define Policies

- Scenario-driven
- Compliance-focused
- Based on context & risk
- Set Auth rules by policy

CONFIDENTIAL

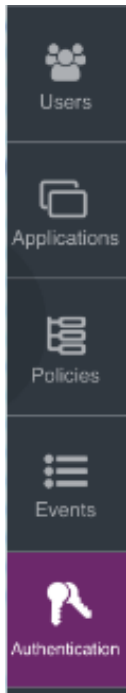
Windows Integrated Authentication

SafeNet Trusted Access can use Windows login to the enterprise

➤ As an authentication factor in the SSO session

Enhances convenience:

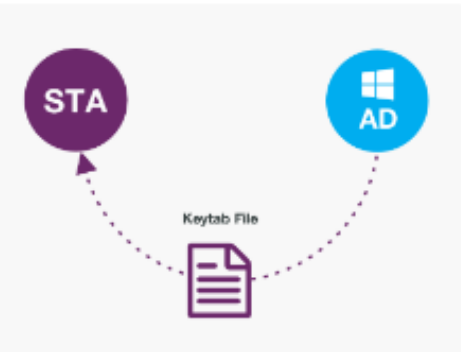
➤ No need to authenticate again after logging in with your Windows domain password



Kerberos (Domain Password Passthrough) ⓘ

Step 1: Active Directory Setup

Step 2: STA Setup



Keytab File
Upload the keytab file generated within Active Directory in Step 1.

| | |
|---|--|
| Active Directory Keytab File Hide details ^ | |
| ACTIVE DIRECTORY DOMAIN example.com.local | PRINCIPAL NAME HTTP/idp.gemalto.com@activedirectorydomain.com.local |

Client Attribute Mapping
Please select which attribute should be mapped against the username entered during authentication.

CLIENT NAME
UPN

When an access attempt occurs, then access is

- Granted**
 Denied

After authenticating using the factors

- Password** ⓘ
- Once per session**
 Every access attempt
- Allow Kerberos (Windows Password Passthrough)** ⓘ
- Token Based Authentication (OTP)** ⓘ
- Once per session
 Every access attempt

PKI/Certificate Based Authentication



PKI

Extend certificate-based authentication to cloud apps

The screenshot displays the 'SafeNet Trusted Access' console. The left sidebar contains navigation options: Dashboard, Users, Applications, Policies, Events, Authentication (highlighted), and Settings. The main content area is titled 'Certificate-Based Authentication' and includes a 'Policies and scenarios' section with a message: 'Certificate-based authentication is not yet enabled in your policies.' Below this is a 'Trusted Issuers' section containing a table with one entry:

| Issuer | Validity Period | Revocation Check |
|--------|-----------------------------|------------------|
| Acme | Jan 20, 2018 - Jan 20, 2020 | ON |

At the bottom of the 'Trusted Issuers' section, there is a '+ Add Trusted Issuer' button.

- Enforce high assurance security across cloud and web apps
- Simplify access for users with cloud and web single sign-on (SSO)
- Elevate trust with a choice of PKI and OTP-based authenticators

Thank you

Vitajte!
Welcome

Karşılama! 歡迎 dobro пожаловать

ברוך הבא ¡Bienvenido! Vítejte! Benvenuto!

Fogadtatás! Iarguralcome! ようこそ

Velkommen! Välkommen!

الدهسو الهأ! Willkommen! 환영

Bienvenue
Tervetuloa! ¡Bem vindo!