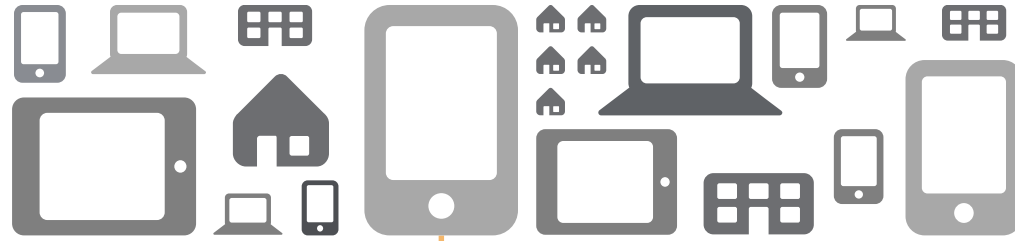# Secure Access in a Hybrid Cloud World

Tabrez Surve – Regional Security Sales Manager

Yasser Elmashad – Security Specialist

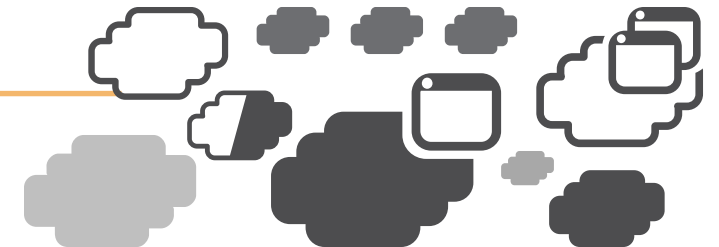# Business Today is Driven by Mobility and the Cloud…
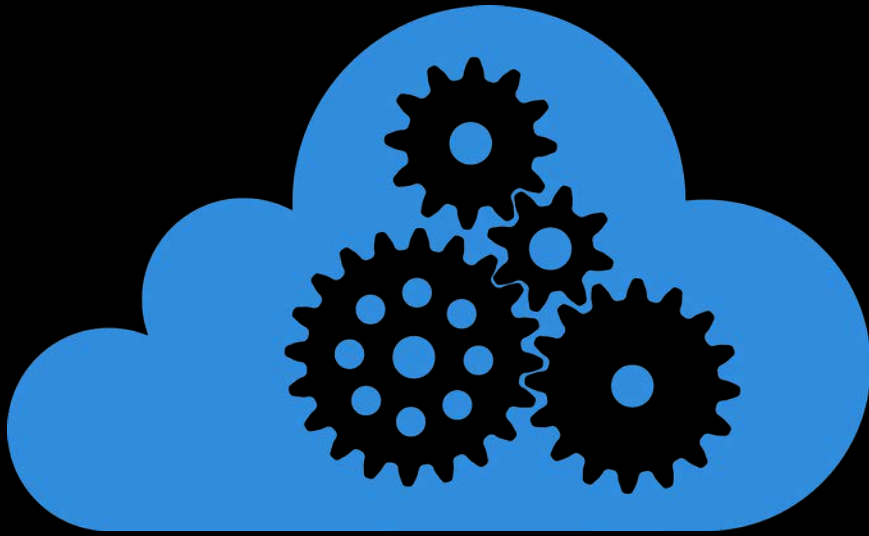
Today's workforce is
Mobile

Most applications are
Web-based apps

Cloud and SaaS-based applications
are being deployed and used faster than ever

Hybrid Cloud is the new normal.

81%
Enterprises have a hybrid cloud strategy[4]

20%
plan to migrate >50% of their Apps to the Cloud

Why are Apps moving to the cloud ?

Improve Time to Market   Reduce OpEx   Reduce CapEx

27%
Improve time to Market

41%
Reduce Opex

21%
Reduce Capex

Sources: F5 State of Application Delivery Survey, 2016

It's an Application World

508 Average number of apps per enterprise[3]

26.8 Average number of apps per worker[2]

3,5 Average number of devices per person[2]

Any App, Any Device, Anywhere !

| More endpoints | More delivery models | More apps |

Sources: [2]Forbes, [3]F5 State of Application Delivery Survey, 2016

From what we can see in the market …

- Majority of our customers adopt the following Hybrid Cloud Strategy
  - Move non Critical Apps to SaaS
  - New Apps with a Cloud 1st Strategy
  - Migrate some existing Apps to a Private Cloud

- Trend to move to Non Mission Critical Apps to SaaS
  - Focus on their business
  - Move from Capex to Opex basic IT services

The Cloud Spectrum
Not all clouds and services created equal...

Private Cloud · SDN · IaaS · PaaS · SaaS

PRIVATE CLOUD
On premises

PUBLIC CLOUD
Off premises

HYBRID CLOUD
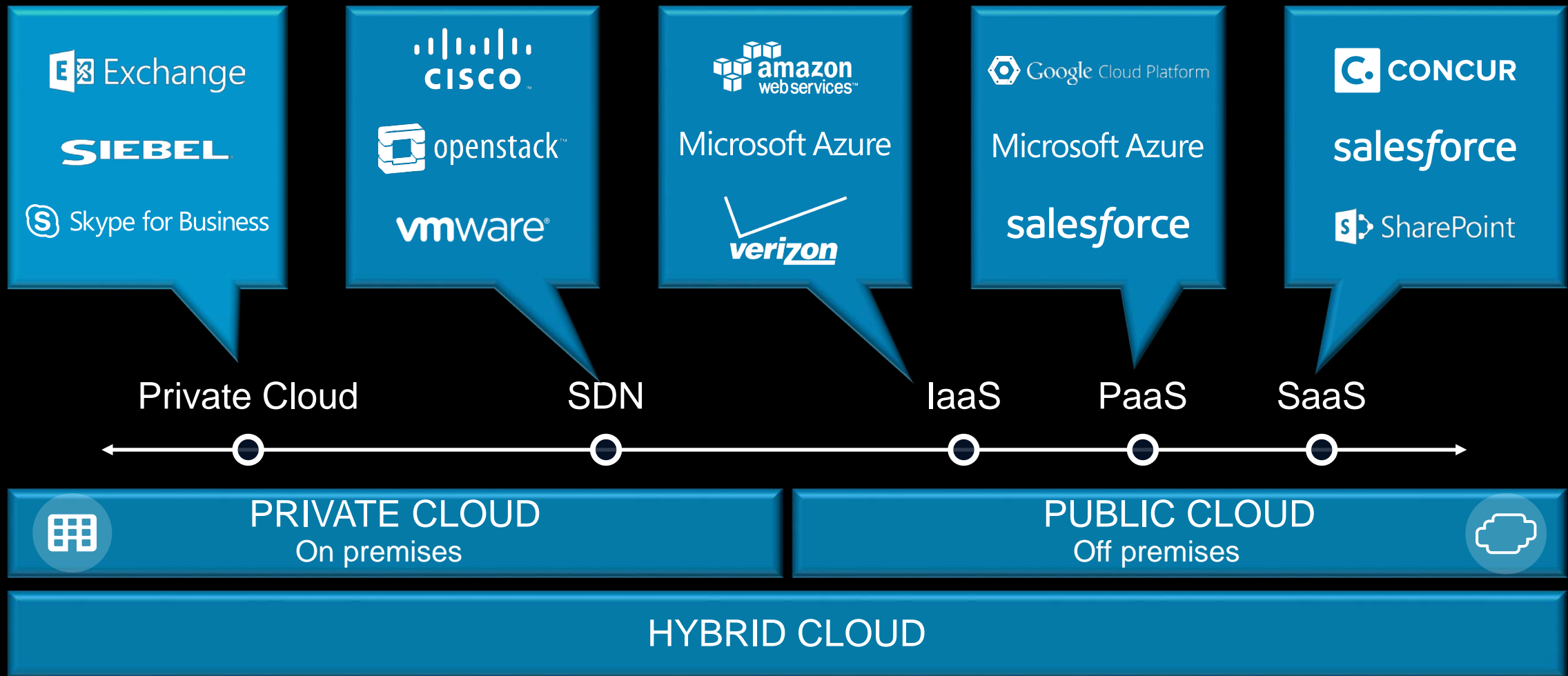
The Problem

Challenges of Managing Access Today

Rapidly expanding, changing mobile workforce

Explosion in number of users, use cases, in-use devices

Increased virtualization

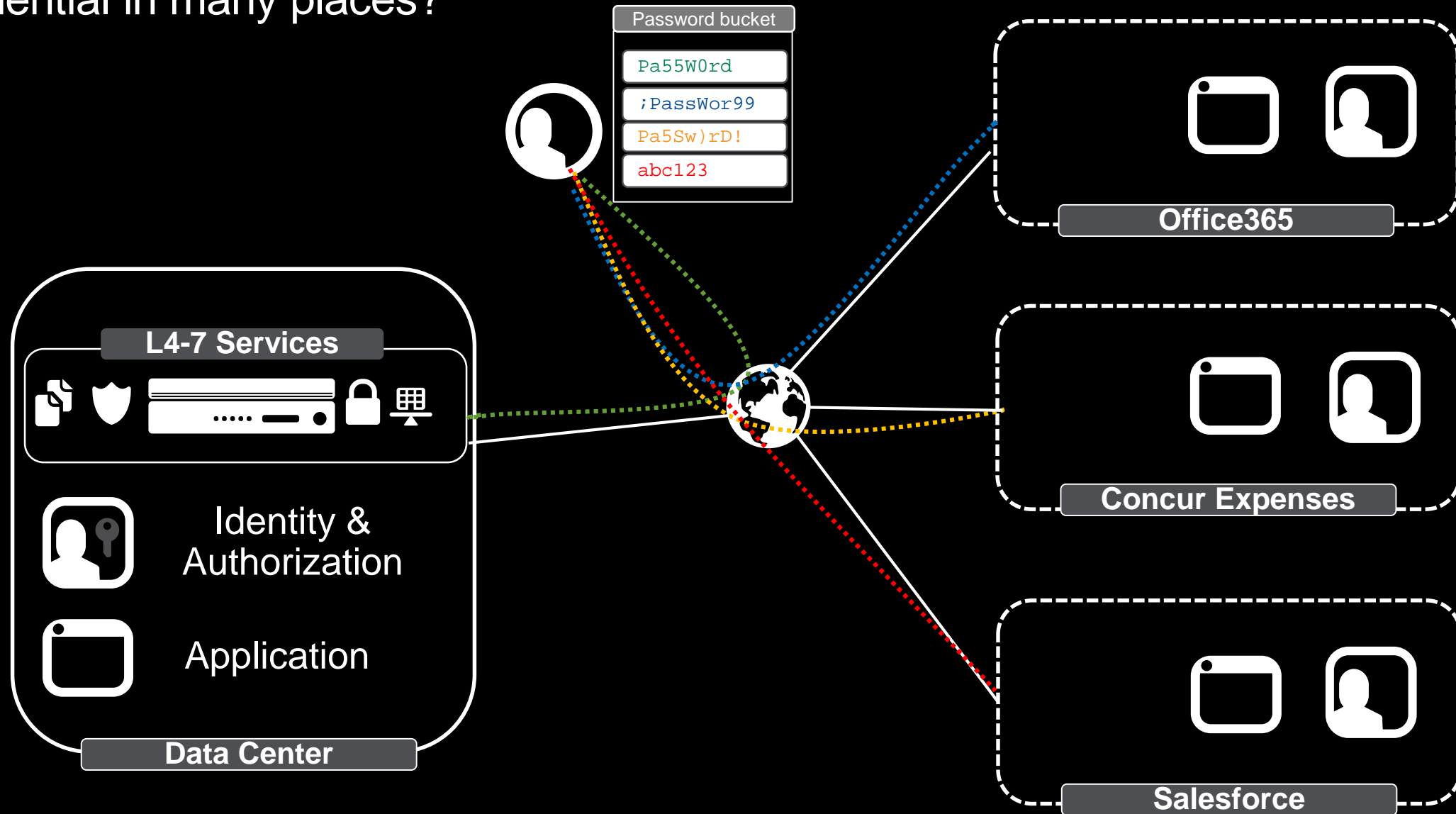Fast rising number of security threats and attacks

Need to manage access based on identity and context

Challenges with Apps moving to the Cloud

- App is moving to the Cloud but it's access policy & security is still customer IT responsability.
  - AAA Management with 3rd parties
    - Do I need to call Concur , MSFT, etc. everytime an employee joins or leaves the organisation to allow/kill its access to SaaS ?
  - Access to Apps in the Cloud still need to follow the same security mechanisms
    - Ex: Some Apps hosted in my DC are not authorised if accessed from non Company issued   devices.
    - How do you ensure your access policy is the same for all your Hybrid Apps.
- User Acceptance
  - Multiple Apps, multiple 3rd parties => multiple passwords.

User's Authentication and Experience
Credential in many places?

Password bucket

Pa55W0rd
;PassWor99
Pa5Sw)rD!
abc123

L4-7 Services

Identity & Authorization

Application

Data Center

Office365

Concur Expenses

Salesforce

Password Fatigue Leads to Weak Passwords and Credentials With Devastating Affects

Rising (monetary) costs of data breaches

$3.8M — **Average total cost of a data breach[1]**

23% — **Increase in data breach cost, '14 to '15[1]**

$154 — **Average cost per lost or stolen record[1]**

Rising (business) costs of data breaches

- Damage to brand reputation
- Compromises sensitive enterprise, employee and customer data
- Can result in significant downtime and lost revenue
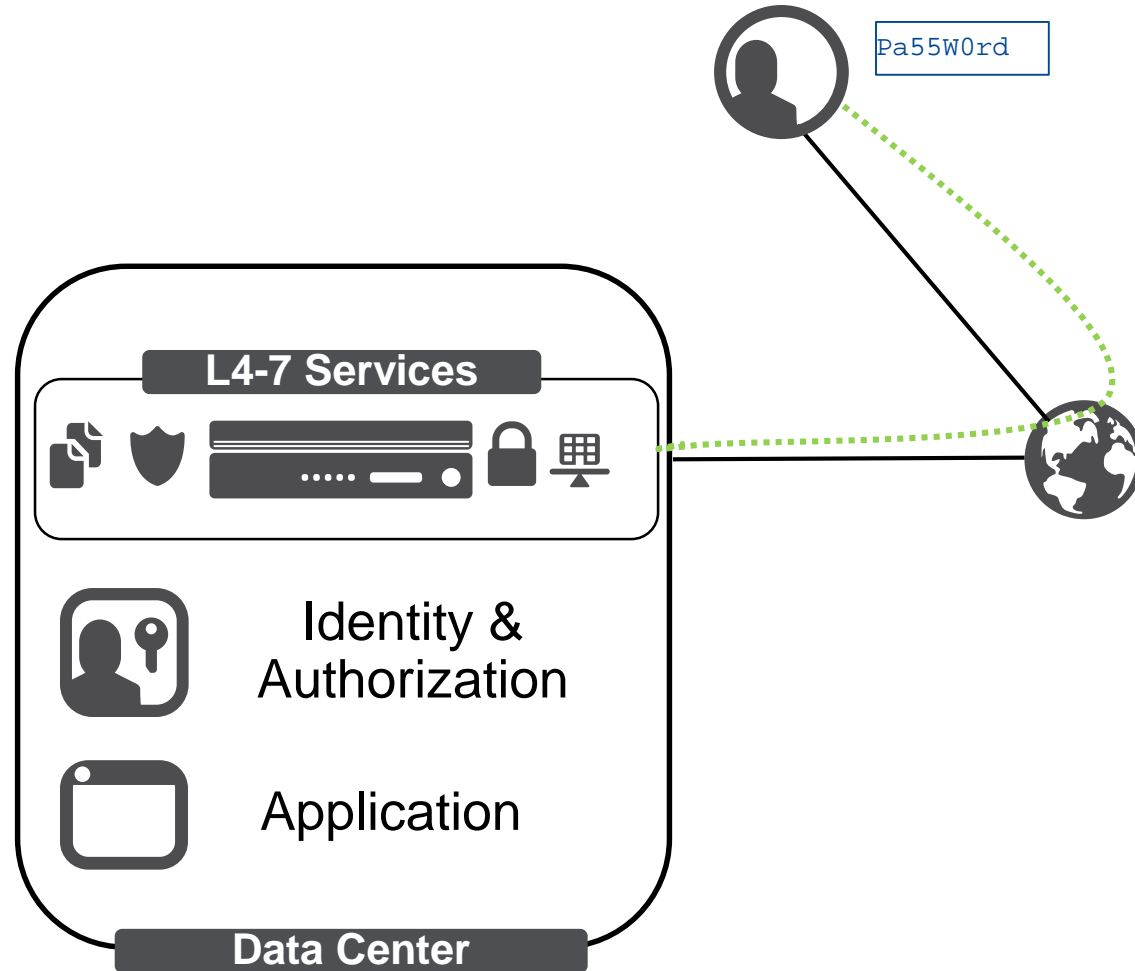- Breaches regulatory and/or government compliance required to conduct business

Solution

Identity Drives Application Access and Accessibility

Identity Used to be Easy

Pa55W0rd

L4-7 Services

Identity & Authorization

Application

Data Center

User Identity ≠ just User ID

Key Benefits:

F5's solution can optimize and prioritize resources.

Unparalleled insight into both known 'good' and known 'bad' traffic flow to maintain application health and protect critical assets

Industry leading intelligence ecosystem

North Korea

User ID	
Location	
End point	
Device health	
Device type	
Malware	
Sensitive Data	
Human	

Allow
Deny
Challenge
OTP
Client Cert.

UK

User ID	
Location	
End point	
Device health	
Device type	
Malware	
Sensitive Data	
Human	

Allow
Deny
Challenge
OTP
Client Cert.

Public Cloud Iaas

Low-Value App

Enterprise Datacenter

High-Value App
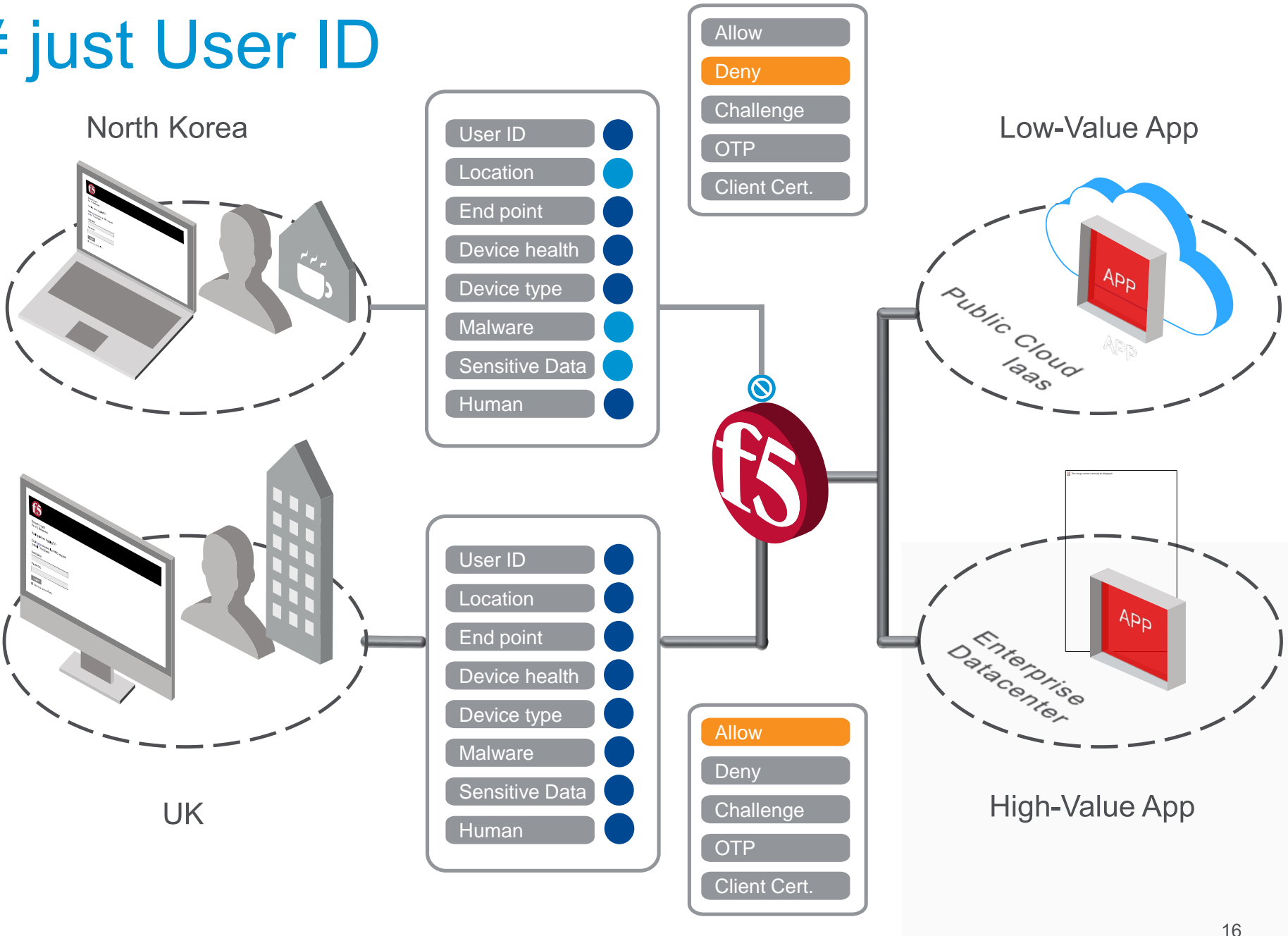
Controlling access through identity

User Identity and Device Information + **Network / Connection** + **Application Health and Risk**
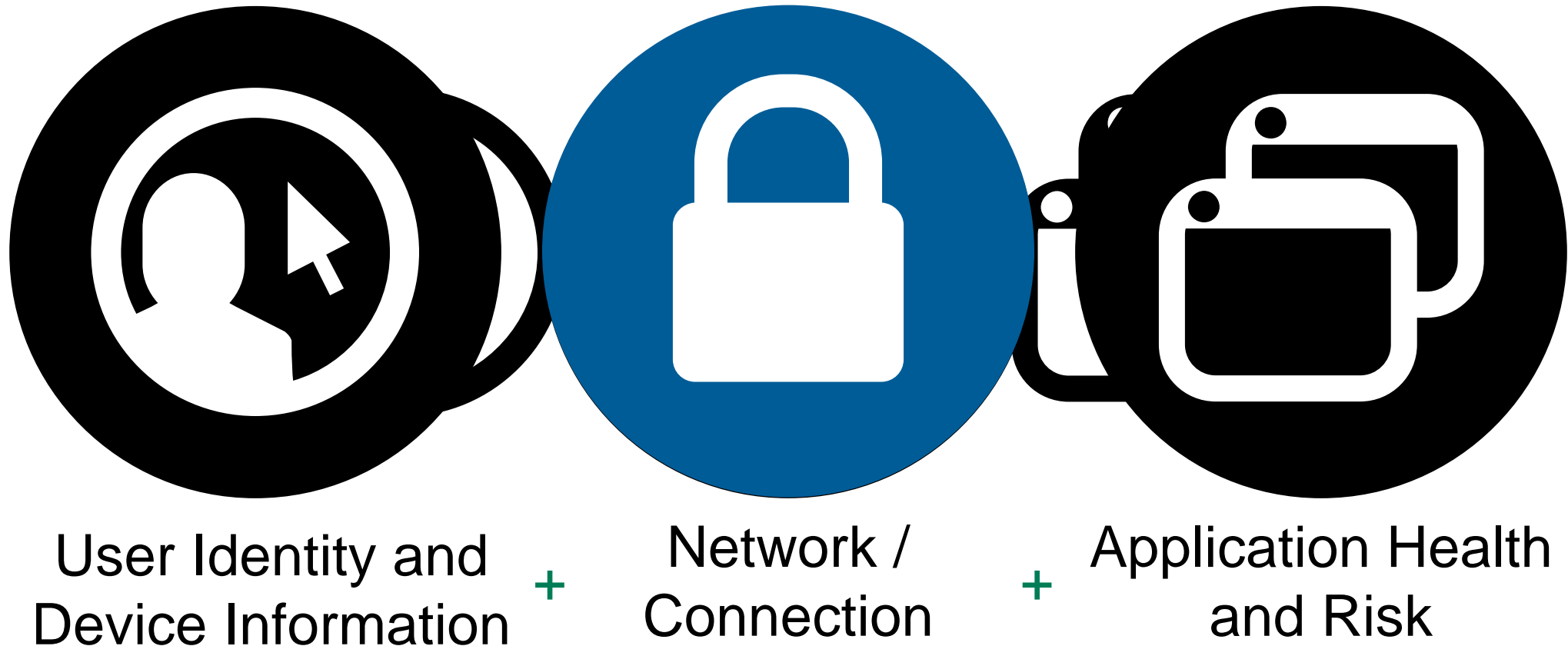
Identity is the Key to Adaptive Authentication and Access

Authentication

Device type and integrity

Operating system

Browser

Location

Access method

App location

App importance and risk

App type/version

Network integrity

Network quality and availability

Connection integrity

F5's Application Access Solution
Authentication, authorization, and SSO to all applications

Virtual Apps

VDI

Secure Web Gateway

Websites/Web Applications

Apps

Access Management

Remote Access and Application Access

Enterprise Apps

APM

VE Virtual Edition

Appliance

Chassis

Mobile Apps

Enterprise Mobility Gateway

Identity Federation/SSO

Cloud, SaaS, and Partner Apps
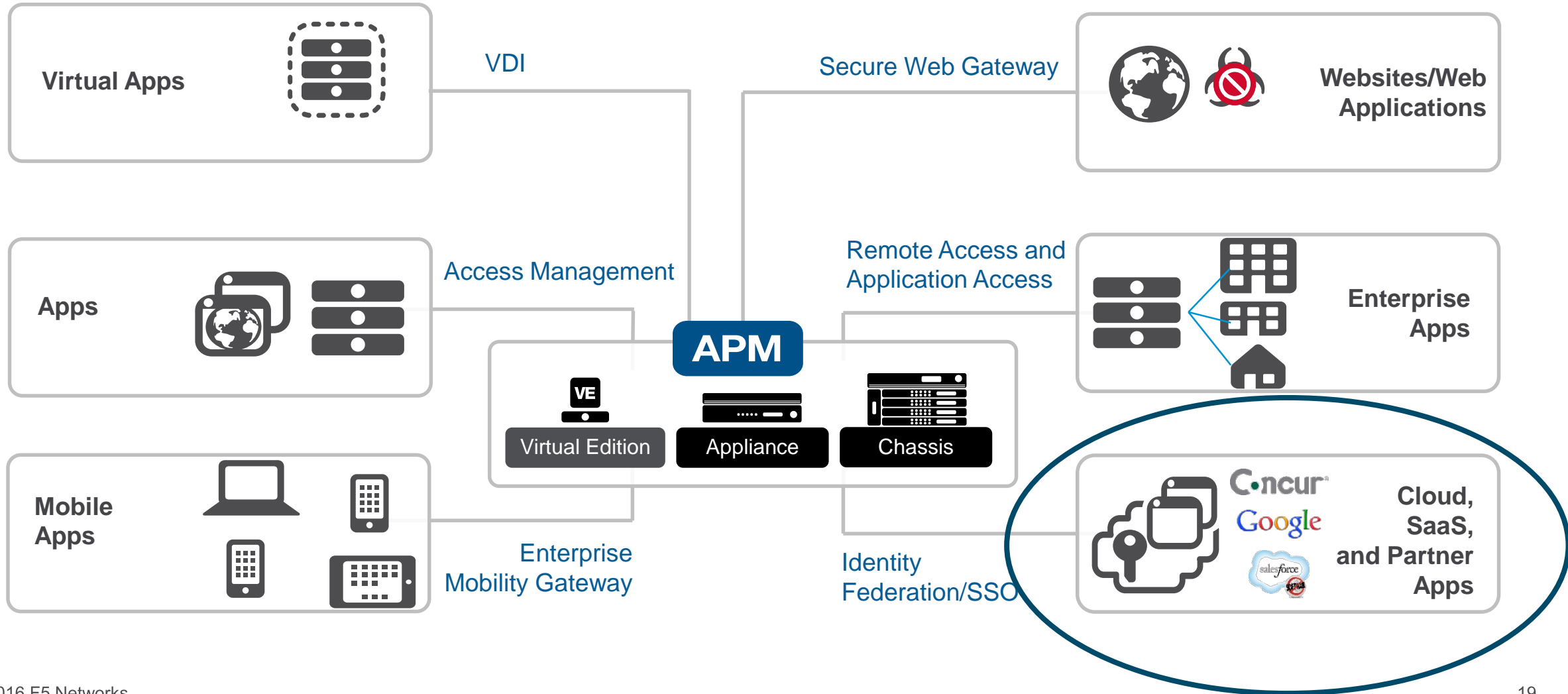
Flexible, Extensible Identity Federation and SSO Support

Users
- ✓ Adaptive Auth
- ✓ Federation (SAML)
- 🔒 Token
- 🔒 Password
- 🏅 Certificates

SSO Selection
Endpoint Validation

Step-Up Auth
Fraud Protection

- ✓ SAML Pass-through
- ✓ Simple Assertion
- 🔒 Kerberos Delegation
- 🔒 Dynamic Forms
- 🏅 Certificates

Apps
Private/Public Cloud
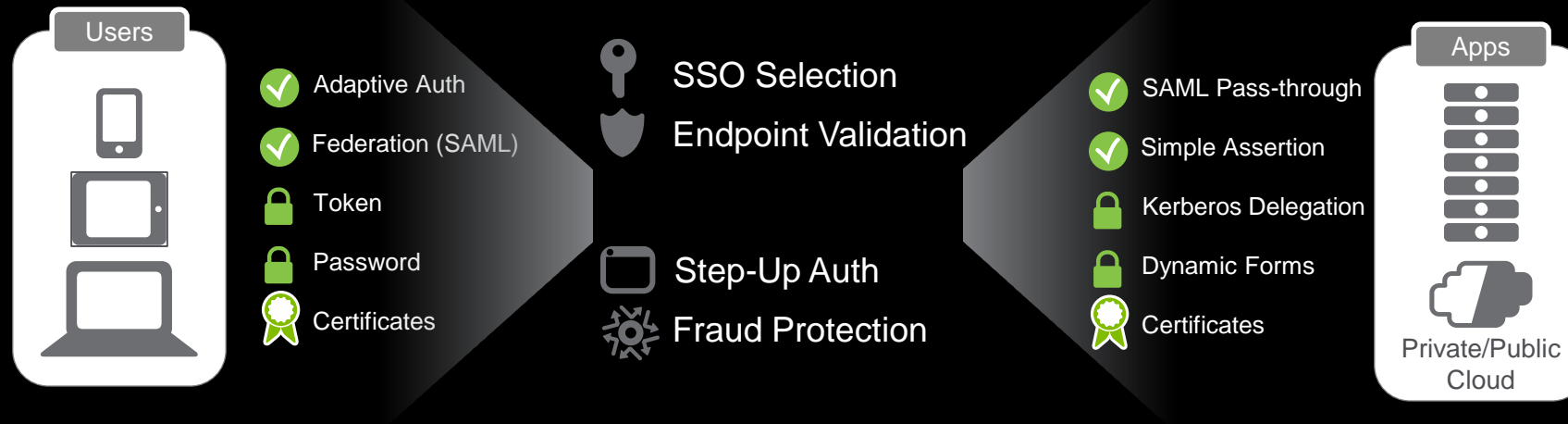
- Transforms one type of authentication into another

- Supports various standards-based protocols (SAML, Kerberos, NTLM)

- Enables flexible selection of SSO techniques appropriate to the application

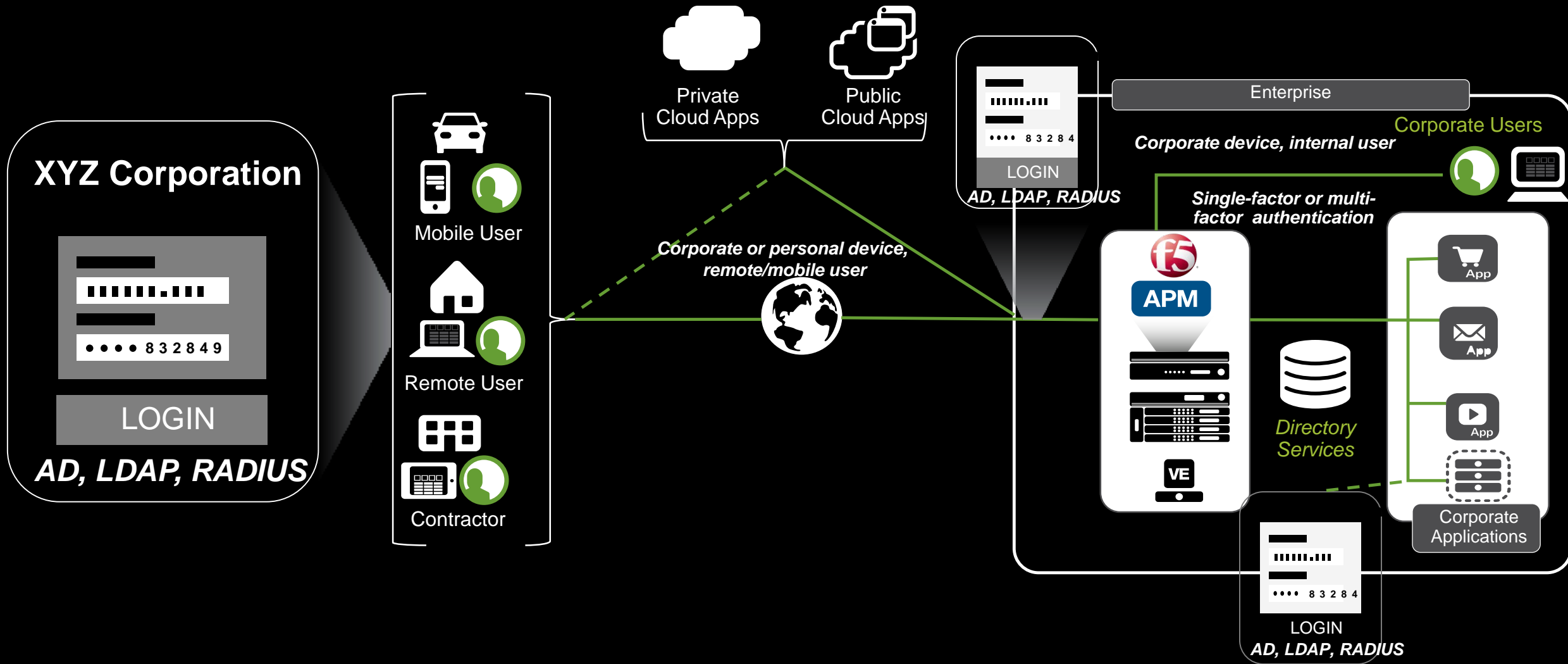- Allows for centralized session control of all applications, even SaaS apps

Federating Identity

Pa55W0rd

SAML IdP

Identity & Authorization

Application

Data Center

SAML SP

Office 365

SAML SP

Concur Expenses
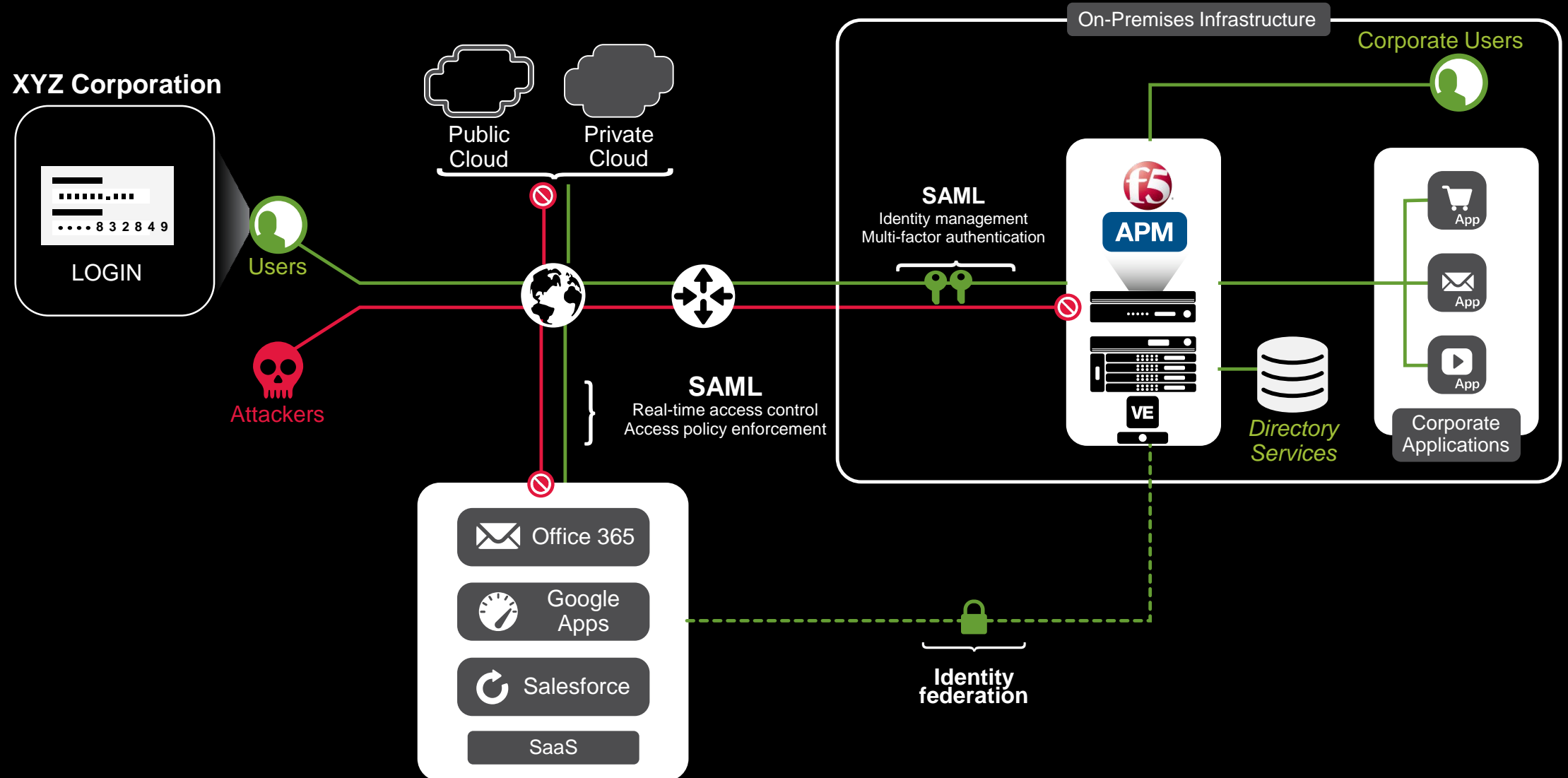
SAML SP

SalesForce
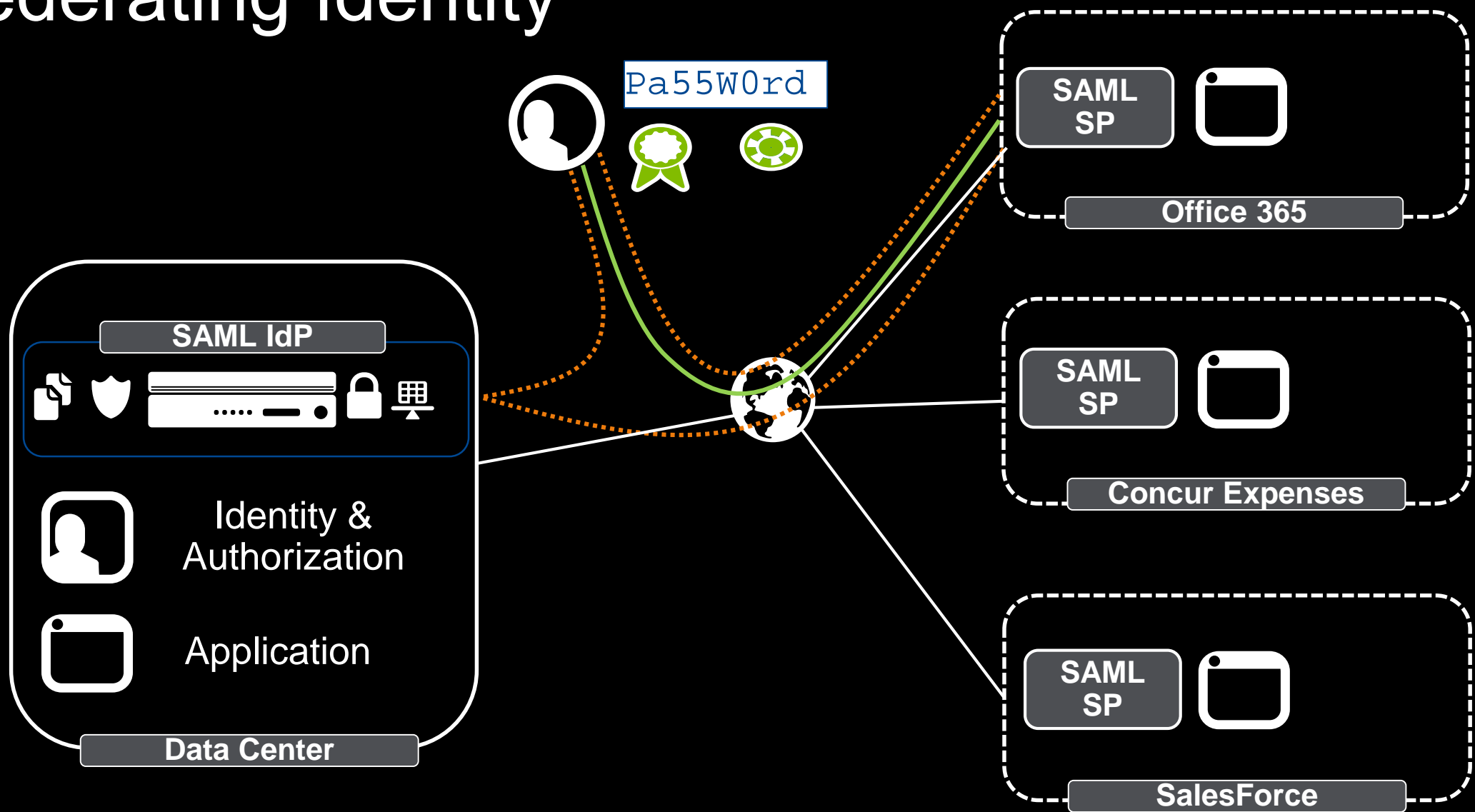
Step-up Authentication

Anonymous access to and re-validation of AD, LDAP, or RADIUS flat-file authentication per request within an access session, for accessing additional, sensitive web URIs, or to extend a session

Private Cloud Apps

Public Cloud Apps

Enterprise

Corporate Users

LOGIN

AD, LDAP, RADIUS

Corporate device, internal user

XYZ Corporation

Mobile User

Single-factor or multi-factor authentication

LOGIN

AD, LDAP, RADIUS

Corporate or personal device, remote/mobile user

8 3 2 8 4 9

Remote User

f5

APM

VE

Directory Services

App

App

App

Contractor

Corporate Applications

LOGIN

8 3 2 8 4

LOGIN

AD, LDAP, RADIUS

Identity Federation with Multi-Factor Authentication

F5 Has a Rich Ecosystem of Multi-Factor Authentication Partners

Benefits of Identity Federation, SSO, and Adaptive Authentication with APM

- ✓ Dramatically reduces costs

- ✓ Delivers seamless access

- ✓ Increases user productivity

- ✓ Simplifies administration

- ✓ Enhanced adaptive access and authentication

Summary

Simplifies

Improves performance and usability, while simplifying administration

Secures

Enhances application and virtualized apps and desktop security

Protects

Expands data loss prevention and guards against web-based attacks

Demonstration

Questions & Answers

Thank you

SOLUTIONS FOR AN APPLICATION WORLD