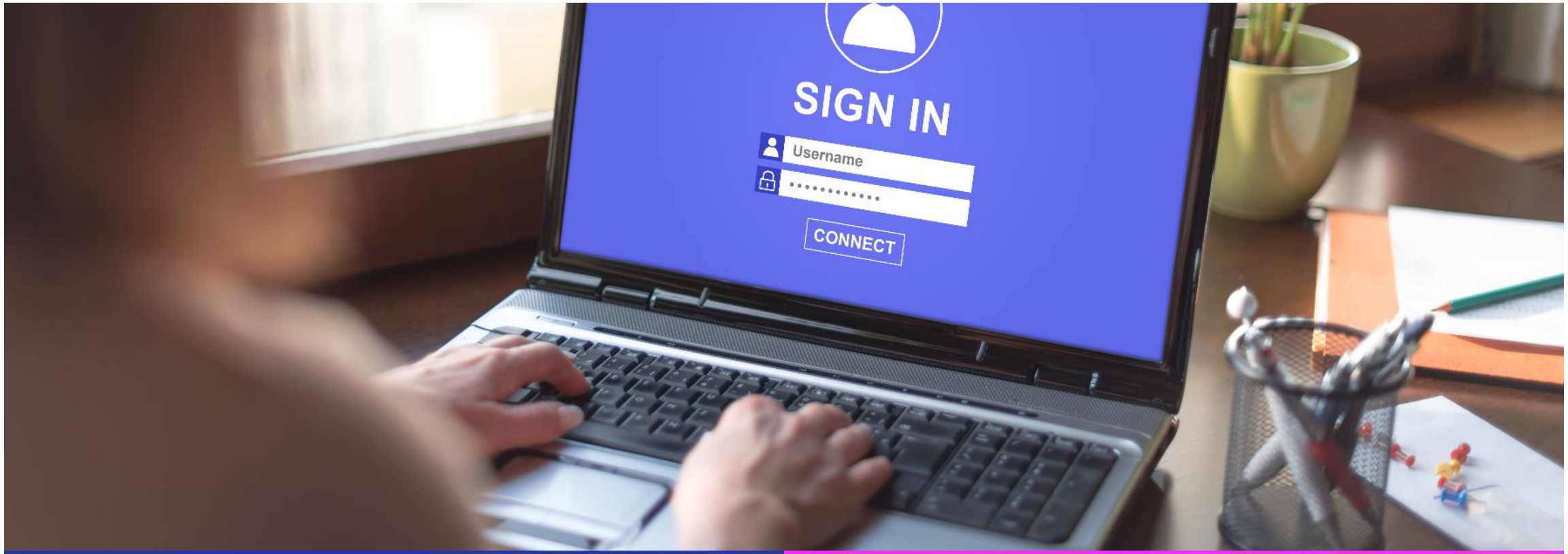
RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M04E

Identity and Access Management (IAM) Emerging Trends and Standards

Salah Machani

Director of Technology
RSA
#RSA

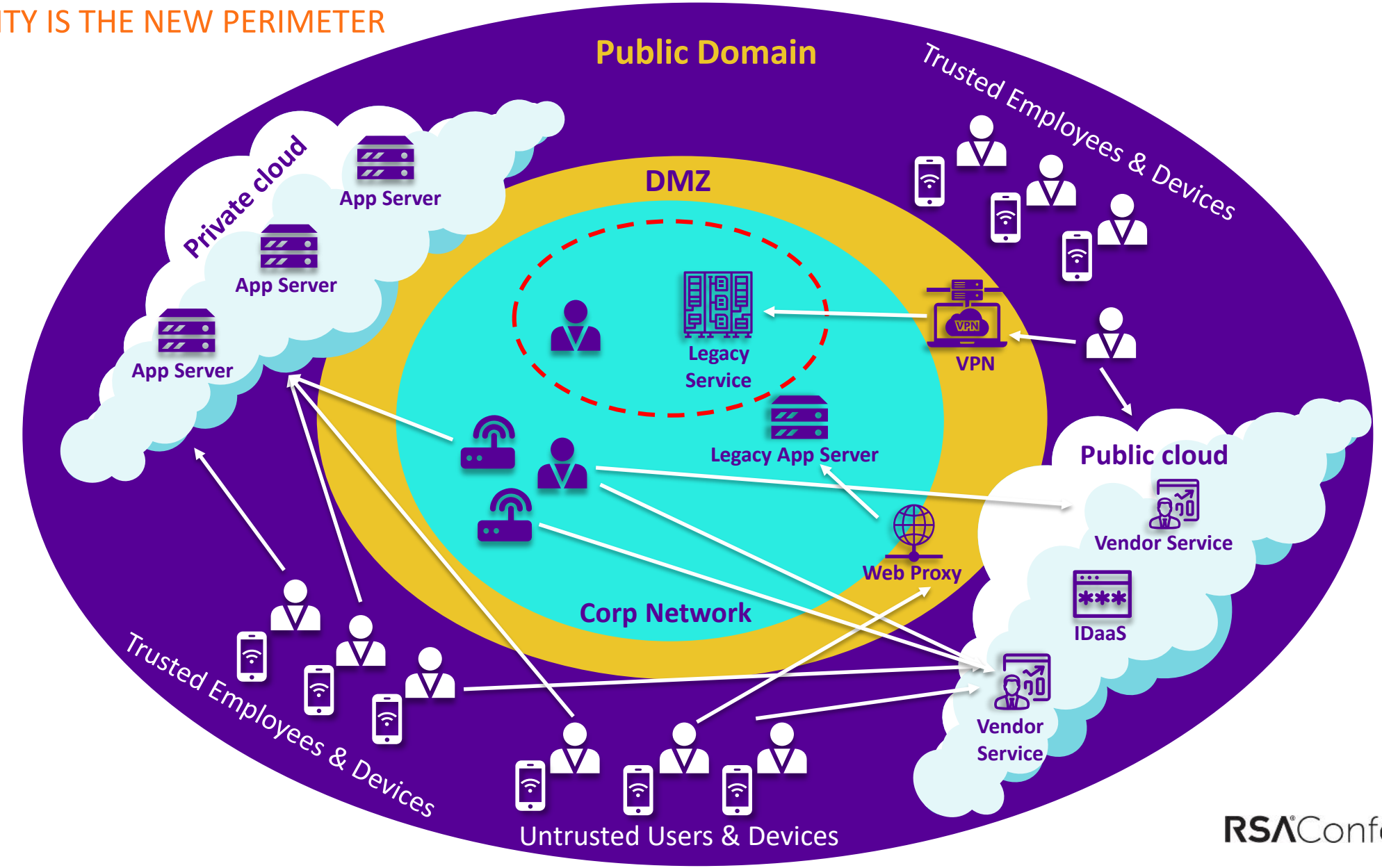


50-60 BILLION IDENTITIES
Collectively held worldwide (IDC)

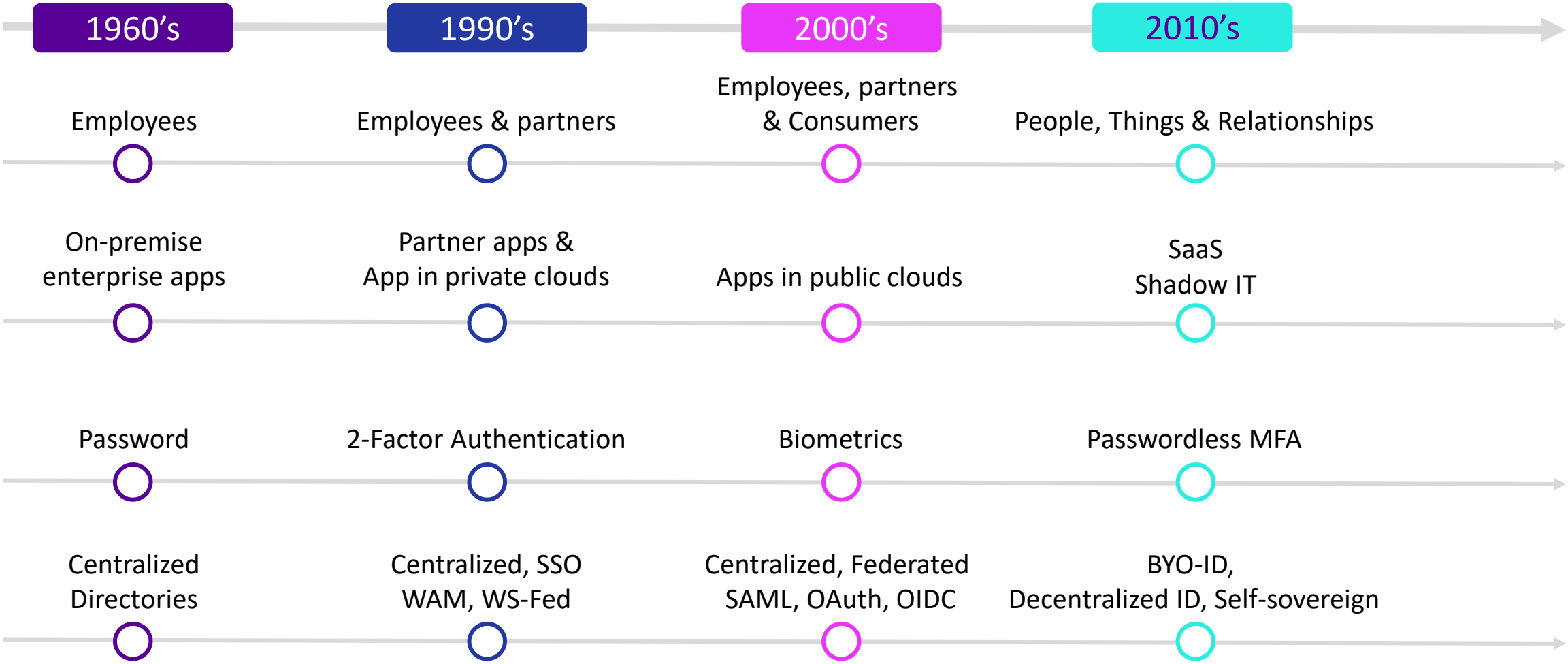
191 ACCOUNTS
Per average business employee (LastPass)

Digital transformation is driving a new reality…

IDENTITY IS THE NEW PERIMETER



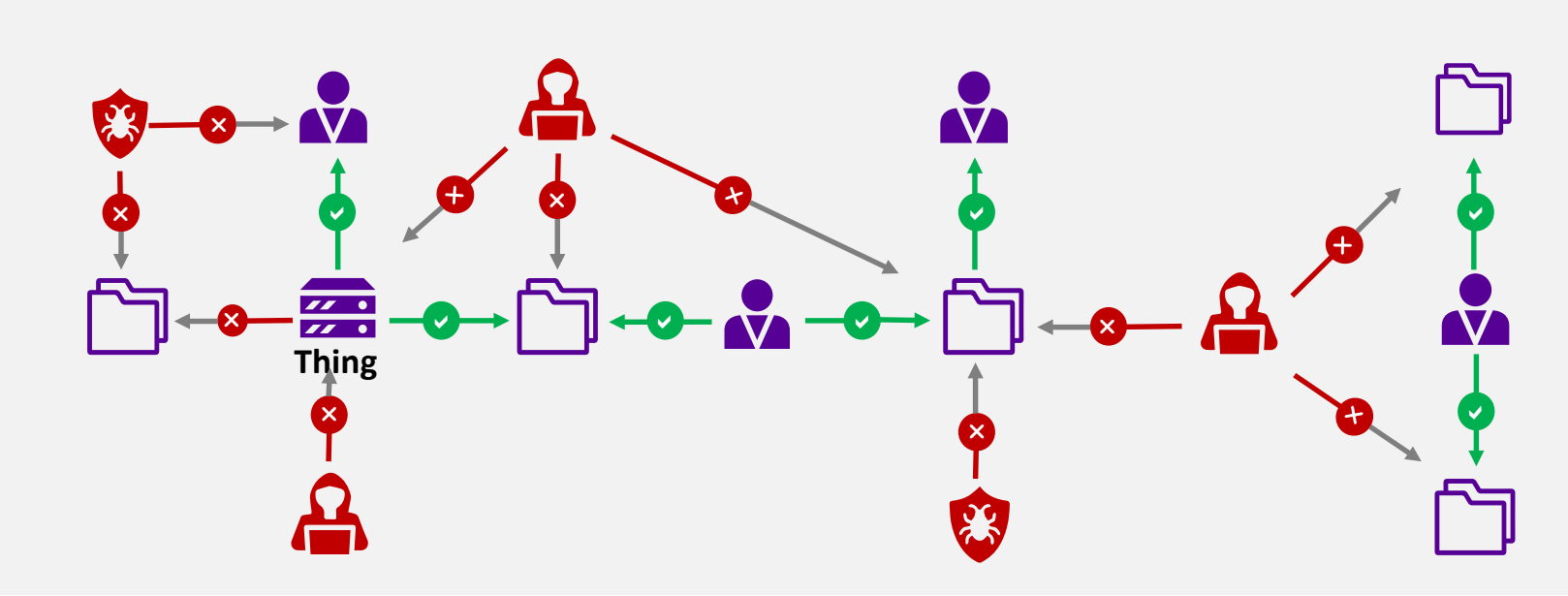
How did IAM evolve over time



Digital transformation requires new methods to manage digital identity risk

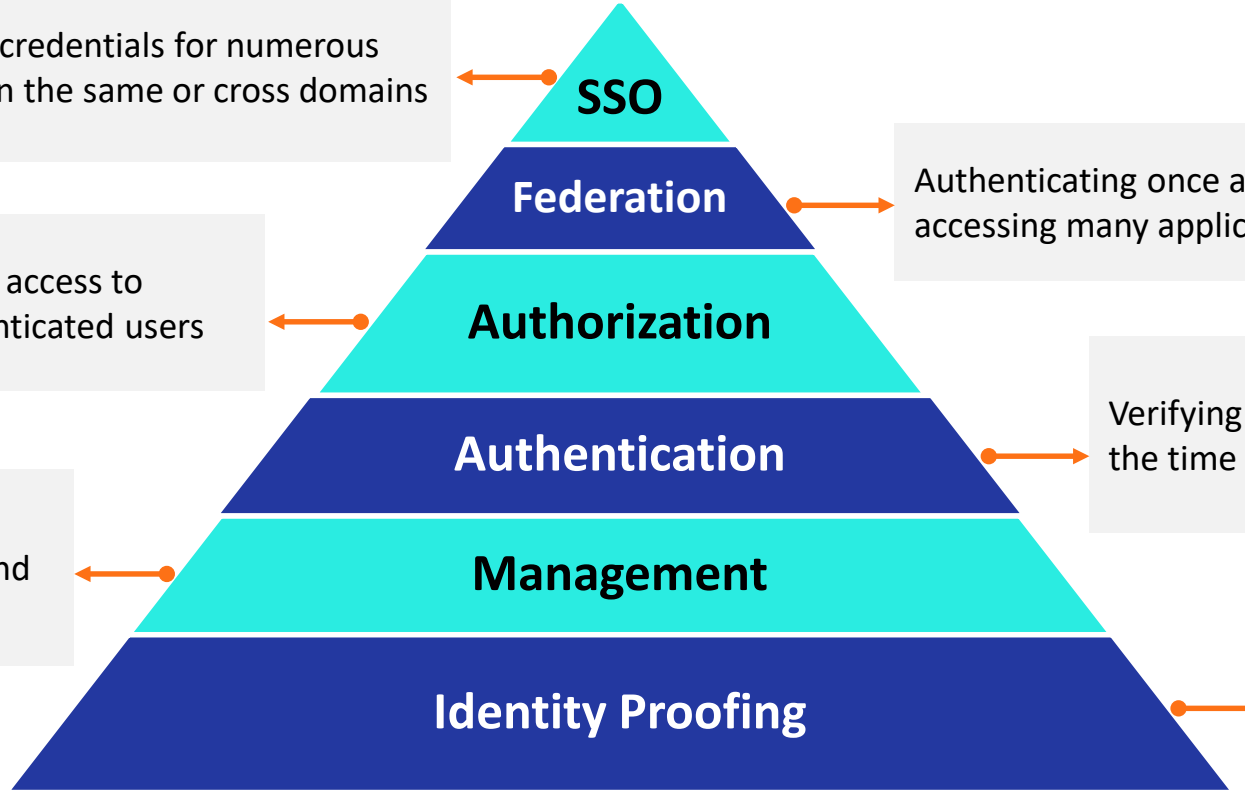
The goal of IAM today

Ensure that the **right people and "things"** get access to the **right resources** (applications, data, and so on) at the **right times**, from the **right device** and **location** for the **right reasons**.



Protected resources: apps, data, services, devices, etc.

IAM key functionality



Managing credentials for numerous apps within the same or cross domains

Authenticating once and accessing many applications

Allowing or denying access to resources for authenticated users

Verifying user credentials at the time of access

Creating, updating, revoking, recovering or deleting identities and associated entitlements.

Verifying claimant real-world identity and binding it to a digital identity

New approaches to manage digital identity risk

- Remote Identity Proofing
- Passwordless Authentication
- Identity Risk Analytics
- Federated Identity and SSO
- Identity-as-a-Service (IDaaS)
- Bring Your Own Identity (BYO-ID)
- Continuous Authentication
- Identity of Things
- Zero-Trust
- Self-Sovereign Identity

TREND#1: Remote identity proofing

In-Person

Remote

TREND#1: Remote identity proofing

METHODS

Electronic Government Issued Documents	BYO-ID Trusted Identity	National Biometric Databases	Trusted Referee
Enhanced Dynamic KBA	Identity Reputation & Graph Analysis	Behavioral Analysis	Proof-Of-Possession

Relevant Standards/Guidelines/Regulations

NIST 800-63-A, KYC, AML

TREND#1: Remote identity proofing

Benefits

- Efficient onboarding and account creation processes
- Flexible workforce
- Reduced fraud and identity theft
- Cost-effective and easier credential recovery processes

TREND#2: Passwordless authentication

A long-standing goal	Gaining real market visibility
Eliminating the need for centrally managed passwords	FIDO2 and W3C WebAuthn API support in browsers and platforms

FIDO2, U2F, UAF, CTAP

WebAuthn API

NIST 800-63-B

TREND#2: Passwordless authentication

Going from this…

Password

To this…

MODERN AUTHENTICATION

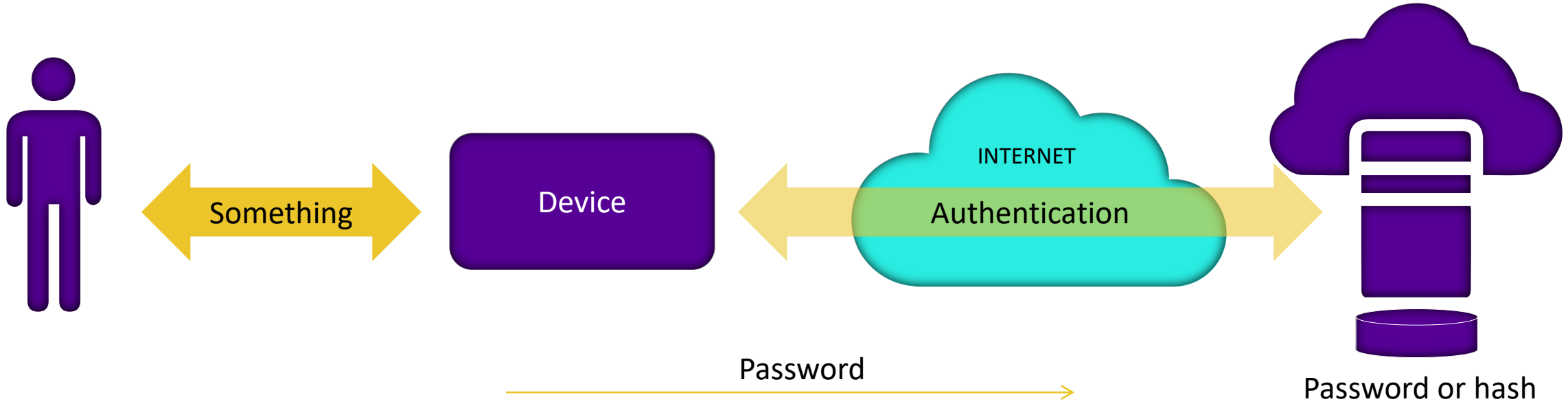
Push | Mobile OTP | Biometrics | Text Msg | Voice Call

HW Token | SW Token | FIDO | Proximity | Wearables

Providing same or higher authentication assurance levels

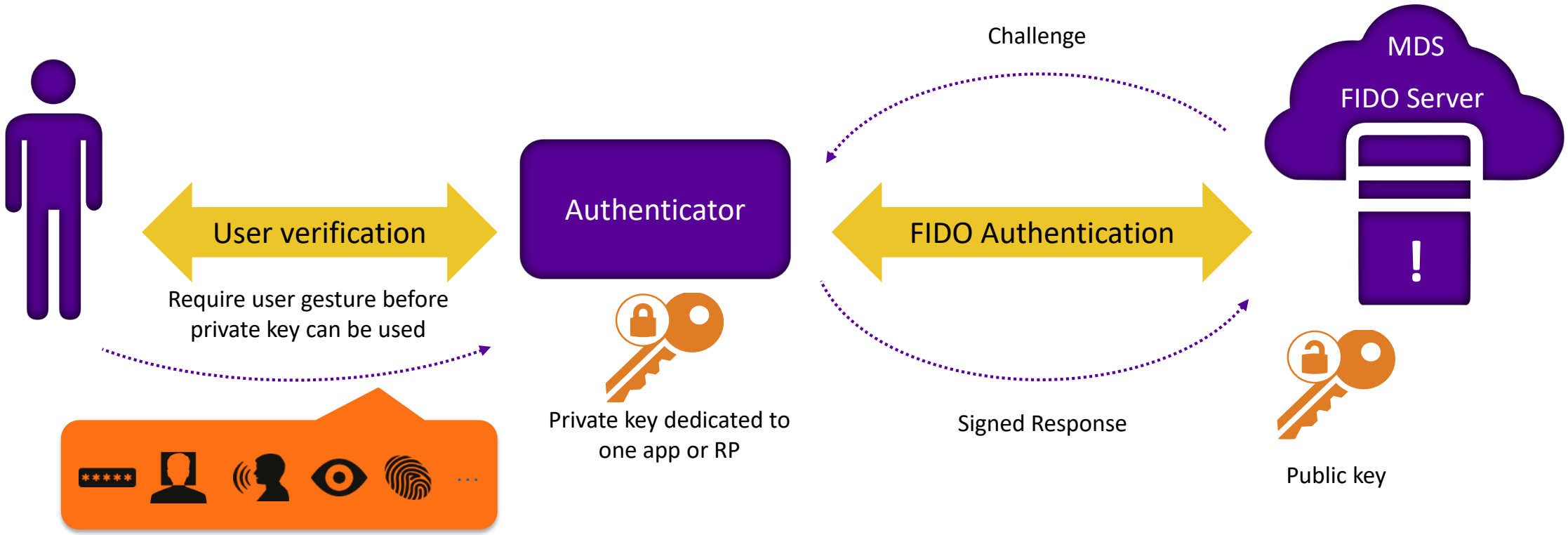
TREND#2: Passwordless authentication

TRADITIONAL ONLINE AUTHENTICATION



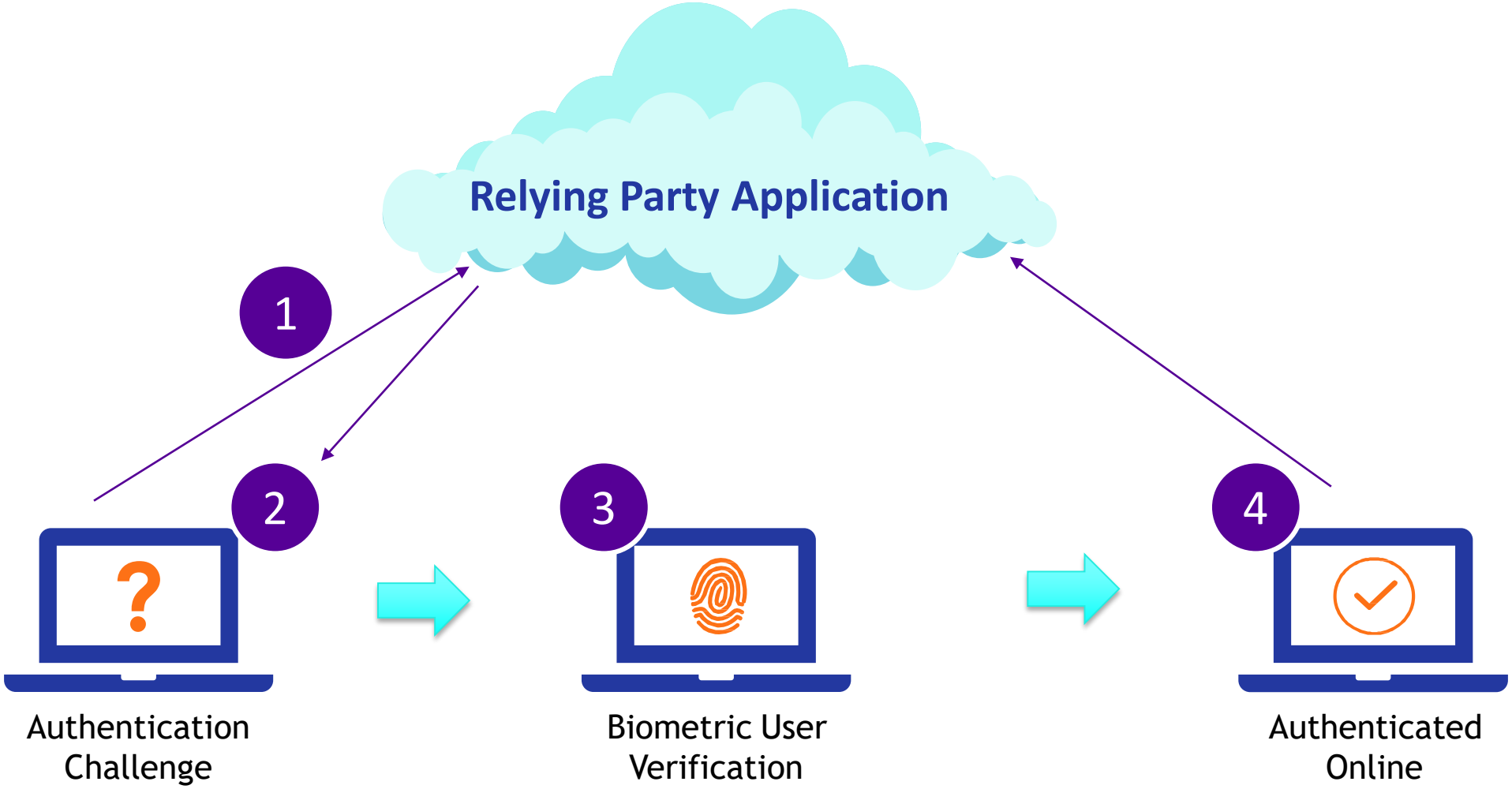
TREND#2: Passwordless authentication

HOW FIDO IS DIFFERENT



TREND#2: Passwordless authentication

PASSWORDLESS AUTHENTICATION WITH FIDO



TREND#2: Passwordless authentication

FIDO Benefits

Convenience

- Simple gestures
- Single authenticator for multiple apps

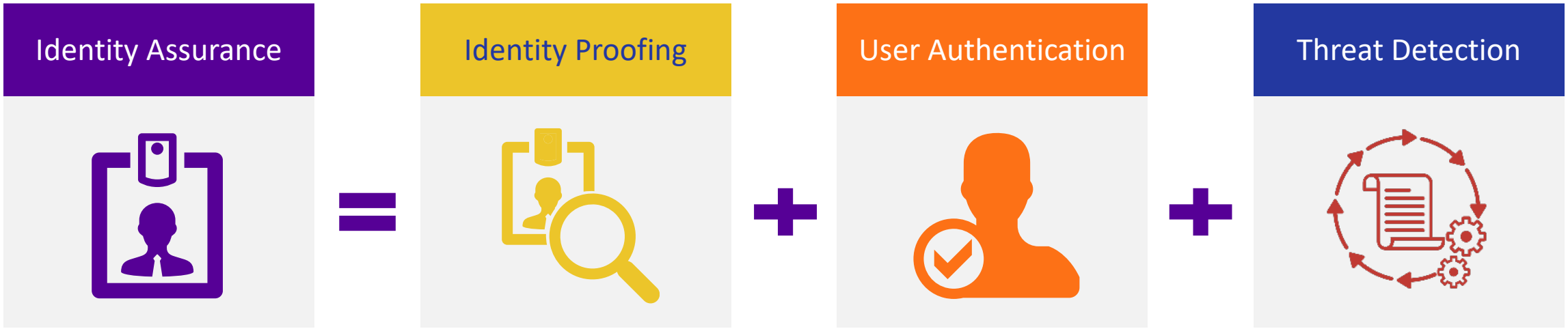
Security

- No secrets on server
- MITM protection
- Phishing protection

Privacy

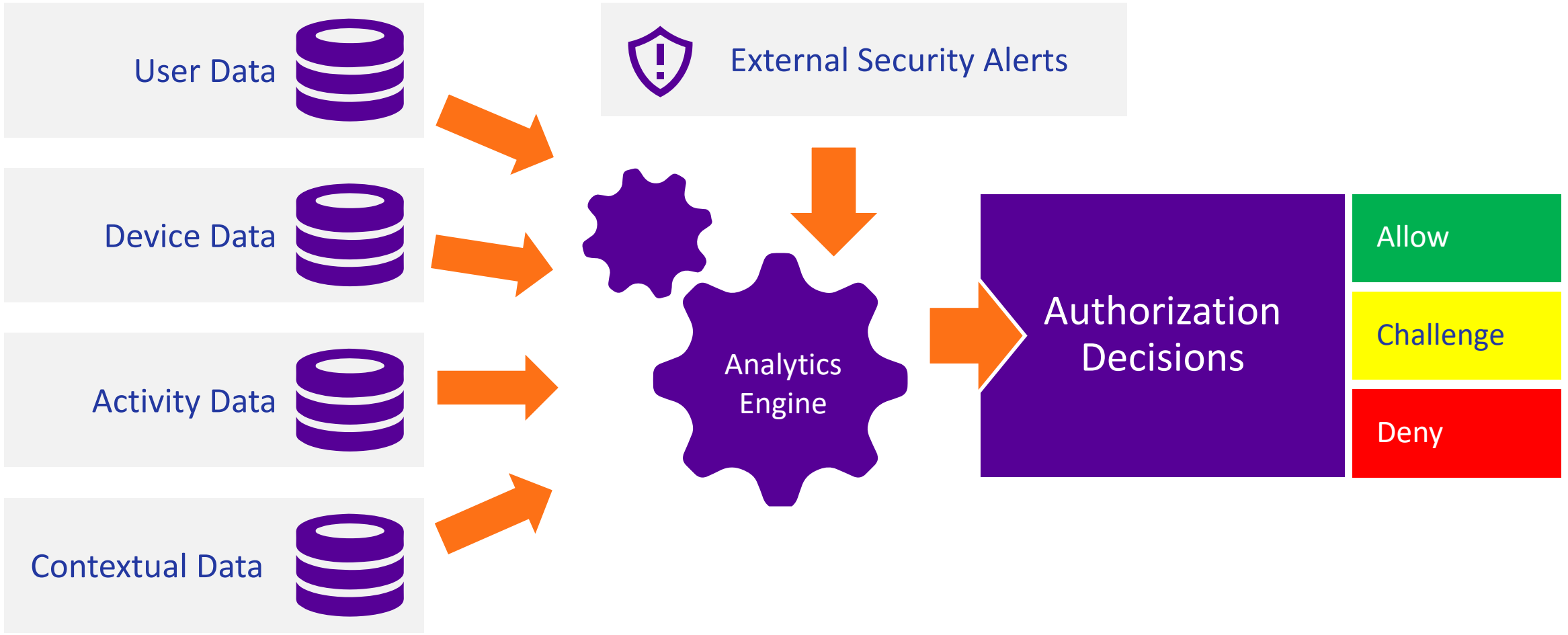
- No PII
- Local biometric
- Non-likability between RPs

TREND#3: Identity assurance with risk analytics



Detect anomalous user behavior

TREND#3: Identity assurance with risk analytics



TREND#3: Identity assurance with risk analytics

Benefits

Reduce and manage risk

- Detecting insider threats
- Stopping attackers using compromised credentials

Provide a better CX and UX

- Reducing administration overhead of access policies
- Providing frictionless user experience when risk is low

TREND#4: Federated identity and SSO

EXPERIENCING RAPID ADOPTION

Well-established Federation protocols

OASIS

SAML

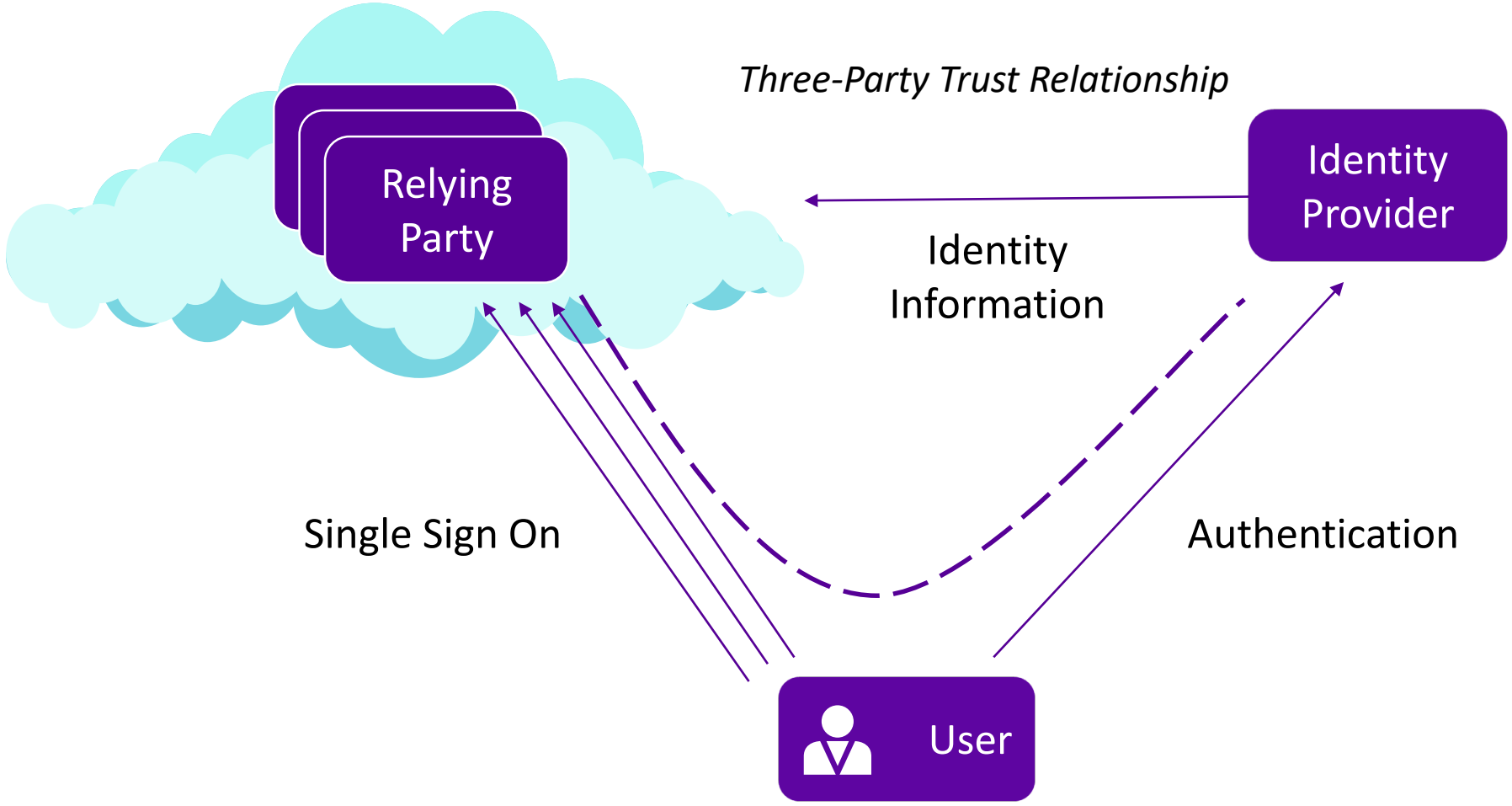
OpenID Connect

- Increased adoption of the cloud
- Increased number of applications and passwords
- Increased workforce distribution

Need for seamless, secure and controlled access to applications across multiple security domains

TREND#4: Federated identity and SSO

HOW FEDERATED IDENTITY ADDRESSES THESE NEEDS?



TREND#4: Federated identity and SSO

Benefits

User

- Sign in once and access multiple applications
- Increased productivity

Relying Party

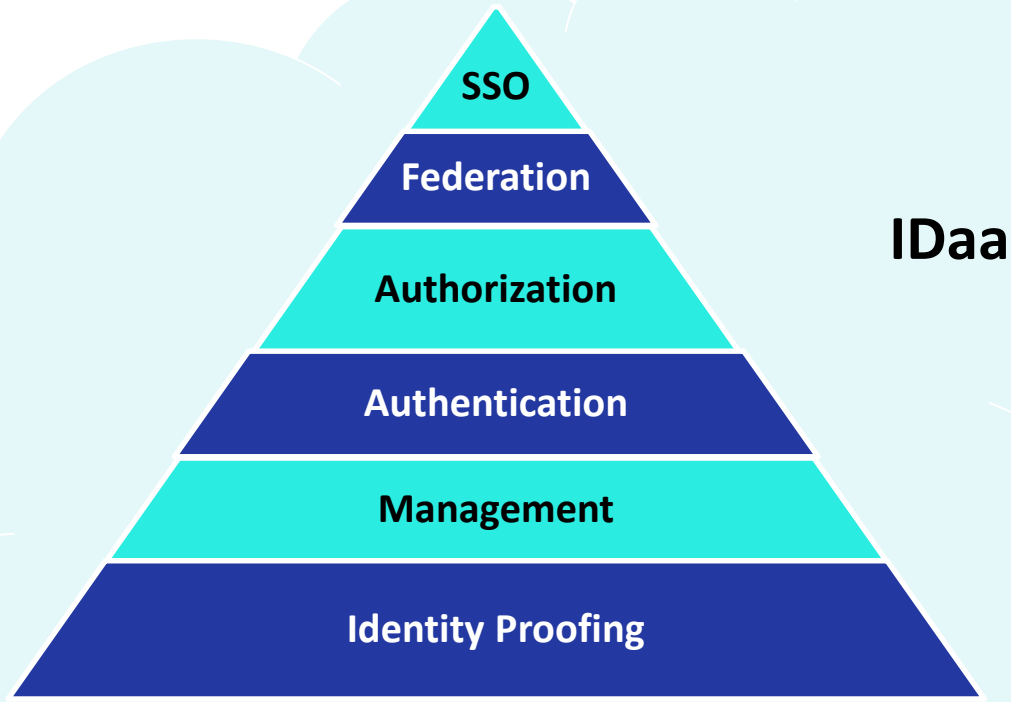
- Move user identity risk and liability to trusted third-party authorities

Identity Provider

- Link user identity to multiple relying parties
- Enforce enterprise policies
- Enable SSO
- Protect user personal info

TREND#5: IDaaS

IAM SERVICES HOSTED AND MANAGED BY A THIRD-PARTY CLOUD VENDOR

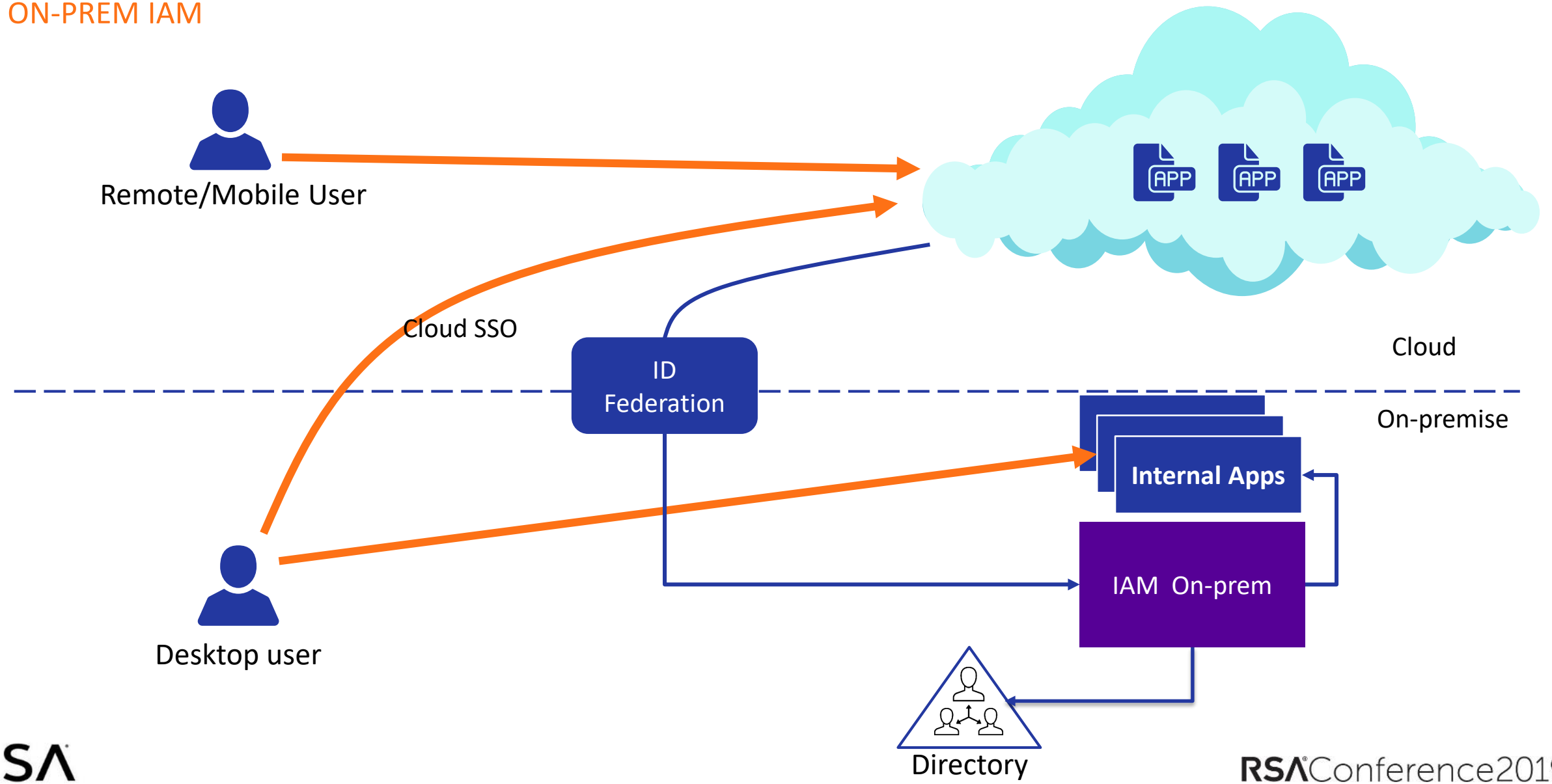


IDaaS

- Cloud-based multi-tenant architecture
- Credential management
- Modern authentication
- Single-Sign on and federation
- Identity risk analytics and intelligence

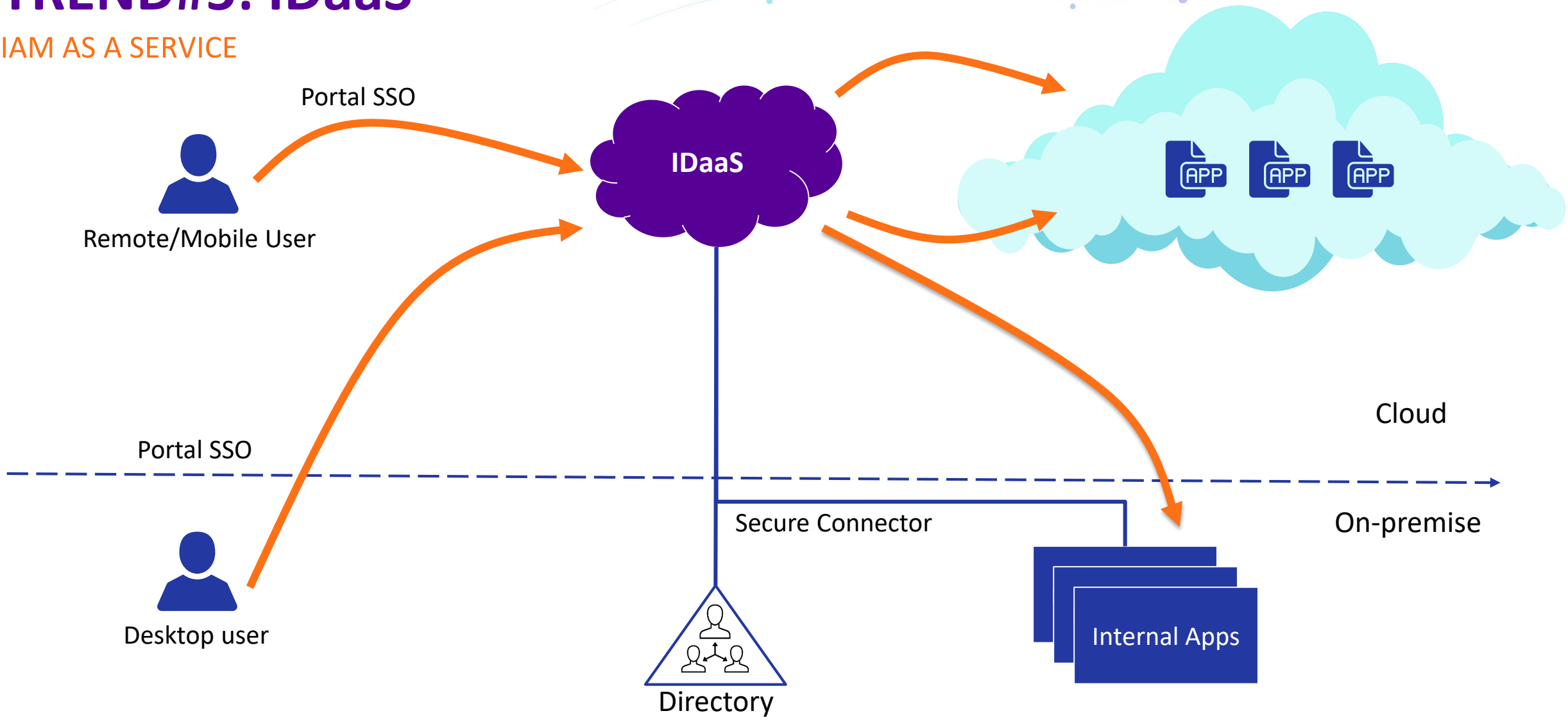
TREND#5: IDaaS

ON-PREM IAM



TREND#5: IDaaS

IAM AS A SERVICE



TREND#5: IDaaS

Benefits

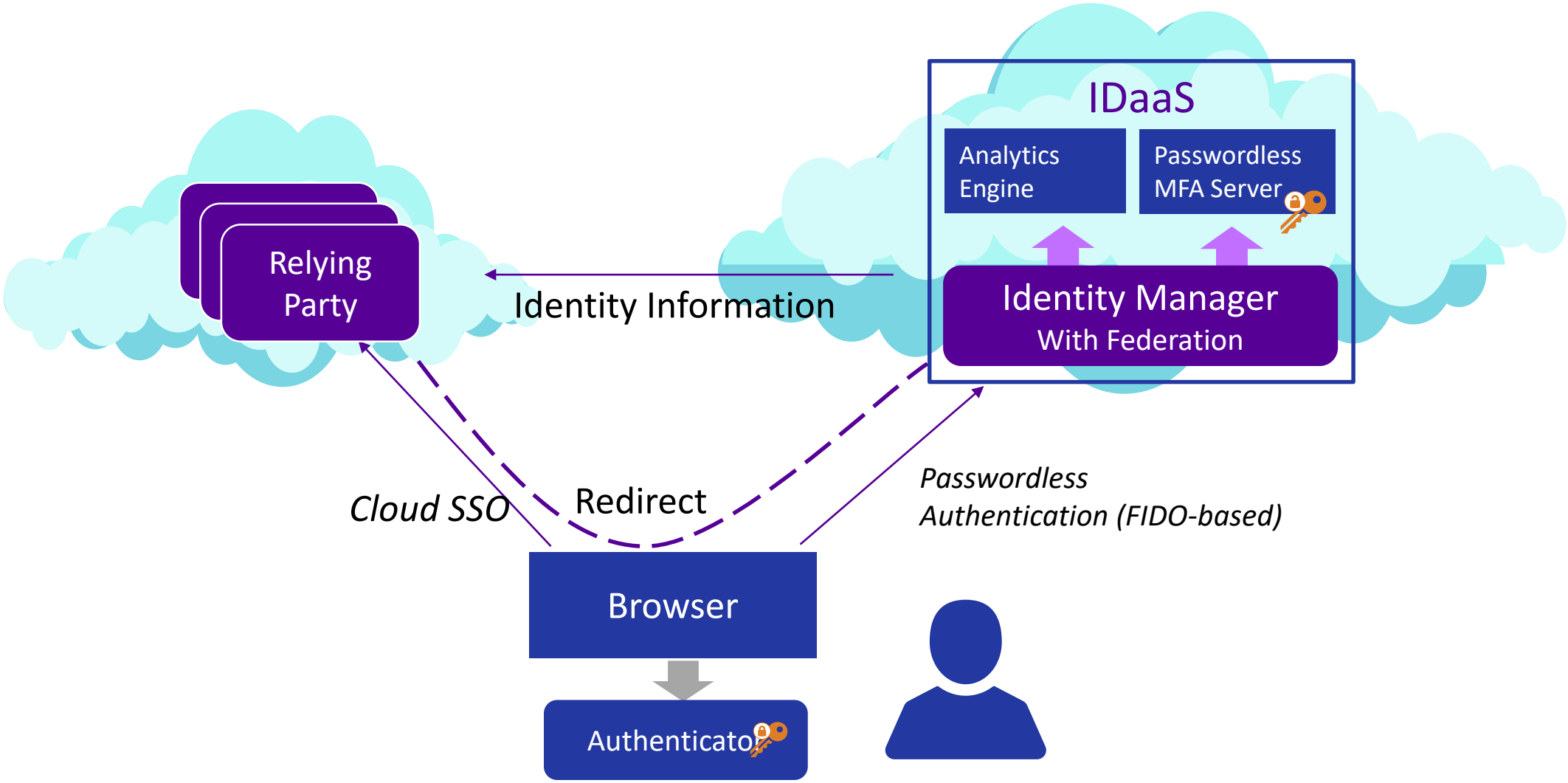
Organizations

- Leverage advanced IAM capabilities
- Manage applications and entitlements using easy and simple tools
- Fill security/identity management skills gaps
- Reduce cost

Users

- Access the same apps using the same authenticaton methods from anywhere
- Leverage self-service interfaces

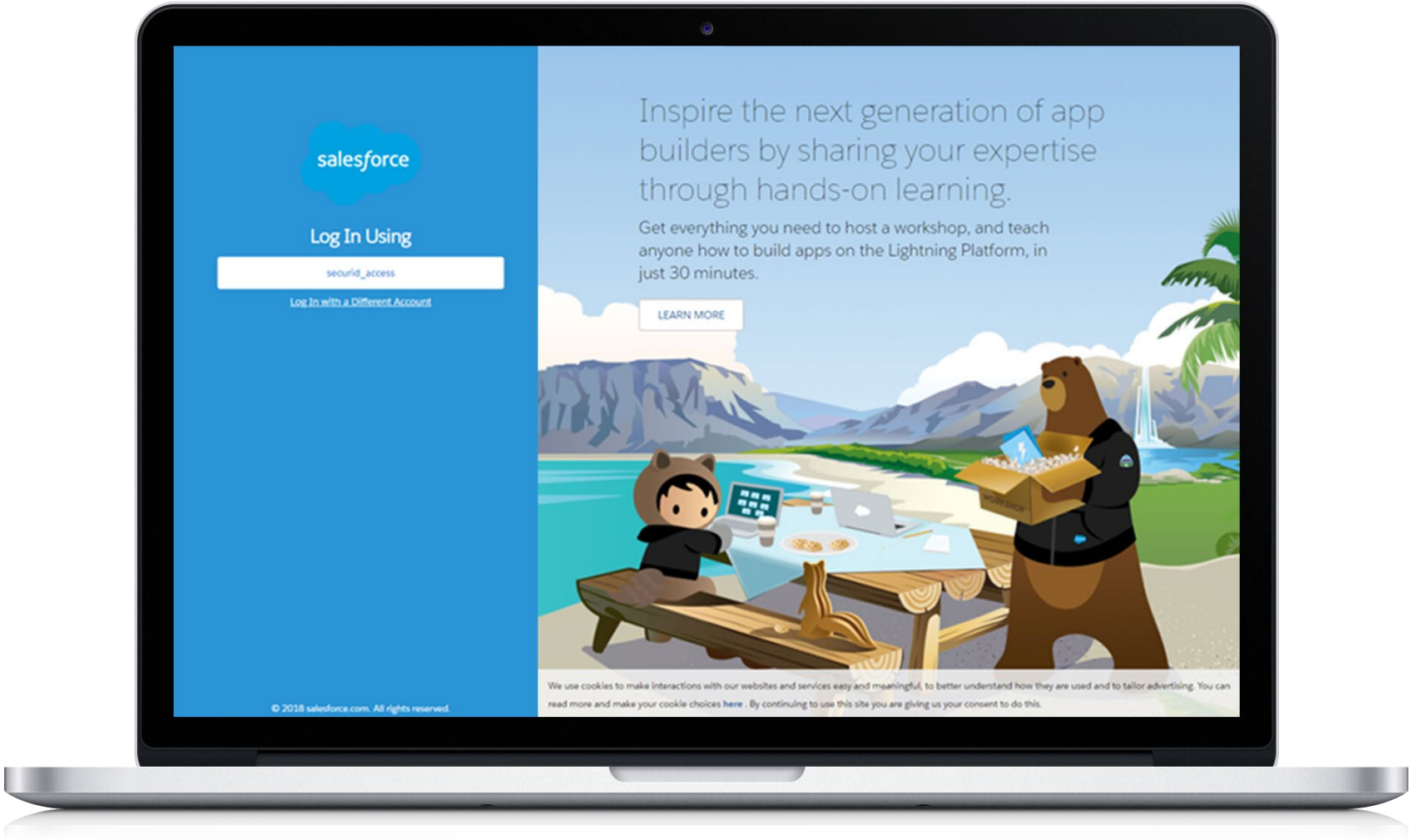
Putting it all together



Putting it all together – in action

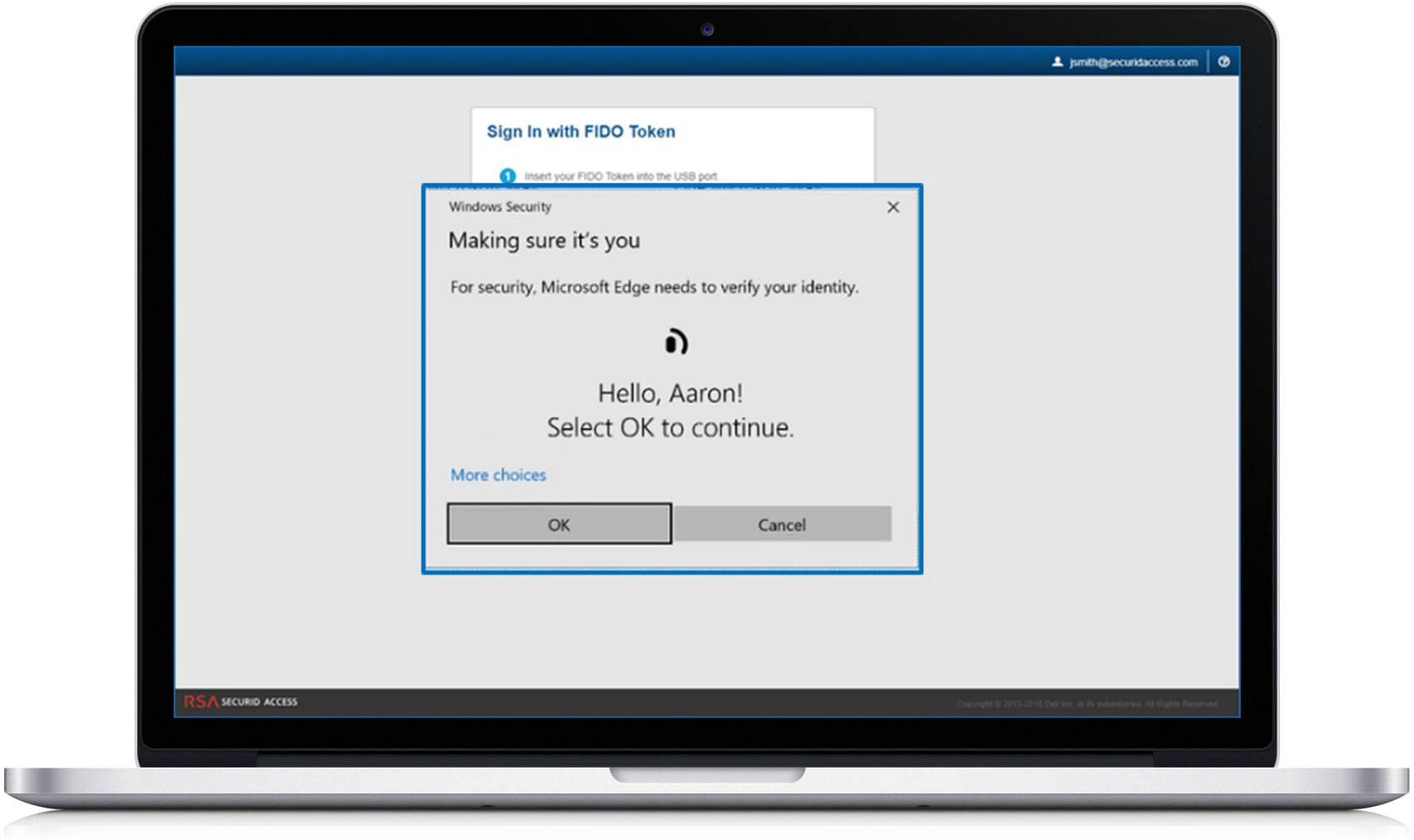
Putting it all together – in action

APPLICATION PROVIDER LOGIN PAGE



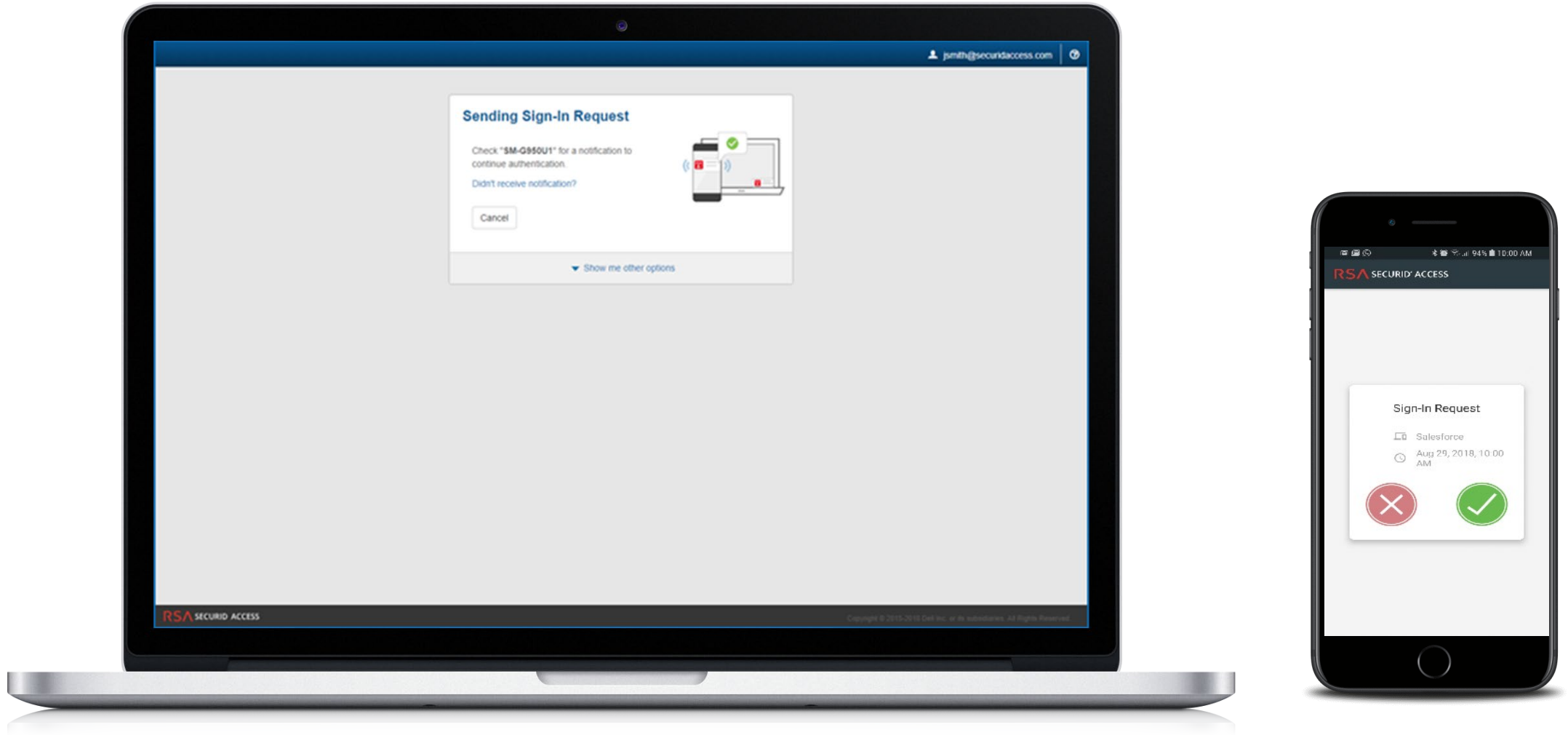
Putting it all together – in action

IDAAS PROVIDER AUTHENTICATION PAGE – USING FIDO2/HELLO

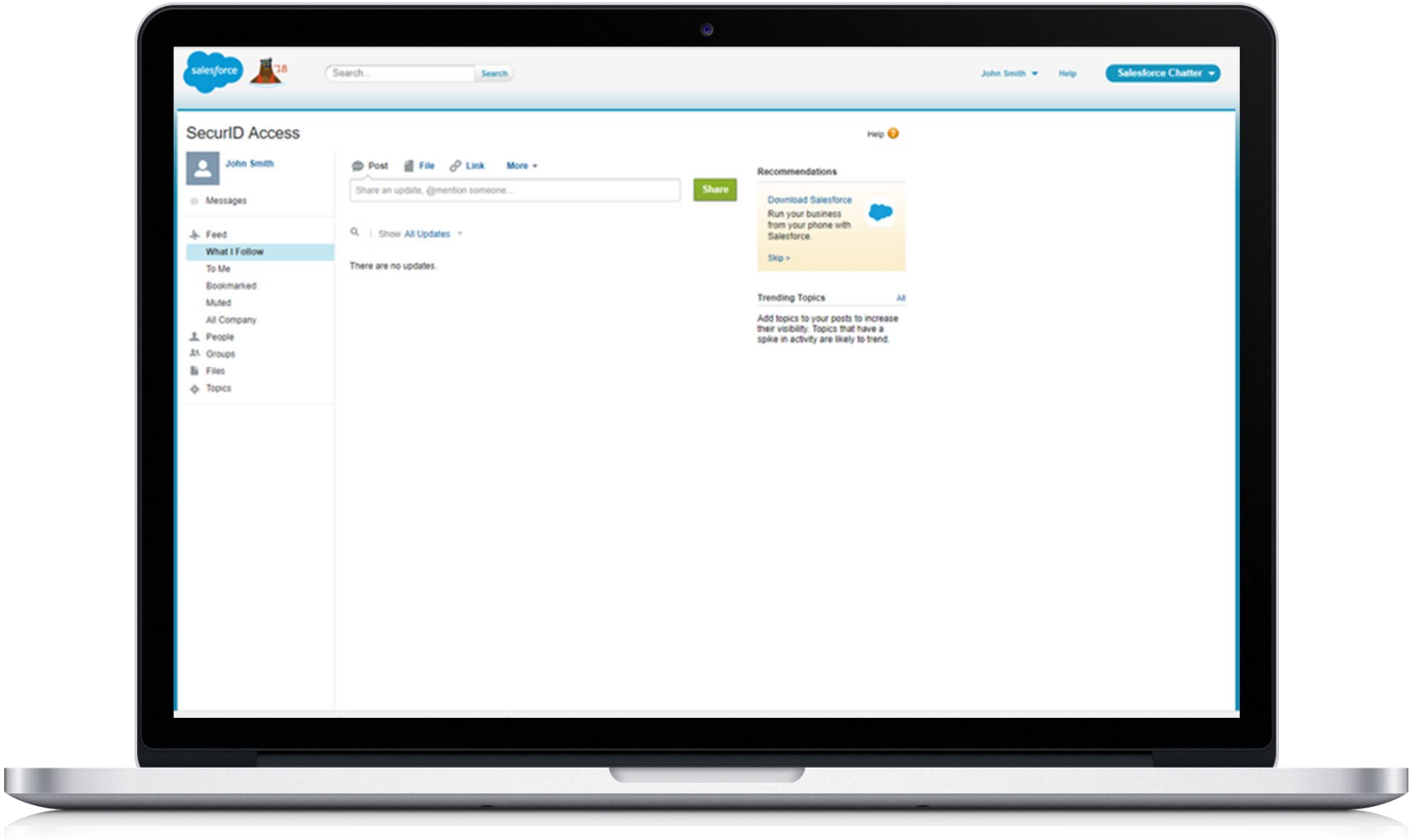


Putting it all together – in action

RISK-BASED/STEP-UP AUTHENTICATION



Putting it all together – in action



Adapt Now!

DIGITAL TRANSFORMATION REQUIRES NEW METHODS TO MANAGE IDENTITY RISK

THIS WEEK

Attend relevant sessions on

- Digital identity risk management
- Passwordless authentication
- Identity analytics for risk awareness
- Zero trust

NEXT SIX MONTHS

Get familiar with emerging standards

- FIDO2, CTAP2 and W3C WebAuthn

Adopt or demand that your IDaaS provider adopts

- Passwordless authentication
- Identity and risk analytics
- Federation and SSO
- Remote identity proofing

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: SEM-M04E

Identity and Access Management (IAM) Emerging Trends and Standards

Salah Machani

Director of Technology
RSA
Salah.machani@rsa.com