THALES | CLOUD PROTECTION & LICENSING

ifrujte citlivá data a využívejte IFA pro ochranu identit

máš Jilík, Petr Kunstat
ales CEE

trava
19

Nový Thales

Our team

80,000

employees

Around the world

68

Countries
global presence

*Revenue**

around
€19bn

A balanced revenue structure

60% Civil

40% Defence

*Based on Thales and Gemalto reported 2017 consolidated income statements.

Innovation

€1bn+

self-funded R&D* 2017

Does not include externally financed R&D.

Would your data be secure after a breach?

The Perception

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

The Reality

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

: 2017 Gemalto Data Security Confidence Index report

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

NCRYPT SENSITIVE DATA

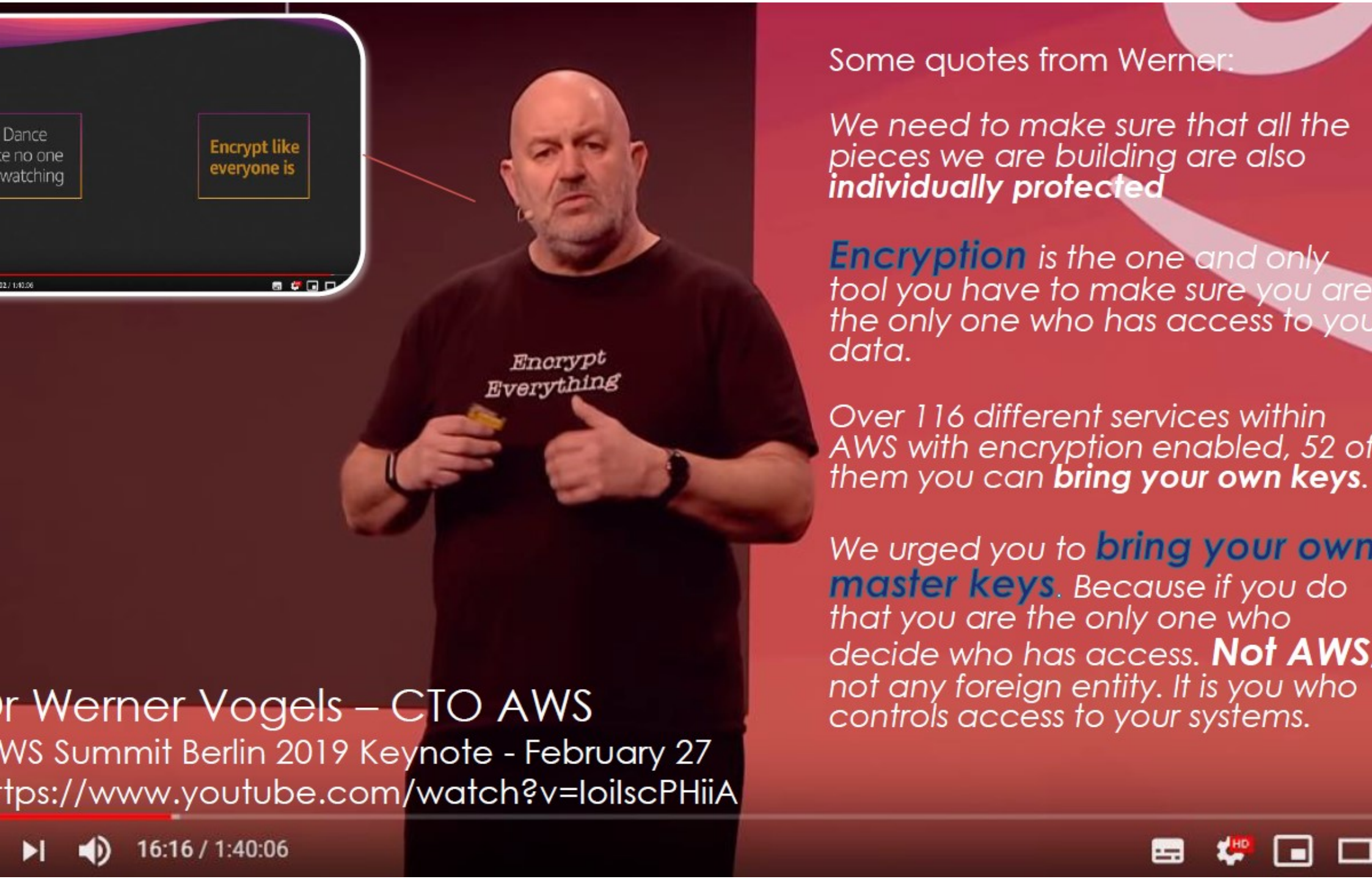
Secure data at rest and data in motion
Secure data across cloud, virtual, and on-premises environments

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


Dance
e no one
watching
Encrypt like
everyone is
Encrypt
Everything
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 you 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.
r Werner Vogels – CTO AWS
WS Summit Berlin 2019 Keynote - February 27
tps://www.youtube.com/watch?v=IoilscPHiiA
16:16 / 1:40:06

THALES

Ochrana Identit a kontrola přístupu k datům

.thalesgroup.com

The main causes of cyber threats

Main cause of attacks

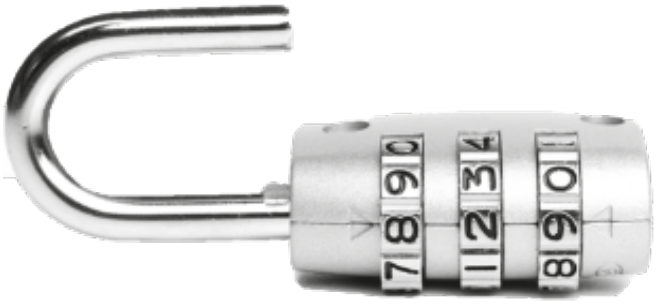
IDENTITY THEFT

69%

of breach incidents came from identity theft

Main cause of damages

UNENCRYPTED DATA



95%

of breaches involved unencrypted data

Data a jejich hodnota na trhu

Cyber Risk Analytics

2019 MidYear Quick
Data Breach Report
Issued August, 2019
Data as of July, 2019

What Did Breaches Look Like So Far in 2019?

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

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

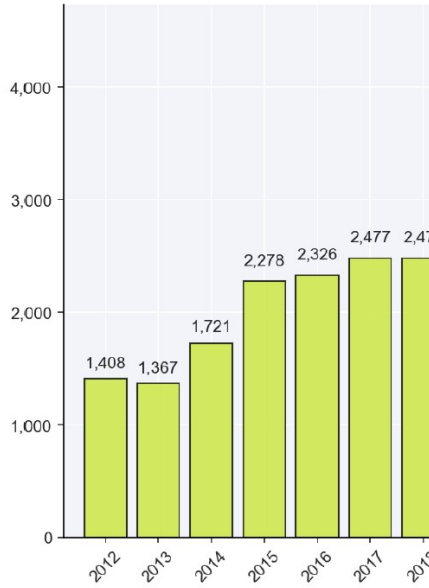
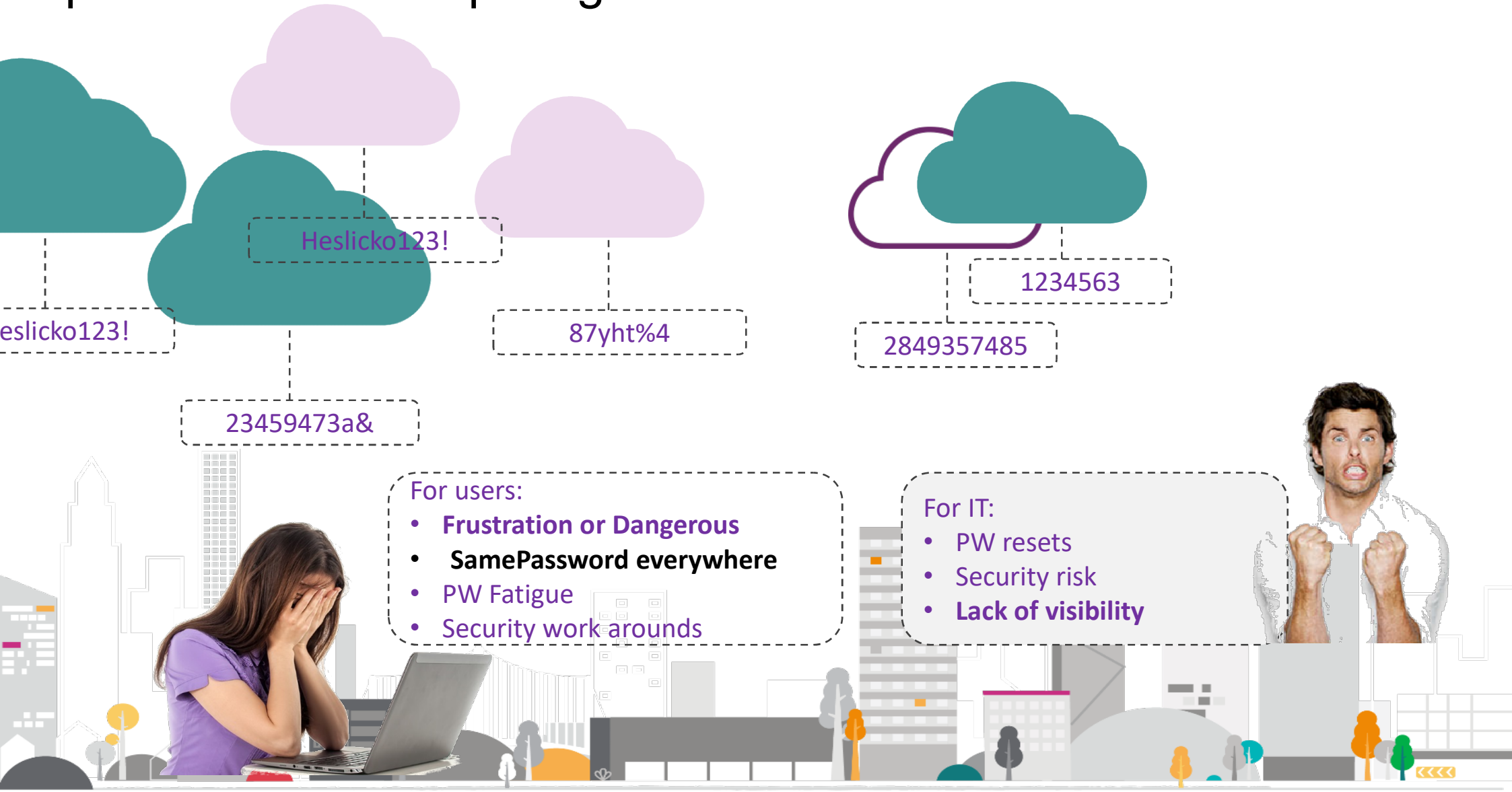
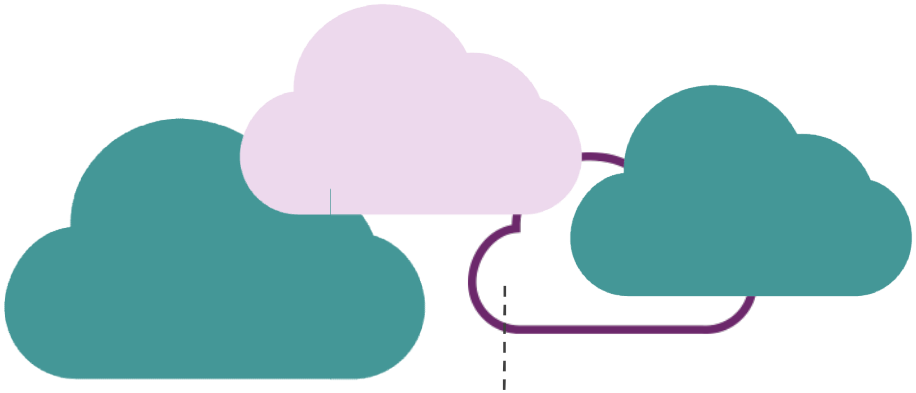


Figure 1: The number of breaches (in millions) added by Q2 in th

Co přinesl Cloud computing



Co řeší SSO a co neřeší

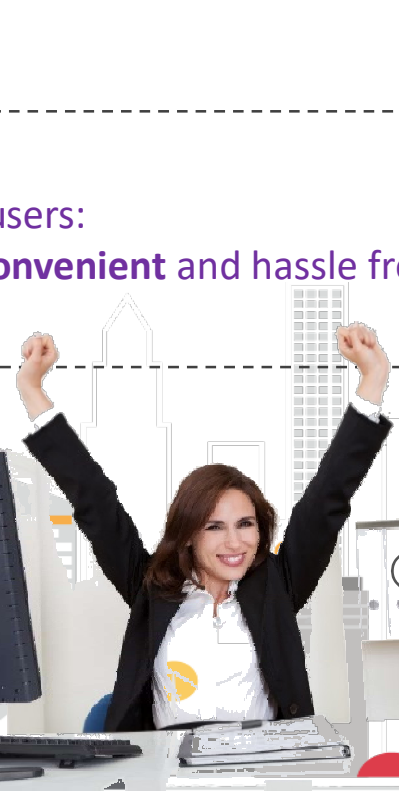


One Credential

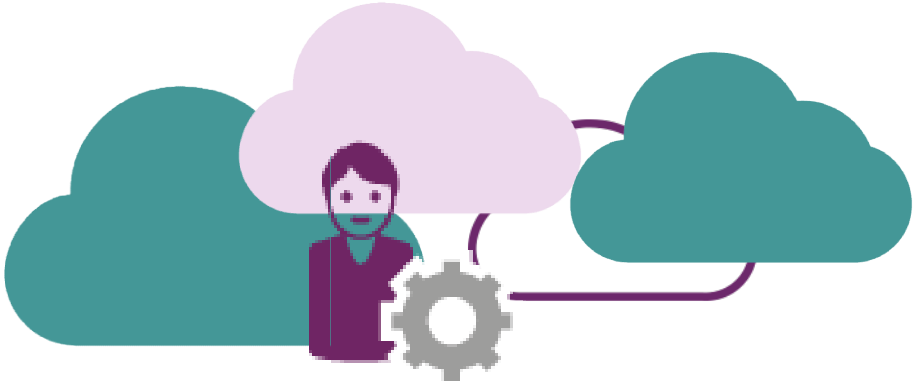
sers:
onvenient and hassle free

Not Ideal for IT:

- Security risk: if the credential is **compromised**, all apps will be vulnerable
- Visibility: Can't track which apps are being accessed and when



Access Management – řízení přístupu k assetům : SSO + IT Control
Win-Win pro uživatele a IT



sers:
uthenticate once and step up
nly when required

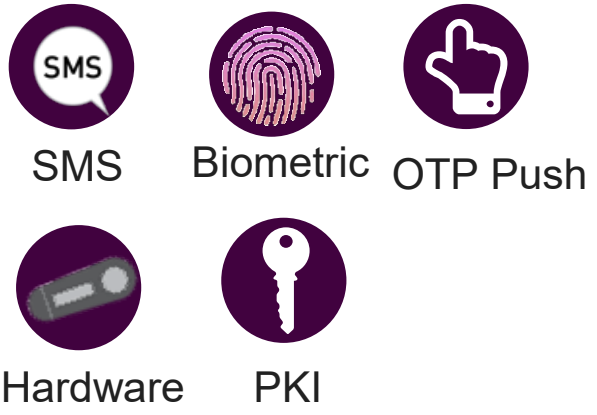
For IT:
- Set the access policy per cloud app
- **Get visibility** on who is accessing what, when and how
- Maintain security, reduce PW workarounds

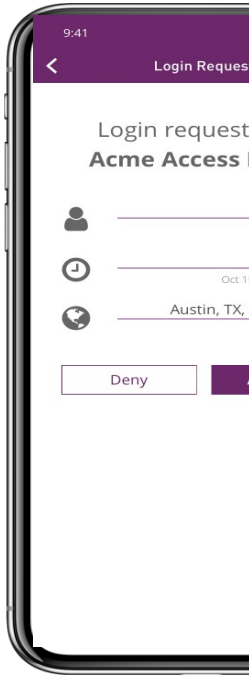
SafeNet Trusted Access

1

IDENTIFY

Validate user's identity

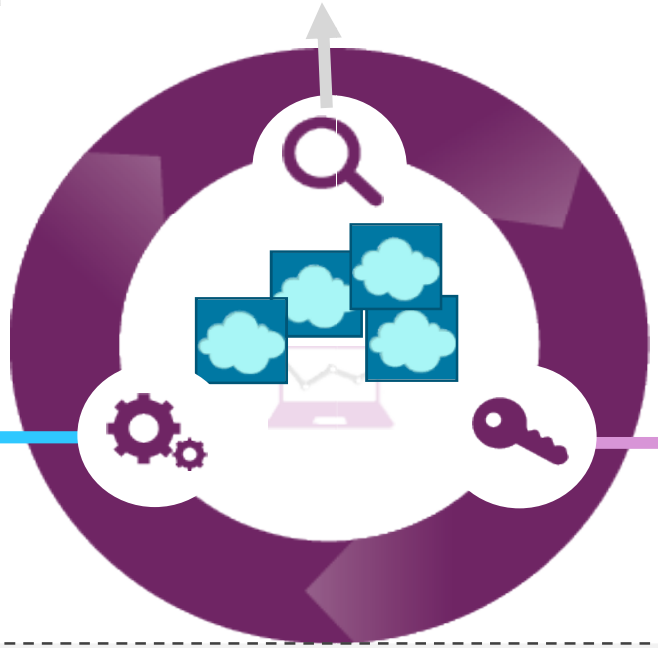




3

APPLY

Apply appropriate access controls, with smart single sign on



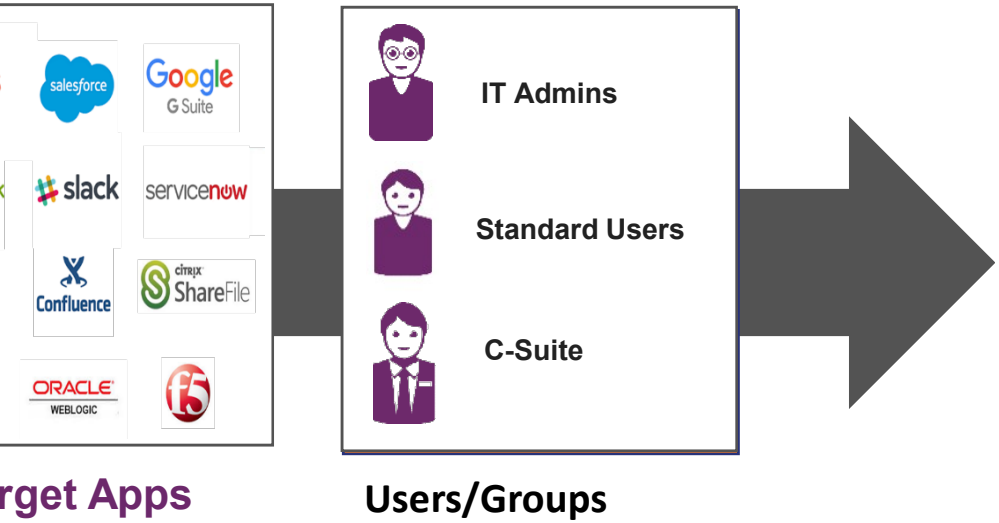
2

ASSESS

Assess which access policy should be applied

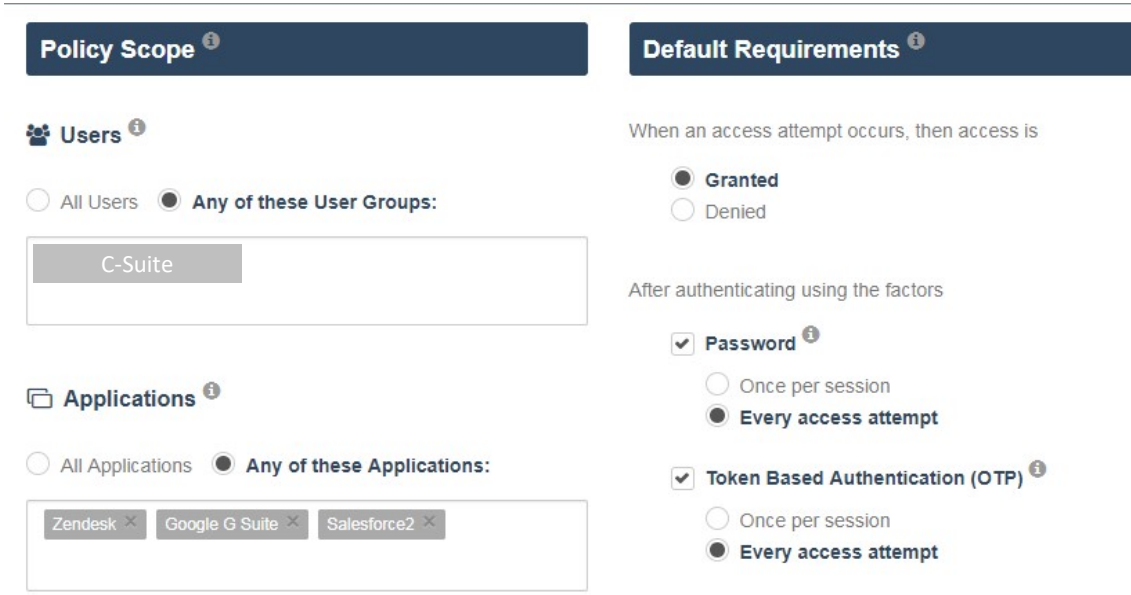
afeNet Trusted Access allows organizations to manage access to cloud applications by validating identities, determining levels of rust and applying appropriate access controls each time the user accesses a cloud service.

MFA – multifaktová autentizace – pro koho, kdy, kde ?



rget Apps

Users/Groups



Adjust

Monitor Risk

Define Policies

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

gemalto

THALES | CLOUD PROTECTION & LICENSING FORUM

hank you