



kreslenyvitp.cz

„Zdravý určitě nejste, protože
dnes už je medicína tak pokročilá,
že zdravý člověk neexistuje.“



Maximalizujte ochranu svých dat a uživatelský komfort.

Petr Kunstat
Cloud Protection & Licensing
CEE Consultant



Thales Group Focuses on Intelligent Systems



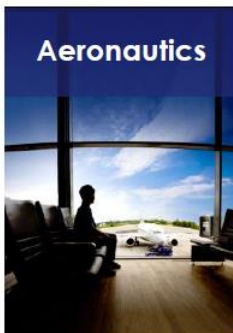
Data
Protection



Identity & Access
Management



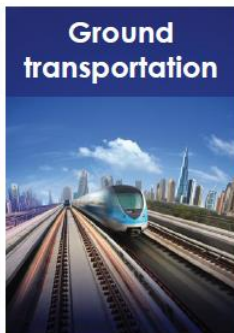
Software
Monetization



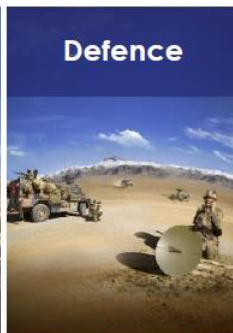
Aeronautics



Space



Ground
transportation



Defence



Security



Massive
Transformation
Cloud Computing

Over **80,000**
employees



1 bn € 
Self-funded R&D*
* Does not include externally financed R&D

68
Countries
Global presence



Sales in 2018 **19 bn €** 



Trends and real cases from the field

Why do we need a Modern Security solution



The main causes of cyber threats

Main cause of attacks

IDENTITY THEFT

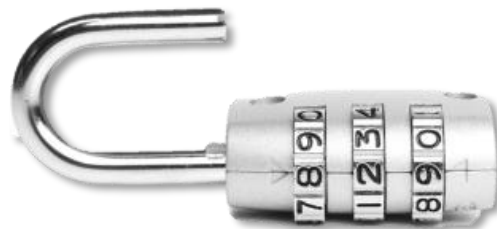
69%

of breach incidents came from identity theft



Main cause of damages

UNENCRYPTED DATA



95%

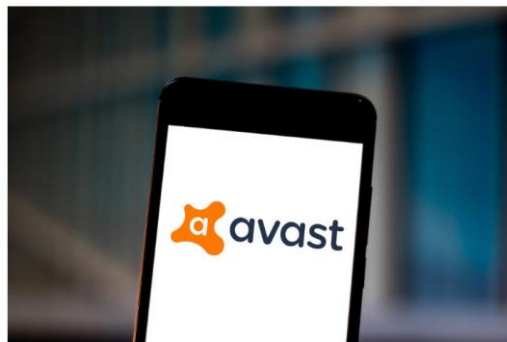
of breaches involved unencrypted data

Mistakes in a security design

Avast

Zatím neznámým a podle všeho velmi zkušeným hackerům se podařilo napadnout interní síť antivirové společnosti Avast. Začátky pokusů o útok se expertům Avastu podařilo zpětně vystopovat až do 14. května tohoto roku. Útok samotný však byl odhalen až 23. září.

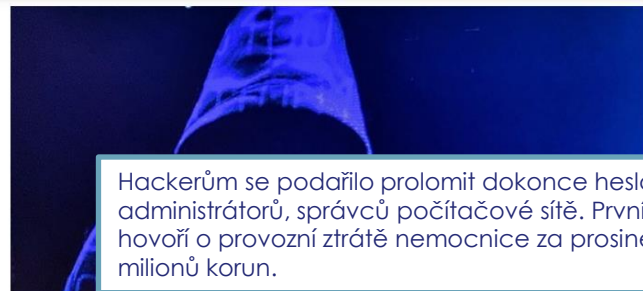
Hackeři **zneužili přístupová práva jednoho ze zaměstnanců**. Jejich záměrem pravděpodobně bylo infikovat malwarem (škodlivým softwarem) populární utilitku CCleaner, kterou Avast od roku 2017 vlastní.



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.

Benesov hospital



Hackerům se podařilo prolomit dokonce hesla IT administrátorů, správců počítačové sítě. První odhady škod hovoří o provozní ztrátě nemocnice za prosinec ve výši 40 milionů korun.

ilustrační snímek | foto: @k3r3n3, Jan Kužník, Technet.cz

Provoz benešovské nemocnice zcela narušil počítačový virus, který v noci napadl nemocniční počítačový systém. Nelze spustit žádný přístroj včetně počítačové sítě. Nemocnice musí rušit i plánované operace. Lékaři odbavují pacienty postaru, jako „před příchodem počítačů“.

T-Mobile

Over **1.5 million customer records** at T-Mobile Czech Republic were stolen by one of its employees, according to local media. **TMCZ 2016**

THALES

THALES



Solution

www.thalesgroup.com



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



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 SEP

- 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



THALES

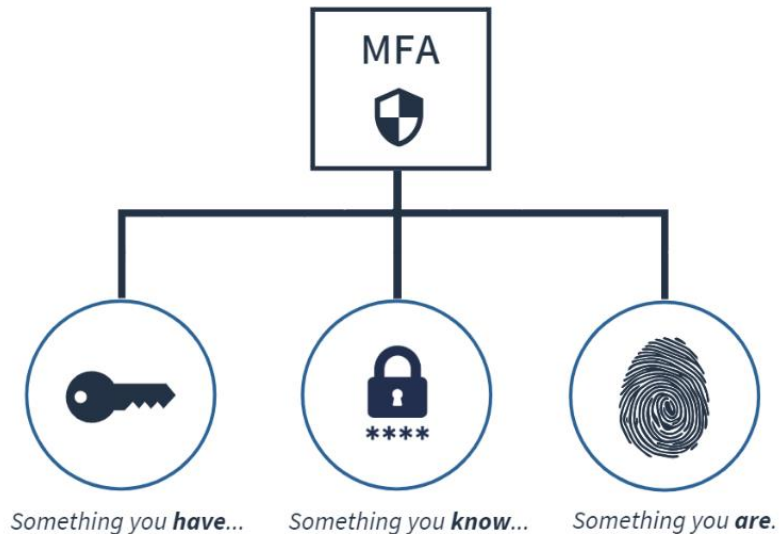


Secure access to your sensitive data & IT resources

www.thalesgroup.com



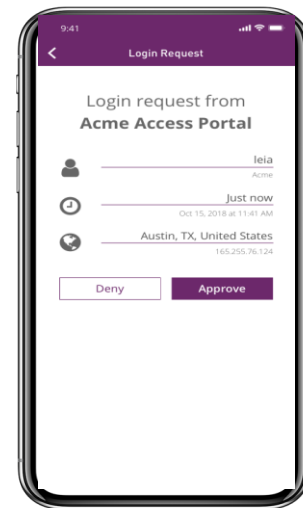
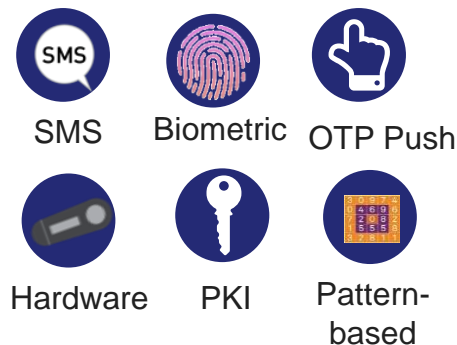
Safenet Trusted Access = MFA + Smart SSO + Access Management



SafeNet Trusted Access



1
IDENTIFY
Validate user's identity



2
ASSESS
Assess which access policy should be applied

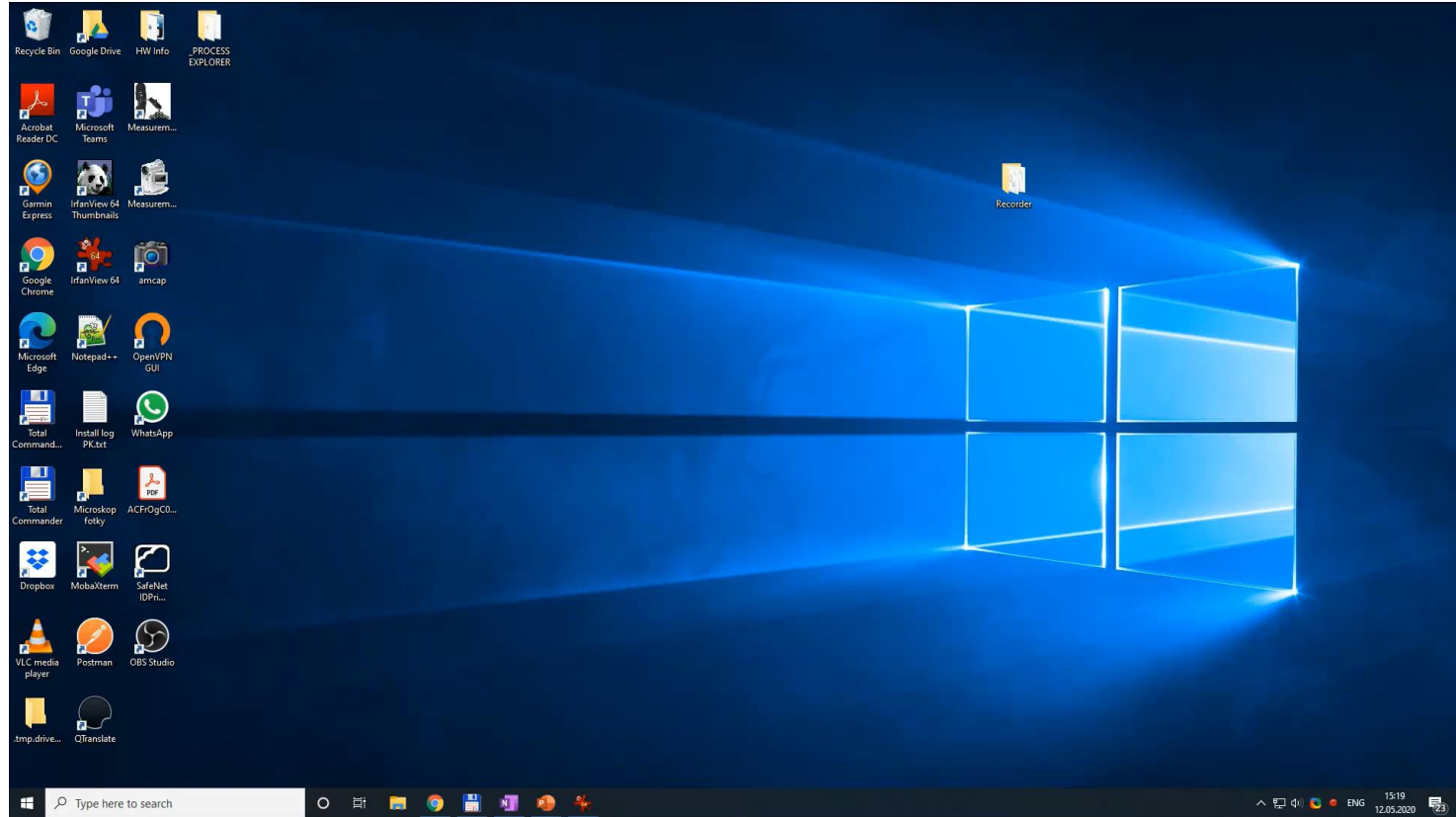


3
APPLY
Apply appropriate access controls, with smart single sign on



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.

Demo Windows Desktop



SafeNet Trusted Access

Universal authentication methods



Password



Kerberos



OTP Push



Hardware



3rd Party



SMS



eMail



PKI



Pattern-based



Passwordless



Biometric



Google
Authenticator

- Utilize the MFA schemes already deployed
- Extend PKI authentication to the cloud
- Offer the appropriate level of assurance
- Offer convenience with Passwordless authentication

Pattern-based Authentication : When you forget your mobile at home

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

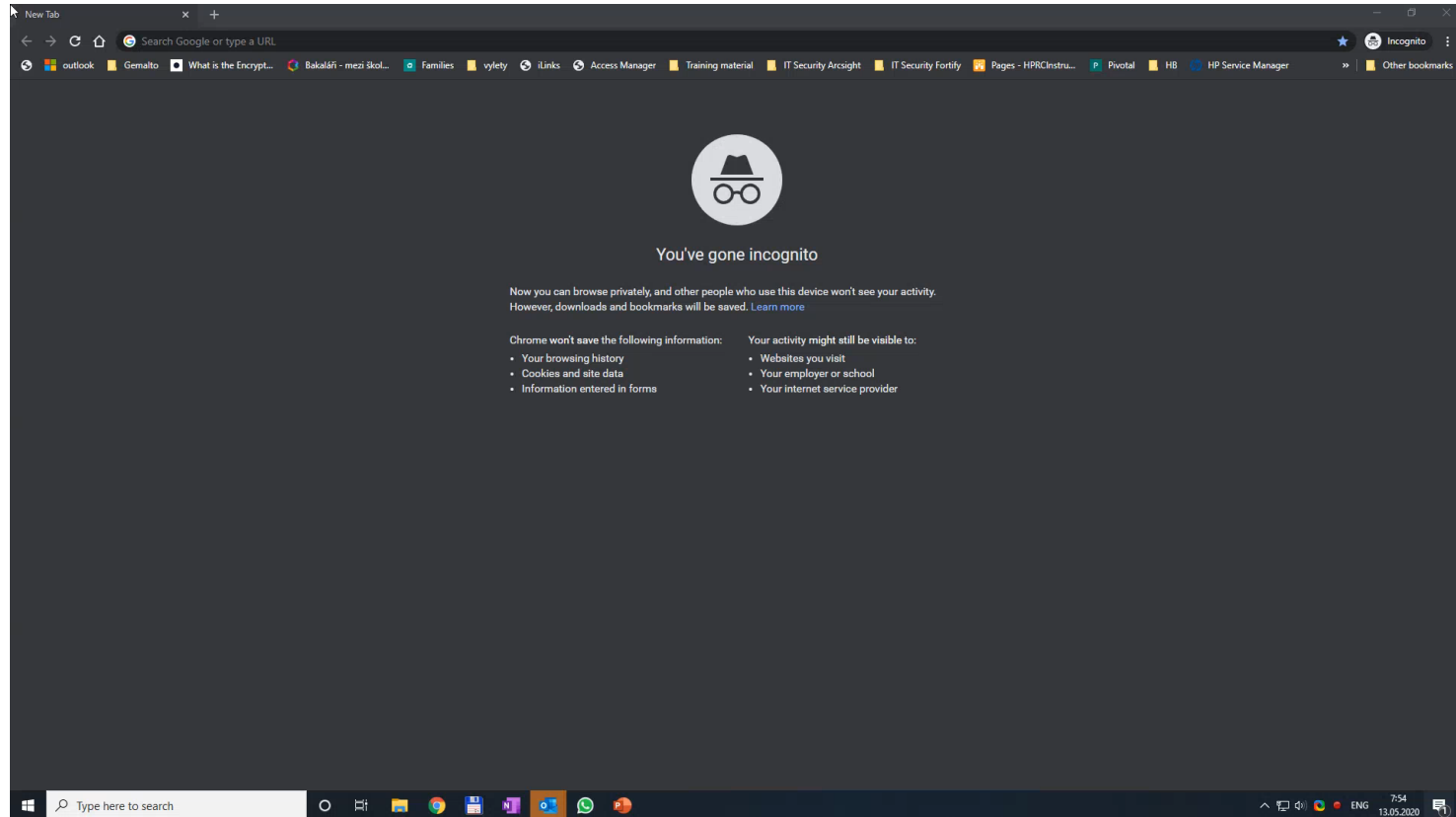
1	5	9	6	6
7	7	8	9	4
2	3	3	8	2
0	5	0	1	2
1	4	5	0	3

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

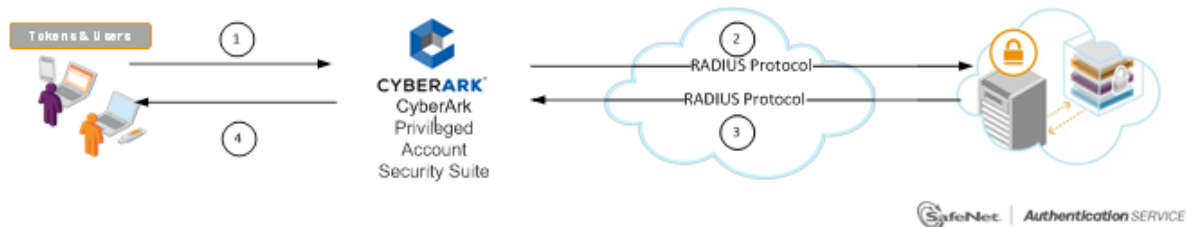
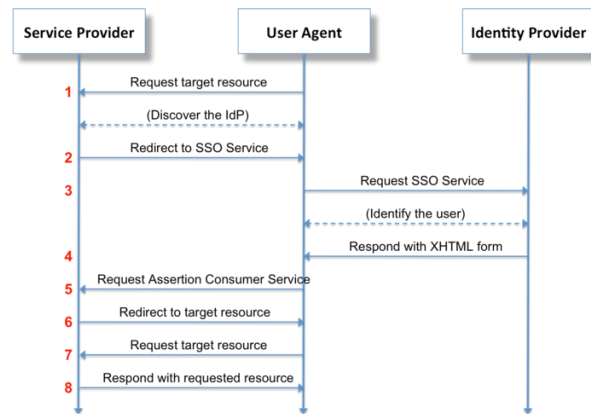
4 In the next login, the same PIP will produce a new OTP

Demo O365



How to integrate your IT applications with STA

- SAML 2.0/OIDC
- Agents – Logon, ADFS, AD
- Radius
- REST/SOAP API for administration



THALES

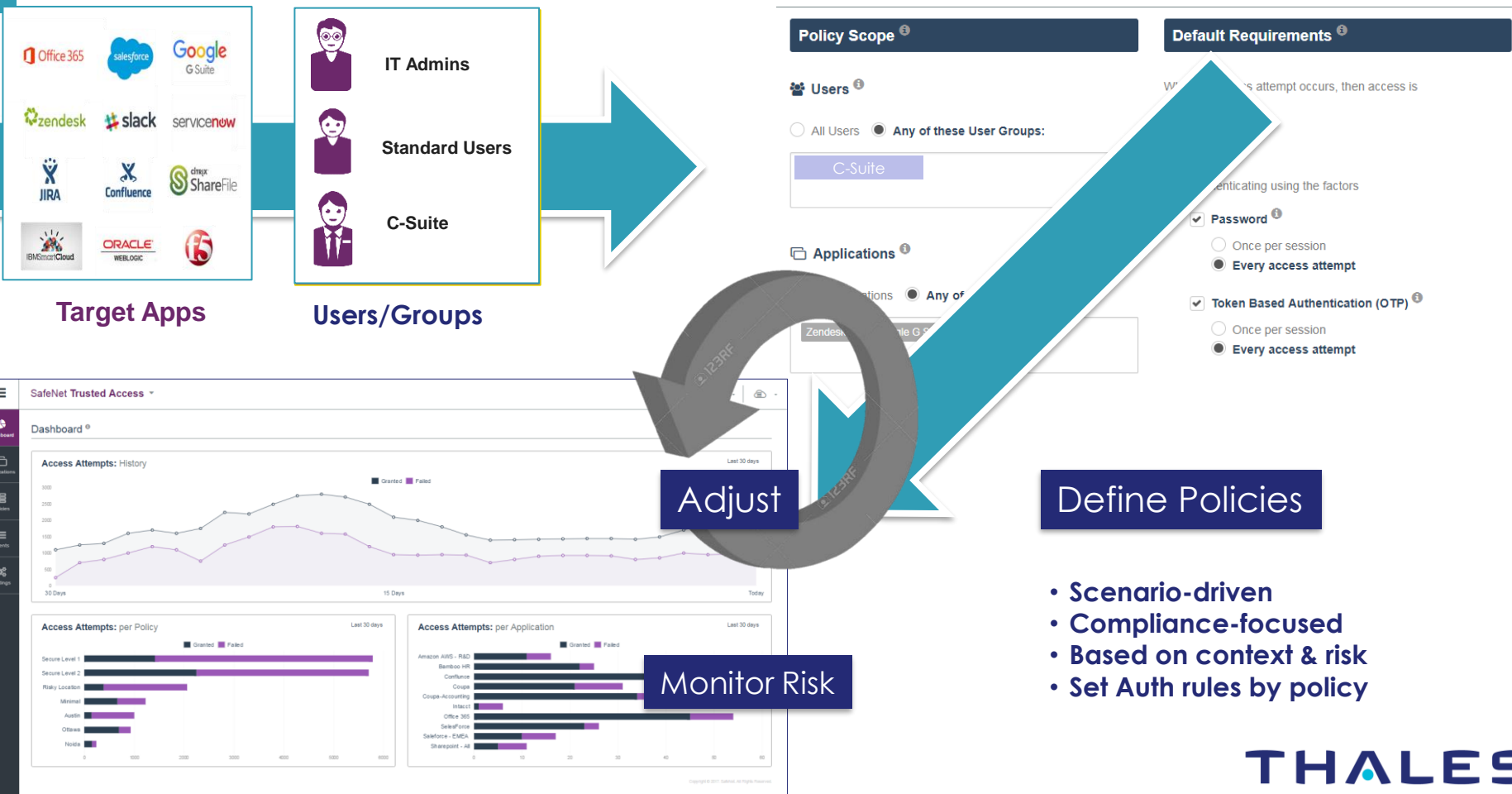


Flexible & Powerful Policy Engine

www.thalesgroup.com



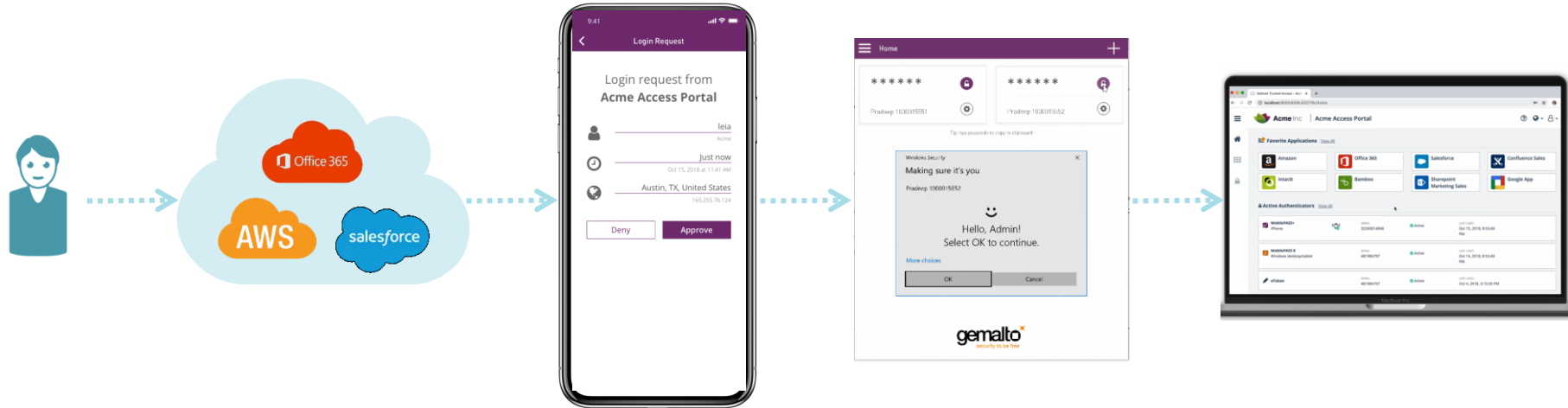
Manage risk through scenario-based policies



Passwordless Authentication

Strong authentication without the need to remember a password

Combination of Push OTP with PIN (Windows Hello / Biometric on iOS or Android)



STA Policy is configured for OTP only, without password; Biometric PIN serves as 2nd factor

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

Users

Applications

Policies

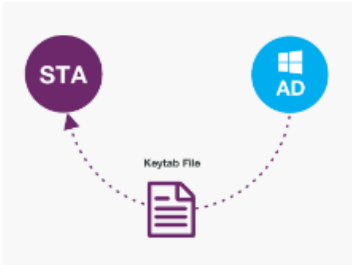
Events

Authentication

✓ Kerberos (Domain Password Passthrough) ⓘ

Step 1: Active Directory Setup


Step 2: STA Setup



The diagram illustrates the relationship between the Security Token Agent (STA) and Active Directory (AD). A purple circle labeled 'STA' is connected by a dashed line to a blue circle labeled 'AD'. A document icon labeled 'Keytab File' is positioned between them, with arrows pointing from both STA and AD to it, indicating that the keytab file is generated within AD and used by the STA.

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/ldap.gemalto.com@activedirectorydomain.com.local

Client Attribute Mapping

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

CLIENT NAME

UPN

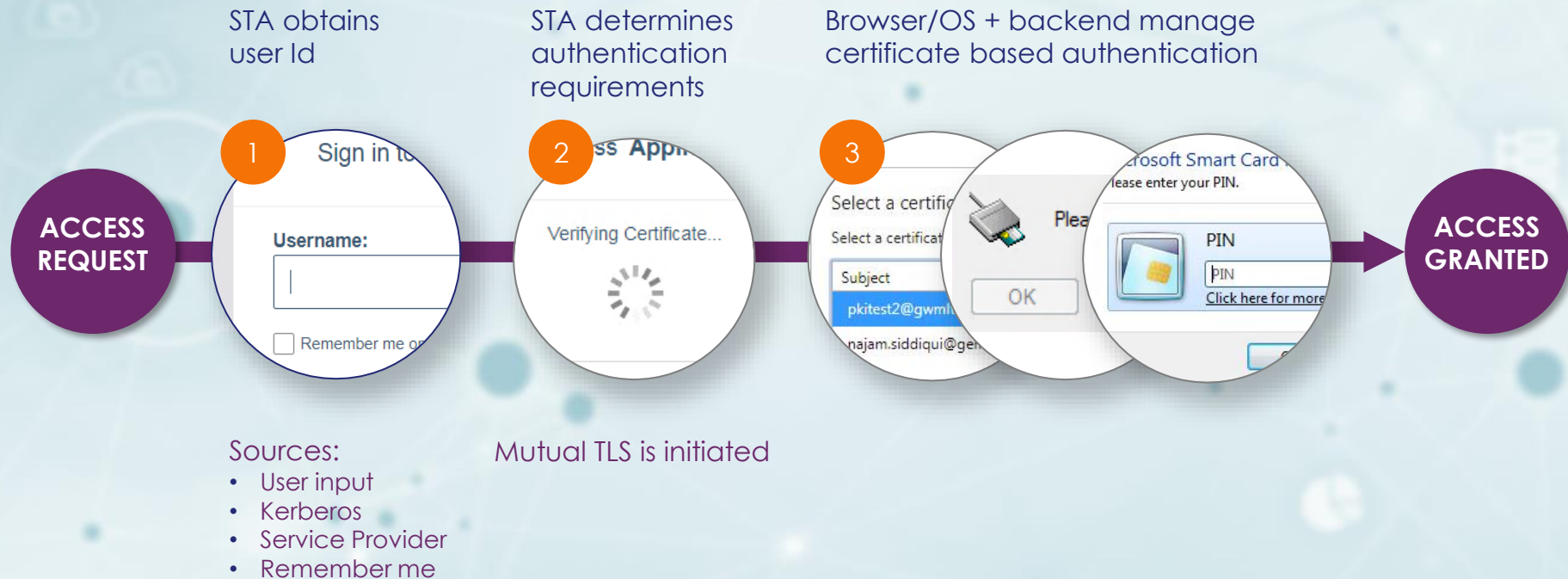
When an access attempt occurs, then access is

- ☒ **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**

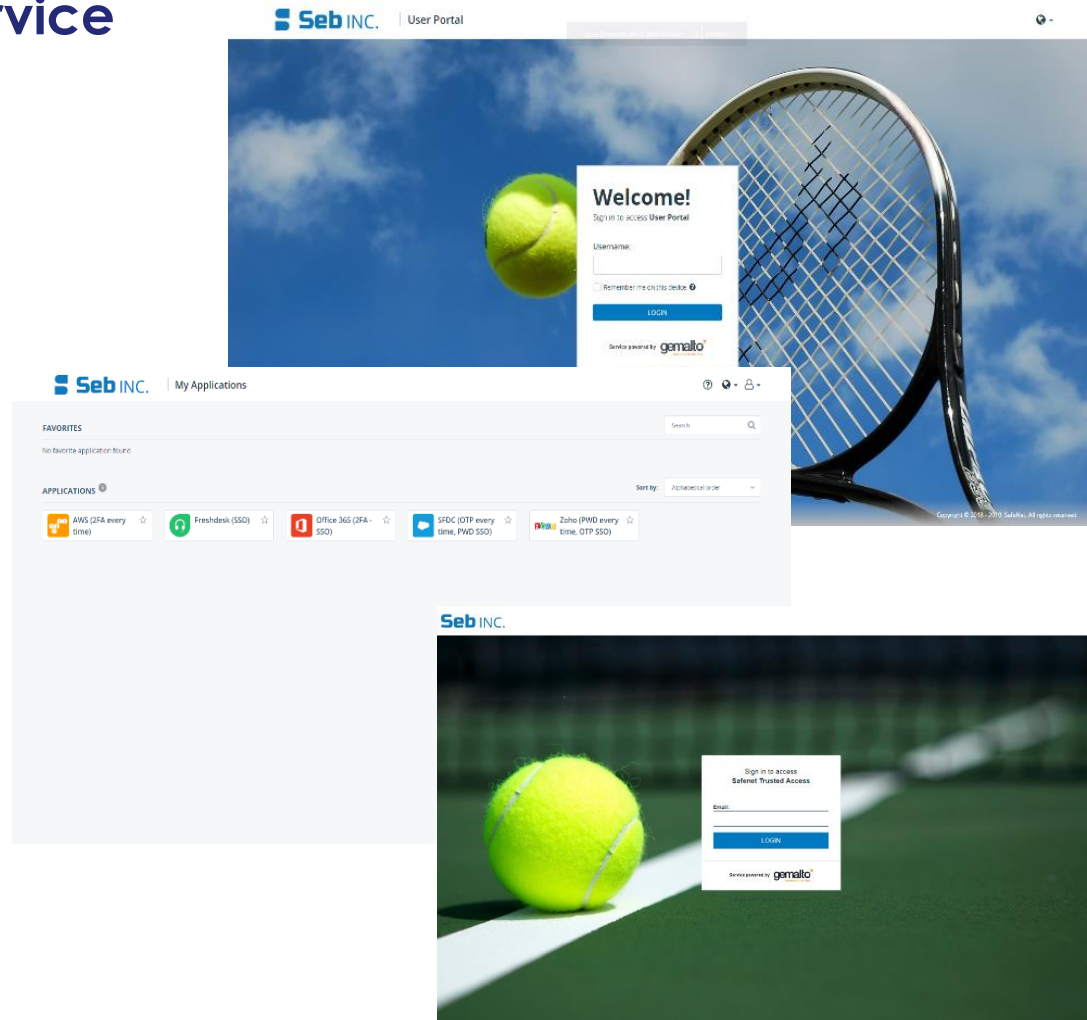
Certificate Based Authentication Flow



Fully Customizable SaaS Service

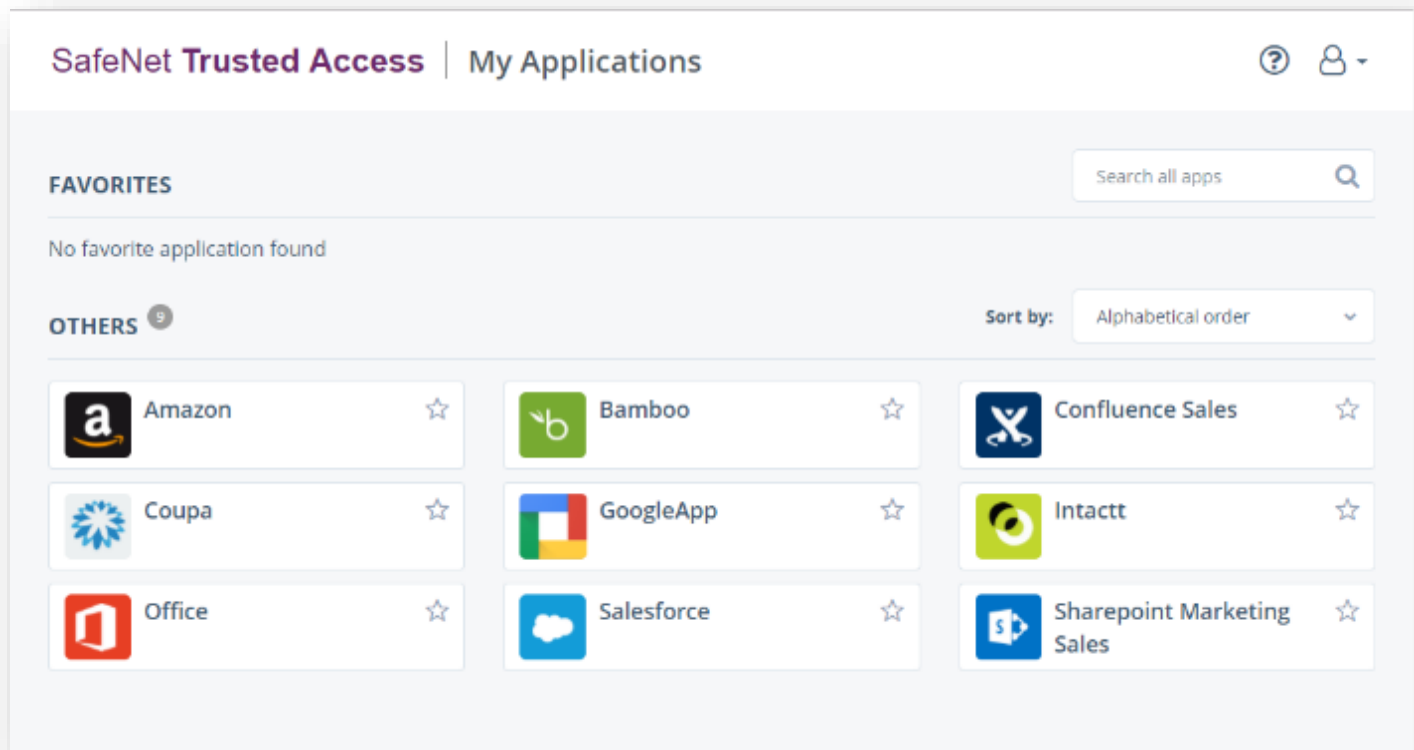
Brand your own service

- SSO Portal
- Self-Service Portal
- Portal URLs
- SMS Messages and Emails
- Token branding options



Launch all apps from a central user portal

Trigger Single Sign On by logging into the user portal



Automated User Synchronization

- **Synch any user store with SafeNet Authentication Service**

- **Periodic synching every 20 minutes**

- Non-intrusive
- Secure encrypted communications
- Multi-domain support (e.g. jill@abc.com, bob@xyz.biz)

- **Supports any user store**

- SQL
- LDAP
- AD
- ODBC
- Lotus
- Novell
- Other via custom field mapping

Integrate user store once, and trigger automated workflows throughout



Visibility into who is accessing which app, when and how

Access event dashboards and unified audit trail

Hundreds out-of-the box templates

Automated delivery

Prove compliance

Integrates with SIEMs (CA, IBM QRadar,...)

All logs can be exported

SafeNet Trusted Access

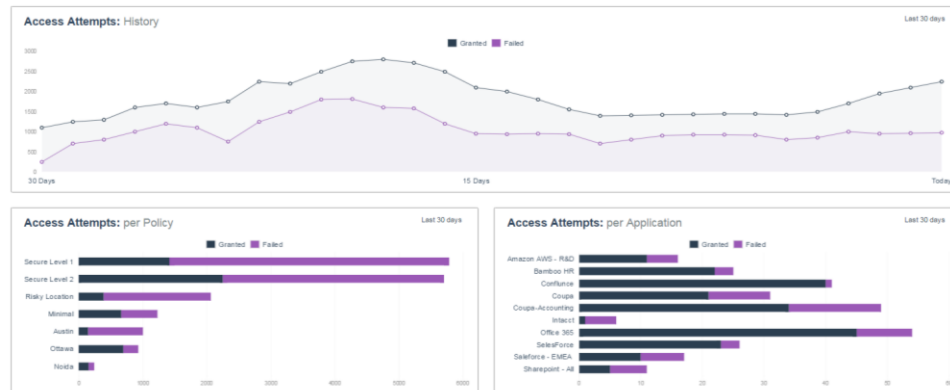
Events

Access Logs Audit Logs

START DATE: May 3, 2018 END DATE: May 7, 2018

Timestamp	User ID	Application	Policy	Scenario	Result	Reason	Credentials	IP Address
May 3, 2018, 8:26:40 PM	Dennis	User Portal	-	-	Failed	Failed to collect context data	-	31.161.187.105
May 3, 2018, 8:22:50 PM	Dennis	User Portal	UserPortal Access	-	Failed	Invalid credentials	Password, OTP	31.161.187.105
May 3, 2018, 8:22:33 PM	Dennis	User Portal	UserPortal Access	-	Failed	Invalid credentials	Password	31.161.187.105
May 3, 2018, 8:22:26 PM	Dennis	User Portal	UserPortal Access	-	Failed	Invalid credentials	Password	31.161.187.105
May 3, 2018, 8:10:40 PM	Guido2	NetScaler Gateway	Low Risk Users	-	Success	-	OTP (Session)	31.161.136.8
May 3, 2018, 8:10:18 PM	Guido2	Salesforce2	Low Risk Users	-	Success	-	OTP (Session)	31.161.136.8
May 3, 2018, 8:10:10 PM	Guido2	User Portal	UserPortal Access	-	Success	-	Password, OTP	31.161.136.8
May 3, 2018, 8:09:02 PM	Guido1	AWS	High Risk Users - AWS	-	Denied	Denied per policy	-	31.161.136.8
May 3, 2018, 8:08:40 PM	Guido1	AWS	High Risk Users - AWS	-	Denied	Denied per policy	-	31.161.136.8
							Password, OTP	31.161.136.8

Dashboard



IDPrime Virtual & FIDO2

IDPV

Thales Security Solution for

- PKI authentication
- Data encryption
- Digital signing



Without a
physical
piece of
hardware



FIDO

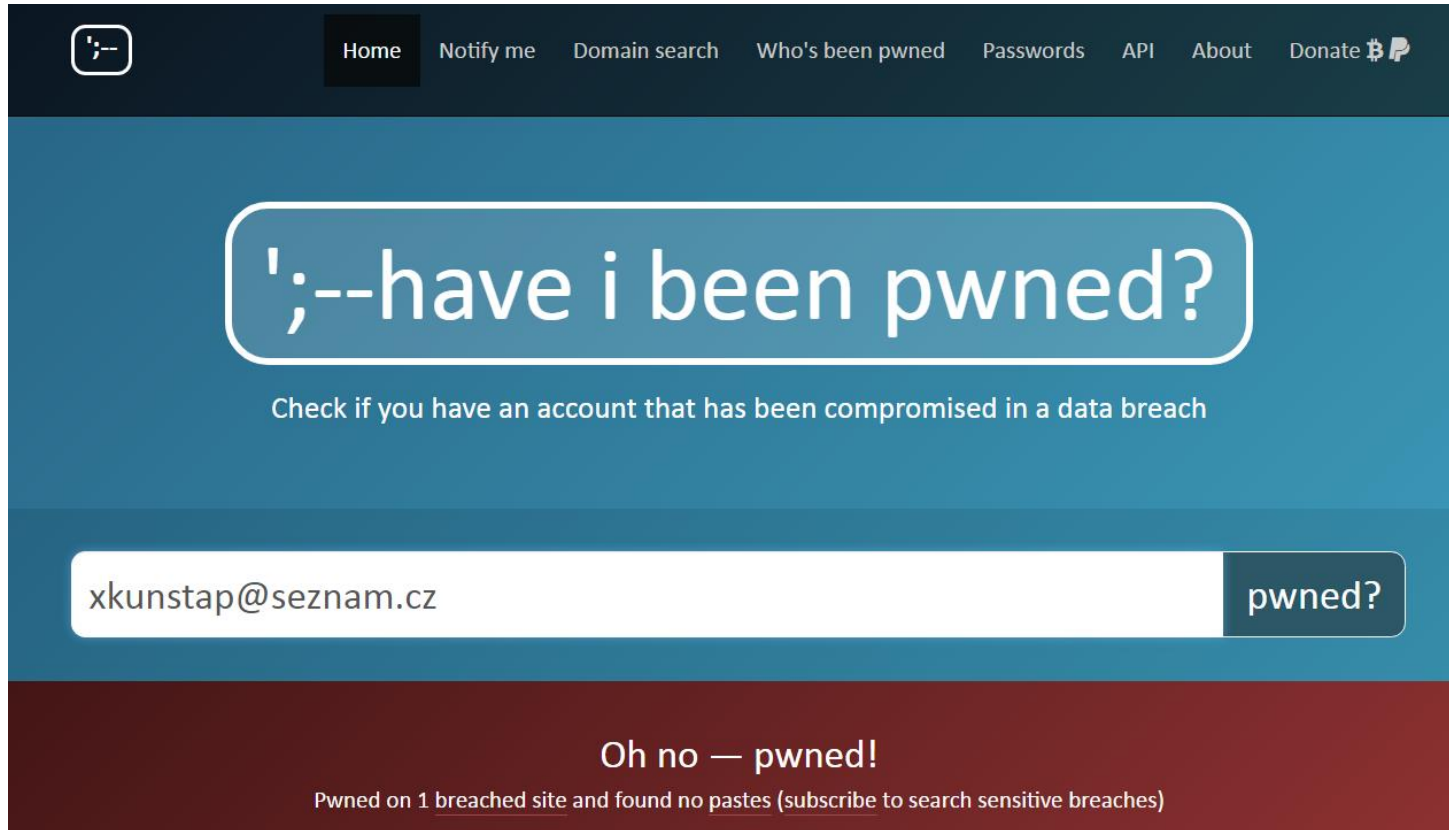


Passwordless



THALES

Do you dare to check?



The screenshot shows the homepage of the 'have i been pwned?' website. The navigation bar at the top includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'have i been pwned?' with a subtitle 'Check if you have an account that has been compromised in a data breach'. A search input field contains the email 'xkunstap@seznam.cz' and a 'pwned?' button. The result section, on a dark red background, displays 'Oh no — pwned!' and 'Pwned on 1 [breached site](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)'.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

xkunstap@seznam.cz pwned?

Oh no — pwned!

Pwned on 1 [breached site](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)