Identity Transformed

Zero Touch in Zero Trust

Soumik Ghoshal

An RSA Business

Market Trends Have Accelerated

Digital Transformation Accelerated

Attack Surface Growing with Remote

Regulatory and Compliance Pressure

CONFIDENTIAL

SecurID™

Today's Critical Business Initiatives

Increasing Expectations for Convenient Access

Implementing Identity Assurance

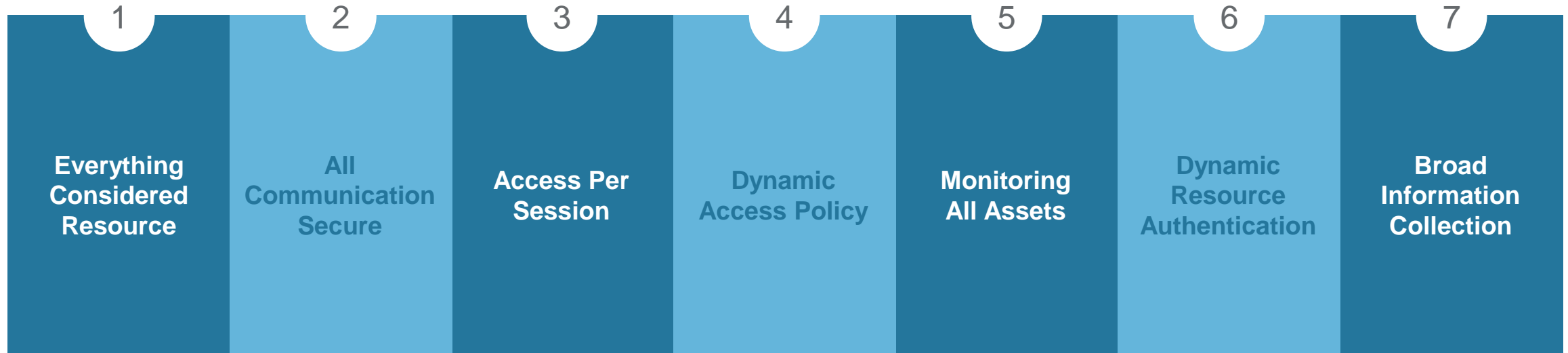Enabling a Remote Workforce

Simplifying Access Governance

Moving to the Cloud

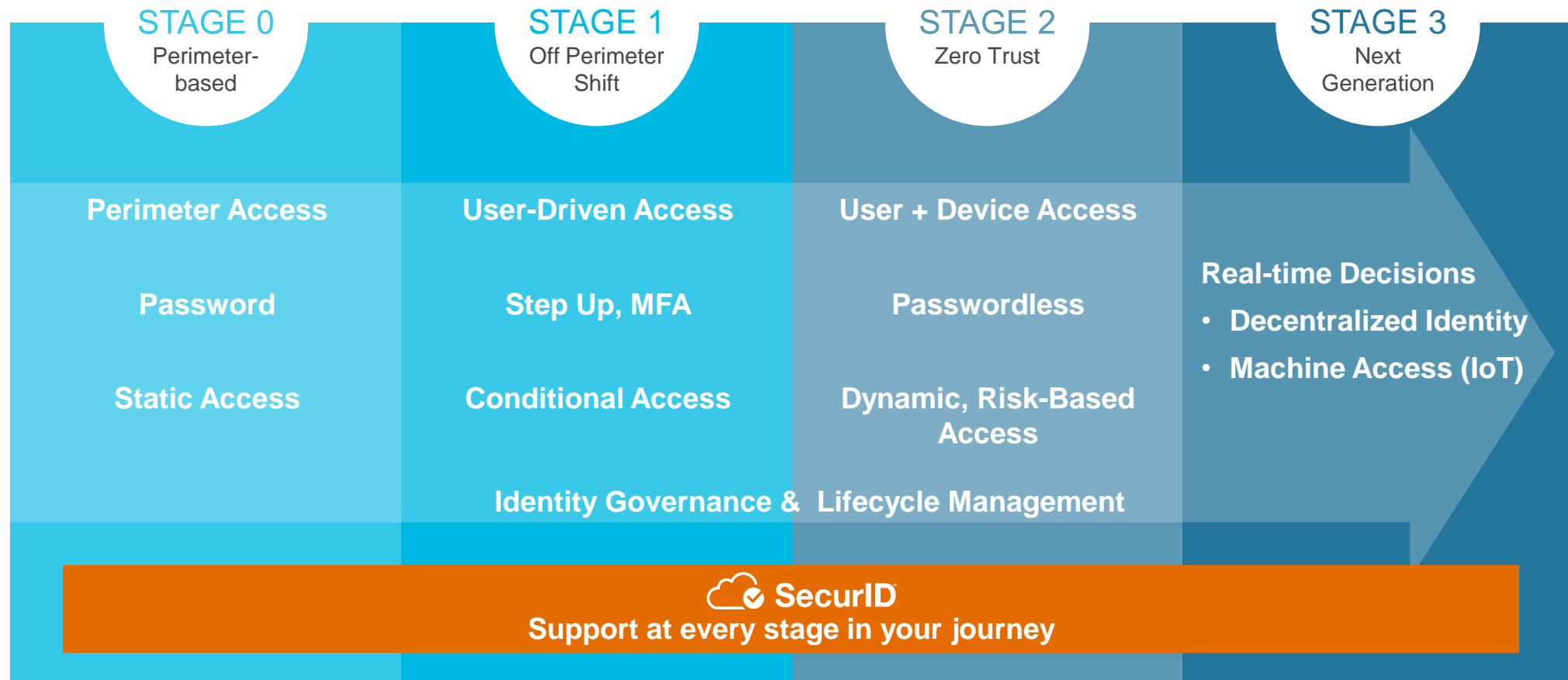Adopting a Zero Trust Security Model

C O N F I D E N T I A L

SecurID™

Zero Trust is Not One Product, It's a Strategy

NIST Seven Tenets of Zero Trust

1	2	3	4	5	6	7
Everything Considered Resource	**All Communication Secure**	**Access Per Session**	**Dynamic Access Policy**	**Monitoring All Assets**	**Dynamic Resource Authentication**	**Broad Information Collection**

CONFIDENTIAL

SecurID™

Identity & Access Management is a Journey

STAGE 0 Perimeter-based	STAGE 1 Off Perimeter Shift	STAGE 2 Zero Trust	STAGE 3 Next Generation
Perimeter Access	**User-Driven Access**	**User + Device Access**	
Password	**Step Up, MFA**	**Passwordless**	**Real-time Decisions** • **Decentralized Identity** • **Machine Access (IoT)**
Static Access	**Conditional Access**	**Dynamic, Risk-Based Access**	
	Identity Governance & Lifecycle Management		

SecurID
Support at every stage in your journey

CONFIDENTIAL

SecurID

Access Today – Manage and Secure Perimeter

Perimeter

User

Company Device

On Premise

User

Company Device + Token

VPN

User

Password

Cloud

CONFIDENTIAL
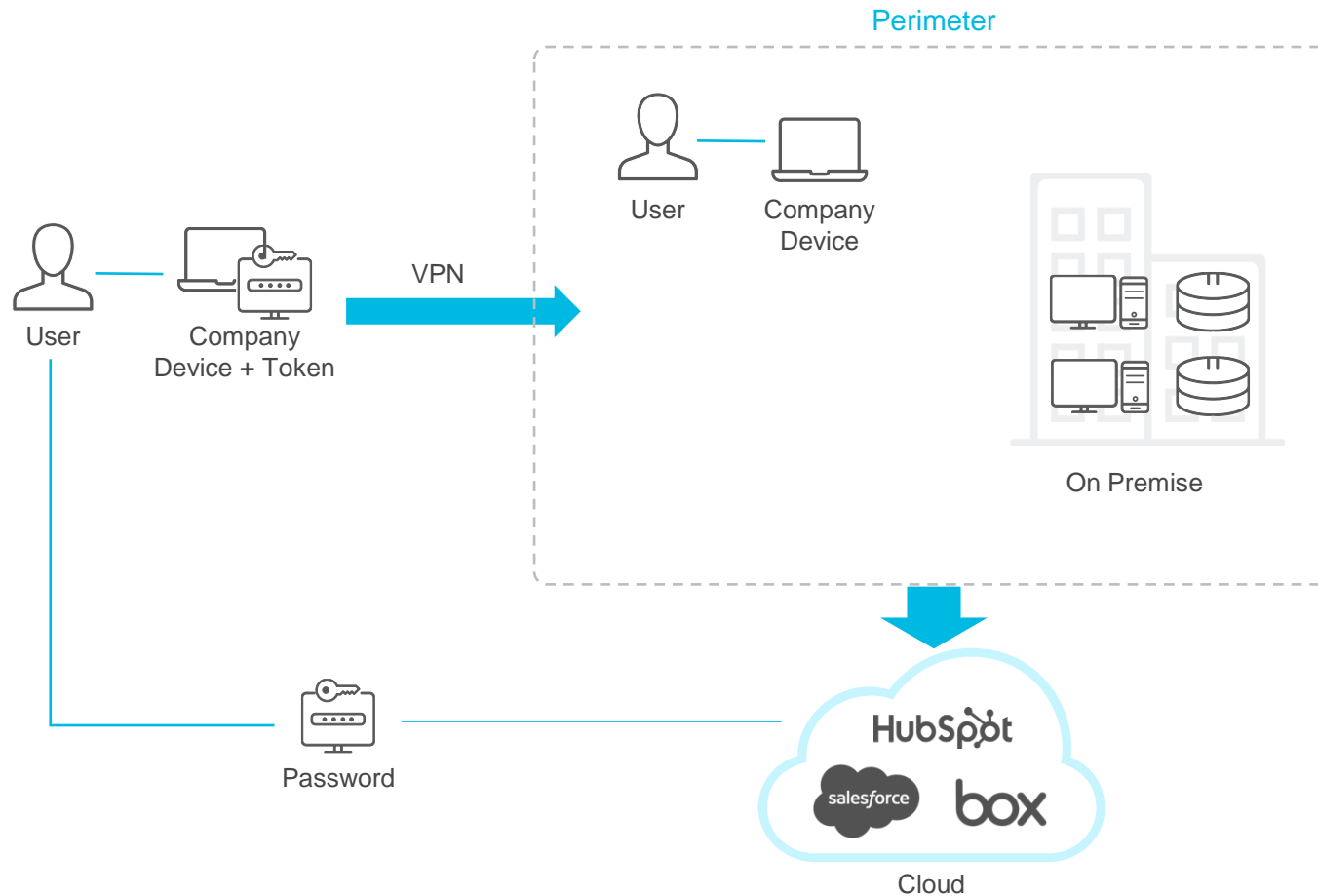
SecurID™

Manage Identity & Access – Dynamic Authentication Perimeter

CONFIDENTIAL
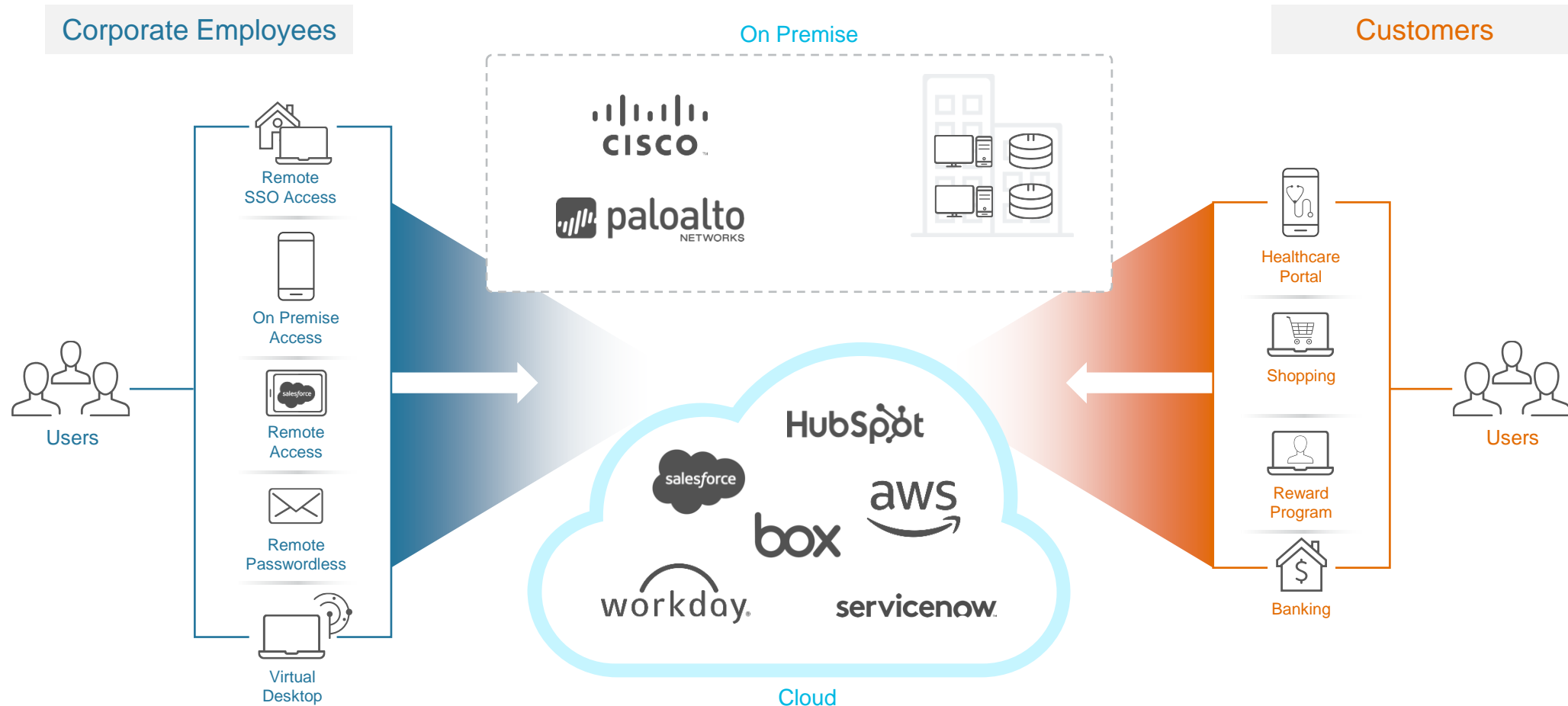
The Way Forward: Identity is Central to Zero Trust Strategy

NFIDENTIAL
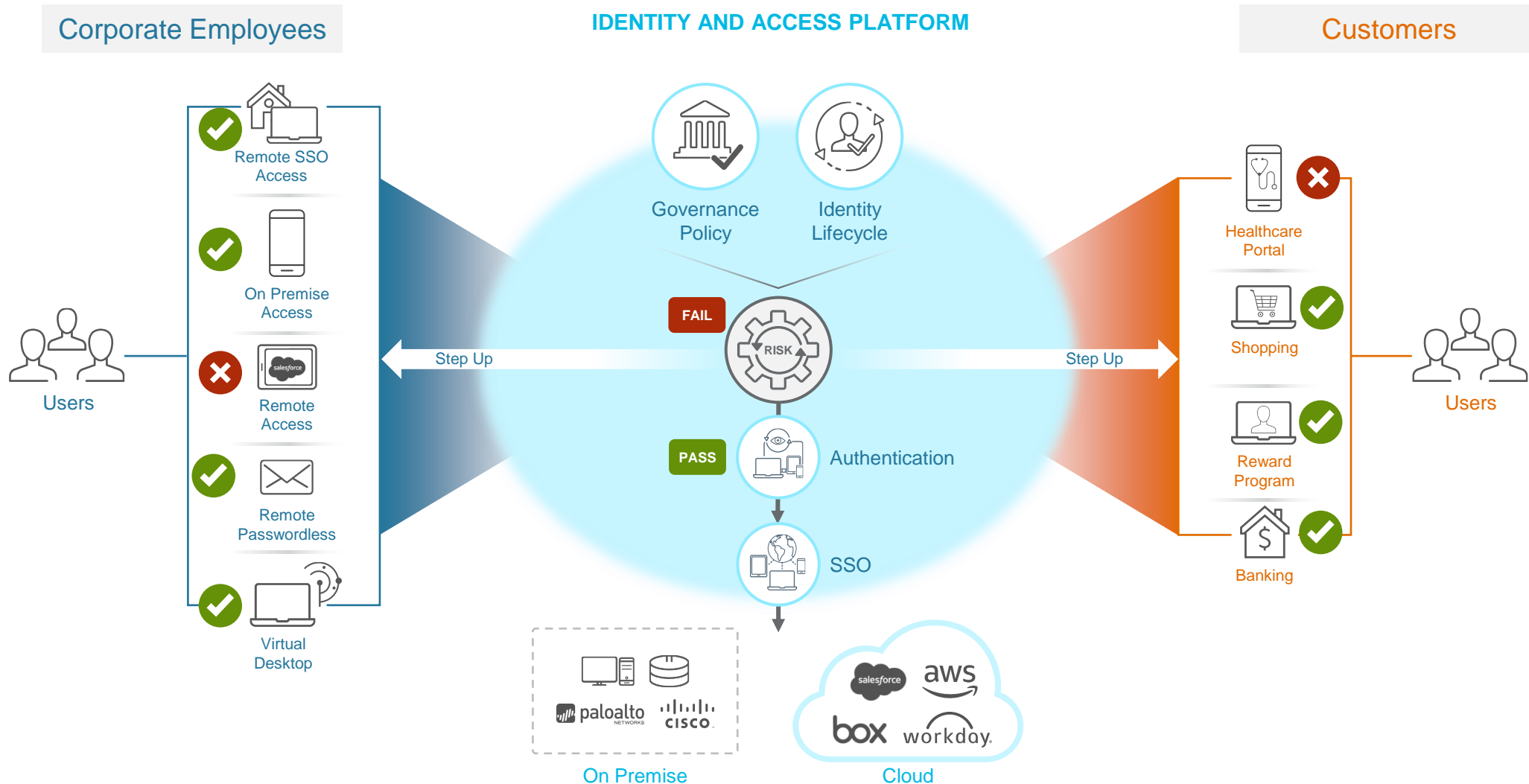
SecurID

How are we helping organizations today?

Modern Authentication
Security and convenience for a mobile and dynamic workforce

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

HW Token · SW Token · FIDO · Proximity · Wearables

Conditional Access & Risk-Based Assurance
Mitigate threats and reduce friction through invisible layers of protection

RBAC / ABAC
Conditional Policy
Levels of Assurance
Machine Learning

RISK

PASS · RISK · DENY

Role · Location · Device · Behavior · External

Enterprise-Grade Credential Management
Secure the entire lifecycle, reduce TCO and enable deployment at scale

EMPLOYEE · ADMINISTRATOR · THIRD PARTY

DIVERSE USERS · CREDENTIAL LIFECYCLE

Bridge Islands of Identity
Complete coverage from ground to cloud with a seamless user experience

Microsoft · SONICWALL · servicenow

CYBERARK · salesforce · CISCO · workday

amazon web services · paloalto NETWORKS · CITRIX · vmware

RSA READY
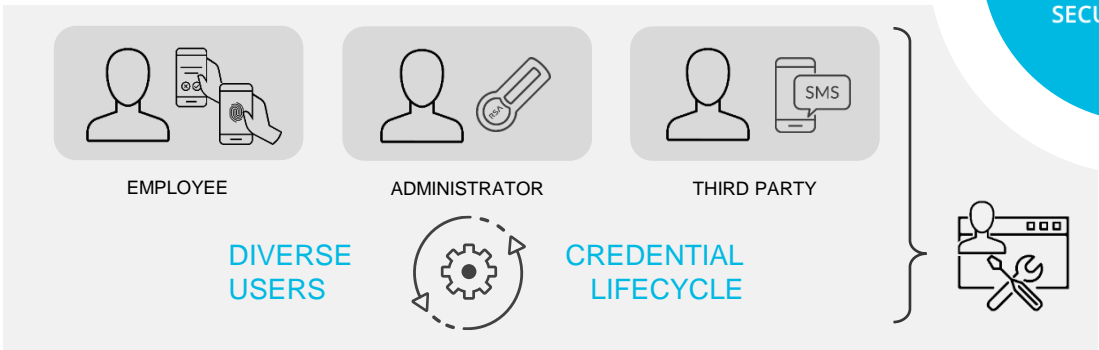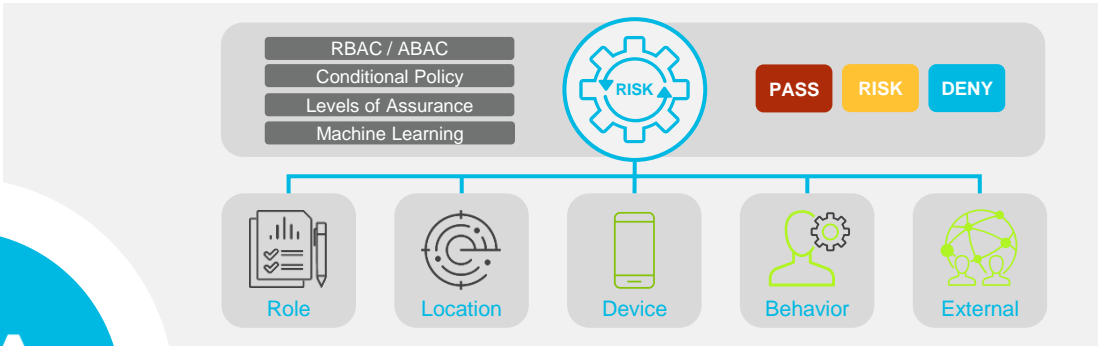
RSA SECURID ACCESS

CONFIDENTIAL

SecurID

SecurID Access Today

Modern Authentication
Security and convenience for a mobile and dynamic workforce

Push	Mobile OTP	Biometrics	Text Msg	Voice Call
HW Token	SW Token	FIDO	Proximity	Wearables

RSA
SECURID® ACCESS

- Range of authentication options—hardware, embedded, software and mobile

- Thought leaders—FIDO board; first mover in tech innovations like wearables and proximity

- Passwordless authentication—online or offline

- Flexibility and choice
    - Organizational policy (*what is allowed?*)
    - User preference (*what do you want to use?*)
    - Role / use case (e.g., SMS for contractors; hardware token for admins; exceptions for users with disabilities)
    - Assurance level (e.g., mobile push for medium trust vs. biometrics for high trust applications)

CONFIDENTIAL

SecurID™

SecurID Access Today

- Role and attribute-based access controls

- Conditional policies (e.g., network, country of origin, geo-fencing, known device, etc.)

- Dynamic risk scoring based on behavioral analysis and ML; tuned at both the individual user and group levels

- Use external sources of risk intelligence to identify risky users and react in real time

- Ability to define complex, hybrid policies combining all of the above

- Risk dashboard provide insights into risk engine tuning for planning and "black box" troubleshooting

Conditional Access & Risk-Based Assurance
Mitigate threats and reduce friction through invisible layers of protection

RBAC / ABAC
Conditional Policy
Levels of Assurance
Machine Learning

RISK

PASS   RISK   DENY

Role   Location   Device   Behavior   External

Pro Tip: Zero Trust Network Access (ZTNA)

Two key principles of Zero Trust:

1) Establishing the *trustworthiness* of a user's identity claim
2) Limiting access to only what that user needs ("least privilege")

With a remote workforce, this cannot be done through static rules. It requires dynamic controls that are context and risk-aware

CONFIDENTIAL

RSA SECURID® ACCESS

SecurID™

SecurID Access Today

- The broadest support from datacenter to cloud

- RSA Ready: 500+ certified solutions; thousands more through open standards
  - RSA proactively tests, certifies, updates, documents and supports every integration
  - Many are embedded in partner products and supported out-of-the-box
  - Strongest support for on-prem and legacy platforms, applications and infrastructure that remain mission critical to most enterprises

- Strong Microsoft partnership including Windows Hello, Azure MFA and O365
  - Day 1 integrations regularly featured in PR and at Microsoft Ignite

RSA SECURID® ACCESS

Microsoft SONICWALL servicenow

CYBERARK salesforce CISCO workday **RSA** READY

amazon web services paloalto NETWORKS CITRIX vmware

Bridge Islands of Identity
Complete coverage from ground to cloud with a seamless user experience

   CONFIDENTIAL

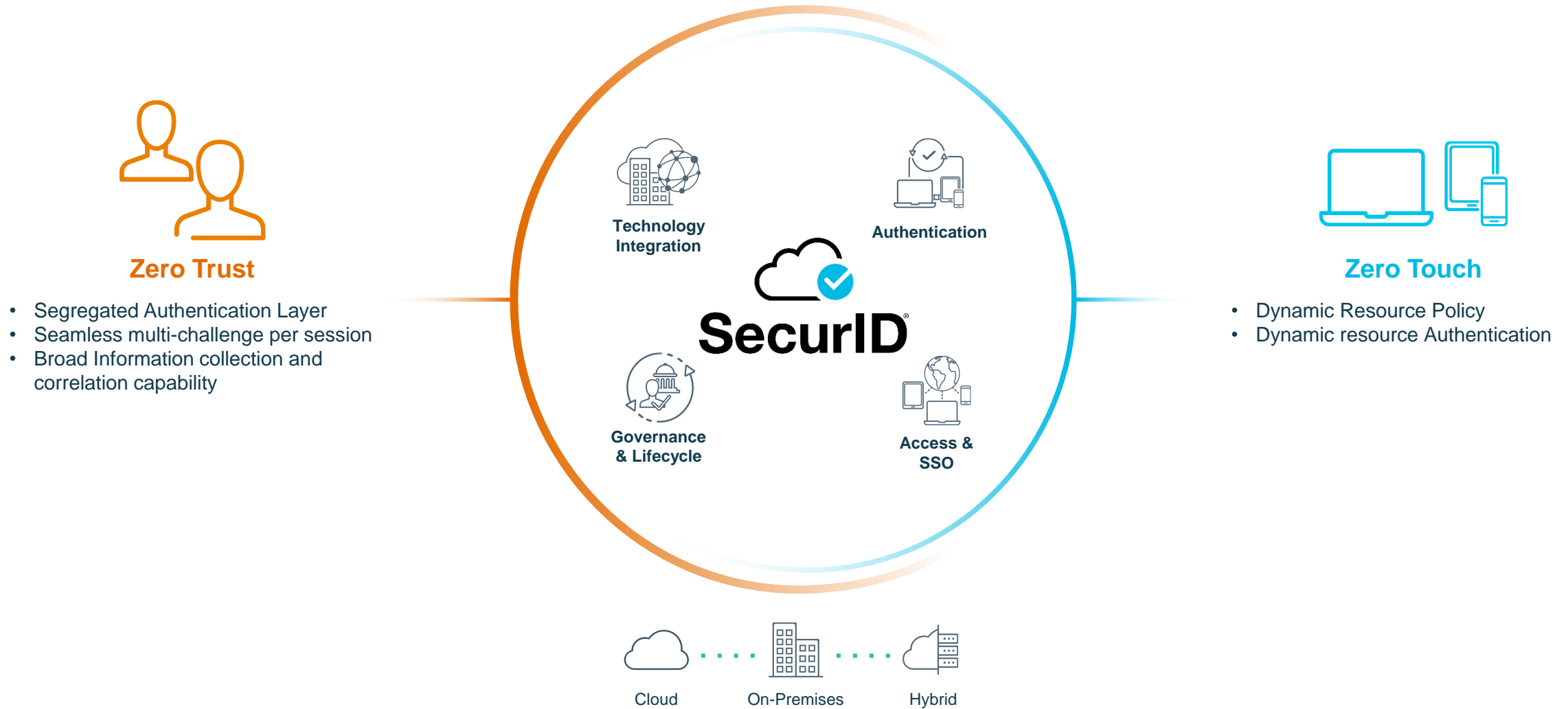SecurID™

SecurID Access Today
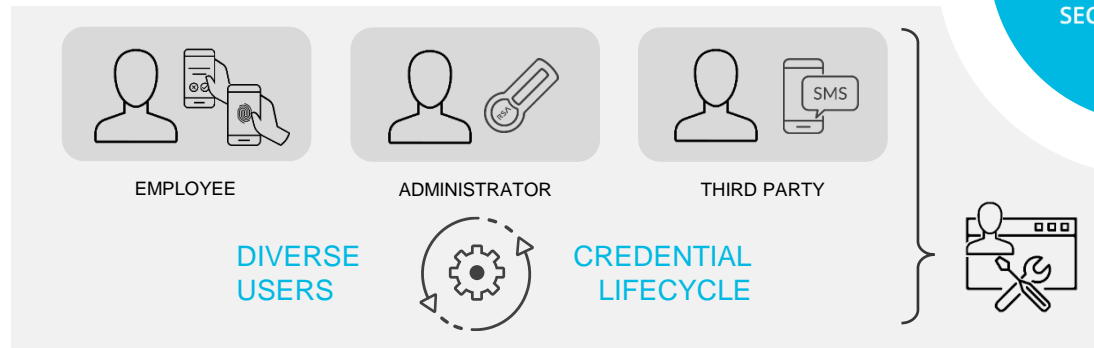
Enterprise-Grade Credential Management
Secure the entire lifecycle, reduce TCO and enable deployment at scale

- SaaS, on-prem, hybrid and virtual to support the deployment needs of any organization

- Highly-available SaaS with on-prem failover

- Enterprise-grade security, features and scale

- Secure the entire credential lifecycle to eliminate weak points like on-boarding, emergency access and credential recovery

- Admin and self-service credentialing to support multiple identity assurance levels and strict regulatory requirements

- Full customization through APIs and Prime for integration with existing back-office systems, processes and workflow

CONFIDENTIAL

Zero Touch in Zero trust

Zero Trust
- Segregated Authentication Layer
- Seamless multi-challenge per session
- Broad Information collection and correlation capability

Technology Integration

Authentication

SecurID®

Governance & Lifecycle

Access & SSO

Zero Touch
- Dynamic Resource Policy
- Dynamic resource Authentication

Cloud   On-Premises   Hybrid

CONFIDENTIAL

SecurID™

40 Years of Innovation in Authentication

RSA

1977: RSA Algorithm

1986:
Time-synchronous OTP (RSA SecurID)

1996:
RSA SecurID software token

2001 - 2002:
SMS authentication
Palm Pilot software token
Windows Mobile software token

2003 - 2005:
RSA SecurID for Windows logon
BlackBerry software token
Site-to-user authentication
SAML 2.0 co-authors

2006 - 2008:
RSA Transaction Signing
RSA FraudAction
PIV / FIPS 201

2009 - 2011:
Risk-based auth for Enterprise
RSA SecurID for iOS & Android
"Credentials Everywhere": SanDisk, Broadcom, IronKey, Upek, Good

2015:
RSA SecurID Access (SaaS)
Mobile Push
Apple Touch ID

2016:
RSA Identity Assurance
Apple Face ID
Apple Watch

2016:
Proximity MFA for Windows
Samsung Fingerprint
FIDO U2F

2018:
Windows Hello
Azure AD MFA

2019:
Threat Aware Authentication
FIDO2 / passwordless
Motiv Ring
yubico

1977 - 2014

2015 - 2020

SecurID

SecurID: The Trusted Identity Platform

EMPOWERING

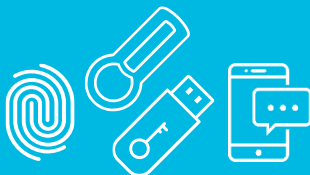**99.99+** percent
Availability

Always-on protection
Hybrid/On-Prem Failover

Tested

500+ certified and thousands
open-source integrations

FLEXIBLE

Range of Tested & Innovative
Authentication Options

50+ million
Identities

Scaled access to any platform,
anywhere, any environment

CONVENIENT

Unified admin and user experience.
Choice: On-prem/cloud, Online/Offline

Optimized

Configurable, Customizable, Automated
Policies and Workflows

C O N F I D E N T I A L

SecurID

Thank You