THALES

Overview

Over **80,000** employees

68 Countries Global presence

1 bn €

Self-funded R&D*

* Does not include externally financed R&D

Sales in 2018

19 bn €

THALES

THALES

Thales CPL-Identity & Access Management

Digital Identity and Security

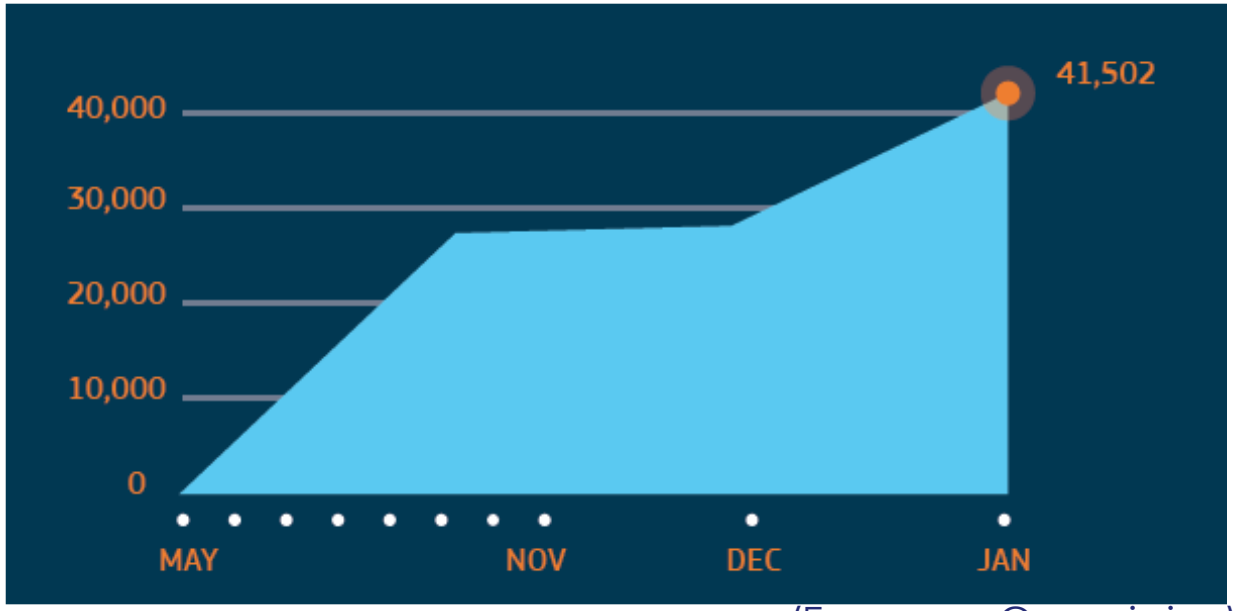
Cloud Protection and Licensing

www.thalesgroup.com

Traditional security is no longer sufficient

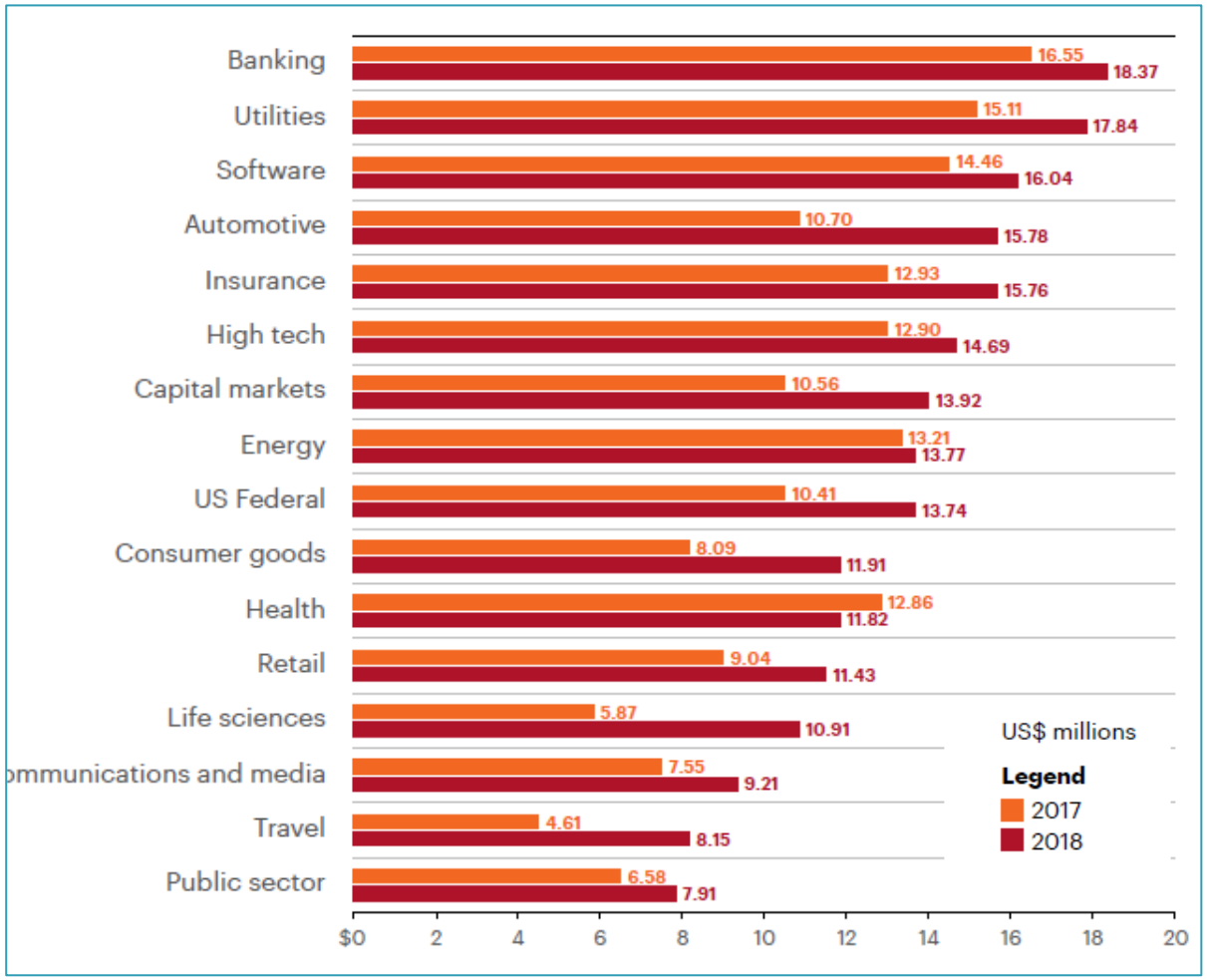
Breaches are growing year-on-year across all sectors

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



(European Commission)

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

81%

of breach incidents came from identity theft

Main cause of damages

UNENCRYPTED DATA

95%

of breaches involved unencrypted data

THALES

Authentication & Access Management

Access Management Challenges

The end of the perimeter

The limitations of legacy IAM

- Focused on inbound & outbound (border/proxy)
- Not context-aware

The loss of security controls

- IT can't control all the applications…but…
- Emergence of Zero-trust model

ID theft on the rise

- Cause of 81% of breaches

Increased regulations

- GDPR, PCI-DSS, DFARS, EPCS, etc.

Cloud services are targets for cyberattacks

49%

of businesses believe cloud applications are the biggest targets for cyberattacks

Data Breaches driving access management adoption

94%

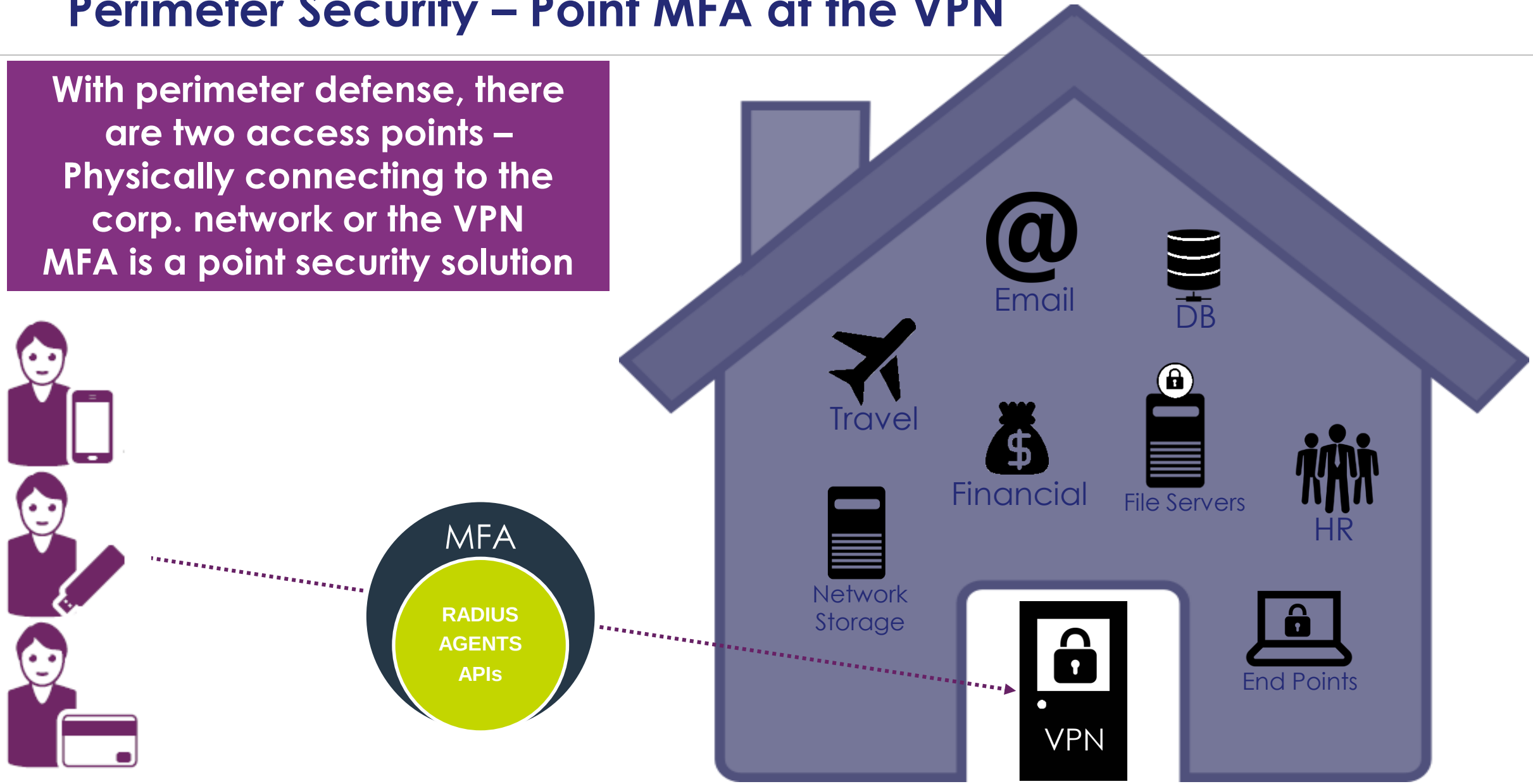
of organizations' security policies have been influenced around access management are influenced by consumer breaches in the last 12 months

62%

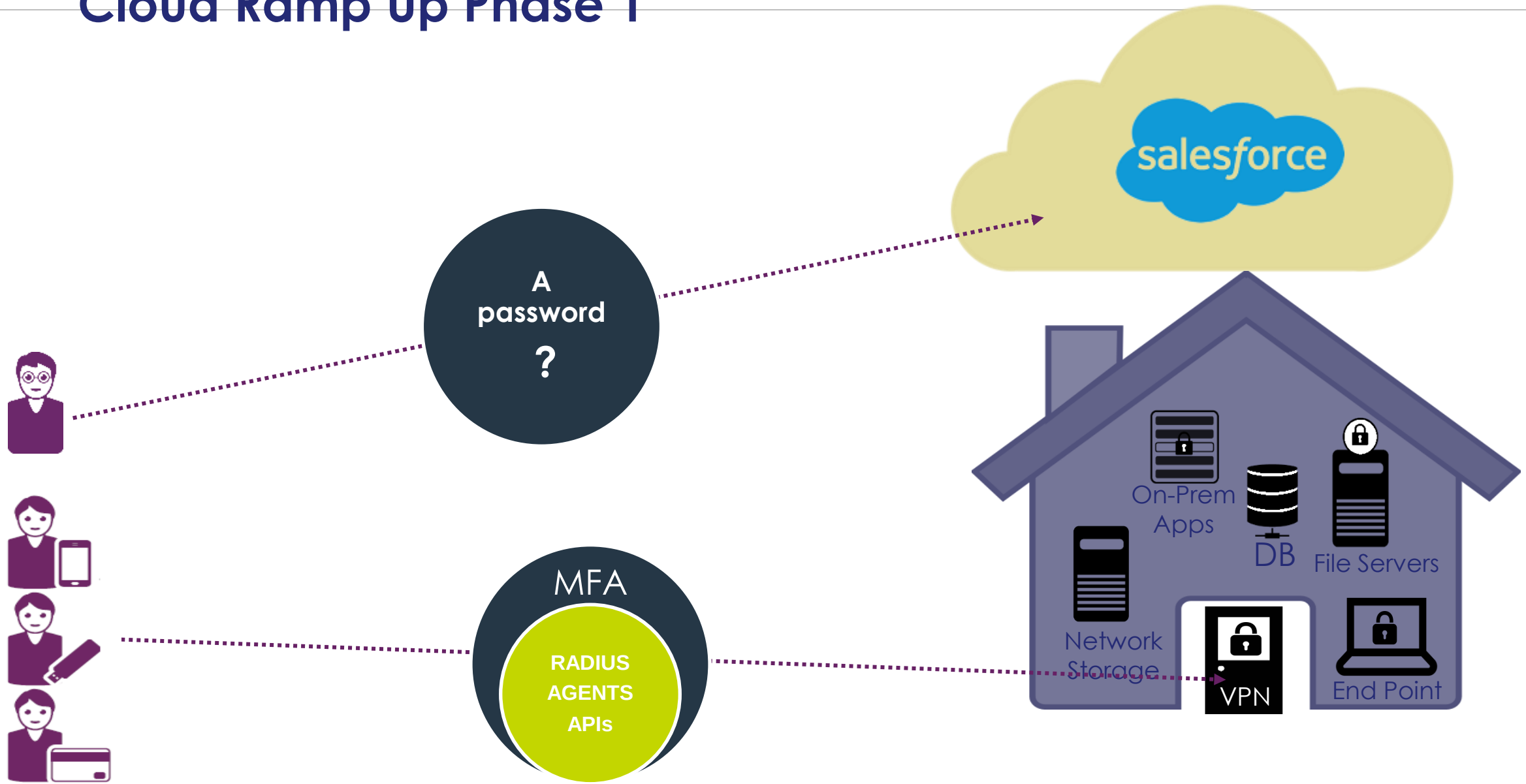
of companies continue to operate without a CISO despite increased cybersecurity awareness

Perimeter Security – Point MFA at the VPN

With perimeter defense, there are two access points – Physically connecting to the corp. network or the VPN MFA is a point security solution

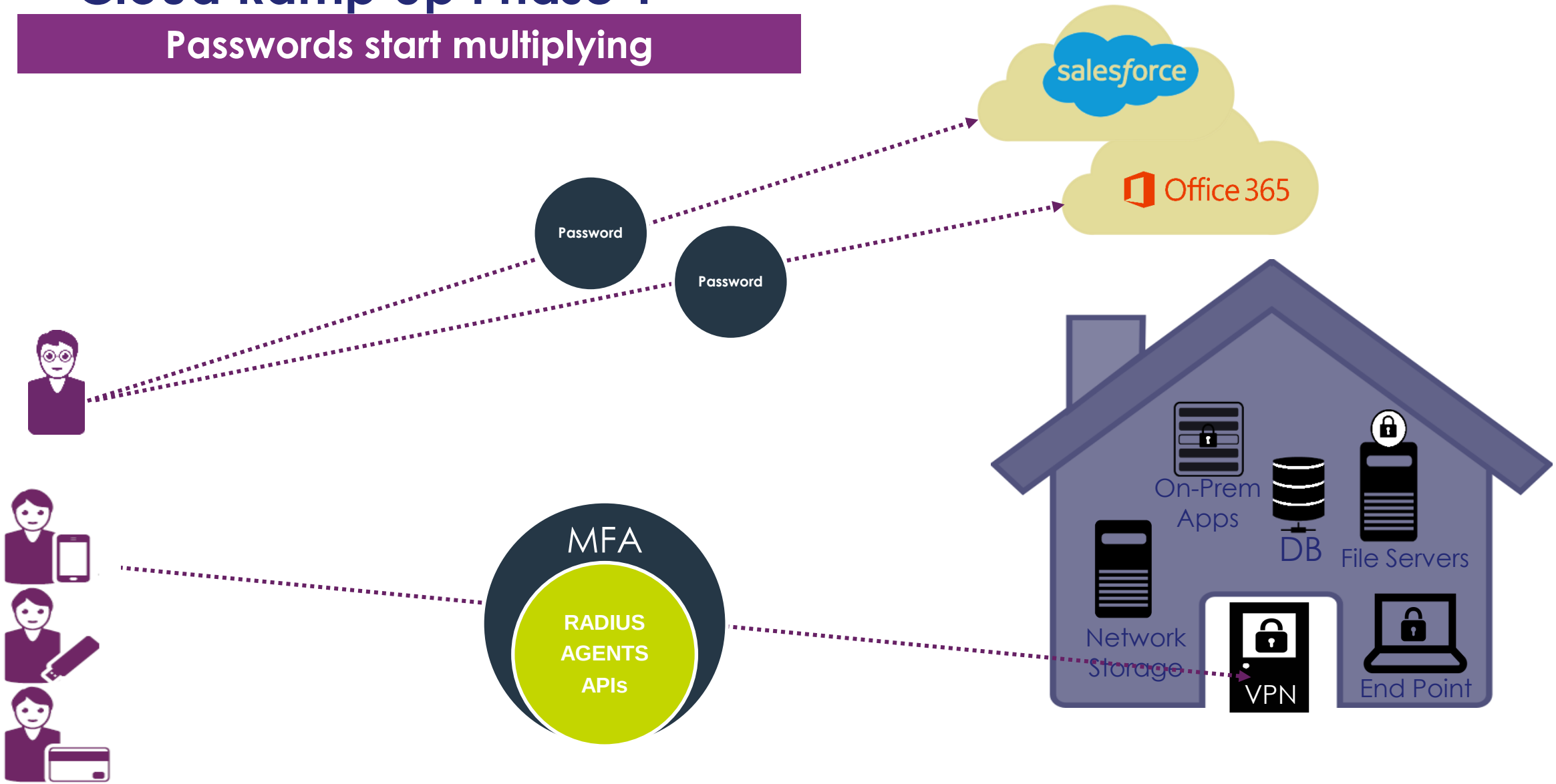


Cloud Ramp Up Phase 1

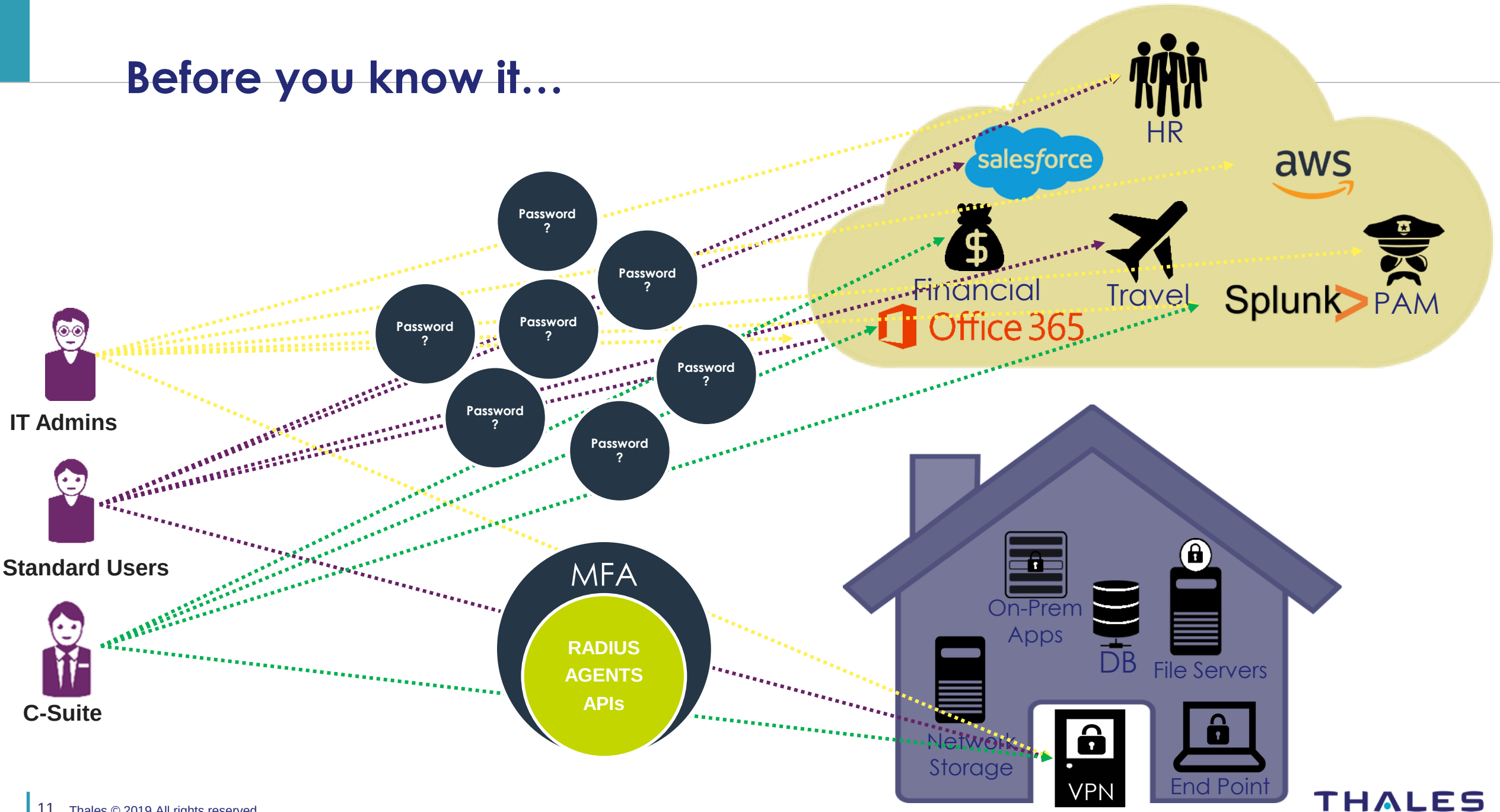


Cloud Ramp Up Phase 1+

Passwords start multiplying



Before you know it…



My day in the cloud

Multiple Logins

&

Lots of SENSITIVE Data !

O365

salesforce

Jira

ADP

zscaler

confluence

Cytric

My day in the cloud

27

O365

salesforce

Jira

ADP

zscaler

confluence

Cytric

THALES

SafeNet Trusted Access

Cloud Access Management Service

Leveraging cloud apps comes with its share of challenges

according to joint Ponemon-Gemalto research.

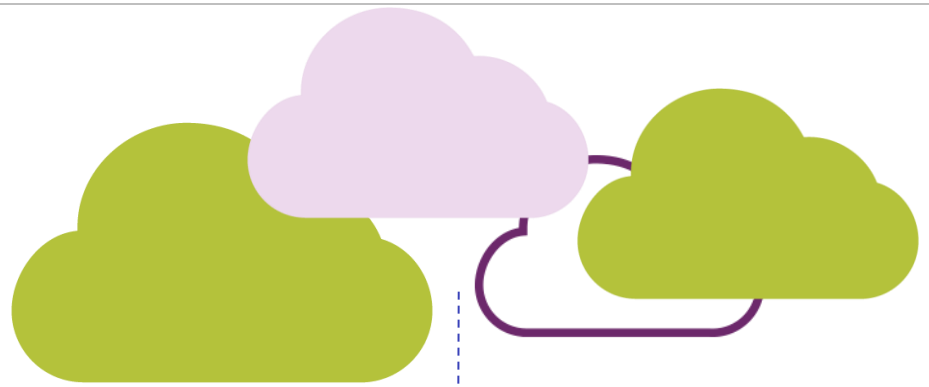
What is Single Sign On?

Single sign-on (SSO) provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various resources.

It eliminates the need to separately log in and authenticate to individual applications and systems, essentially serving as an intermediary between the user and target applications.

Source: Gartner

SSO offers a partial solution…

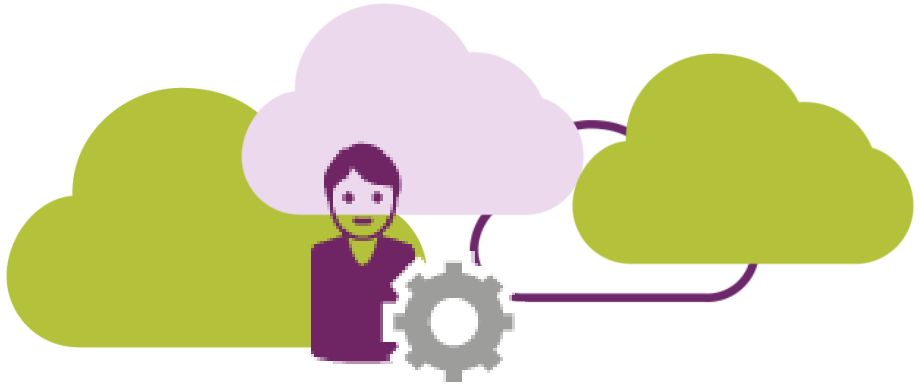


One Credential

For users:
- Convenient 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: SSO + IT Control Win-Win for Users and IT



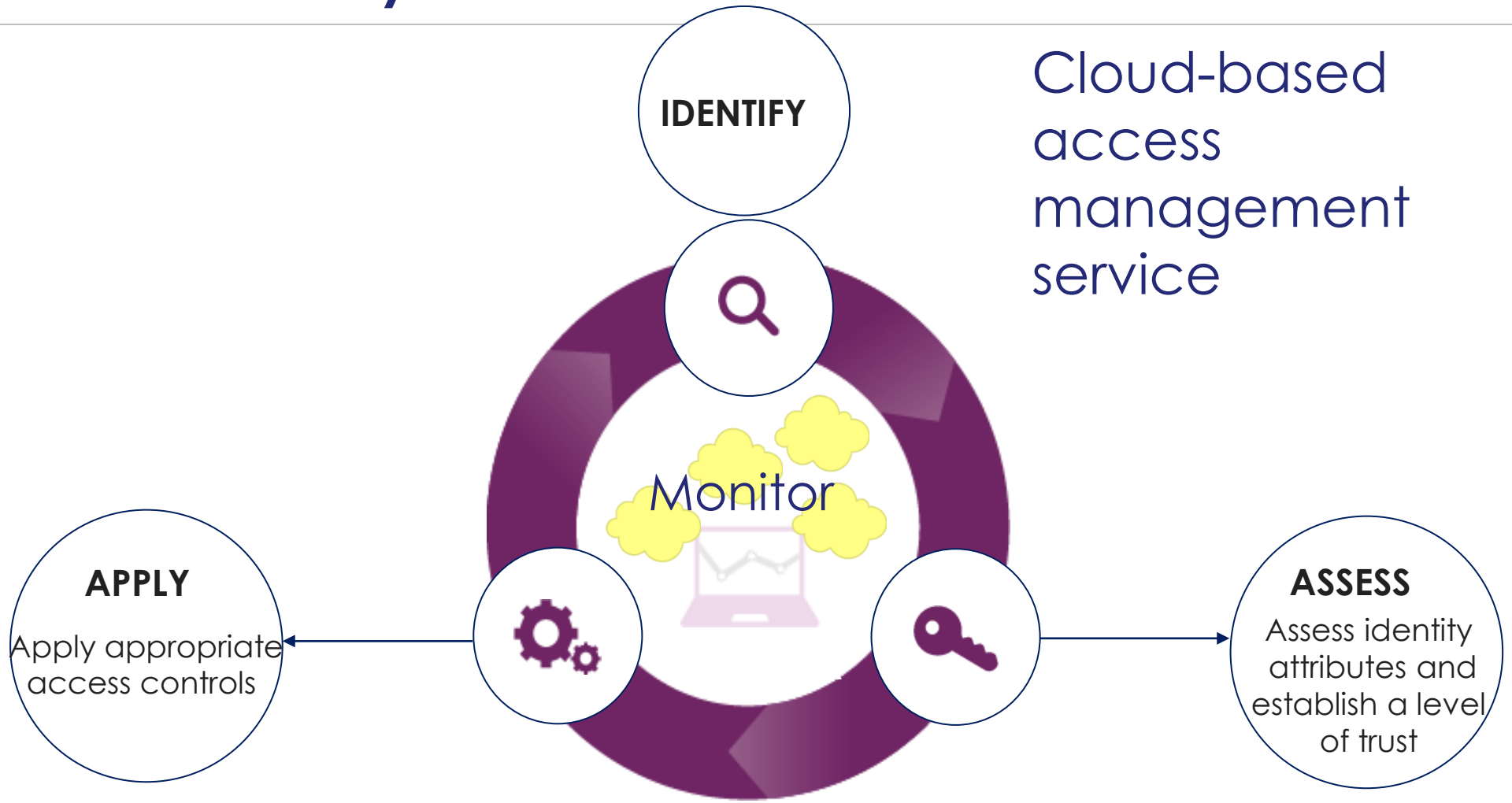
For users:

- Authenticate once and step up only 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

STA Functionality



Cloud-based access management service

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.

Manage risk through scenario-based policies

Office 365 · salesforce · Google G Suite · zendesk · slack · servicenow · JIRA · Confluence · citrix ShareFile · IBMSmartCloud · ORACLE WEBLOGIC · f5

Target Apps

IT Admins

Standard Users

C-Suite

Users/Groups

Policy Scope

Users

All Users · Any of these User Groups:

C-Suite

Applications

Any of

Default Requirements

…s attempt occurs, then access is

…enticating 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

THALES

Adaptive and Contextual attributes for STA

Network:

- IP address ranges whitelist or blacklist
- Detection of Anonymizer (anonymizing proxy or anonymizing VPN

Operating System:

- Allows you to determine the access policy based on the operating system type and version being used. For example, you can block access from unsupported operating systems.

User Device:

- Adjust the policy behavior based on whether the device is known for the user. For example, you can lower the authentication requirements when the device is known.
- Known Device : is the device known for this user based on past authentication

Location:

- Country whitelist or blacklist
- Change of country
- Drive different outcomes when a user has changed countries since their last access.

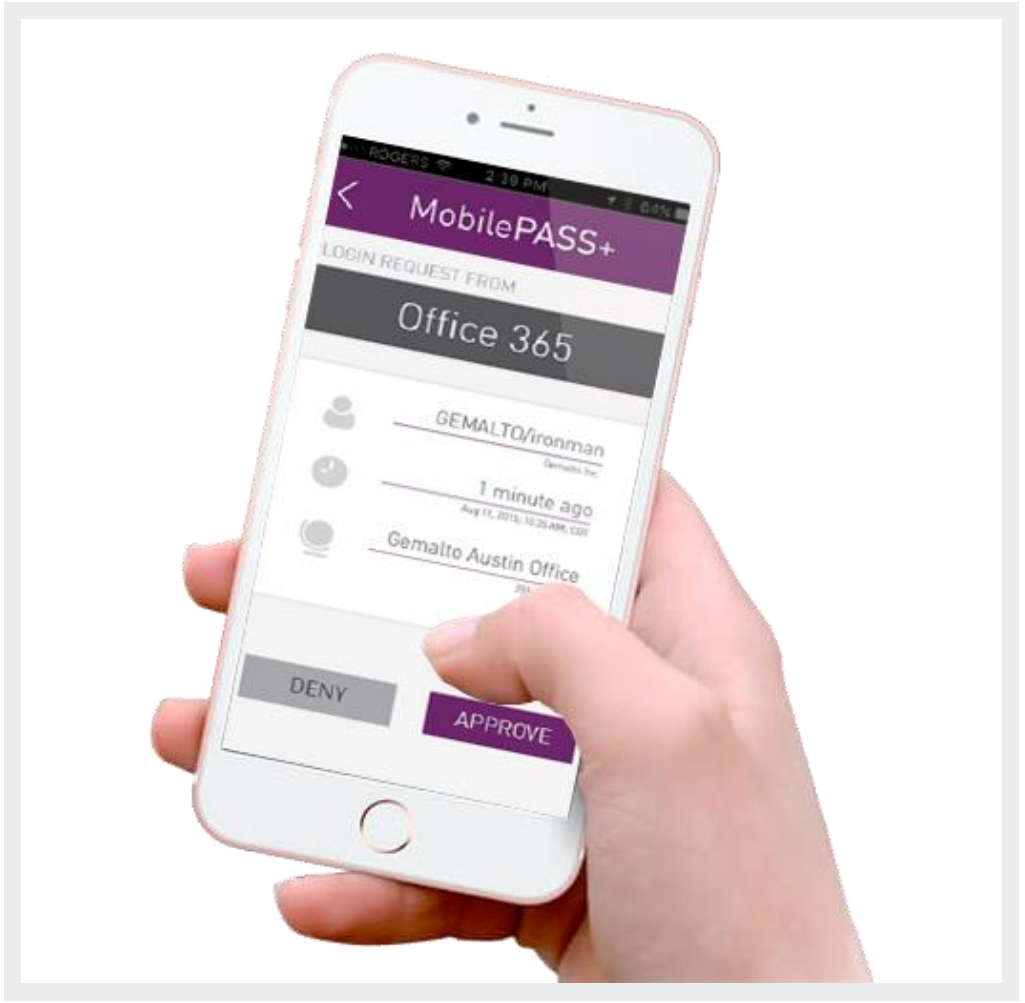
Scenario-based Access Policy Enforcement

Tailor Access Policies to App Sensitivity and User Role

- Step-up security for privileged accounts, such as C-Suite users and IT admins
- Step-up security for high value apps (e.g. VPN, Salesforce)
- Deny access or step-up authentication based on contextual Information

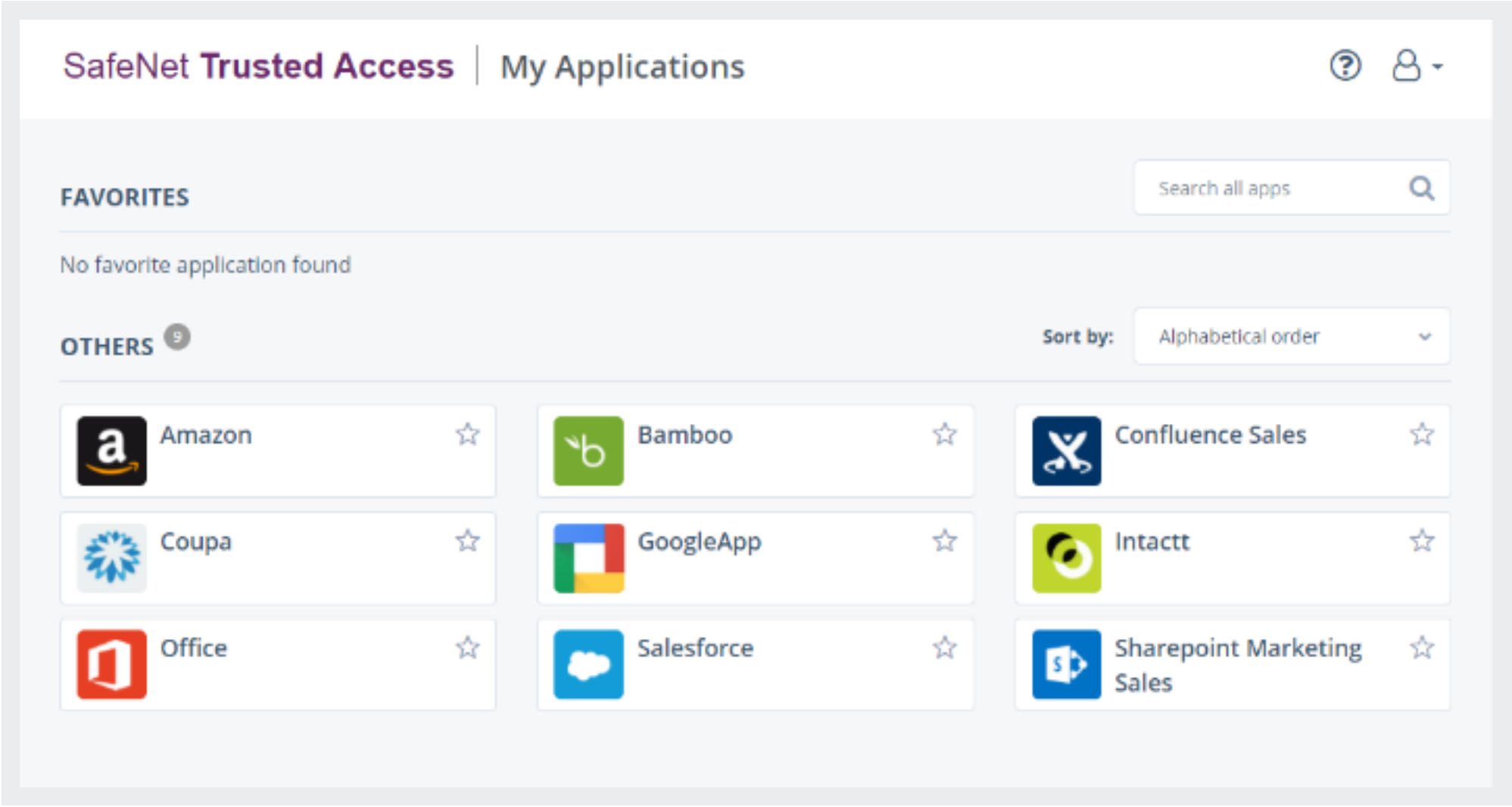
Tailor Access Policies to App Sensitivity and User Role

- Contextual information used to reduce access friction
- Leverage user's current Active Directory password



Launch all apps from a central user portal

Trigger Single Sign On by logging into the user portal



SafeNet Trusted Access

Universal authentication methods


Password


Kerberos


OTP Push


Hardware

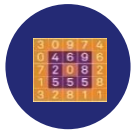

3rd Party


Google Authenticator

SMS


eMail


Voice


Pattern-based


PKI


Passwordless


Biometric

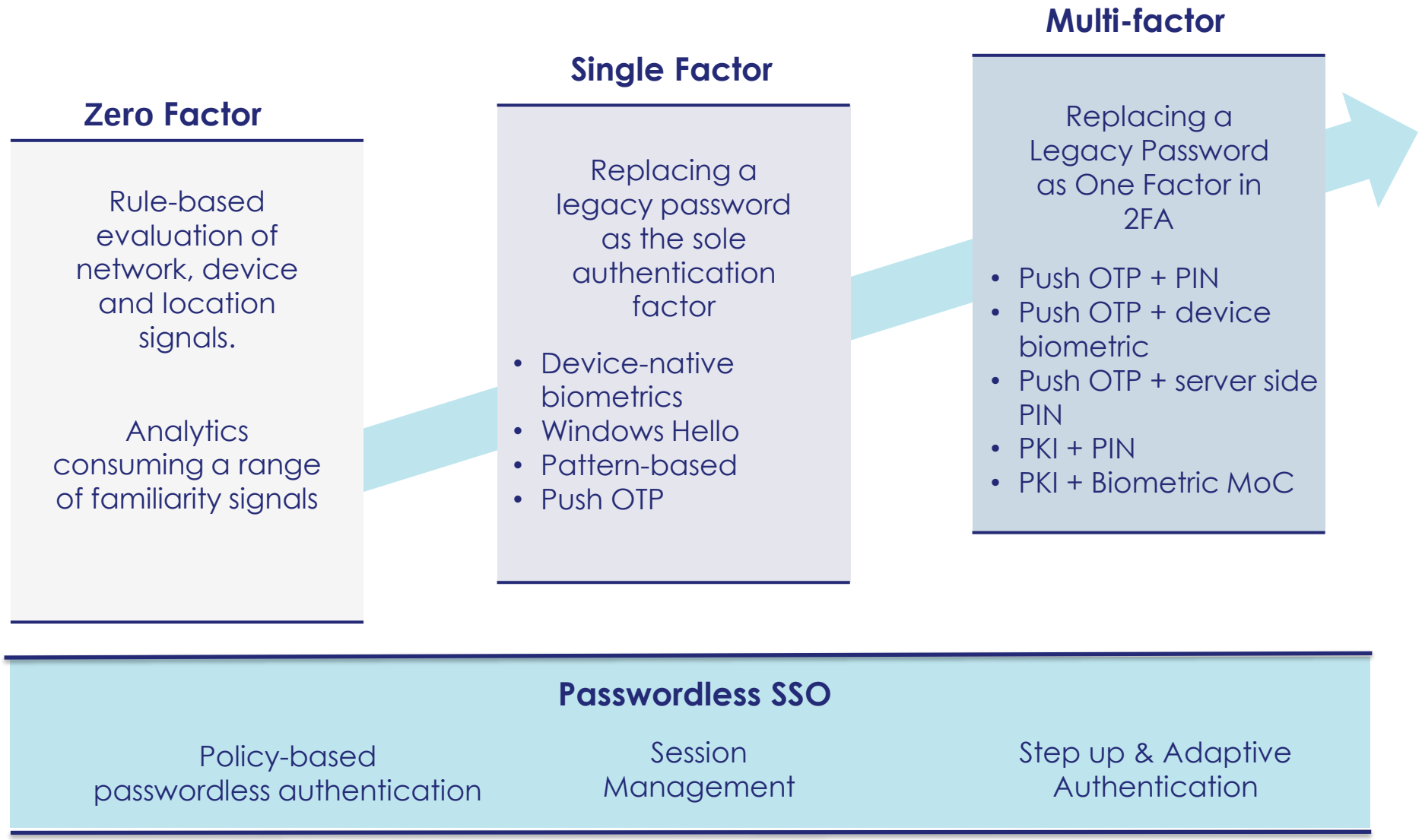
- Utilize the MFA schemes already deployed
- Extend PKI authentication to the cloud
- Offer the appropriate level of assurance
- Offer convenience with Passwordless authentication

PKI Transformation: Extending PKI to New Use Cases

Allow organizations to:

- Secure their cloud transformation with PKI:
  - Use hardware smart cards to authenticate to cloud and web-based apps
- Enable secure employee mobility:
  - Access apps from any device via VDI using virtual PKI smart cards

Assessing Models of Passwordless Authentication



SECURITY CHOICES

Flexible
Risk Based
Comprehensive

THE FOUNDATION

THALES

Why SafeNet Trusted Access?

Visibility

Know which access controls are applied to user access

Track cloud app usage

Know who is accessing which app and when

Security

Ensure the appropriate security policy is applied to each access attempt

Ensure the appropriate level of trust is applied

Scalability

Add new user groups, cloud apps and access policies as needs evolve

Eliminate help desk overheads associated with lost and forgotten passwords

Centrally define access policies for all your cloud apps

Convenience

Ensure users gain convenient access to apps through smart Single Sign On (SSO)

Enable users to log in to all their applications with a single identity

SafeNet Trusted Access
Built-in Integration Templates

Office 365 · salesforce · Google G Suite · amazon web services · GoToMeeting · box

zendesk · slack · servicenow · Dropbox · bambooHR · WordPress

JIRA · Confluence · Citrix ShareFile · Evernote · MobileIron · Symantec Blue Coat

IBM Connections · Oracle WebLogic · f5 · zscaler · PulseSecure · Drupal

Bring Your Own Apps

+

SAML 2.0 generic template

New templates added continuously…