



www.celaespanama2019.com

CELAES 2019

XXXIV Congreso Latinoamericano
de Seguridad Bancaria

Latin American Banking Security Conference

PANAMÁ • JUNIO JUNE 20 - 21, 2019



C



THALES

Roman Baudrit

**Thales Cloud Protection and Licensing
Thales Digital Identity and Security**



Thales Digital Identity & Security

- Protect 80% of payment transactions in the world
- Leader in card personalization
- Leader in GSM SIM and eSIM
- Leader in Key Management
- Leader in Payment, Cloud and GP HSM
- Leader in Software Monetization



Digital Transformation - Demand

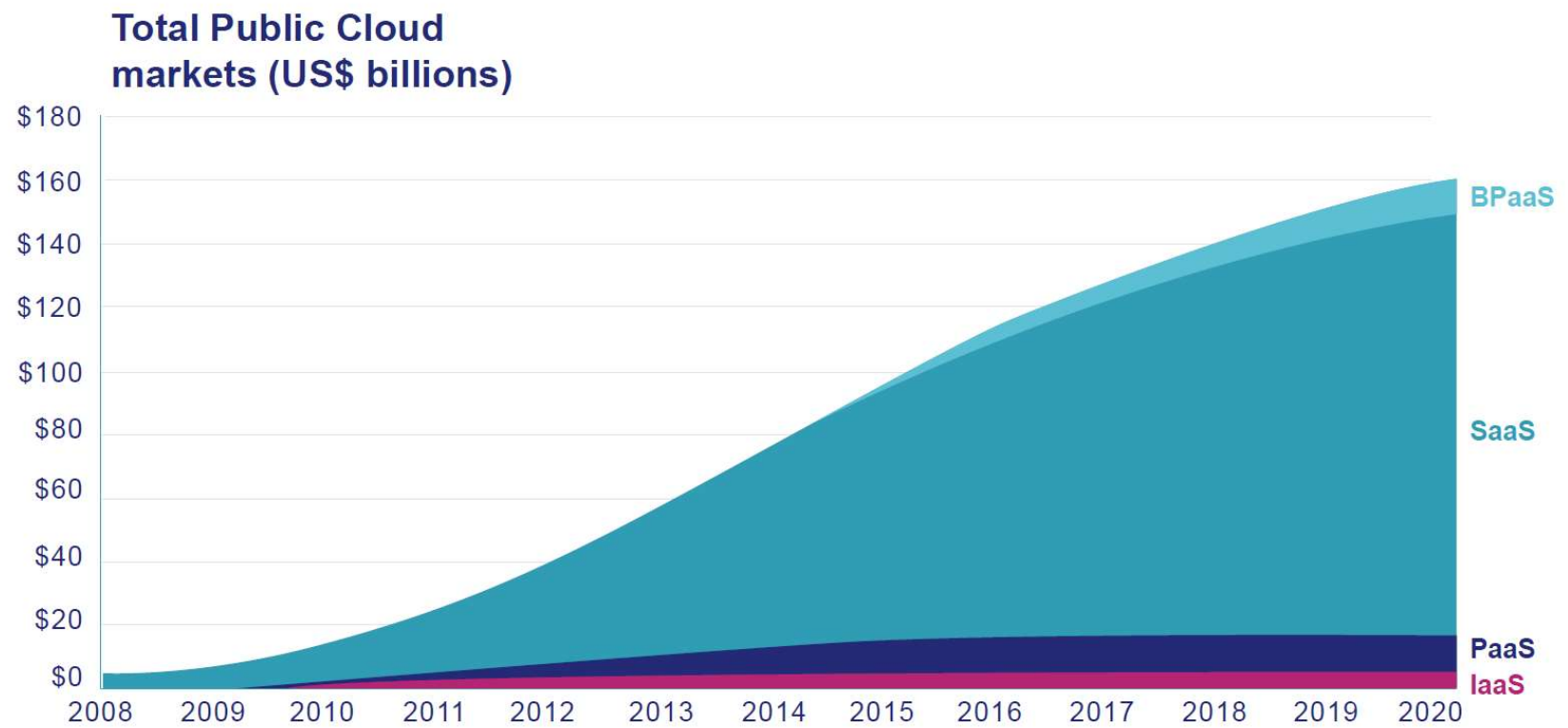
- Financial Consumer Profiling
 - In the past customer expected data integrity and systems availability
 - Now financial institutions have to deal with several customer profiles
 - Early adopters or enthusiasts – mostly online
 - Conventional customers – mostly F2F and Cash/Check
 - **The mid-range customers are 65%+**
 - Implications in customer service, products, communications, fidelitization and processes



Digital Transformation - Demand

- Consumers EXPECT more
 - Integrated propositions vs traditional services
 - Leasing – Renting – Financing – Insurance – Reselling
 - Mass personalization
 - Spending habits and money management
 - Data is shared based on advice and deals
 - What will I get back for sharing my information
 - Integration across physical and digital channels
 - Omnichannel banking experience
 - Consumer trust more but are less loyal
 - Consumers trust their bank to hold data while delivering value add

Cloud Computing Unprecedented Growth



Source: Forrester Research

Cloud is reshaping the way our customers do business



Massive Transformation
Cloud Computing



Data
Protection



Identity &
Access Management



Software Licensing &
Protection

Shared Responsibility Model Illustrates Data Security Roles

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Customer Responsibility

Provider Responsibility

| |
|----------------|
| Data |
| Application |
| Runtime |
| Middleware |
| O/S |
| Virtualization |
| Servers |
| Storage |
| Networking |

| |
|----------------|
| Data |
| Application |
| Runtime |
| Middleware |
| O/S |
| Virtualization |
| Servers |
| Storage |
| Networking |

| |
|----------------|
| Data |
| Application |
| Runtime |
| Middleware |
| O/S |
| Virtualization |
| Servers |
| Storage |
| Networking |

The Misconnect

71% of enterprises use sensitive data in cloud environments

71%

But only 30% use encryption in these environments.

30%

*Source: 2019 Thales data
Threat Report by IDC*

Removing Cloud Security Complexity

Complementing Public Clouds with Operational Efficiency,
and Enabling Greater Control for Reducing Risk

Sensitive
Data



Native Cloud
Encryption



Control Keys and Simplify
BYOK



Bring
Your
Own Key

Highly
Sensitive
Data

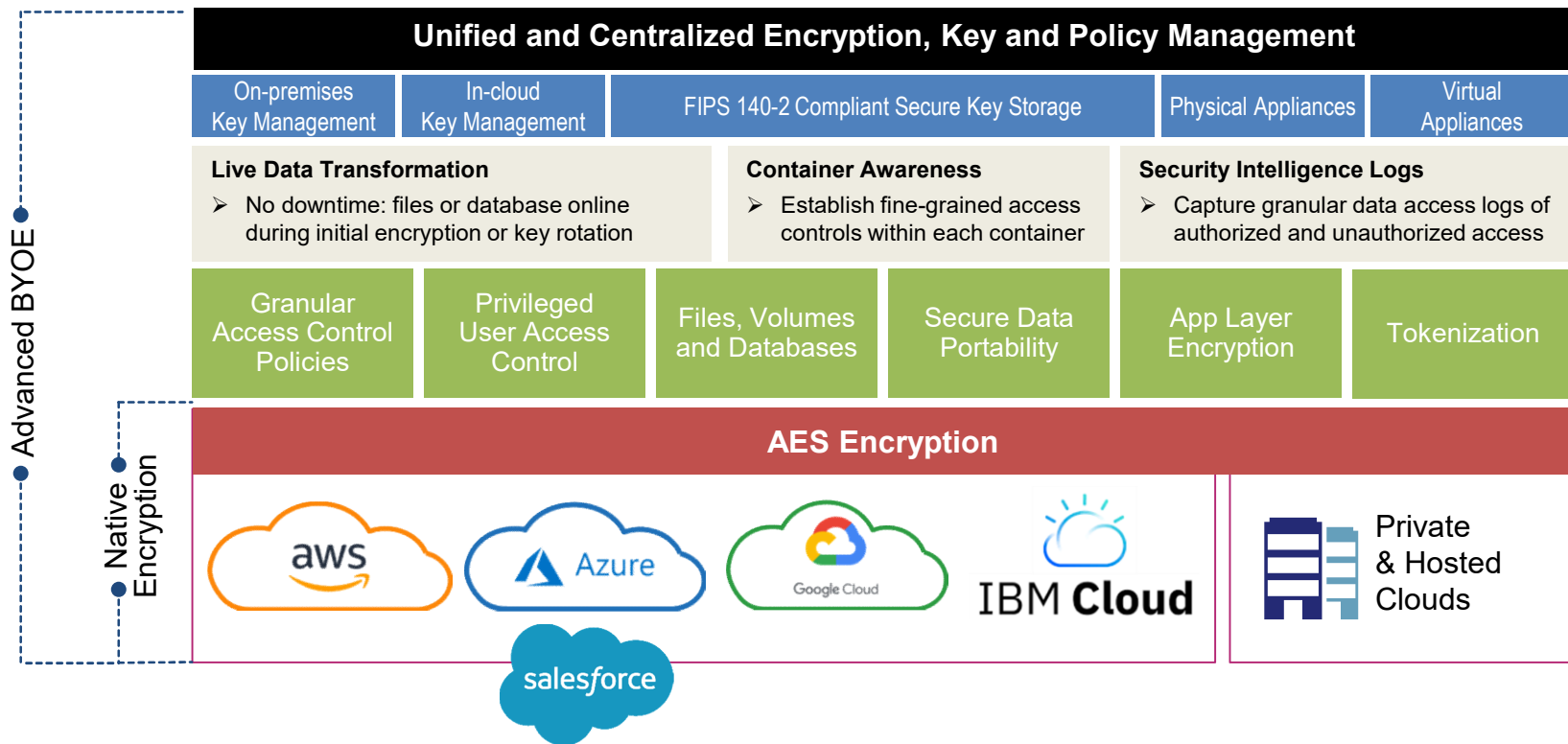


Full Protection in the Cloud

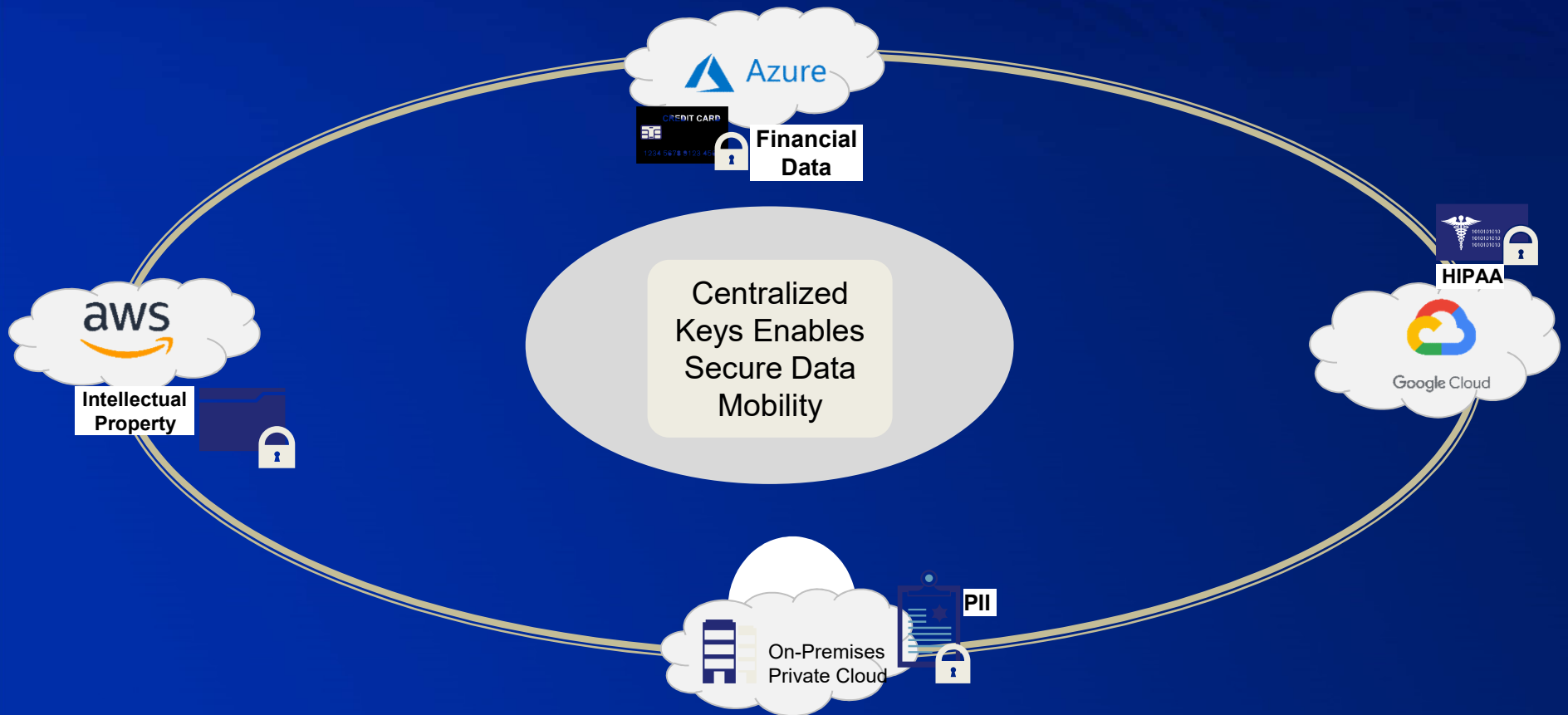


Bring Your
Own
Encryption

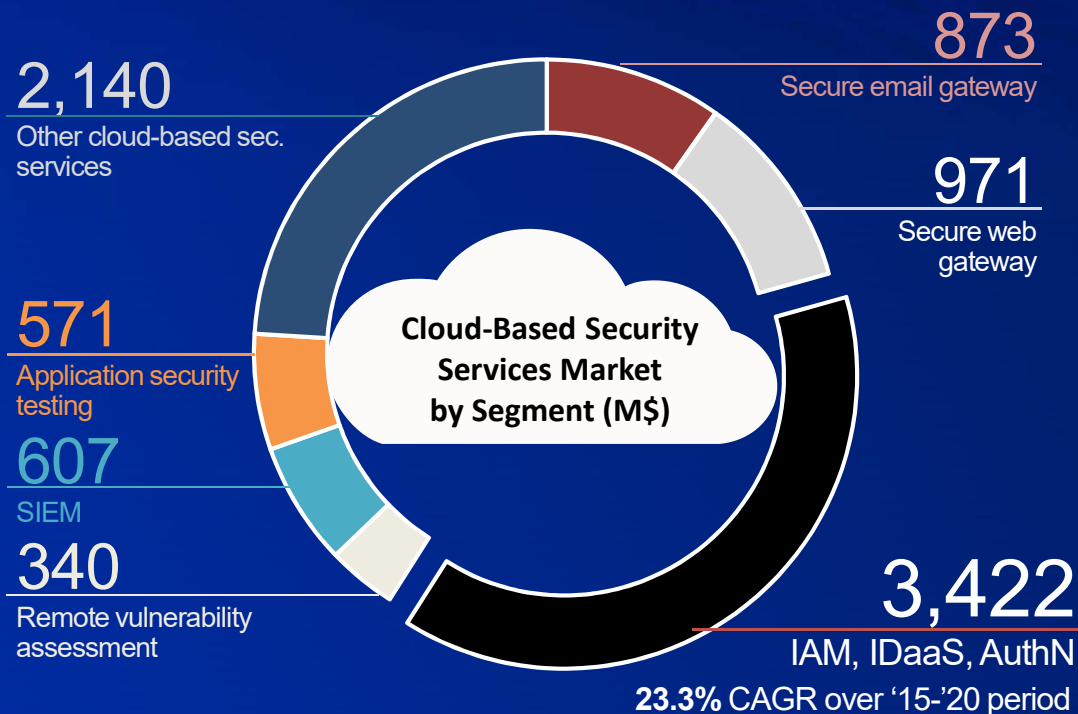
Bring Your Own Encryption for Multicloud Security and Control



Encrypted “Lift and Shift” is Only Possible with BYOE



Cloud based security as an enabler to this new approach



Looking Towards Enterprise 2.0



Users

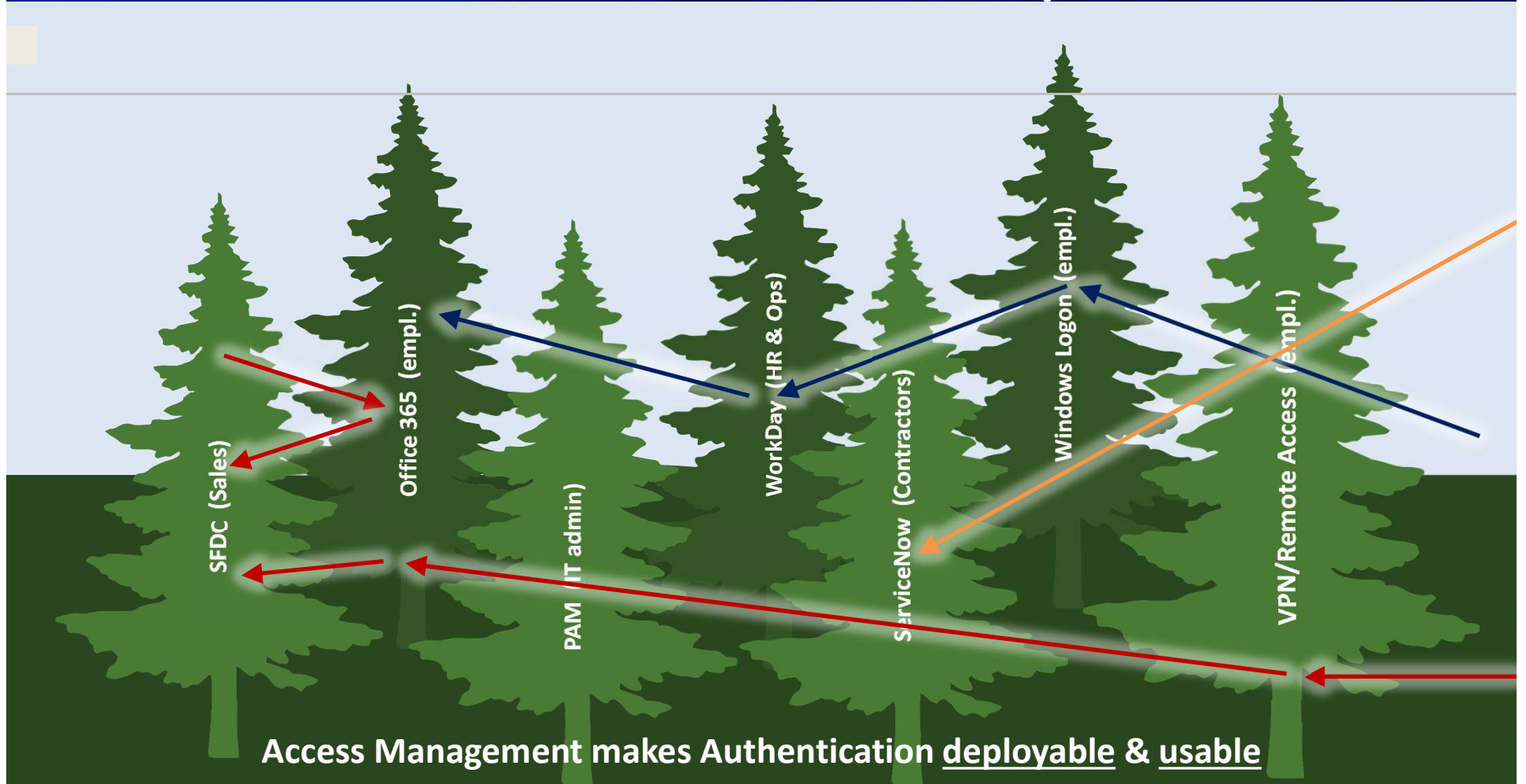
- Broader & mixed population
- From anywhere
- From any device
- Higher expectations (tools, UX)



IT Department

- Pressure to increase user & business efficiencies
- More demanding user base
- Higher pace of techno adoption
- Distributed & not fully managed resources
- Budget – Cloud economics

The New Landscape



Fueling the need for a new approach to Security



Perimeter Free

- No control at the perimeter
- No need to re-route traffic to proxies



Pushing Security to

- The user
- The targeted resource
- Irrespective of the underlying network topology (zero-trust)



Flexible & Adaptable

- Intelligent & context-aware
- Access policies balancing
 - Security goals
 - vs. usage scenarios (UX)

Define suitable security with universal authentication methods



Password



Kerberos



Hardware



Software



Oath



Google
Authenticator



SMS



eMail



Voice



OTP Push



Pattern-
based



PKI



Passwordless



Biometric



Windows
Hello*



FIDO*

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

Determine who, when and how users log in to apps



PKI Transformation for Cloud

- 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



Access Management



The Future of Access Management (Enterprise 3.0)



■ Anomaly Detection (ML)



■ Passwordless AuthN / UX



■ Active Protection



■ API Security



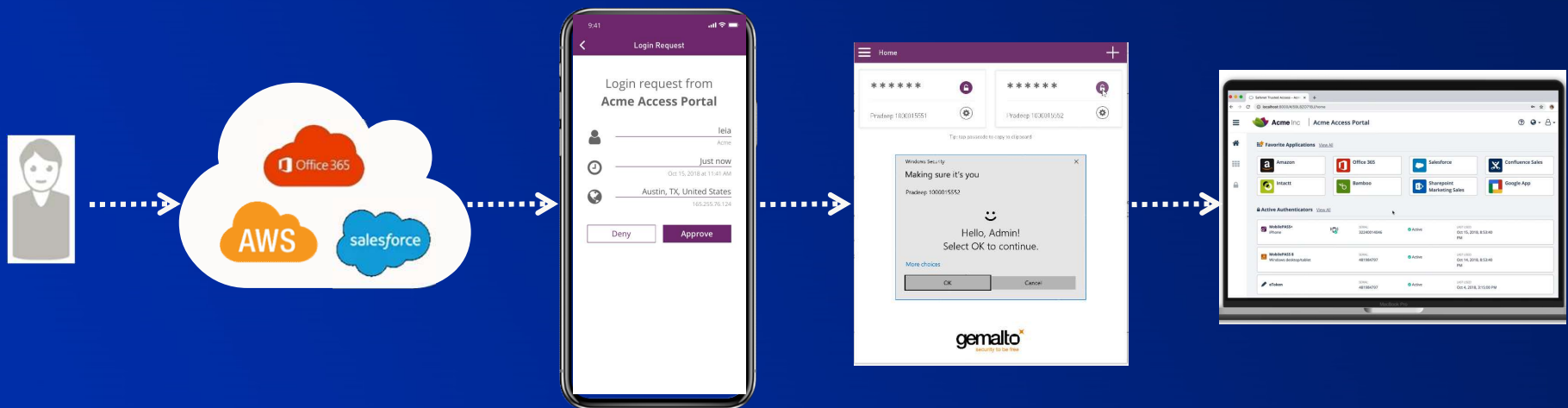
■ Cloud Ecosystem Integration



Passwordless authentication

Strong authentication without the need to remember a password

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





CELAES 2019
XXXIV Congreso Latinoamericano
de Seguridad Bancaria,
Latin American Banking Security Conference
PANAMÁ · JUNIO JUNE 20 - 21, 2019



Thank you!

roman.baudrit@thalessecurity.com

+1 305 898 8665