

THALES



Access Management

cpl.thalesgroup.com



Dal fondo degli oceani alle profondità dello spazio e del cyberspazio



N. 1
al mondo nella protezione dei dati

N. 2
al mondo nei sistemi satellitari ad uso civile

N. 2
al mondo nella segnaletica ferroviaria

N. 1
al mondo nella gestione del traffico aereo

N. 2
al mondo nell'intrattenimento di bordo

N. 3
al mondo negli avionici commerciali

N. 1
fornitore europeo di sensori avanzati

N. 1
al mondo nelle soluzioni aeroportuali sicure e intelligenti



Oltre **80.000** dipendenti



68 Paesi
Presenza globale



1 miliardo di €
Ricerca e sviluppo autofinanziato*

*Non include ricerca e sviluppo finanziato da fonti esterne



Vendite nel 2019
19 miliardi di €

Thales Cloud Protection & Licensing

Le nostre
soluzioni



N. 1
al mondo negli HSM
per uso generale

N. 1
al mondo negli HSM
per pagamenti

N. 1
al mondo negli
HSM cloud

N. 1
al mondo nella
crittografia dei dati

N. 1
al mondo nella
gestione delle
chiavi

N. 2
al mondo
nell'autenticazione
basata sul cloud

N. 1
al mondo nella
protezione software

N. 1
al mondo nella
vendita di licenze
software



Oltre **2.600**
dipendenti



Presenza in 25
Paesi



750 tecnici in
tutto il mondo



30.000 clienti in
tutto il mondo

I marchi a cui ci affidiamo per proteggere la nostra privacy utilizzano Thales

Le tecnologie e i servizi di Thales aiutano a proteggere **oltre l'80%** delle transazioni a livello mondiale, nonché le informazioni aziendali e governative più preziose

Autenticare

Incorporiamo software sicuro in dispositivi e oggetti per autenticare persone e cose

Proteggere

Eseguiamo software sicuro su piattaforme per proteggere e crittografare i dati attraverso le reti

Cause principali di attacco

FURTO CREDENZIALI

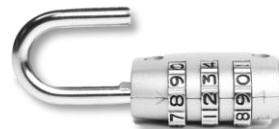
69%

dei data breach è causato dal furto delle credenziali



Cause principali di danno

DATI NON CIFRATI



95%

dei data breach avvengono a causa di dati non cifrati

EasyJet vittima di maxi-attacco hacker, sottratti dati di 9 milioni di clienti


EasyJet è
consenti
milioni c

☰ MENU | 🔍 CERCA

la Repubblica

ABBONATI

QUOTIDIANO **R**

ACCEDI 

☰ MENU | 🔍 CERCA

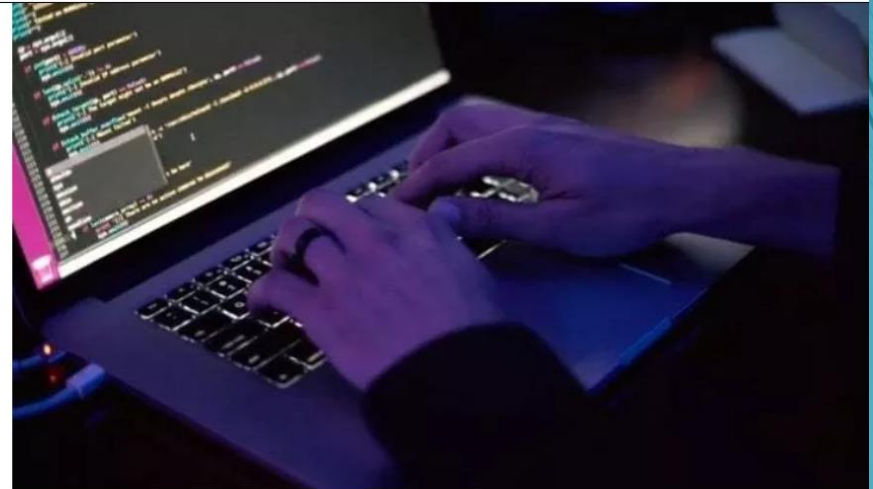
LinkedIn viola nuovo: in vendita online i dati degli iscritti

di Emanuele Capone

Rubate informazioni su LinkedIn di milioni di utenti, indirizzi (mail e fisici), dati di posizionamento, account e username su altri social network, sesso, datore di lavoro e pure stipendio di 700 milioni di iscritti

Quarantamila computer dell'azienda di software Kaseya a rischio per l'attacco hacker

L'offensiva a base di ransomware viene attribuita dagli esperti al gruppo REvil, fino a 150 mila dollari i riscatti chiesti



THALES

Perché l'AM tradizionale è un problema?

Le password danneggiano l'esperienza dell'utente ed «ostacolano» la sicurezza



L'adozione di tecnologie emergenti offusca i «confini aziendali legacy»

I controlli di sicurezza tradizionali non sono adeguati per proteggere i remote workloads ed i dati nel cloud

Credenziali compromesse: scenario

Credential Stuffing

- 20+ milioni di account sondati ogni giorno

Phishing

- 0.5% di tutte le email in entrata

Password spray

- 16% di tutti gli attacchi

Il costo medio di un record rubato è di \$ 148 e il costo totale derivante da una violazione dei dati è in media di \$ 3,86 milioni





**Soltanto
il 22%**

degli intervistati ha affermato di essere molto preparato a gestire i rischi di sicurezza causati dalla pandemia.



81%

teme che il lavoro da remoto dai dipendenti apporti rischi / minacce alla sicurezza.

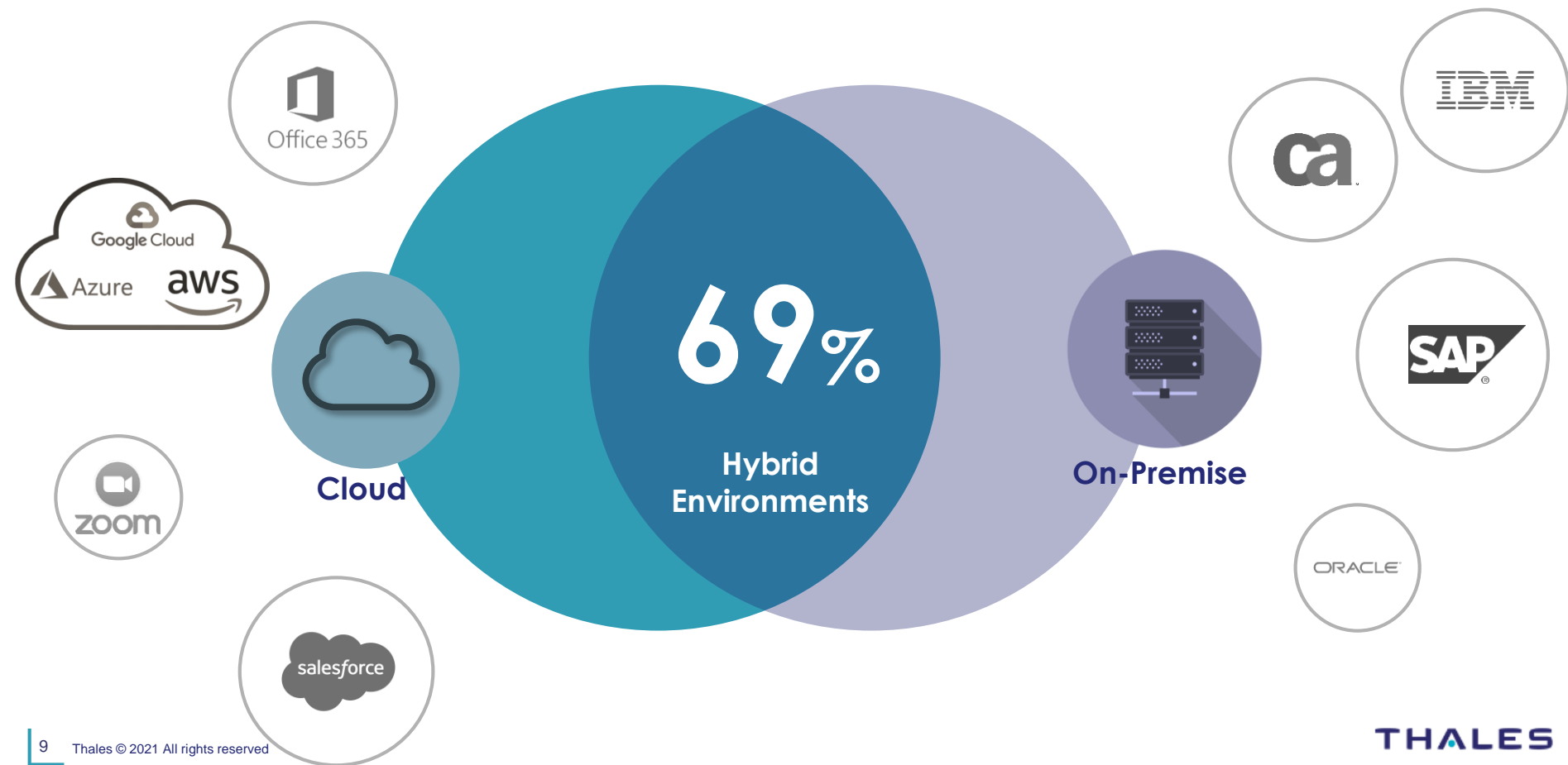


46%

ha indicato la privacy e la sicurezza come l'investimento più importante durante la pandemia.

La relazione sulle minacce verso i dati per il 2021 di Thales si basa su un'indagine che ha coinvolto oltre 2.600 professionisti della sicurezza e dirigenti esecutivi, di cui oltre 950 in Europa.

Reality Check - La maggior parte del mondo On Hybrid



I rischi della Cloud Migration



46% di tutti i dati delle organizzazioni europee è archiviato nel cloud

.....
43% dei dati delle organizzazioni europee nel cloud è sensibile

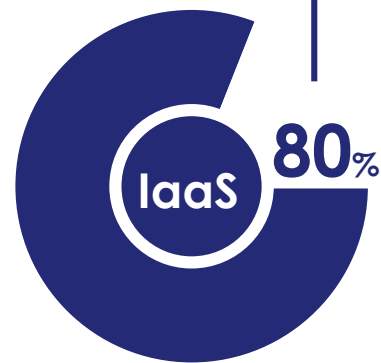
2 o più provider PaaS



11 o più provider SaaS



2 o più provider IaaS



Un mondo MultiCloud!

31%

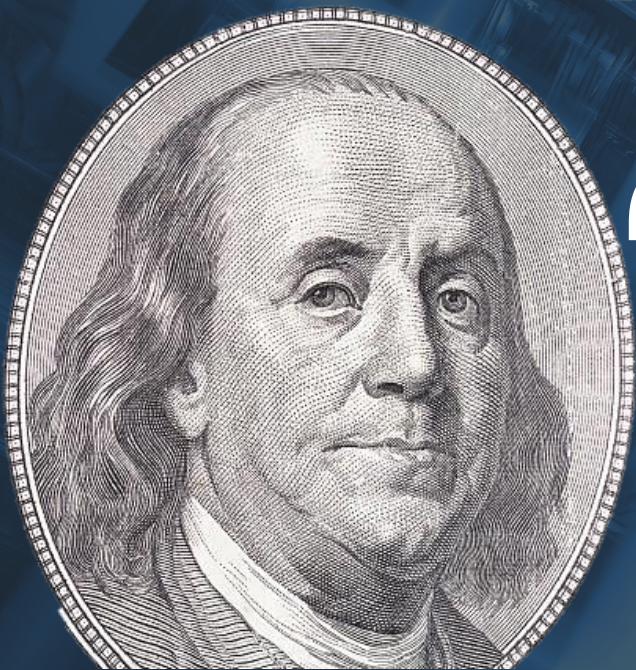
ha una strategia formale e ha attivamente adottato una politica Zero Trust.



76%

si affida ad alcuni concetti Zero Trust per modellare la strategia per la sicurezza del cloud.

La relazione sulle minacce verso i dati per il 2021 di Thales si basa su un'indagine che ha coinvolto oltre 2.600 professionisti della sicurezza e dirigenti esecutivi, di cui oltre 950 in Europa.



“

Tre persone possono
tenere un segreto, se
due di loro sono morte.

”

Benjamin Franklin

Cosa s'intende per autenticazione? – Chi sei esattamente?

L'autenticazione è il processo di identificazione univoca di una persona o di un dispositivo.

I seguenti tre fattori vengono spesso utilizzati per il processo di autenticazione:

Qualcosa che conosci (ad esempio una password o un PIN)

Qualcosa che hai (ad esempio una smartcard o il telefono)

Qualcosa che sei (ad esempio riconoscimento facciale o fingerprint)



Emma Miller
ID -0011A



Emma Miller
ID -0023D



Emma Miller
ID -0503F



In un mondo in cui l'identità è il nuovo perimetro, la nostra missione è offrire un accesso attendibile in un mondo non affidabile.



Benefici del *nostro* access management

Accesso basato su policy

Ottimizza la comodità e la sicurezza dell'accesso per tutte le app e i servizi

Autenticazione a più fattori

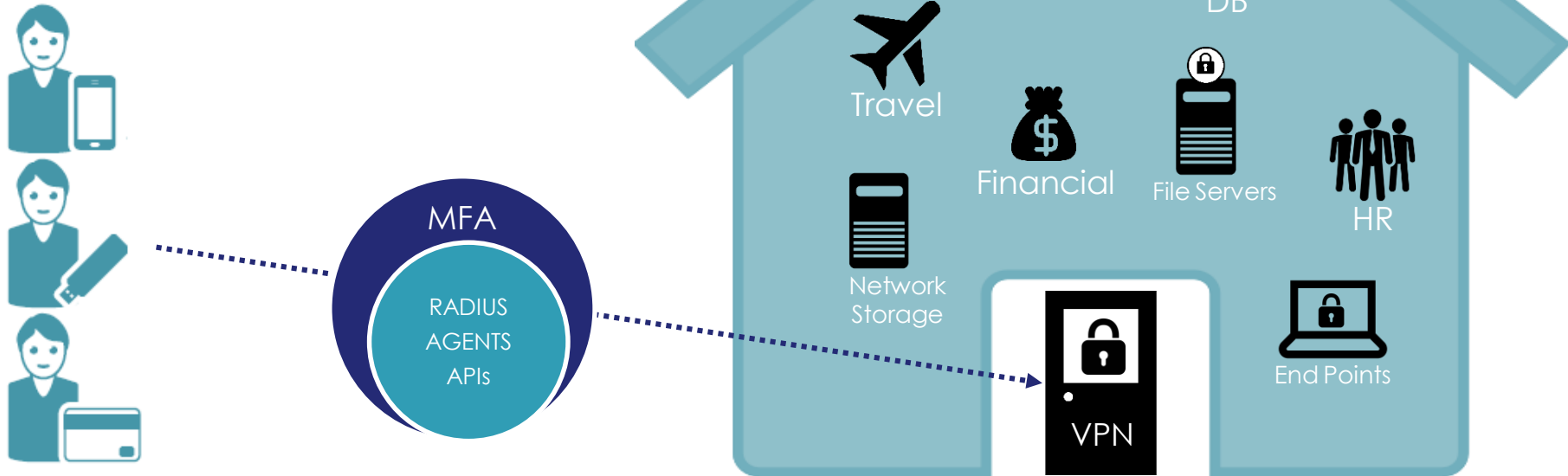
Previene i data breach applicando il giusto livello di sicurezza per le tue app on-prem e in cloud

Single Sign On Intelligente

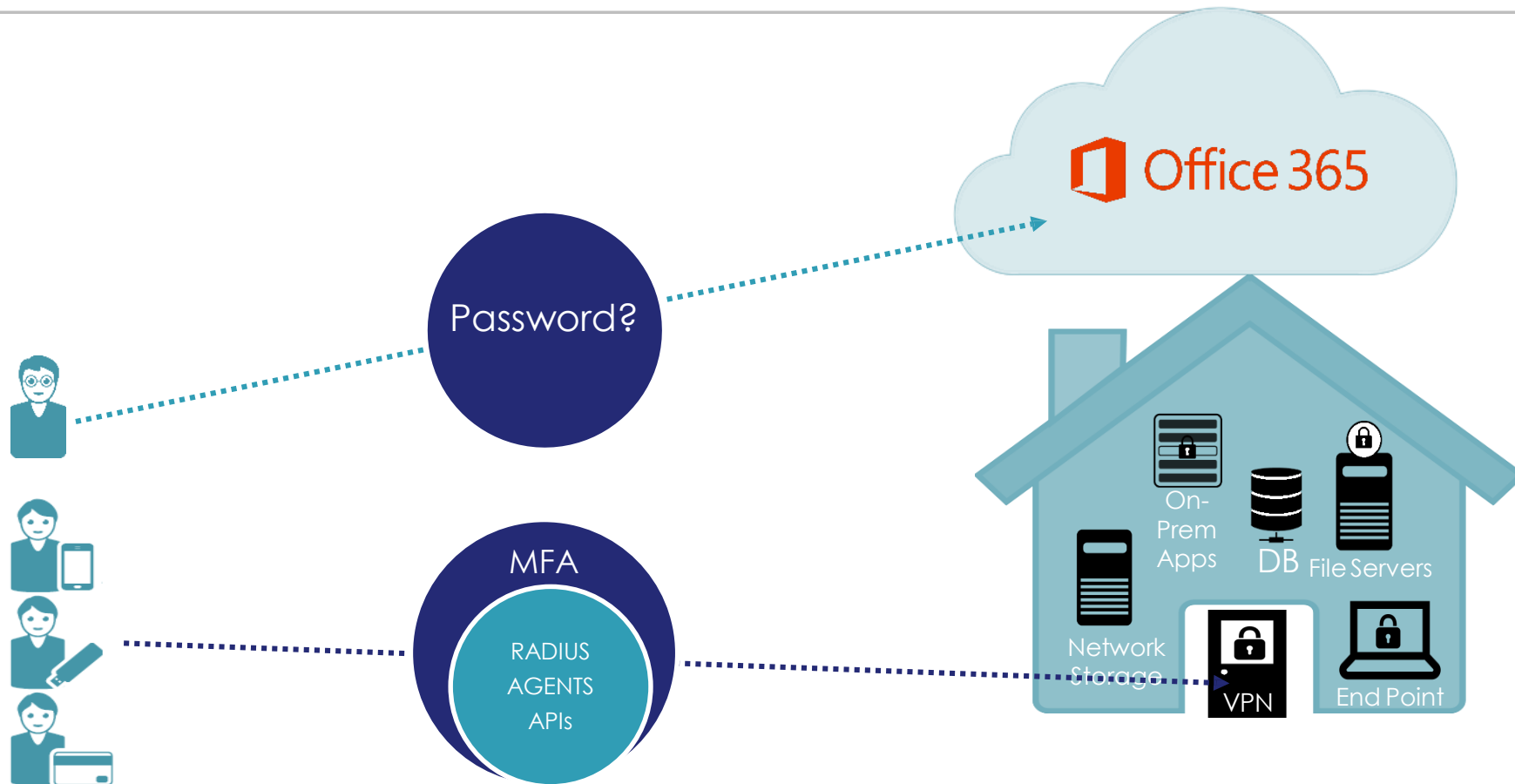
Rendi facile e sicuro per gli utenti l'accesso alle app



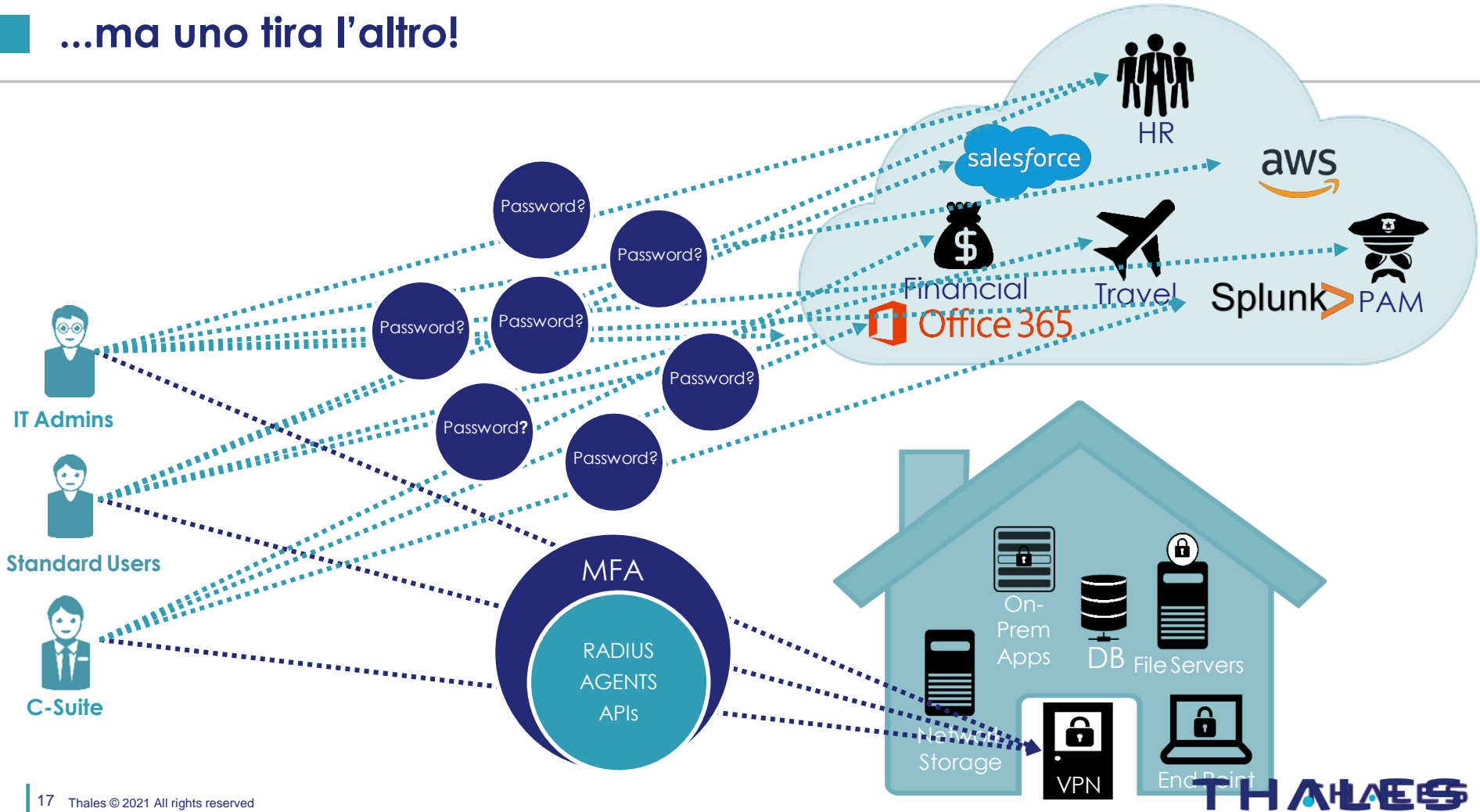
Sicurezza perimetrale – MFA & VPN



Un primo approccio nel cloud...



...ma uno tira l'altro!



Applica quindi il giusto livello di sicurezza

Accesso alle console admin
Richiesta sempre autenticazione con smartcard



Smartcards



Admin IT



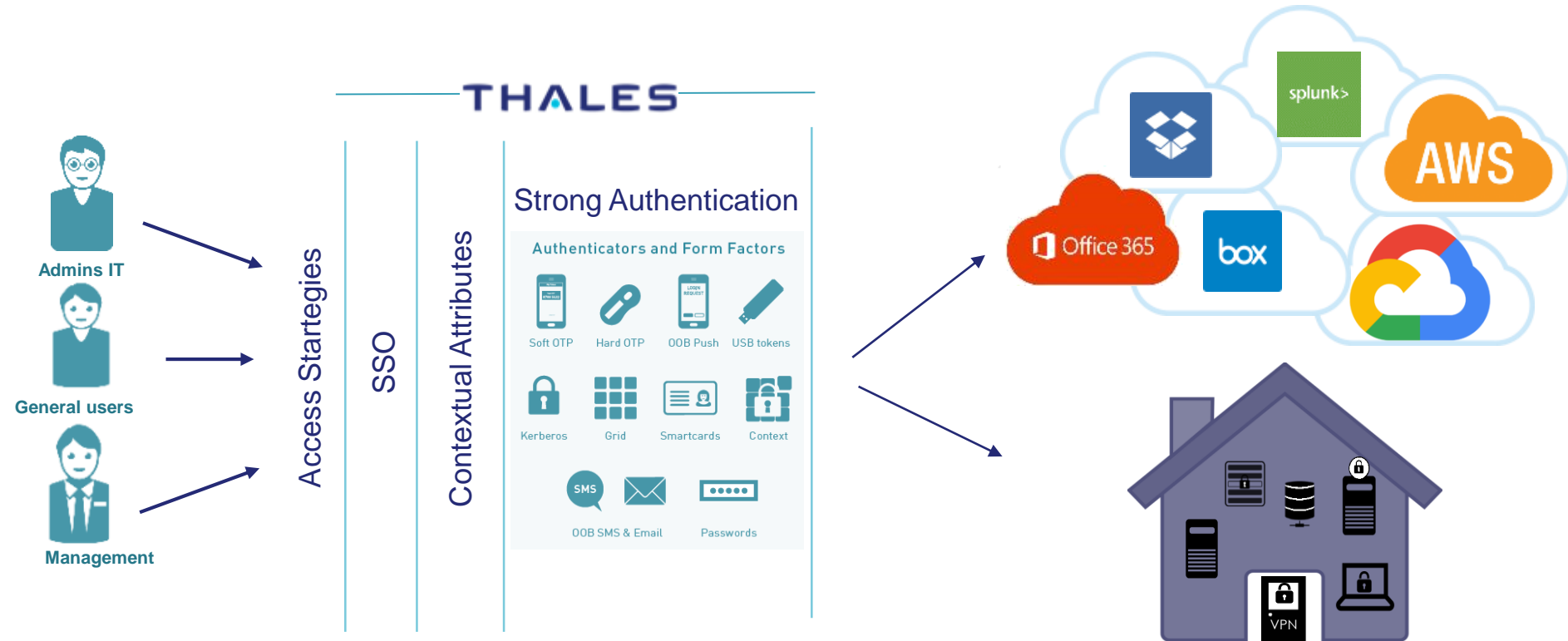
Applica quindi il giusto livello di sicurezza



Applica quindi il giusto livello di sicurezza



Definire strategie che tengano conto del ruolo e del contesto per applicare il giusto livello di sicurezza al momento giusto, per applicazione, per utente.

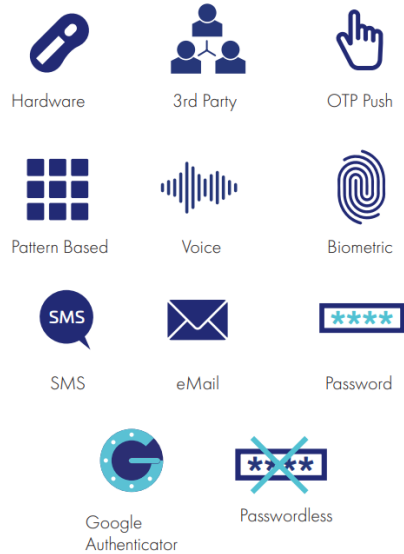


Il nostro portafoglio prodotti in 3 Pillars

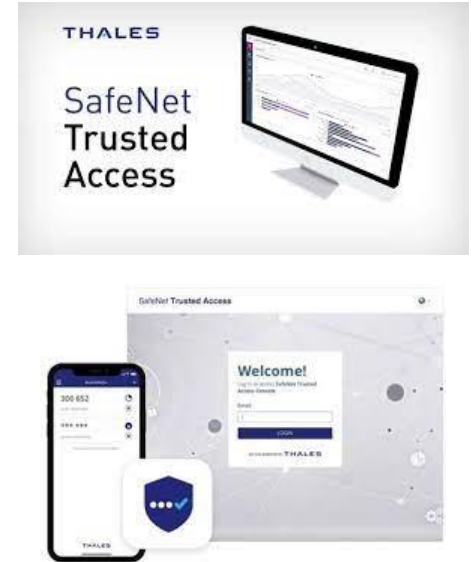
HW PKI



On-prem Authentication



Cloud-based Authentication



SafeNet Trusted Access – Interlocutori

PRIMARY STAKEHOLDER



CISO

Ci assicuriamo che siano in atto i giusti framework di rischio e sicurezza in modo che l'organizzazione sia conforme alle normative e non venga violata



IT Manager

Implemento le decisioni politiche prese dal CISO. Voglio una soluzione che si adatti al mio ambiente e che sia facile da implementare



Support

La mia preoccupazione principale è assicurarmi che le nuove soluzioni non comportino un aumento delle chiamate di assistenza e supporto



End User

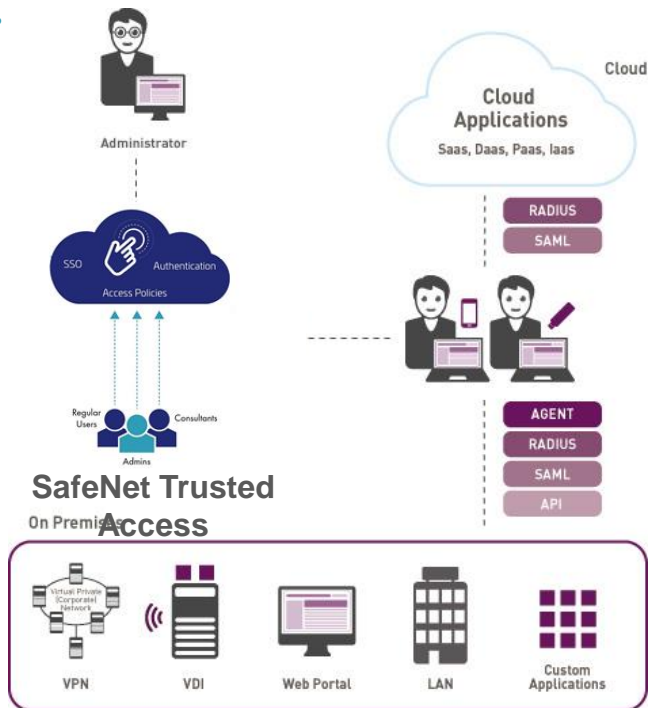
Abbiamo bisogno di un modo facile e conveniente per accedere a tutte le app



Finance

TCO e costi operazionali da ridurre

STA fornisce *strong authentication-as-a-service* in un ambiente cloud completamente sicuro.



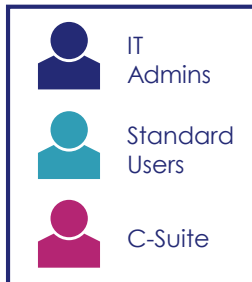
Protect Everything – il nostro mantra per quanto riguarda l'autenticazione delle identità.

Web app e cloud app sono protetti mediante integrazione con protocollo SAML.

STA è altamente flessibile e permette l'integrazione sia con soluzioni cloud che on prem.

Application Management semplificato

1. Identifica target apps e users



Policy Scope

Users

All Users Any of these User Groups:

C-Suite

Applications

All Applications Any of these Applications:

Zendesk, Google G Suite, Salesforce

Default Requirements

When an access attempt occurs, then access is

Granted Denied

After authenticating using the factors

Password

Once per session Every access attempt

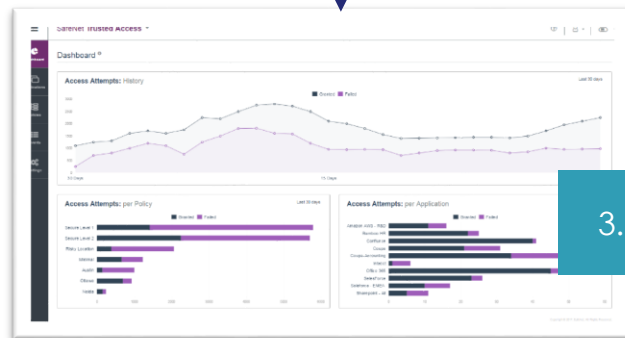
Token Based Authentication (OTP)

Once per session Every access attempt

2. Definisci le Policies

4. Adjust

- Scenario-driven
- Compliance-focused
- Setting di regole di autorizzazione "by policy"



3. Monitor Risk

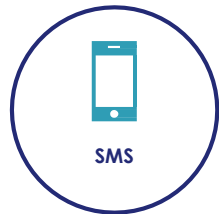
Autenticazione universale

Unico fattore

Più fattori

Senza password

Adattivo



Utilizza gli schemi di MFA già distribuiti

Estende l'autenticazione PKI ai servizi cloud

Offre il livello di sicurezza appropriato

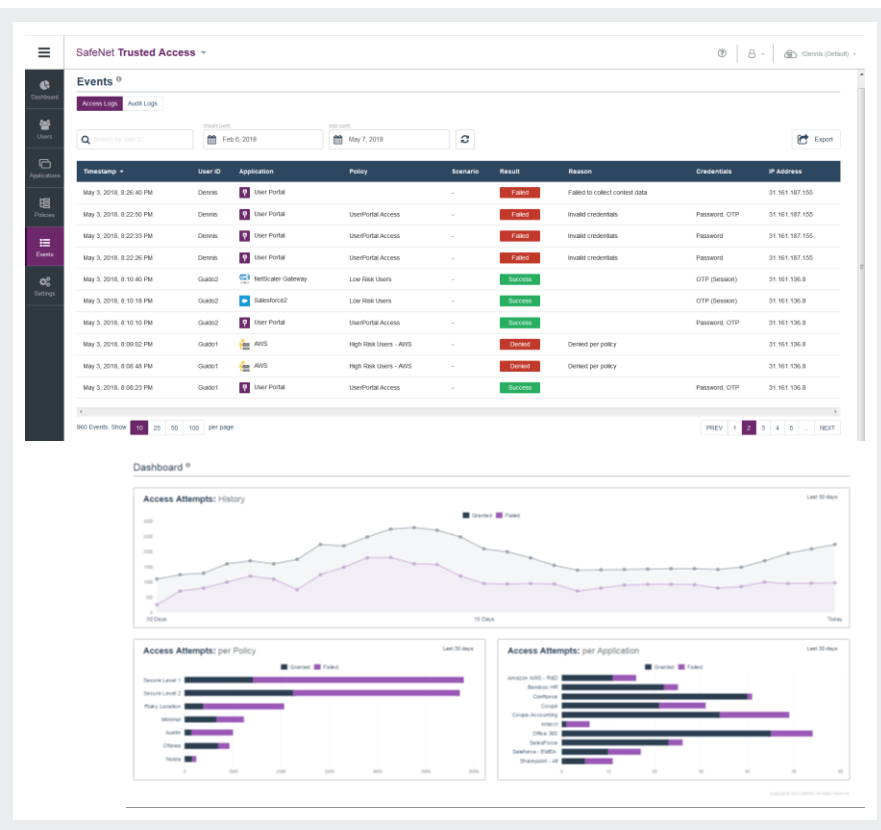
Offre comodità grazie ad una autenticazione senza password

Dashboard

Compliance

Integrazione con SIEM e Syslog

Basati su agenti o su Rest API



■ Schedulabili

■ Consultabili dal portale o disponibili per l'invio via email

■ Diversi formati (HTML, CSV, XLS)

■ 50 template già disponibili e configurabili

■ Disponibili log di Sicurezza, Billing, Inventario e Audit

Snapshot Assignment Tokens Groups **Reports** Self-Service Operators Policy Comms

Available Reports

Add

Select and customize reports from this section to add to My Report List.

Report Class: Compliance

Report	Class	Description
Auth Node Billing	Compliance	Reports all auth nodes, configuration and status.
Authentication History - Chronological Descending	Compliance	Reports authentication history in chronological order.
Authentication Metrics	Compliance	Equivalent to snapshot metrics.
Enrollment - History	Compliance	Reports detail and status of all self-enrollments.
Operator Activity - Detail	Compliance	Reports operator activity, actions, results.
Operator Activity - Logons	Compliance	Reports operator logons in a date range.
Operators (Internal) with Static Passwords	Compliance	Reports operators with static password credentials.
Push OTP Authentication History	Compliance	Reports on push notification and authentication result history in chronological descending order
Users - All - with Tokens and Tasks	Compliance	Reports users with their assigned authentication methods and active, locked or expired provisioning tasks.
Users - Inactive	Compliance	Reports Users that have not authenticated for N days.

Displaying: 1 to 10 of 15

Token FIDO



- **SafeNet eToken FIDO**
- **eToken 5300 FIDO**
 - Supporto degli use case PKI

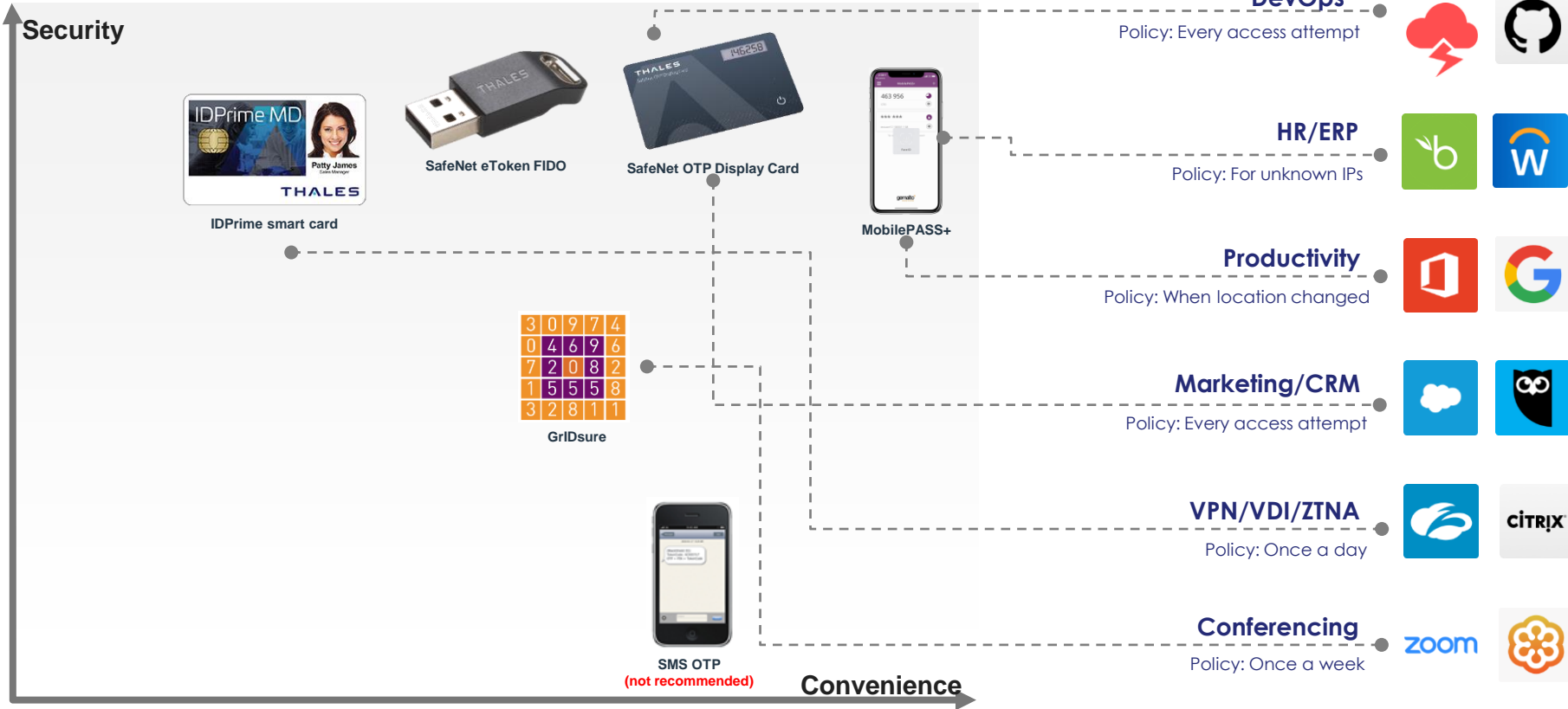


- **IDPrime 3940 FIDO**
 - Interfaccia NFC
 - Supporto degli use case PKI



FIDO/CTAP 2.0 /U2F compliant and certified (functional and security certifications)

Esempio: Flexible Authentication Method & Access Policies



Elementi differenziatori

Deploy Facile

- Go Live rapido
- Completamente automatico
- Policy setup facile ed intuitivo
- Facile da utilizzare (MobilePass)

Migliore Risk Management

- MFA Granulare
- Vendor Agnostic
- Cloud neutral
- Conditional access

“Excellent TCO Better Value”

- Pricing competitivo
- Servizio MFA-AM integrato
- Licenza All in one
- Multiple tokens inclusi

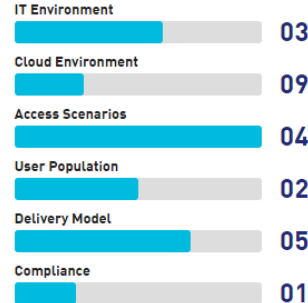
Access Management Risk Assessment tool

THALES

ADVANCED STAGE

Access Management Evaluation

Based on the data you provided, you are looking to protect 3 infrastructure applications and are using 3 cloud application[s]. Currently, it appears that your users have multiple profiles, meaning they are comprised of different user groups, who would need different access to different resources. For example, a standard employee will most likely need different access rights than someone in an HR role vs an IT administrator. Assessing the different kinds of identities you have in your organization determines which applications a user can access and what kind of permissions they have within the application. Taking it one step further, access management will help determine how the user's identity is verified and validated upon their login attempt. Lastly, based on the data you provided the applications that your users are accessing contains sensitive data. In terms of



<https://www3.thalesgroup.com/access-management-risk-assessment-tool/index.html>