



SafeNet Trusted Access Management

Peter Wilbrink – Director business development,
Identity & Access Management

Last updated: April 16, 2019



Thales & Gemalto: A New Profile

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

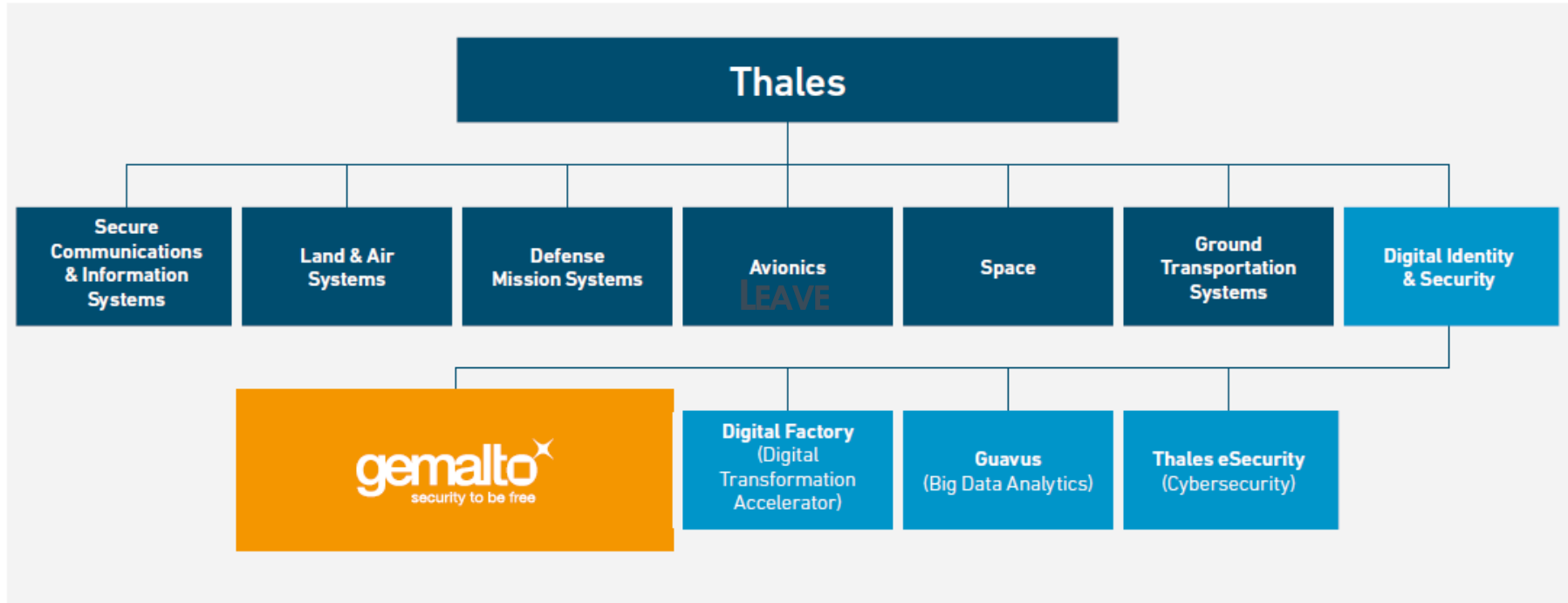
€1bn+
self-funded
R&D* 2017



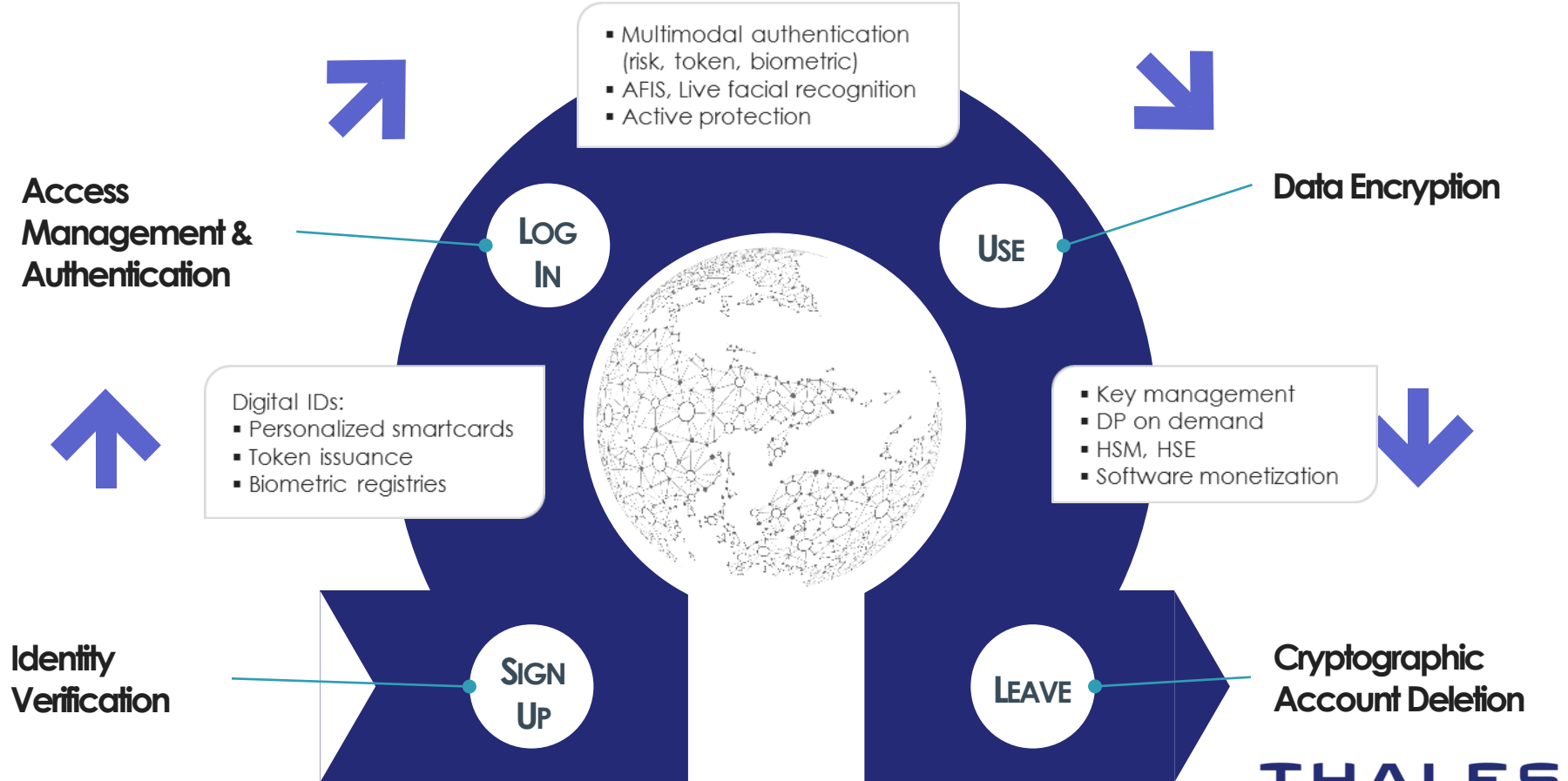
Does not include externally
financed R&D.

Thales Cloud Protection & Licensing

Combining existing digital assets in a dedicated global business unit



Protecting the entire digital service cycle





Thales Access Management and Authentication Solutions

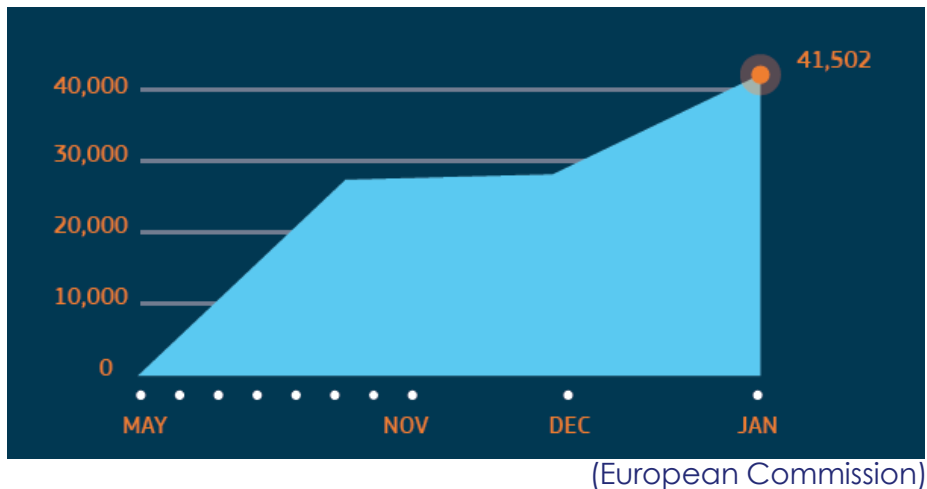
www.thalesgroup.com



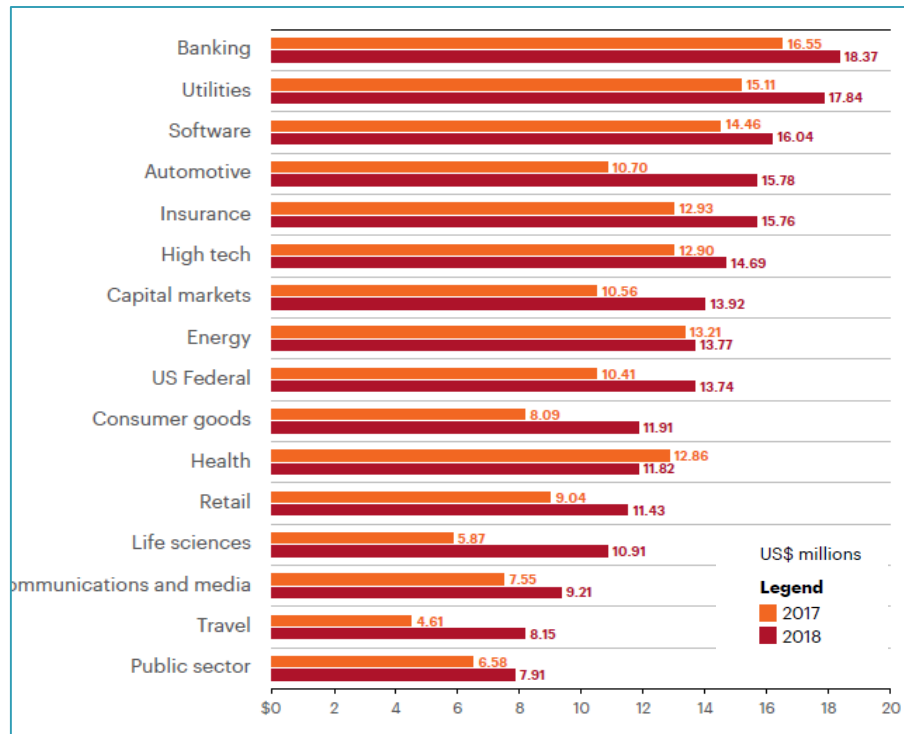
Traditional security is no longer sufficient

Breaches are growing year-on-year across all sectors

Since May 2018, the EU has received 41,500 notifications of data breaches



Annual Cost of Cybercrime by Industry



Ponemon 2019 Cost of Data Breach Report

THALES

The main causes of cyber threats

Main cause of attacks

IDENTITY THEFT

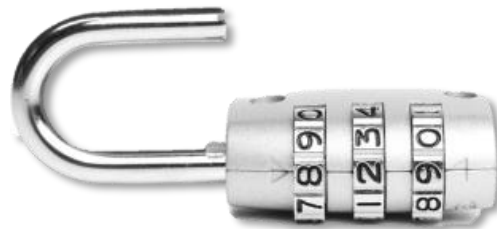
69%

of breach incidents came from identity theft



Main cause of damages

UNENCRYPTED DATA



95%

of breaches involved unencrypted data



27

Average number of cloud applications
used by companies

Why are Cloud Apps Especially Vulnerable to Attack?

- Login page is in the public domain
- Nothing protects the login page except for a password
- Passwords are typically shared among applications
 - FB breach...
- Privileged users – no barriers in place...

Millions of Office 365 Accounts Hit with Password Stealers

Phishing emails disguised as tax-related alerts aim to trick users into handing attackers their usernames and passwords.

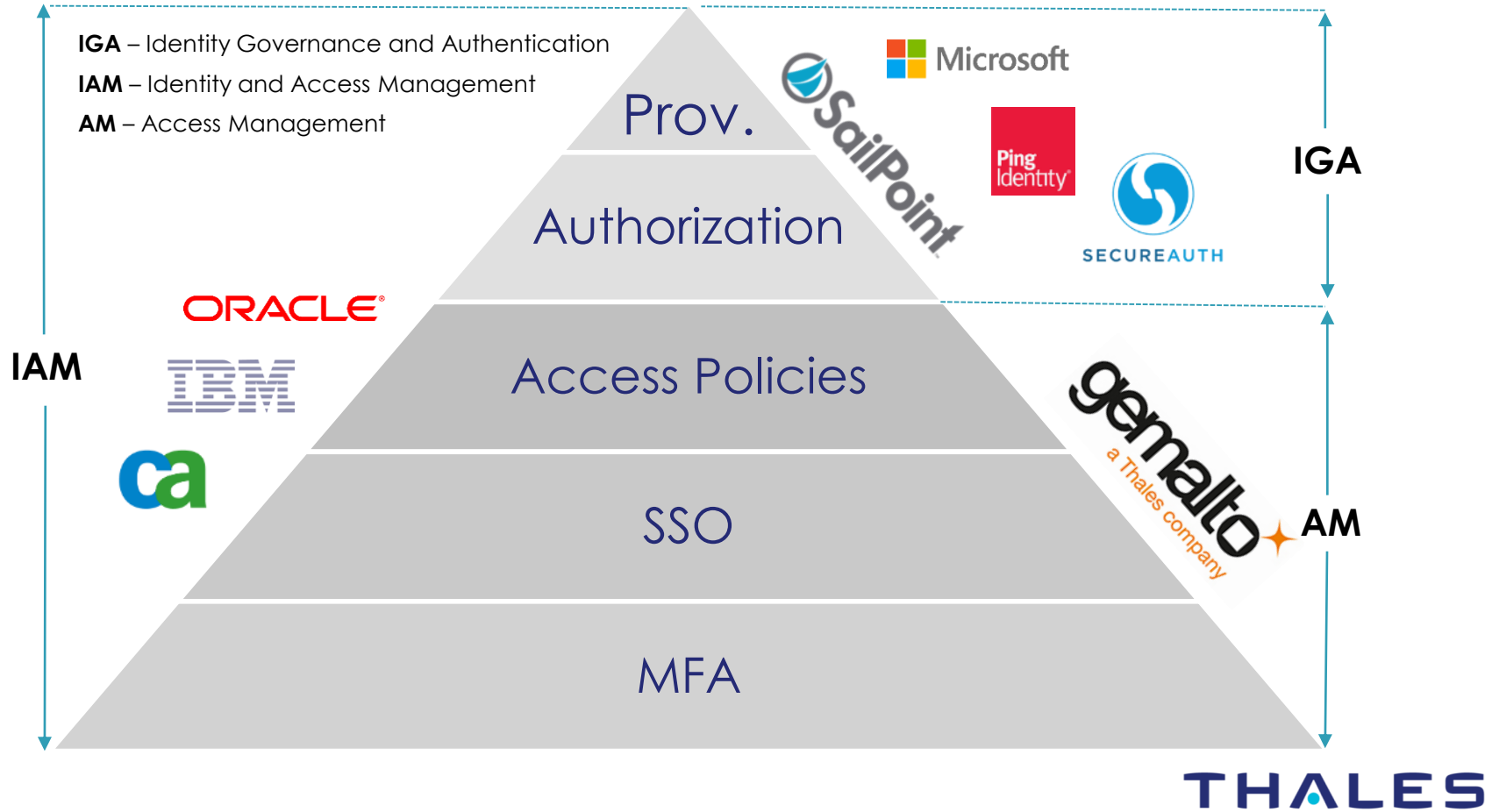
A new wave of phishing attacks aims to dupe users and steal their passwords by disguising malicious emails as tax-related notifications from the IRS.

Barracuda Networks last month flagged a "critical alert" when it detected attack attempts to steal user passwords. This threat lures victims with Microsoft 365 Office files claiming to be tax forms or other official documents; attackers use urgent language to convince people to open the attachment.

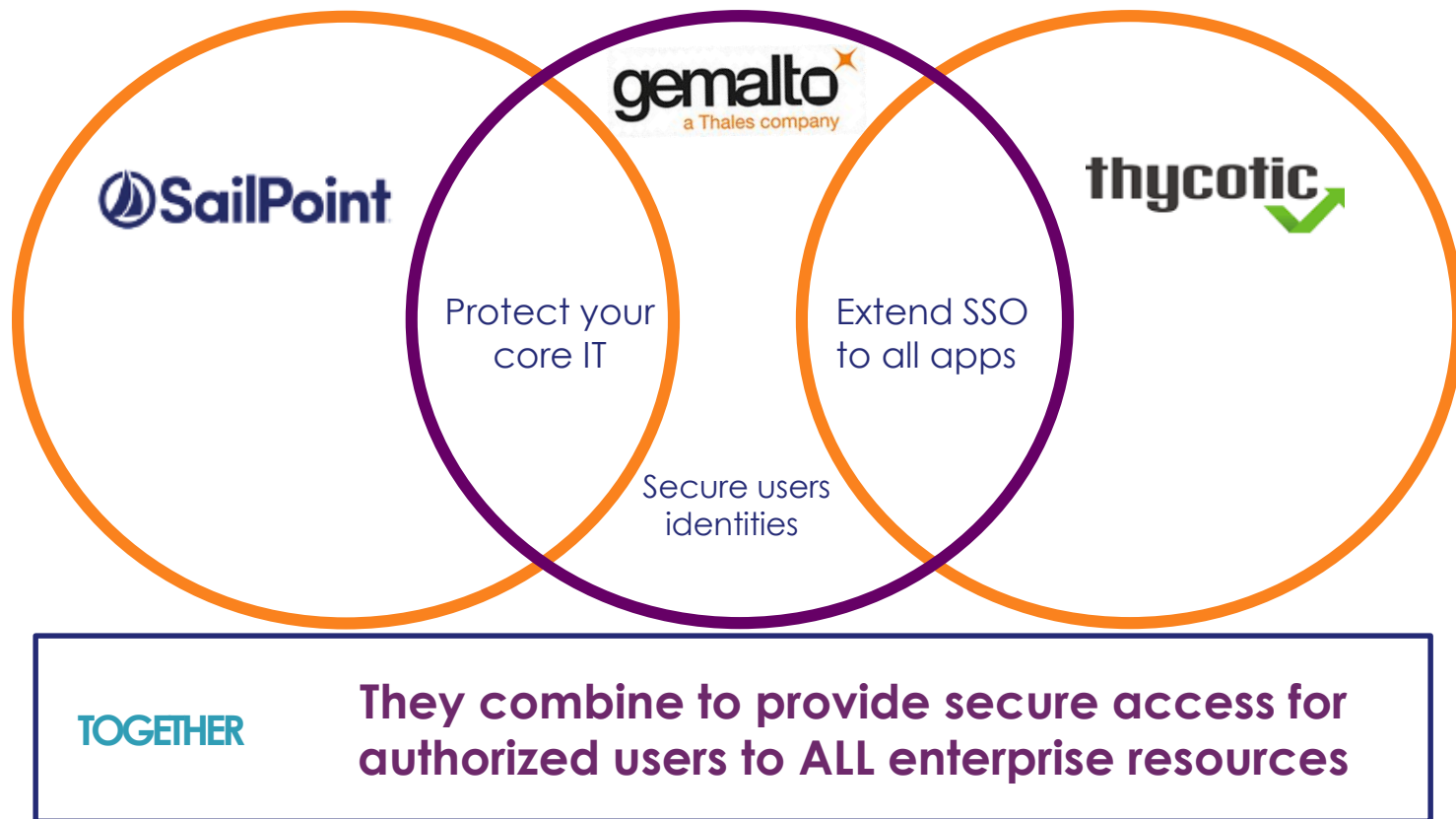
Examples of this tactic include files named "taxletter.doc" and phrases like "We are apprising you upon the arisen tax arrears in the number of 2300CAD." The use of popular file types like Word and Excel, which are globally known and used, further ensures victims will fall for it.

"Today's documents are far more active ... you're putting in a lot of content, media, links," says Fleming Shi, senior vice president of technology at Barracuda, comparing this threat with phishing attacks of the past. "Bad guys are leveraging the dynamic, active manner of the documents today to weaponized their files."

How STA is positioned in the IAM market

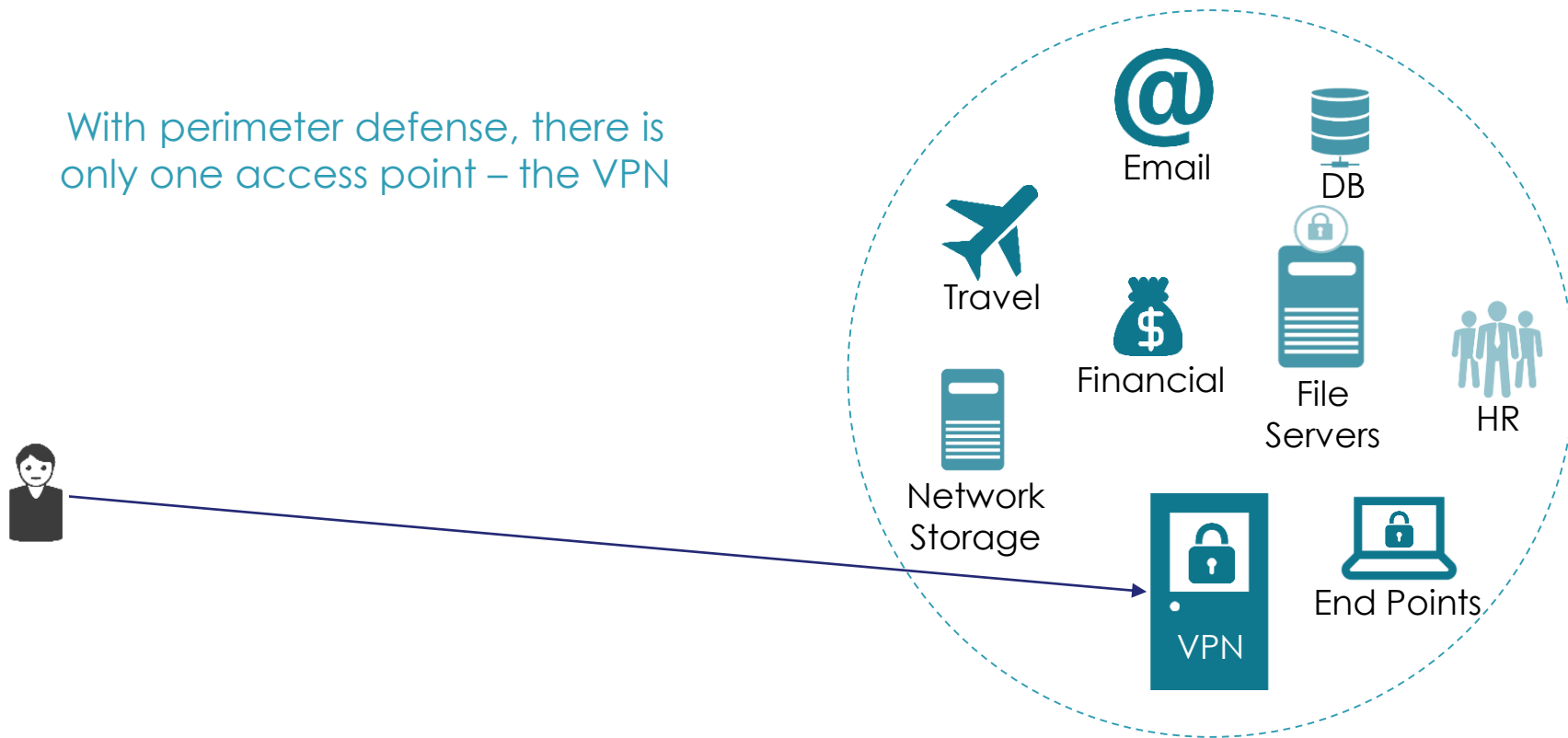


Access Management extends your Security Perimeter



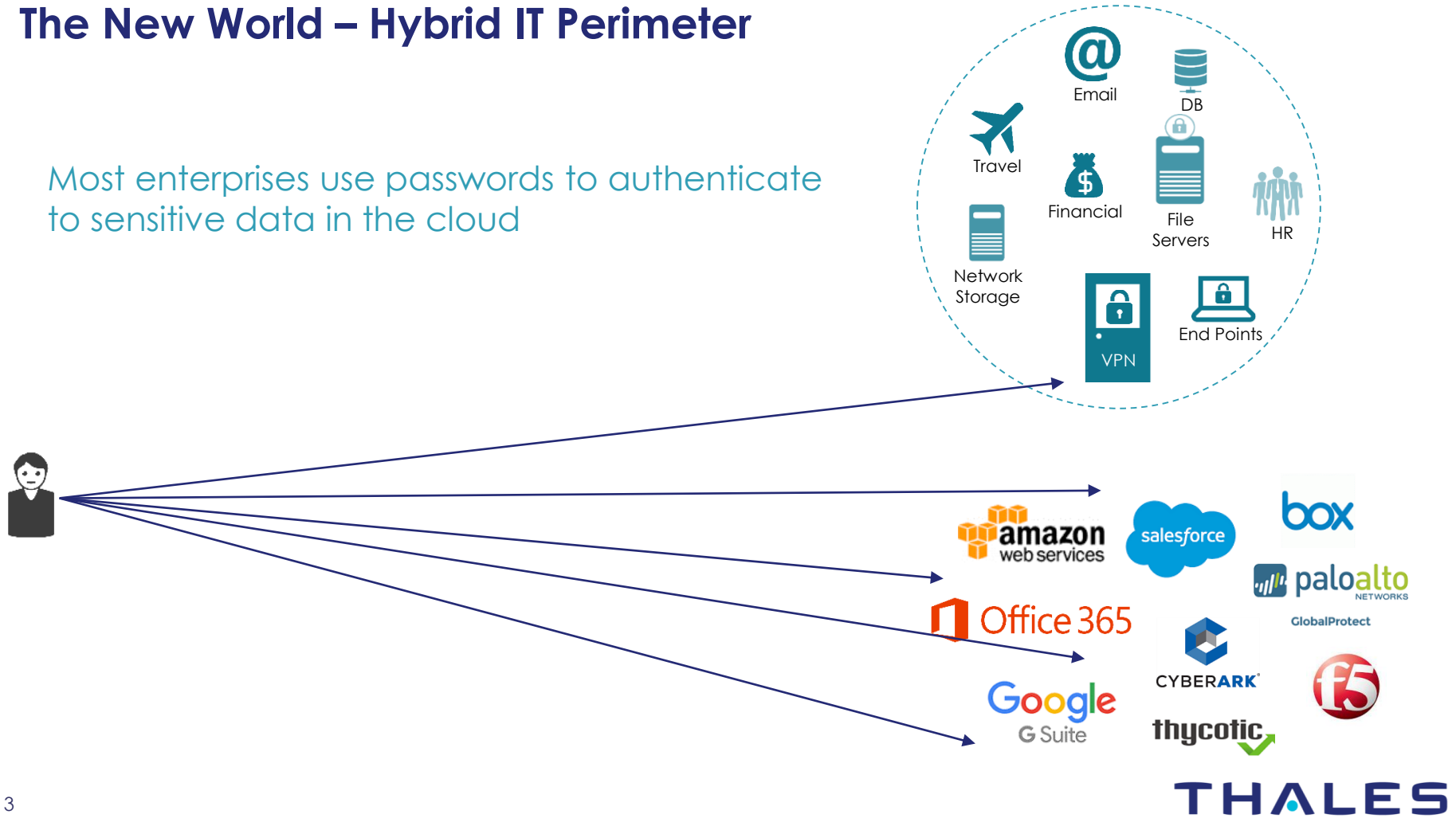
Good Old Perimeter Security

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



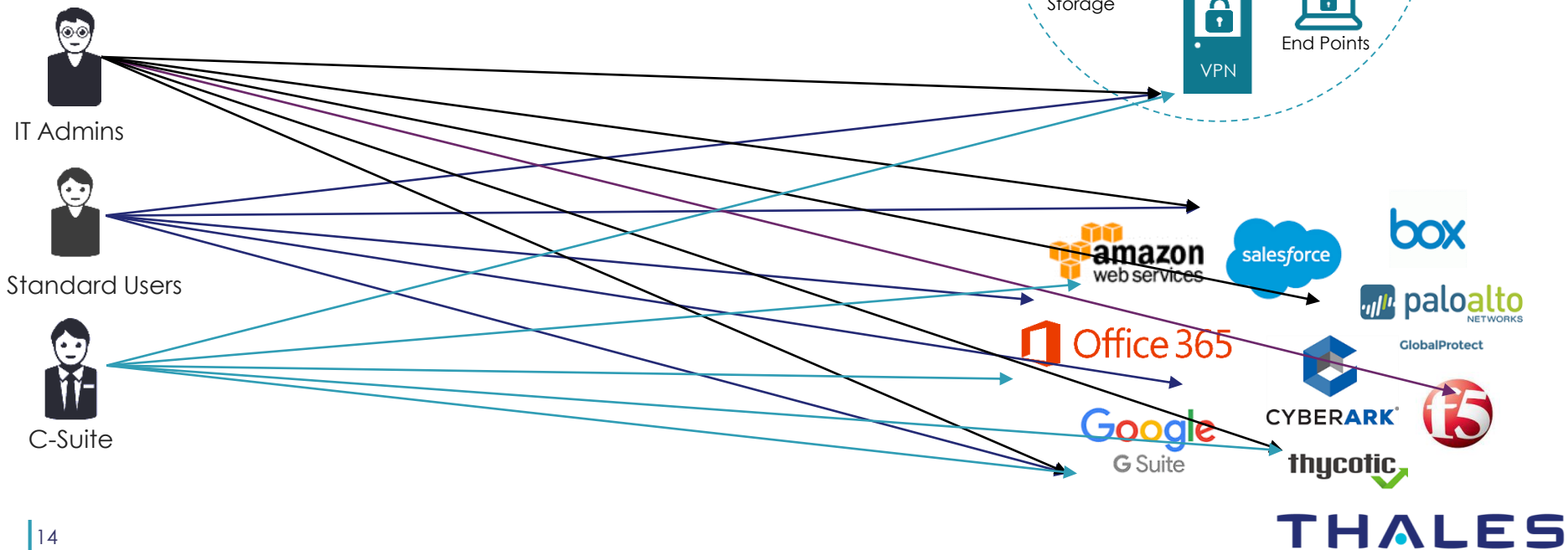
The New World – Hybrid IT Perimeter

Most enterprises use passwords to authenticate to sensitive data in the cloud



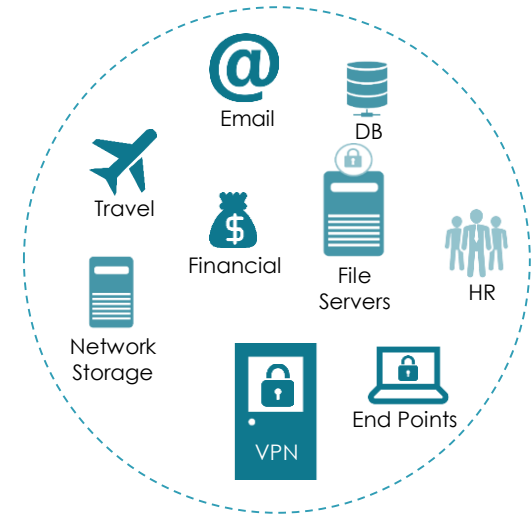
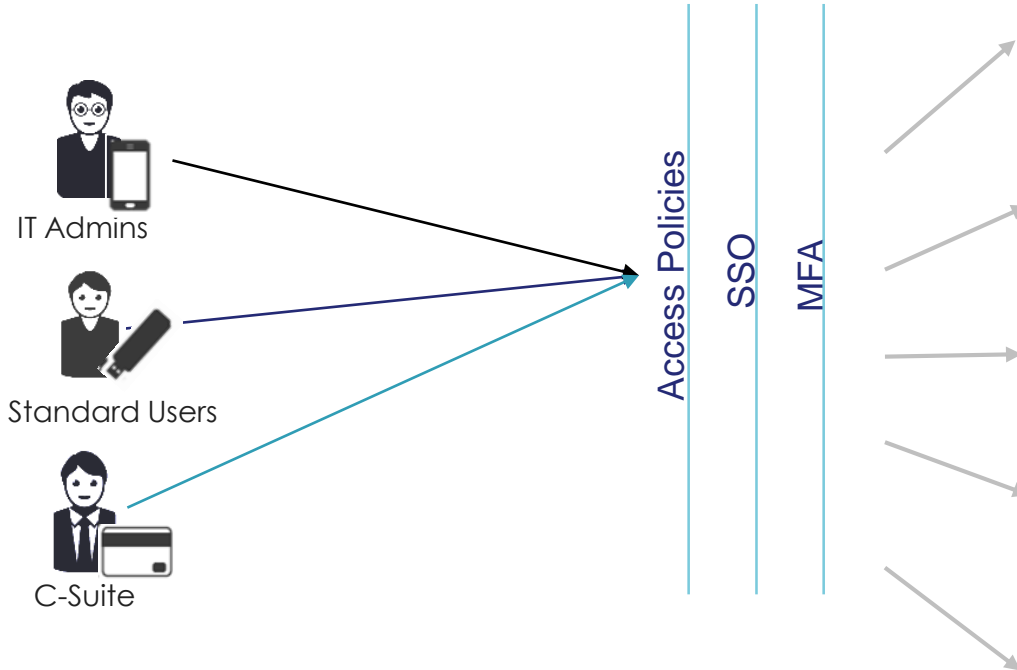
The New World – Hybrid IT Perimeter

Different users need access to sensitive data stored inside the perimeter and in the cloud



The New World

Multi-Factor Authentication



THALES

The New World

Multi-Factor Authentication



IT Admins



Standard Users



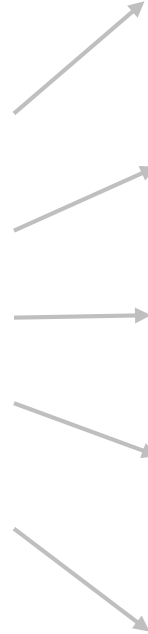
C-Suite

STA

Access Policies

SSO

MFA



SaaS / IaaS

CLOUD APPS

RADIUS
SAML
OIDC
AGENTS
APIs



On-prem Apps

FIREWALL

PAM

VDI



VPN

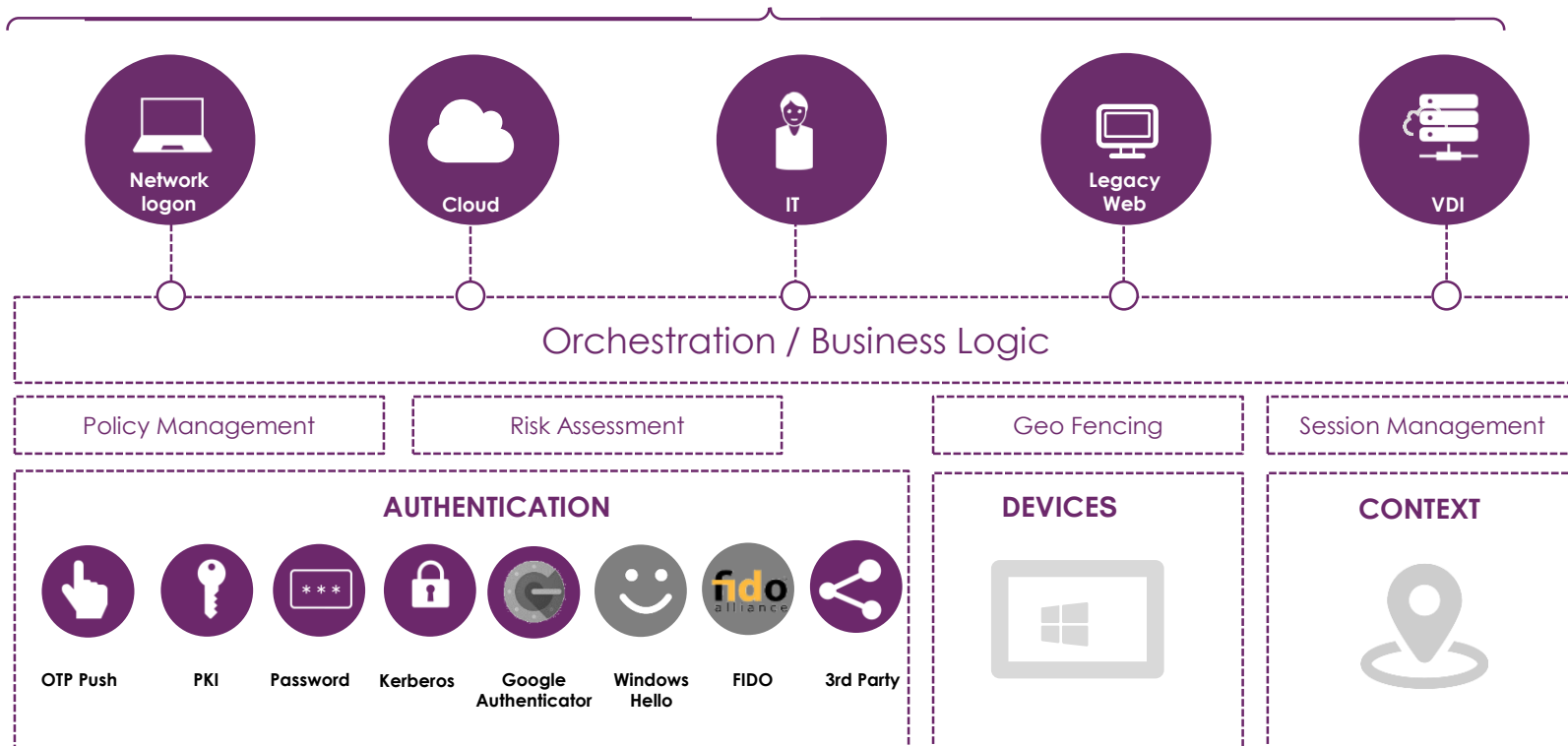


THALES

SafeNet Trusted Access

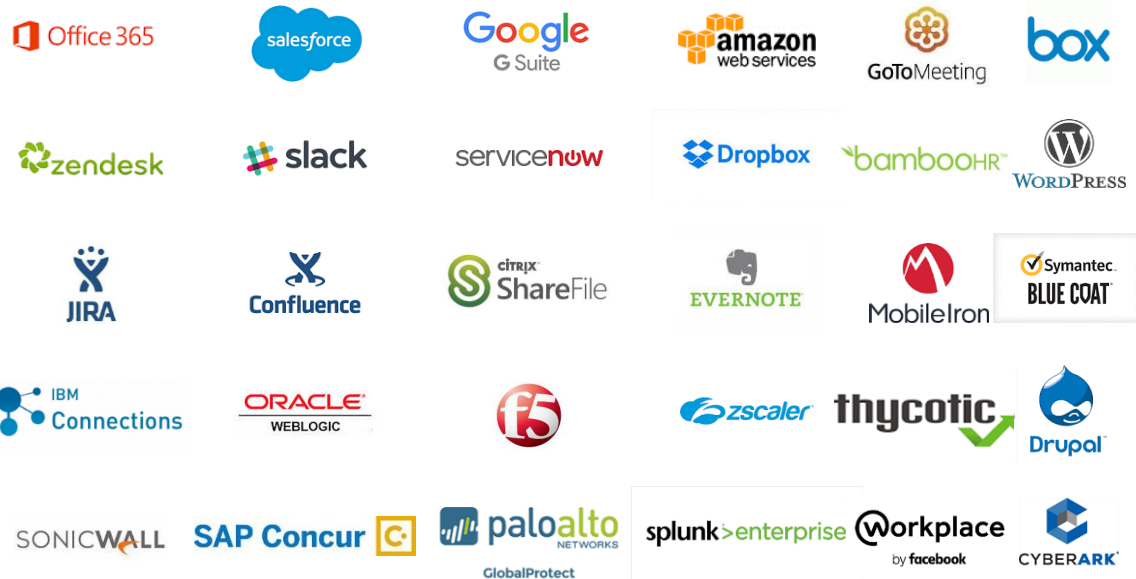
Prevent Breaches | Secure Cloud Transformation | Simplify Compliance

SafeNet Trusted Access



SafeNet Trusted Access

Supporting the cloud and web-based apps you use...



Bring Your Own Apps



SAML 2.0
OIDC
generic wizard

and many more...

THALES

SafeNet Trusted Access

Universal authentication methods



Password



Kerberos



OTP Push



Hardware



3rd Party



Google
Authenticator



SMS



eMail



Voice



Pattern-
based



PKI



Passwordless



Biometric

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

Integrated Windows Integration

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

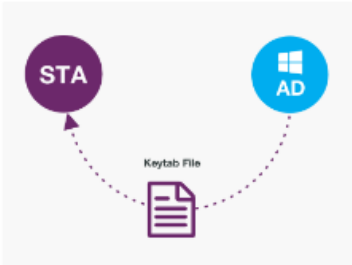
Events

Authentication

✓ Kerberos (Domain Password Passthrough) ⓘ

Step 1: Active Directory Setup

Step 2: STA Setup



The diagram illustrates the integration between a Service Target Agent (STA) and an Active Directory (AD) server. 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 the AD to the file and from the file to 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

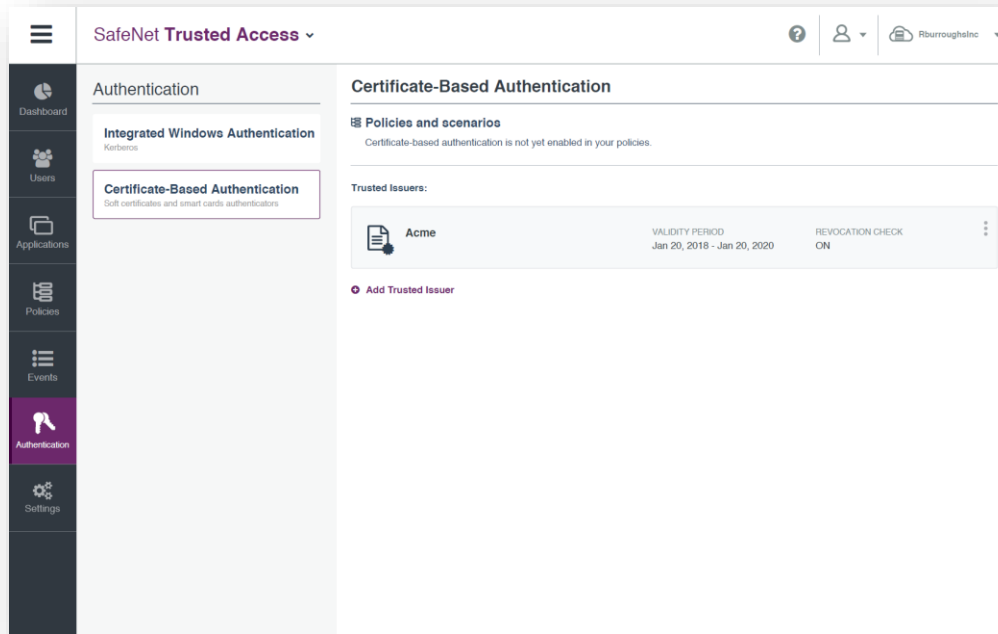
- ☒ **Password ⓘ**
- ☒ **Once per session**
- ☐ Every access attempt
- ☒ **Allow Kerberos (Windows Password Passthrough) ⓘ**
- ☒ **Token Based Authentication (OTP) ⓘ**
- ☐ Once per session
- ☒ **Every access attempt**

PKI/Certificate Based Authentication



PKI

Extend certificate-based authentication to cloud apps

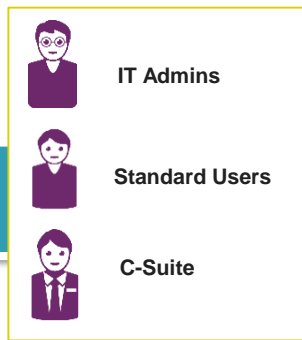


- Enforce high assurance security across cloud and web apps
- Simplify access for users with cloud and web single sign-on (SSO)
- Elevate trust with a choice of PKI and OTP-based authenticators

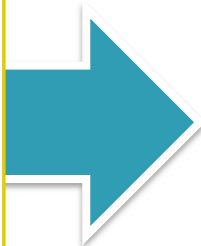
Manage risk through scenario-based policies



Target Apps



Users/Groups



Adjust

Monitor Risk

Policy Scope

Users

☐ All Users ☒ Any of these User Groups:

C-Suite

Applications

☐ All Applications ☒ Any of:

Zendesk, Salesforce, Google G Suite

Default Requirements

When an authentication attempt occurs, then access is granted if:

☒ Password

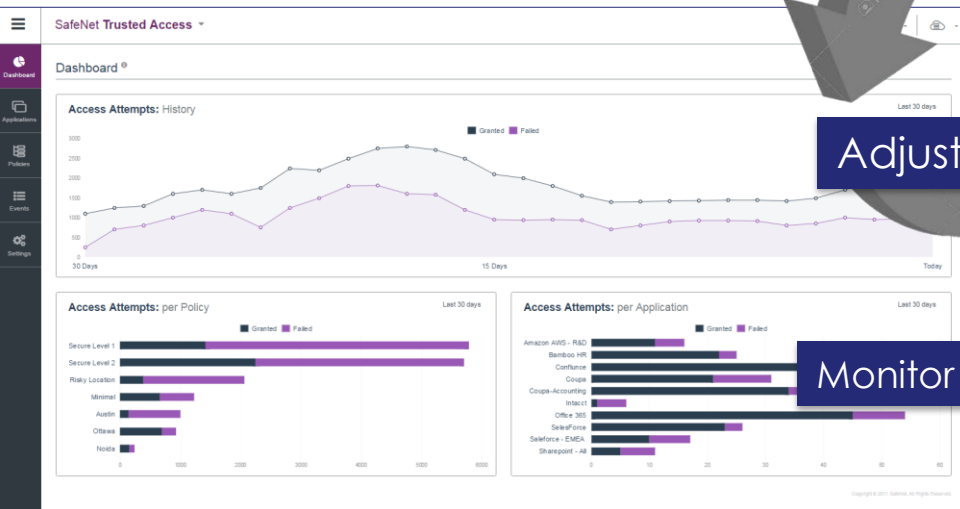
☐ Once per session ☒ Every access attempt

☒ Token Based Authentication (OTP)

☐ Once per session ☒ Every access attempt

Define Policies

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



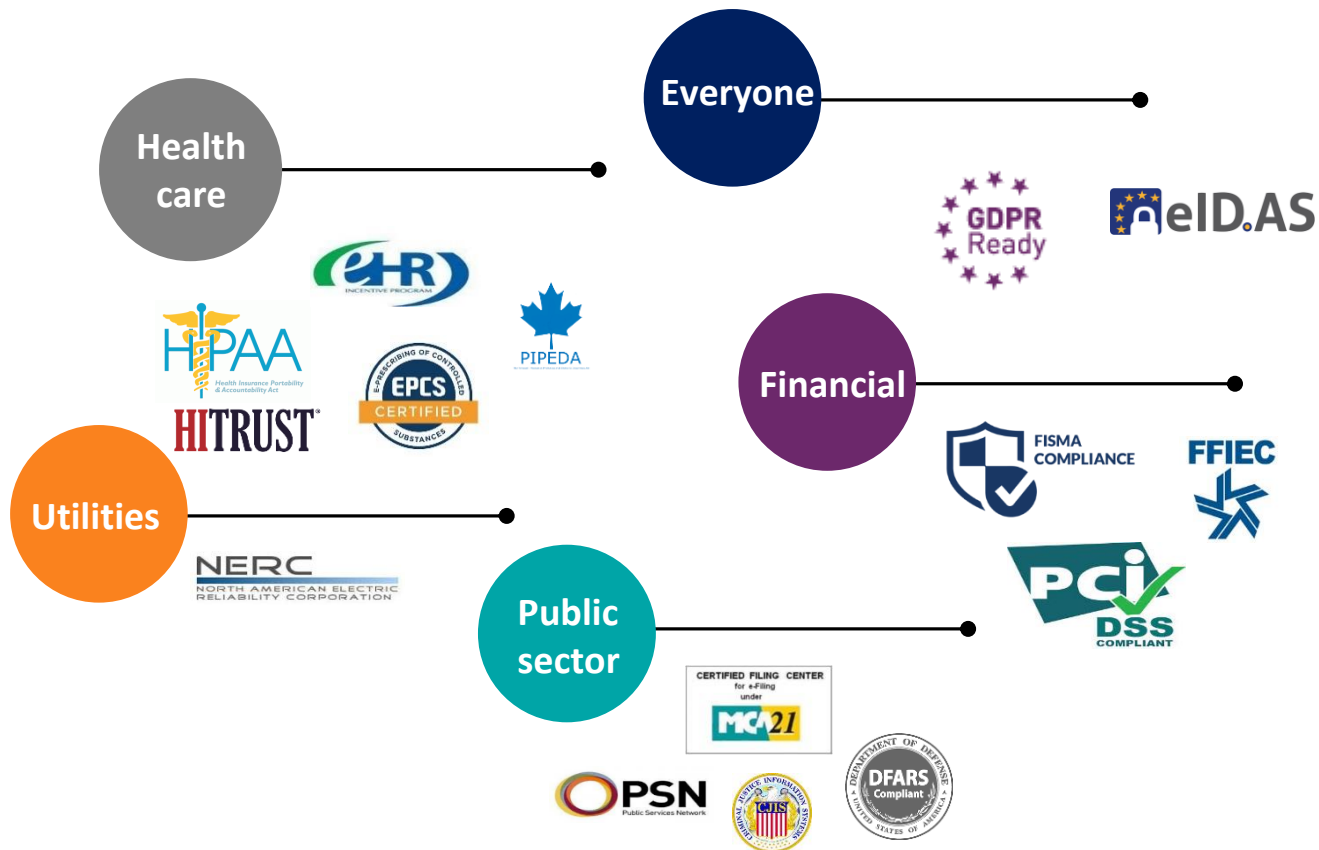
SafeNet Trusted Access

Configure a policy in 3 mins...

- Powerful policy configuration wrapped in an easy to use policy engine...
- Control exactly who, when, why and how users or groups accesses an app
 - Who: Include individual users or predefined groups
 - When: Specify when groups or users can access an app
 - Why: Define policies with clear business outcomes:
GDPR compliance, privileged access, admin access
 - How: Determine the authentication method for each policy

All it takes is about 3 minutes...

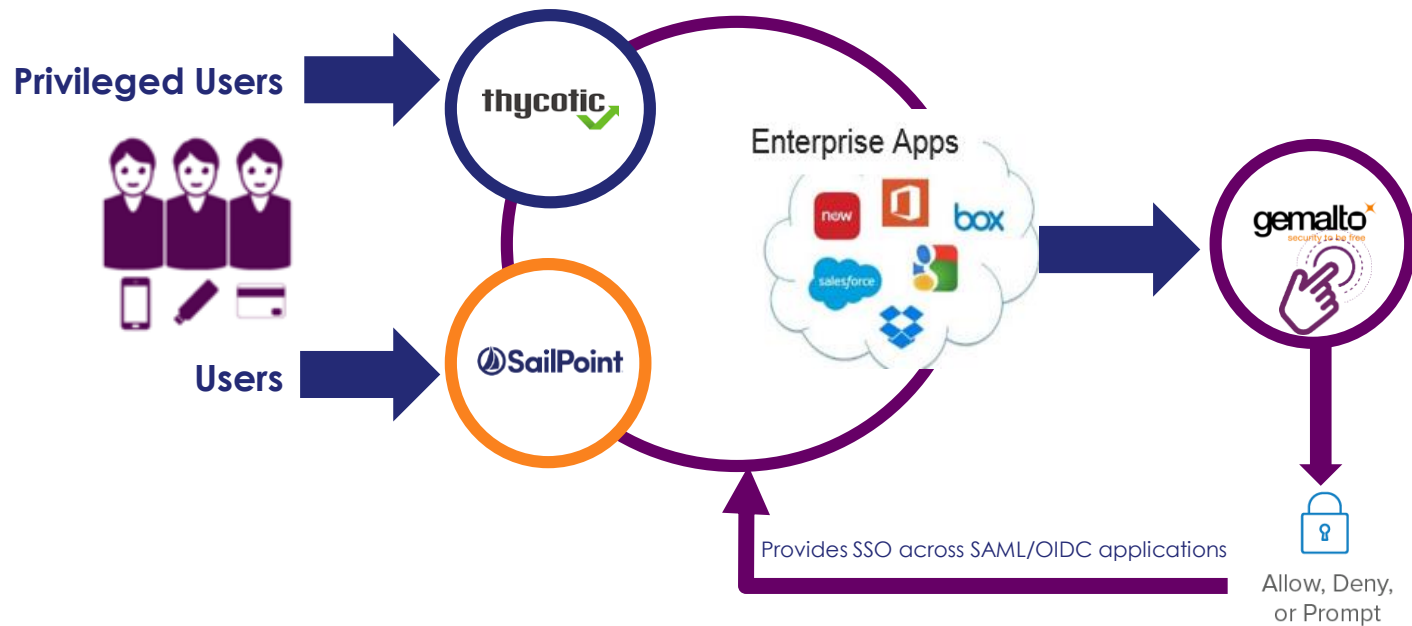
Comply simply with regulations



Thales solutions
address
security across
industry
segments

THALES

SafeNet Trusted Access Protects all Apps and all Users



Move Securely to the Cloud with SafeNet Trusted Access

- **Prevent** breaches

- **Enable** cloud transformation securely

- **Simplify** compliance

Access Management – Your Partner for the Long Terms

- 30 years in Identity & Access Management
- More than 25,000 IAM customers and more than 30 million users
- Pioneer in cloud-based authentication, with more than 4.5 million paying subscribers
- PKI authentication leader



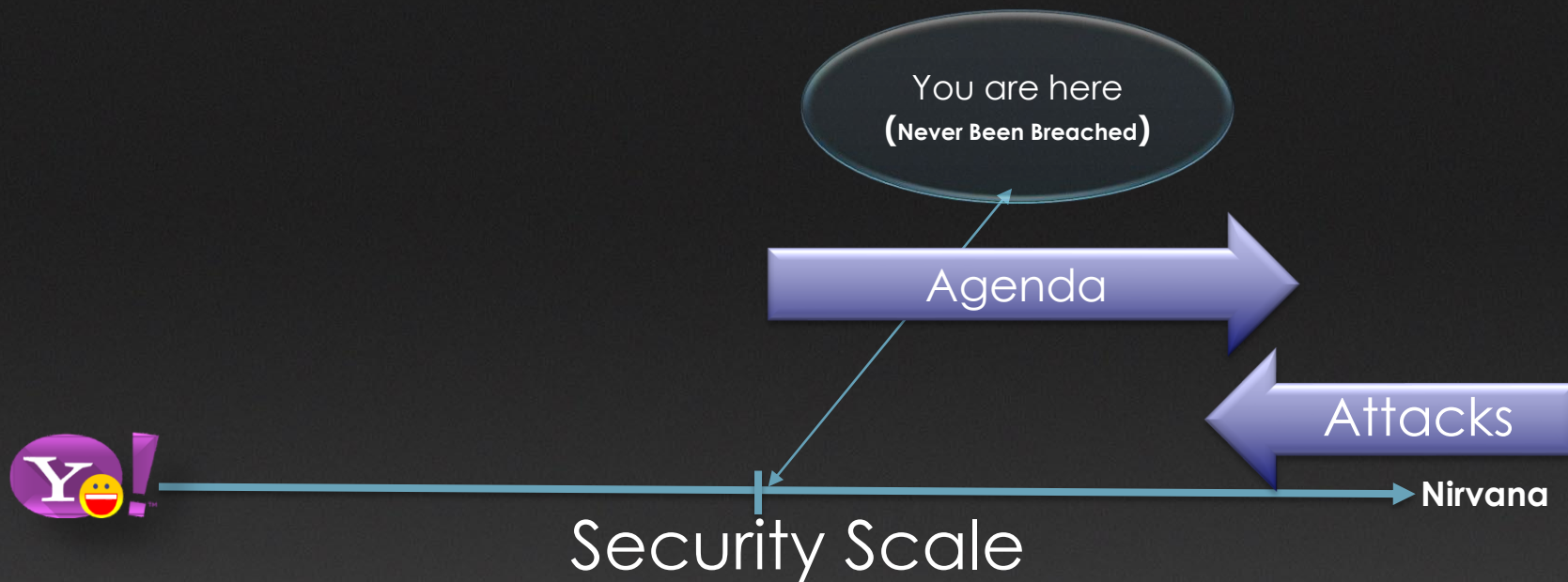
THALES



www.thalesgroup.com



Agenda



Data Economy

60

Spotify

13 New Songs Added

15,220,700 Sent

Text

Twitter

456,000 Tweets send

2.5 Quintillion bytes a day

Riders take 45,787 trips

Uber

Google

Conducts 3,607,080 searches

Uses 2,657,700 GB of Internet Data

Americans

Amazon

Make \$ 258,751.90

Attacks are overcoming traditional security methods every minute

2,600,968,280

Records exposed in 2017

is a result of

1,765

data breaches globally

100% Irrelevant for 99% people

EVERY DAY

EVERY HOUR

EVERY MINUTE

EVERY SECOND

Number of records
compromised

7,125,940

296,914

4,949

82

More than 96% of all data breaches involved data that was **NOT**
ENCRYPTED

A full-body shot of Dr. Evil from the Austin Powers International Man of Mystery. He is bald, wearing a grey jumpsuit, and has a wide-eyed, crazed expression. He is holding up both hands in peace signs. A large black nuclear missile is balanced horizontally across his shoulders. The background is a dimly lit control room with various screens and equipment.

Think like a bad guy



Script Kiddies

Organised Gangs

CAAS
(Cybercrime AAS)



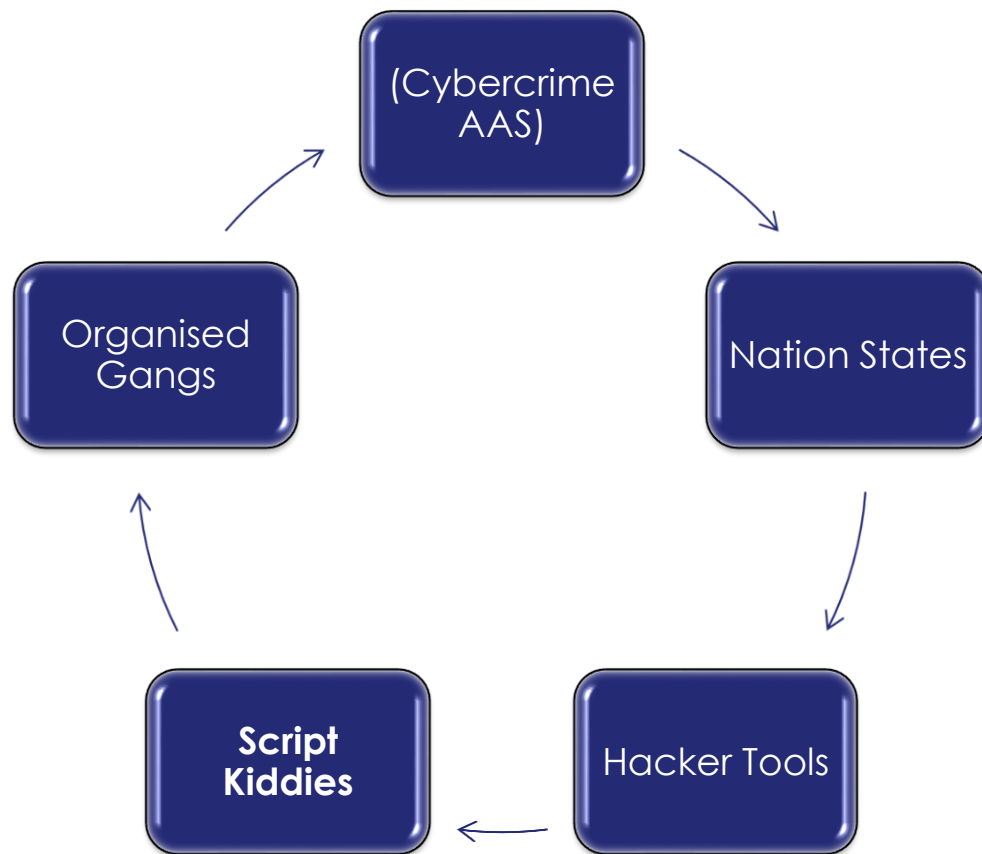
Nation States

THALES

Duqu, “Son of Stuxnet”

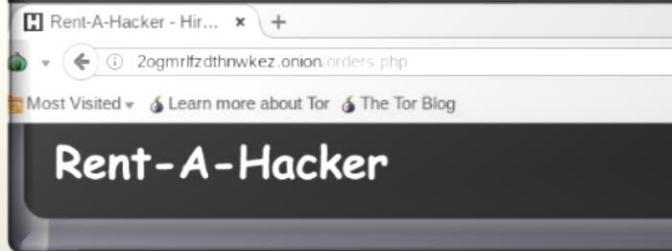
- **What it is**
 - A trojan announced by Symantec on 20 October 2011
- **What it targets**
 - Microsoft Windows
- **How it spreads**
 - Zero-day exploit in Microsoft Word documents
- **What it does**
 - System profiler and **info-stealer**
 - Exfiltrates data to C&C servers
 - Unspecified companies in France, Netherlands, Switzerland, Ukraine, India, Iran, Sudan, Vietnam, UK, Austria, Hungary, Indonesia...
- **Who did it**
 - No attribution to date

- **Why “Son of Stuxnet”?**
 - Methodology and portions of code identical to Stuxnet
 - Effects and purpose appear different



RESEARCH

ATM malware is being sold on market



Free test ...for serious customers"

contact me:
ICQ- [redacted]

"There are discounts for regular clients"

Our service:

- There are discounts for regular clients
- Free test for 5-10 minutes (only for serious customers)
- Anonymity (no one knows who did have a particular order)
- In the case of the order refunds for the remainder of the order

In the case of the order refunds for the remainder of the order

HACKING TOOLS & SERVICES

Account Hacking Program	\$12.99 (See more details on page 10)
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts \$15 - \$60
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental \$750 Monthly Full Rental \$1,200 Monthly Support \$150
Disdain Exploit Kit	Day \$80, Week \$500, Month \$1,400
Stegano Exploit Kit: Chrome, FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day \$2,000 Unlimited Traffic, Month \$15,000
Microsoft Office Exploit Builder	Lite exploit builder \$650 Full Version \$1,000
WordPress Exploit	\$100
Password Stealer	\$50
Android Malware Loader	\$1,500
Western Union Hacking Bug For World Wide Transfer	\$300
DDoS Attacks	Week long attack \$500 - \$1,200
ATM Skimmers: Wincor, Slimm, NCR, Diebold	\$700 - \$1,500
Hacking Tutorials	Multiple Tutorials \$5 - \$50

aaS - Password cracking service

Nice introduction

Your victim details

"where did you heard about us?"



nets, RATs, virus, ransomware and malware creation.



Elitehackingservices •

Peasant



2017, 01:24 AM (This post was last modified: 11-26-2017, 03:08 PM by Elitehackingservices.)

... offering a load of rats botnets and various viruses and ransomware for sale.

... can contact me on elitehackingservices@gmail.com or skype tiaslove.

... es vary depending on what you need.

How Are We Prepared For Cyber Attack

There is no perimeter.
You cannot "fight back".

It's not a fight of equals

There are no rules.
It's not a one to one fight.
Attacker is always anonymous

Attacker have to succeed just once

The intention is not just to defeat the defence



Is cloud answer?





Pizza as a Service 2.0

<http://www.paulkerrison.co.uk>

Tradition
On-Premises
(legacy)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Homemade

Infrastructure as a
Service
(IaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Communal
Kitchen

Containers as a
Service
(CaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Bring Your Own

Platform as a
Service
(PaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Takeaway

Function as a
Service
(FaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Restaurant

Software as a
Service
(SaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Party

Configuration

Functions

Scaling...

Runtime

OS

Virtualisation

Hardware



You Manage



Vendor Manages

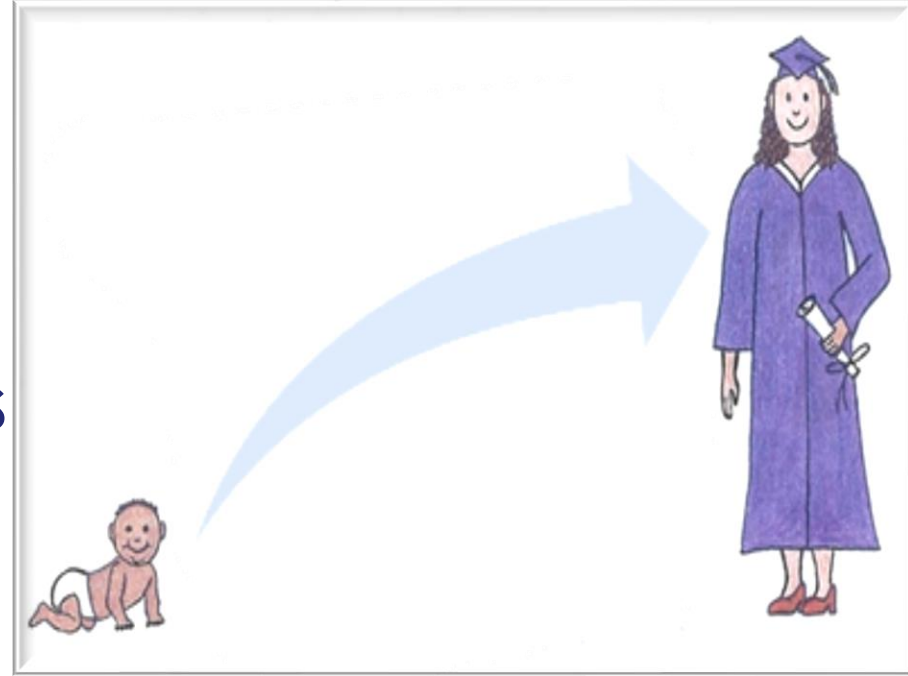
Ten Years worth of problem in six months

Traditional Datacenter



vs

Cloud





Why we fail?



Who is more scary???



Hackers

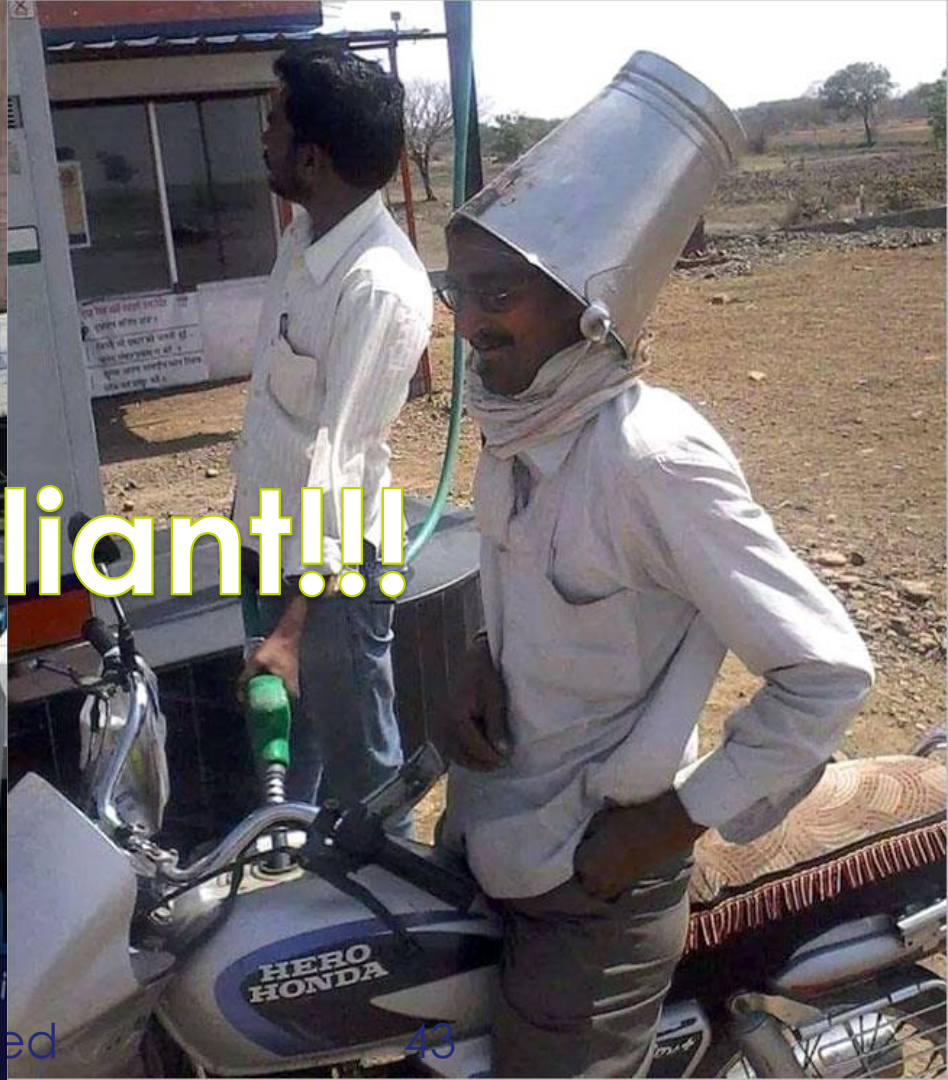


Security Team





Compliant!!!

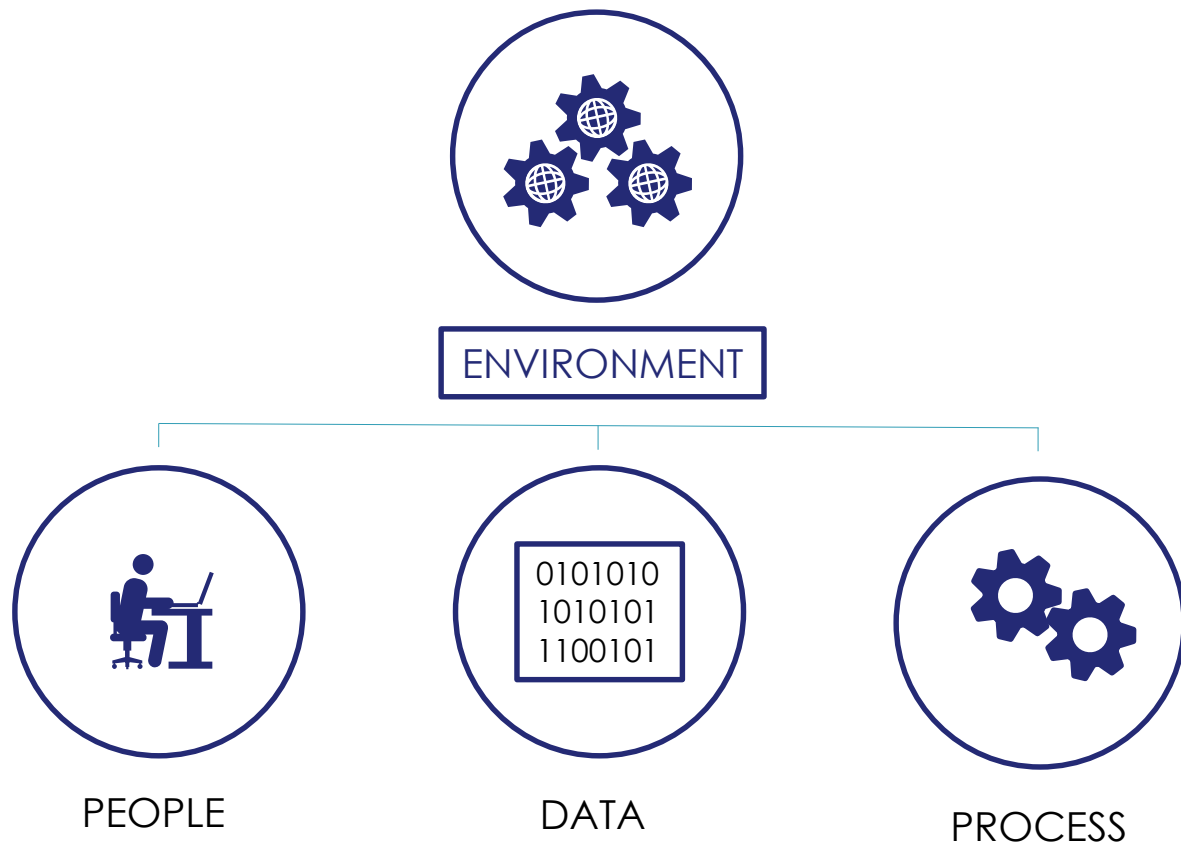




Access Control Simplified

www.thalesgroup.com







PEOPLE



EMPLOYEES



3RD PARTIES



CONTRACTORS

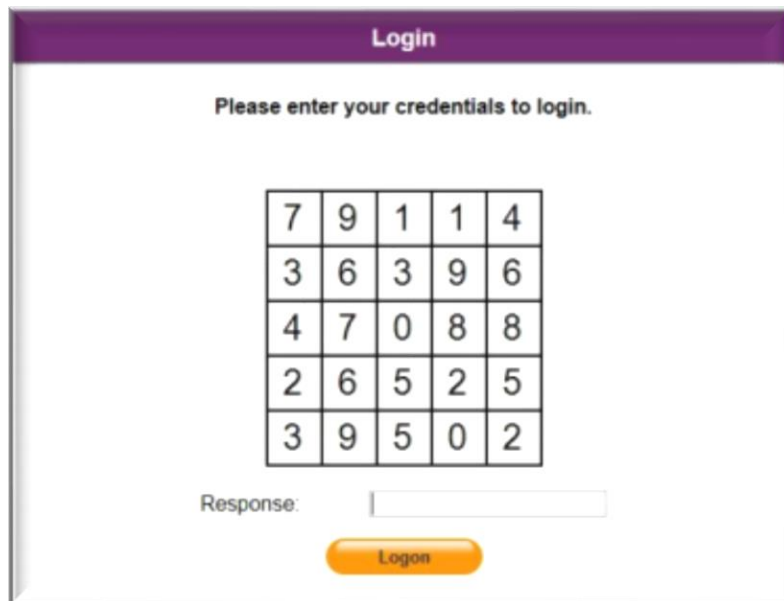
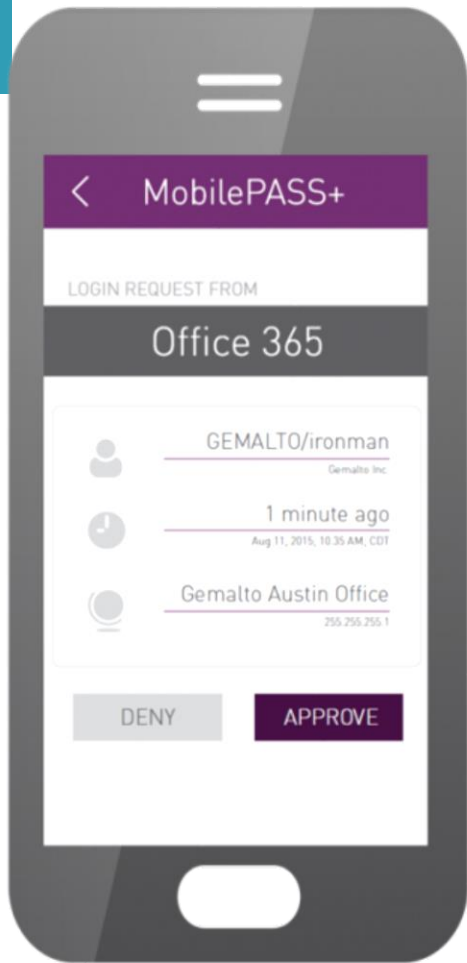
What's Wrong With Passwords?



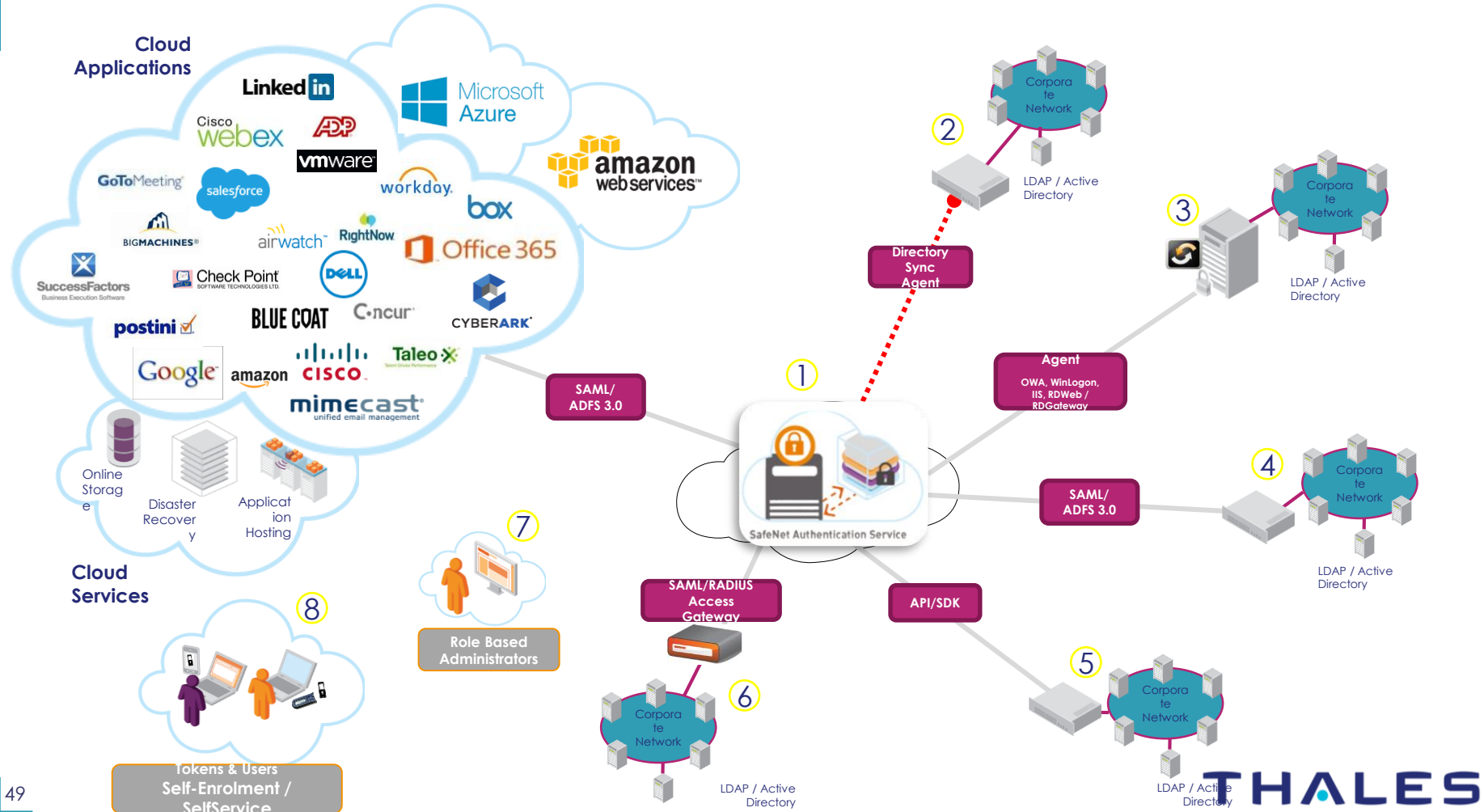
We knew the problem with static passwords even before we started to use them in cyber space



The solution was to increase the security of the passwords however everyone forgot to consider how many passwords humans can remember.



Where To Enable Two Factor A





Single Sign On

www.thalesgroup.com



User Experience vs Security

Choose very complex password



Enter password for each application



Single Sign On



Single Sign Off



Network



Cloud



IT



Legacy Web



VDI

Orchestration / Business Logic

Policy Management

Risk Assessment

Geo fencing

SSO Session Management

AUTHENTICATION



OTP Push



PKI

* * *

Password Kerberos



Windows Hello



FIDO



3rd Party

DEVICES



CONTEXT



THALES



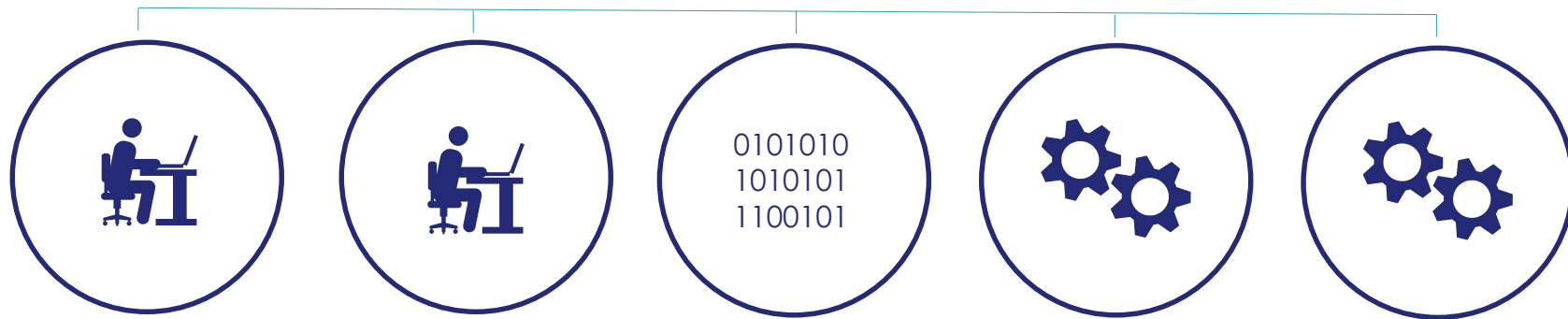
Data Security Simplified

www.thalesgroup.com





DATA LOCATIONS



DB

FILE

FOLDER

VM

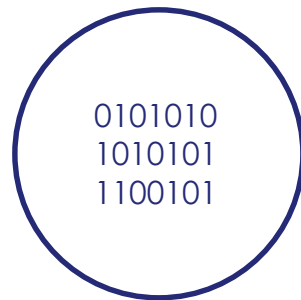
NETWORK



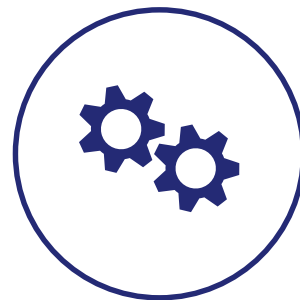
PII



CREDIT CARD



HEALTH CARE



TRADE SECRETS



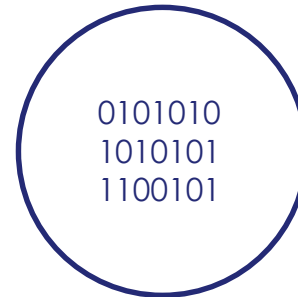
SOLUTIONS



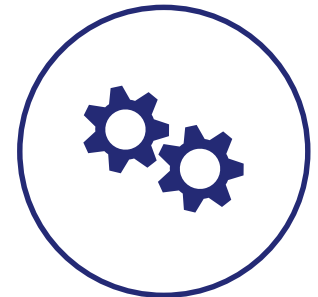
AUTHENTICATION



ENCRYPTION



KEY MANAGEMENT



ROOT OF TRUST

#1: Why is Encryption Secure?

Example: AES128 = $3,4 \times 10^{38}$ Keys

Assuming
a Super Computer can calculate ~ 1 Billion Keys / second,
we have 100 Super Computers,
we find the key in the 1%.

Finding the Key takes 10^{22} years. Universe is 10^{11} years old.

Attacks On Cryptography

- Ciphertext-Only attack
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Differential cryptanalysis – Side Channel attack
- Linear cryptanalysis
- Implementation attacks
- Replay attack
- Algebraic
- Rainbow Table
- Frequency Analysis
- Birthday Attack
- Social engineering for key discovery
- Dictionary Attack
- Brute Force
- Reverse Engineering
- Attacking the random number generators
- Temporary Files

Is “just” Encrypting data good enough?

- ✧ Ransomware
- ✧ Database encryption with weak access controls
- ✧ Full Disk encryption with user-name & Password



Path of Least Resistance: Break the Lock or Steal the Key?



#2: Why do we need external Key Management?

No one tries to crack encryption by calculating the keys...


It's easier to use the key and decrypt the data

Separate Keys from Data and Store/Manage Keys securely



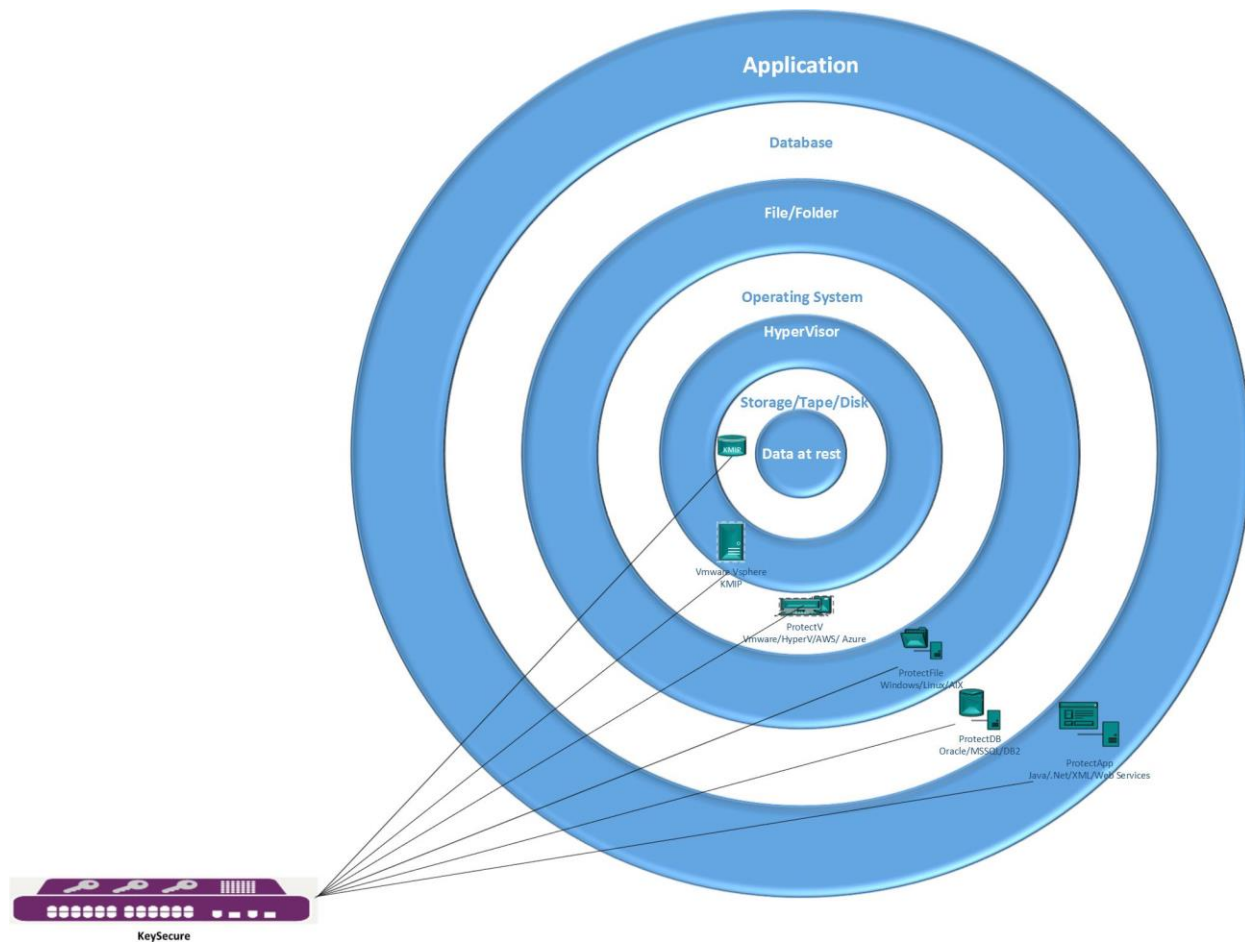
Data Encryption Simplified



A close-up shot of a dragon's head, likely from the movie 'The Hobbit: The Desolation of Smaug'. The dragon's mouth is wide open, revealing a dense array of sharp, orange-brown teeth. Its scales are dark and spiky. In the foreground, the back of a person's head with long, flowing white hair is visible, looking towards the dragon. A speech bubble is overlaid on the image, containing the text:

Honey,
Do you know how
to ride this thing?

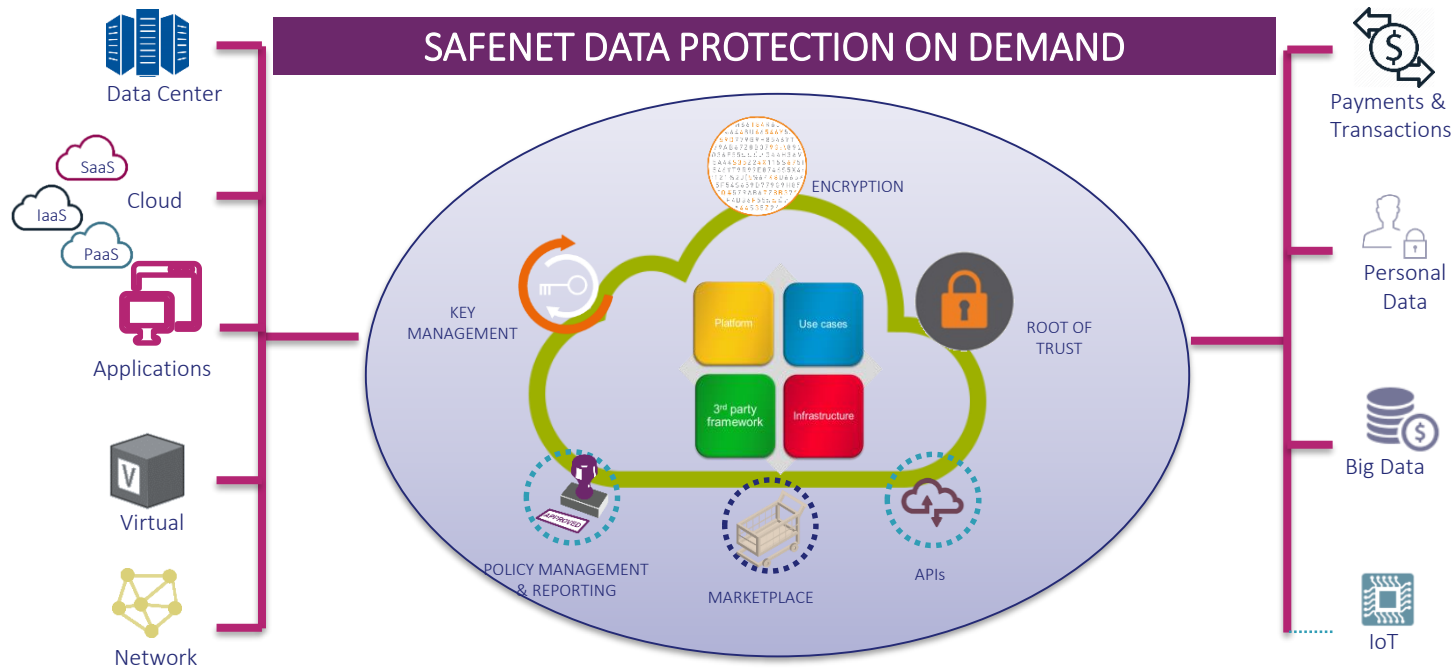
Where to Encrypt and Manage Keys?



Data Protection Now Available On Demand

Protect Everywhere

Protect Everything



Taking Traditional HSM and Encryption and Making it Consumable as a Service

Benefits for Customers

Designed to offer security-as-a-service quickly and easily



Zero upfront investment



White labelled versions



Easy to integrate into hundreds of applications



Centralized management



Multi-tenant capabilities



User friendly marketplace



Cloud-based pricing



Third-party API support



Automated:-
Deployments,
Billing, etc

Thank you, Drive Through



5/22/2019

67



Thank you

peter.wilbrink@thalesgroup.com

www.thalesgroup.com

