

Controlware Security Day 2022



Authentifizierung in der Cloud, On-Prem oder Hybrid?

Erik Teschner

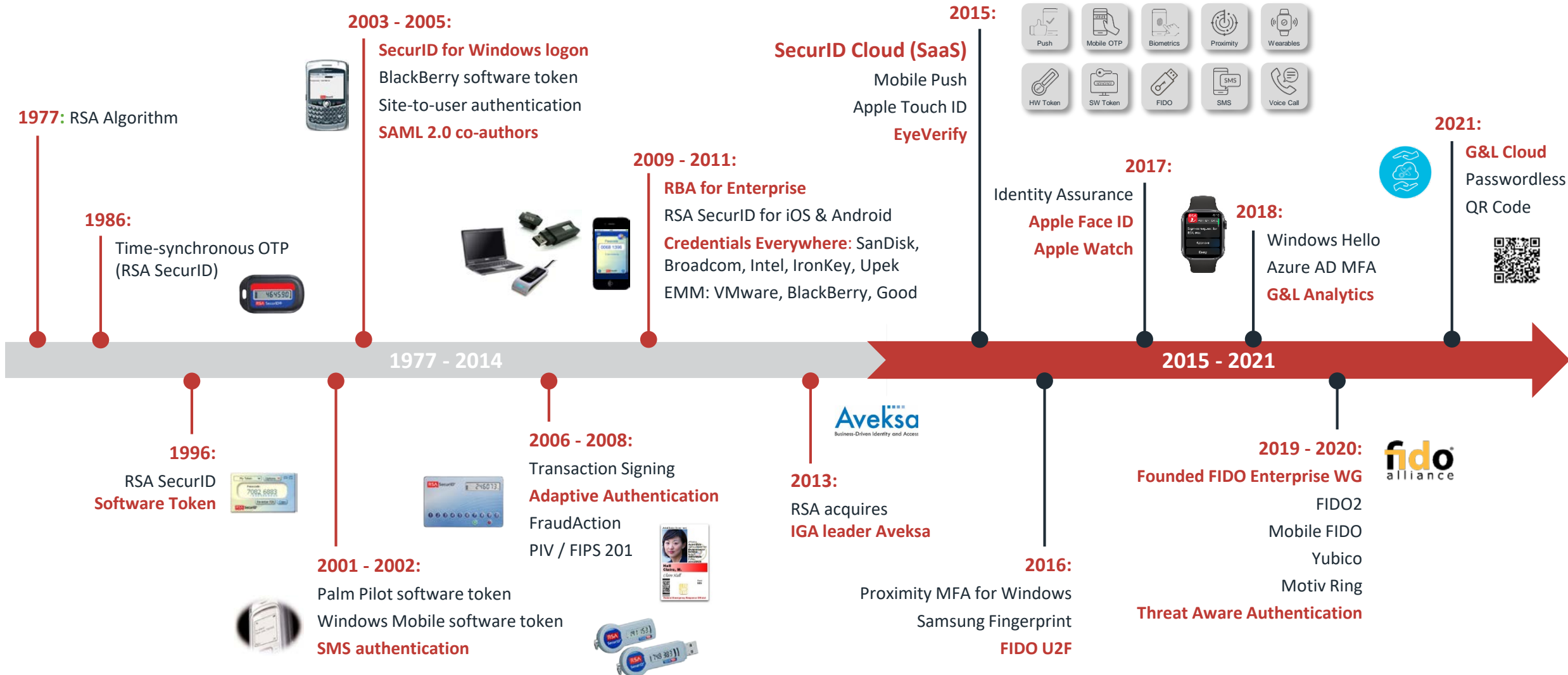
Systems Engineer | RSA

erik.teschner@securid.com



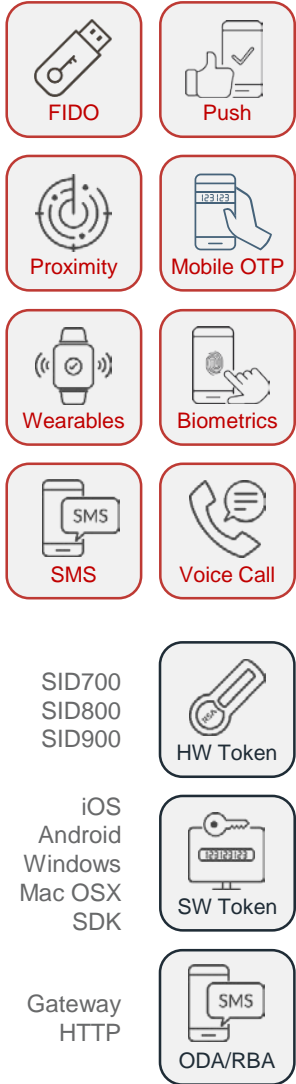
controlware

40 Jahre Innovation im Bereich IAM



SecurID – Trusted Identity Platform

AUTHENTICATORS



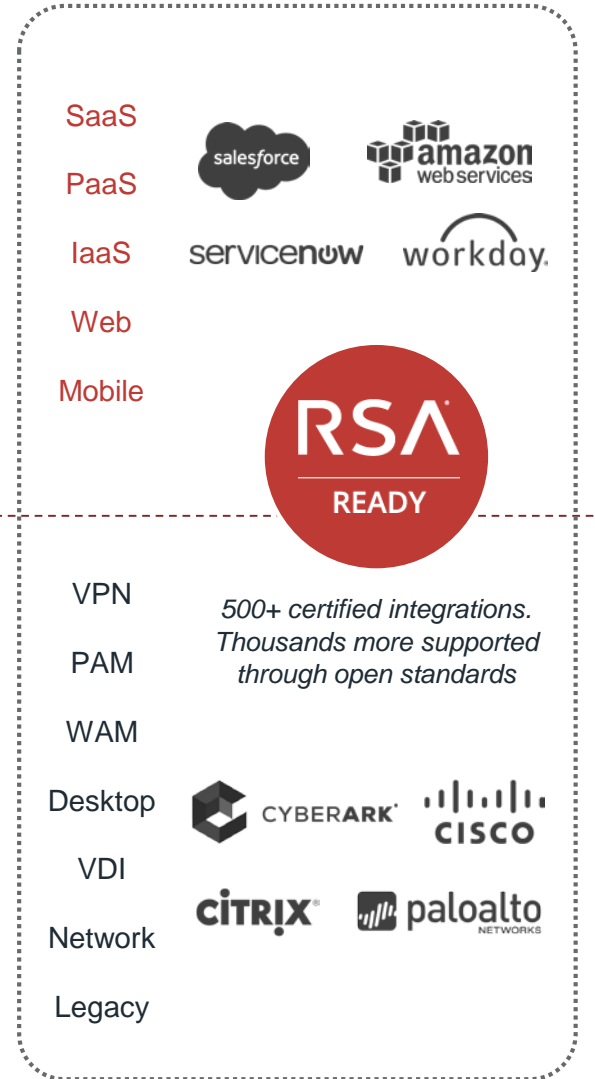
Dynamic Identity Confidence Scoring



Policy & Context

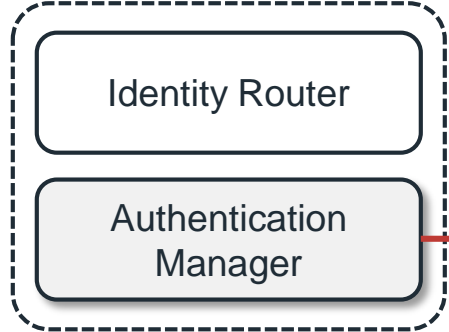


APPLICATIONS



Cloud Authentication Service

Cloud
On-Prem



AM Prime

Self Service

SAML / WS-Fed / OIDC

Agent / RADIUS / SDK

REST API

Modern MFA

Traditional OTP



Enterprise Workflow Integration & Customization

Business Imperatives



Hybrid
Work



Digital
Experiences



IT
Modernisierung



Cybersecurity

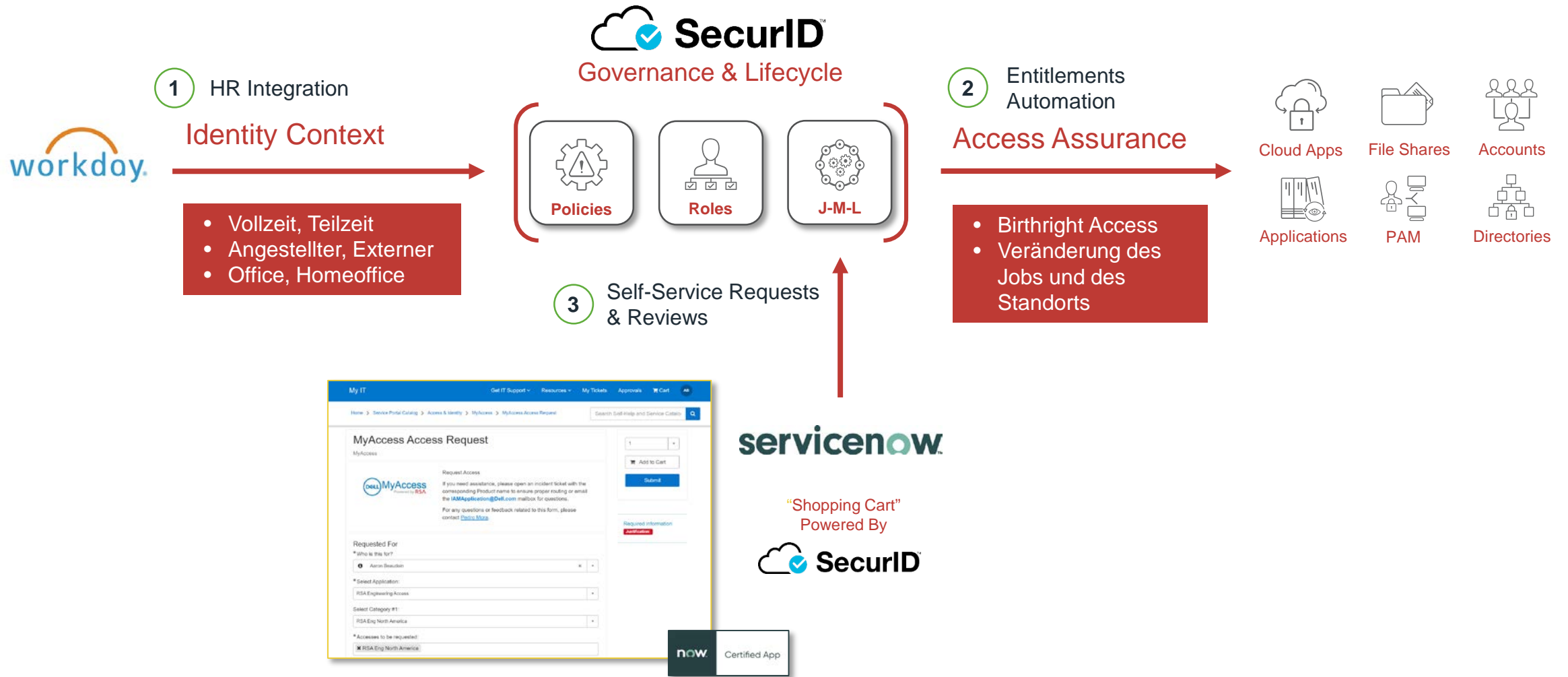
Hybrid Work

Die neue Normalität einer hybriden Workforce

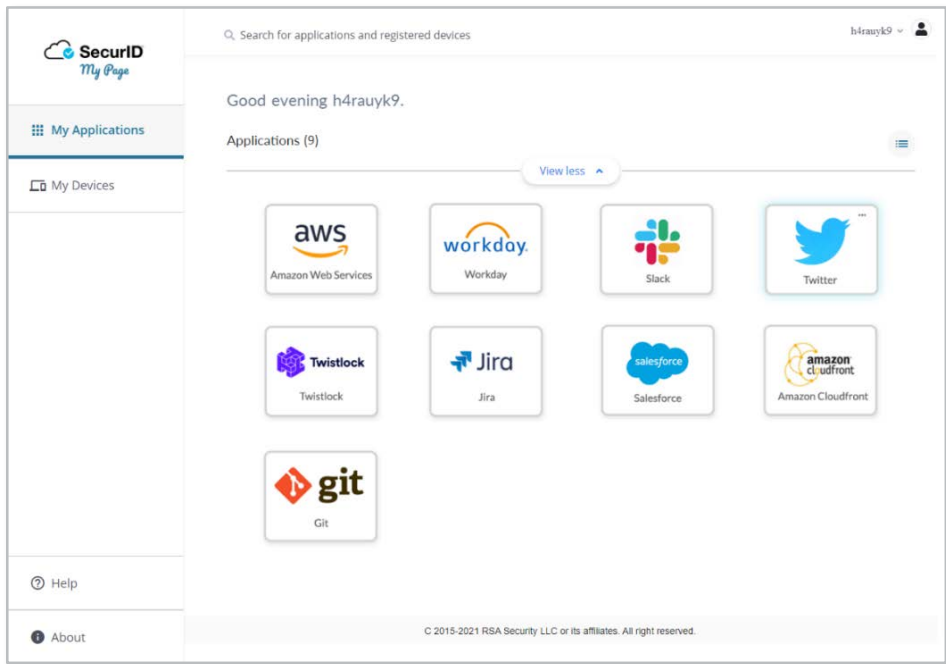
Die Herausforderungen einer hybriden Workforce



Wie managt man eine sich ständig verändernde Workforce?



Produktivitätssteigerung durch SSO und Self Service



My Page 2.0

- Cloud SSO Portal
- Integrierter Self-Service
- Cloud (SAML) und On-Prem Apps (IDR proxy)
- Voll anpassbar
- Userfreundliche Features

NEU

My Page 2.5

- OpenID Connect (OIDC)
- Externe Authentifikatoren
- Universal Passwordless
- Passwortmanagement

Ende 2022

My Page vNext

- Erweiterter Credential & Account Self-Service
- Integration von SecurID Prime Features

Anfang 2023

Digital Experiences

Vereinfachung der Online Collaboration und Interaction mit einer immer vielfältigeren User Base

Digital Experiences

Herausforderungen für Kunden

Unternehmen treiben mehr Online Collaboration und Informationsaustausch voran

Externe User mit unterschiedlichen Anforderungen und Bedürfnissen

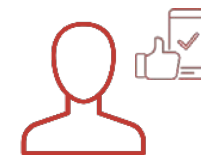
Hohe Erwartungen an eine gute User Experience

Negative Folgen (\$\$\$) einer schlechten User Experience

Sicherheit muss ein integrierter und reibungsloser Bestandteil der User Experience werden



Mitarbeiter



Partner



Kunde

Authentifizierung für jeden User und Use Case



- 1 Hardware Tokens:** kritische Infrastruktur, sichere Umgebungen, On-Prem Use Cases
- 2 Desktop Authentifikatoren:** Schnelles User Enrollment, ideal für Use Cases bei denen kein Smartphone benutzt werden kann/darf
- 3 Große Auswahl an Authentifikatoren:** Authentifikatoren für jeden Use Case, egal ob On-Prem, Hybrid oder in der Cloud



Goldener Standard



Hybrider Authentifikator

Auswahl an Authentifikatoren



Unterscheidungsmerkmal



Eine moderne und reibungslose User Experience

EINFACH

Moderne
Benutzeroberfläche, QR-
basiertes Enrollment

ALLE USER

Smartphone, PC, macOS,
Hardware Tokens

ZUGÄNGLICH

VPAT/WCAG compliant

VEREINHEITLICHT

Ein Authentifikator für
On-Premise, Hybrid und
Cloud

PASSWORDLESS

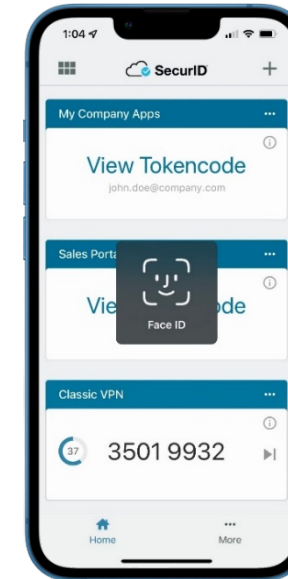
Wachsendes Angebot an
Optionen

BENUTZERDEFINIERBAR

SDK, API und Prime

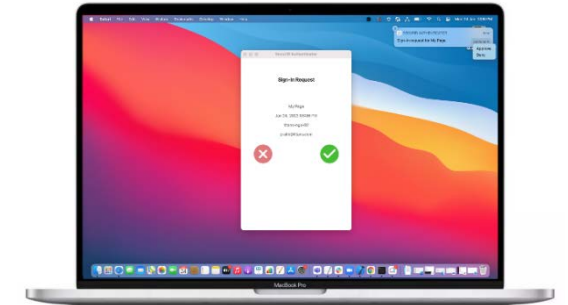
NEU

iOS/Android



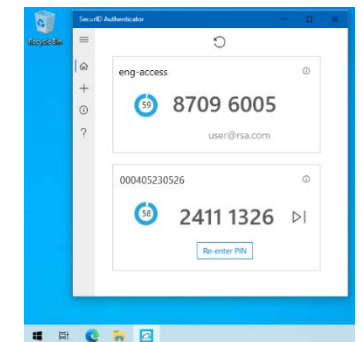
NEU

macOS



NEU

Windows 10/11



Ende 2022

DS100 Hardware Token



SecurID Cloud User Store

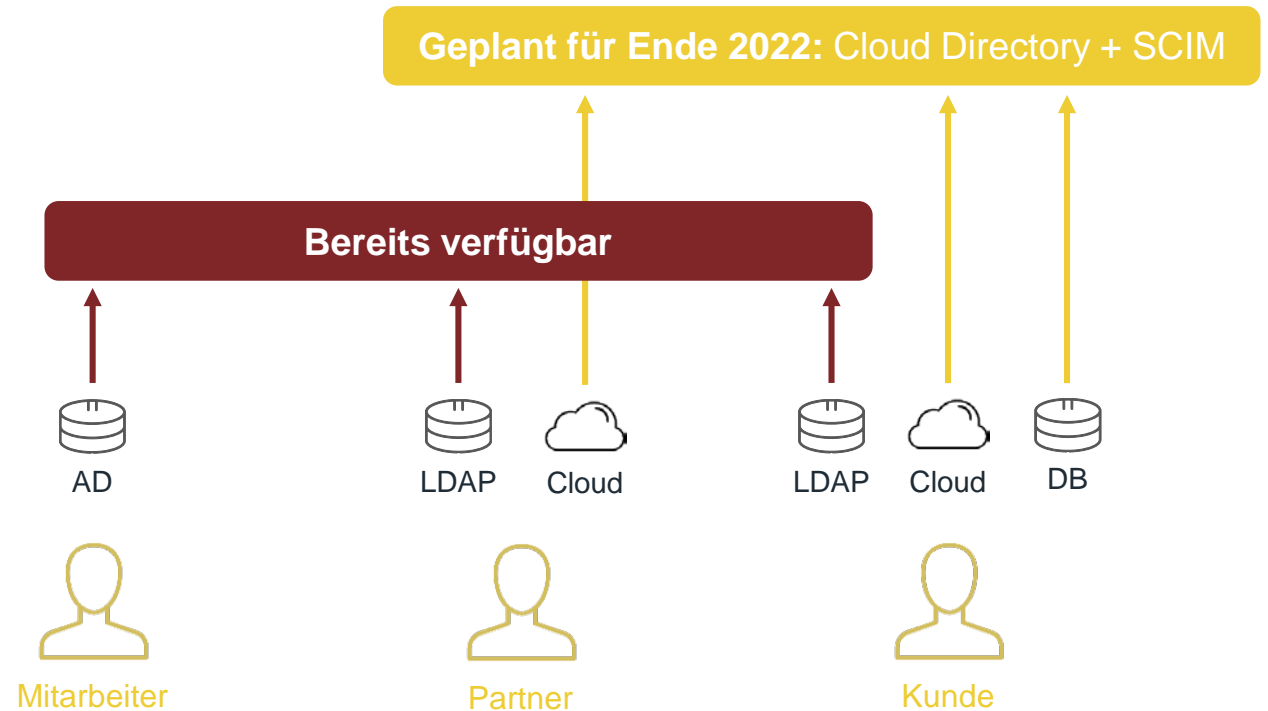
Identity Management für Ihre Mitarbeiter (WIAM), externen Mitarbeiter (XIAM) und Kunden (CIAM)

User Store v1.0

- Natives Cloud Directory für externe User
- Für User, die nicht in einem traditionellem AD/LDAP sind

Zukünftige Use Cases

- Migration von der internen Datenbank des Authentication Manager
- On-demand Trials und POC's
- Cloud-only Deployments



IT Modernisierung

Journey von On-Premise zu Hybrid zu Cloud
(und darüber hinaus)

IT Modernisierung

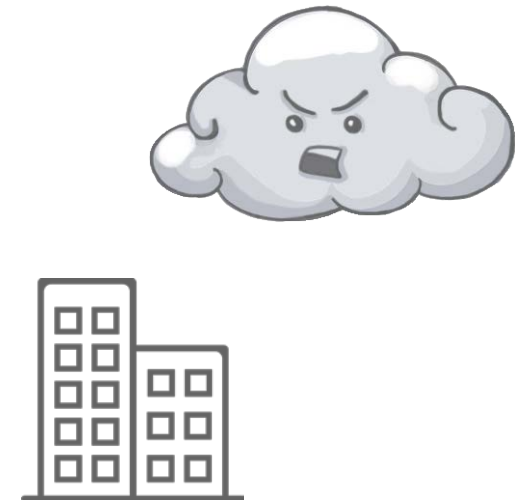
Herausforderungen für Kunden

Große Unternehmen haben immer noch viele Legacy On-Premise-Applikationen

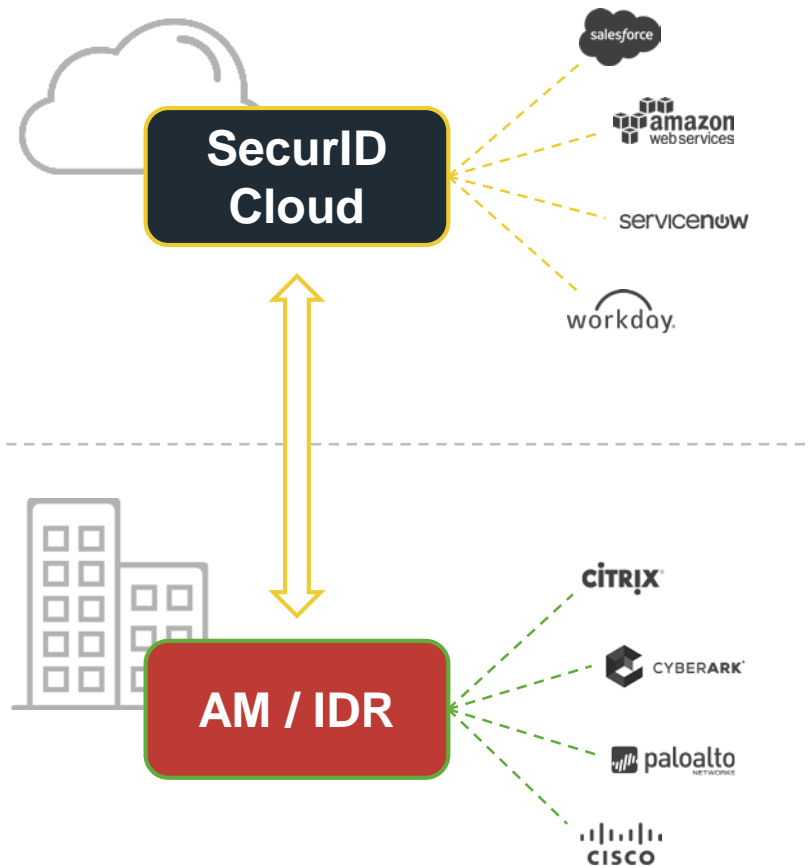
Bei geschäftskritischen Anwendungen und privilegierten Usern wird der Cloud nicht vertraut

Anhaltende Bedenken hinsichtlich der Sicherheit oder Zuverlässigkeit der Cloud

Upgrades sind umfangreich, sehr störend und teuer



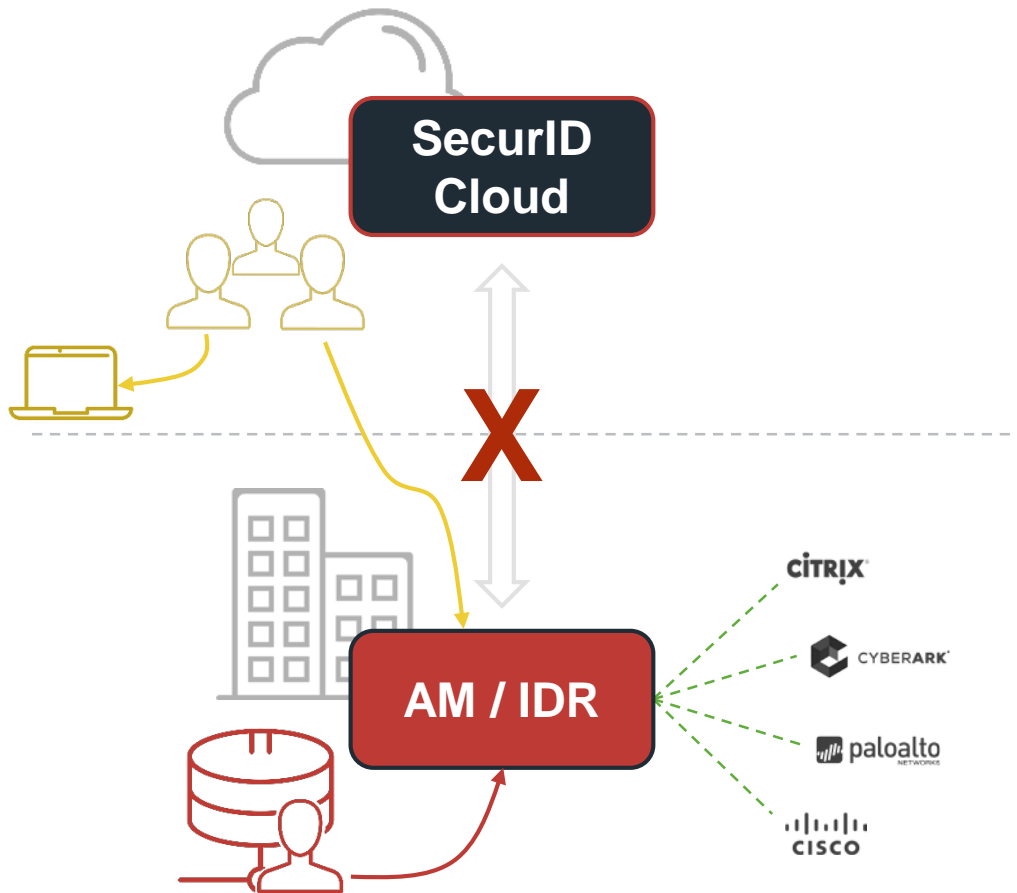
On-Prem-Apps gehören zu den kritischsten (und am schwierigsten zu integrierenden) Anwendungen



RSA ADVANTAGE

- 1 Nativer Support:** RSA ist in Hunderten von traditionellen IT-Anwendungen vorkonfiguriert
- 2 Legacy Apps:** Große Auswahl an Integrationen mit On-Prem Legacy Applikationen
- 3 Cloud Ready:** Cloud-Authentifikatoren sind rückwärtskompatibel mit Legacy Integrationen (AM-Proxy)
- 4 RSA Ready:** Vielzahl an unterstützten, getesteten und zertifizierten Integrationen

Zuverlässige Unterstützung für die kritischsten Anwendungsfälle



"Wenn diese Anwendung ausfällt, können wir unser Business nicht weiterführen. Wir würden diese Anwendung niemals in die Cloud verlagern."



RSA ADVANTAGE

- 1 On-prem users:** Privileged Users & Credentials können getrennt und On-Prem verwaltet werden
- 2 Hybrid HA: Alle Benutzer** (On-Prem + Cloud) können weiterhin auf wichtige On-Prem-Anwendungen zugreifen, wenn die Cloud nicht erreichbar ist.
- 3 Offline authentication:** Windows- und macOS-Laptops sind stark abgesichert, auch offline

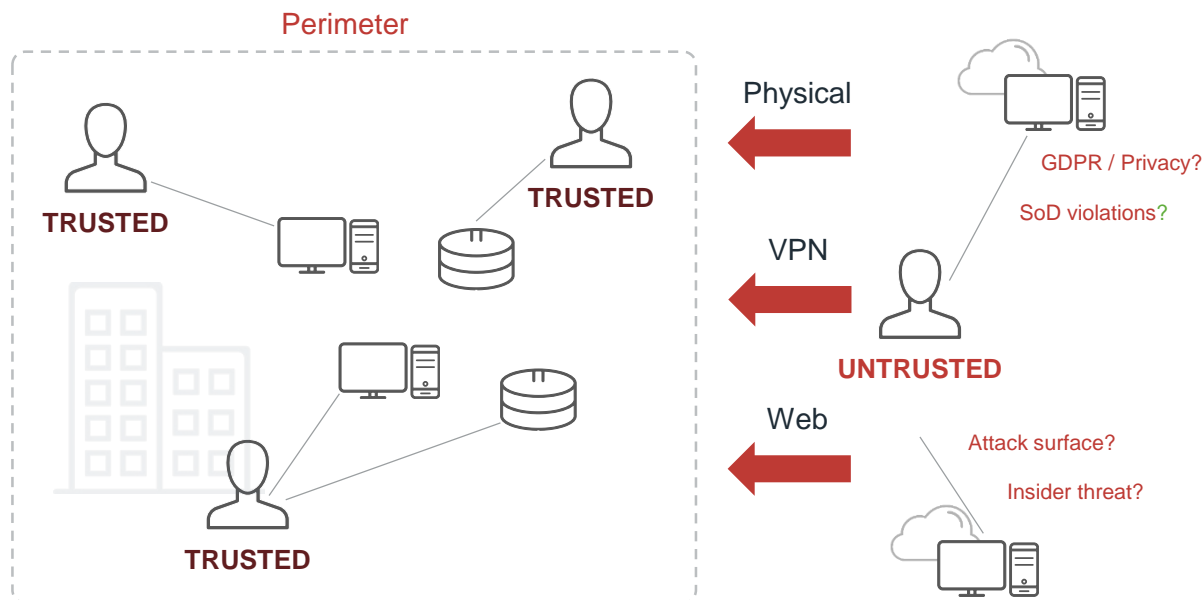
Cybersecurity

Understanding and adapting to zero trust frameworks

Perimeter-basierte Sicherheit ist nicht mehr wirksam

Vor Zero Trust

- Jeder, der sich innerhalb des Unternehmensbereichs befindet, genießt implizites Vertrauen.
- Netzwerkinterne Benutzer können auf alles zugreifen



Herausforderungen

Immer mehr Network Entry Points

Mehr User und Apps außerhalb des Perimeters

Negative Auswirkungen eines uneingeschränkten Zugangs

Zero Trust Paradigmenwechsel: Identity ist der neue Perimeter

Hauptprinzipien

RSA ADVANTAGE

Starke Authentifizierung des Benutzers

Der richtige Authentifikator für jeden Benutzer

Überprüfung jeder einzelnen
Zugangsanfrage

Umfassende Governance und Lifecycle

Dynamische Risikobewertung des
Zugangs in Echtzeit

Conditional Access und risikobasierte
Authentifizierung

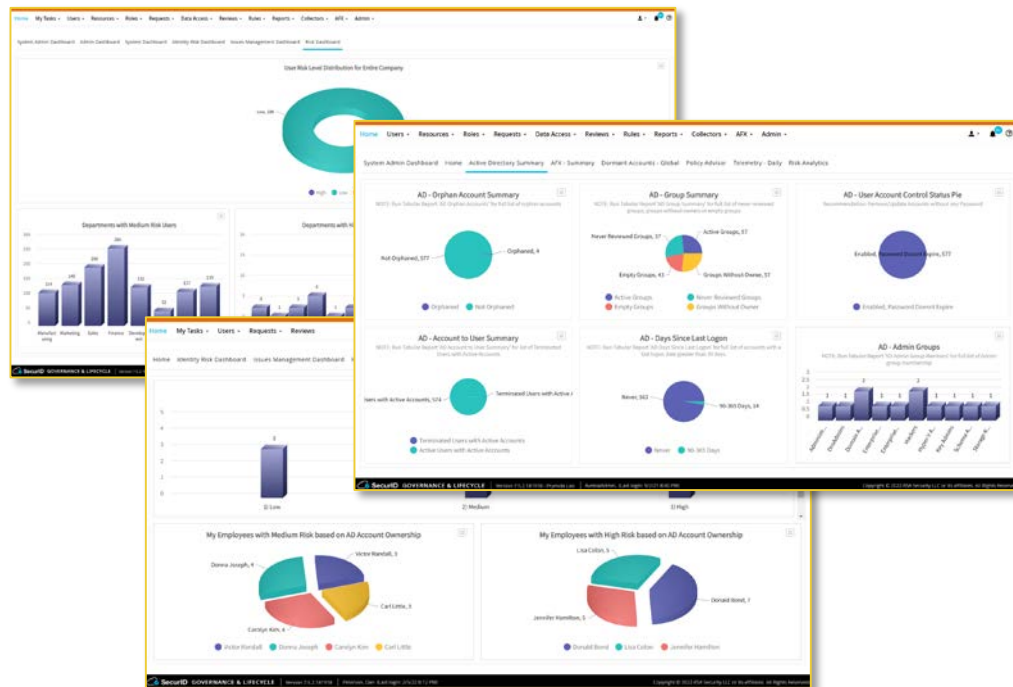
Neubewertung eines jeden neuen
Zugriffsantrags

Hybride Plattform, vollständiger Schutz von On-
Prem bis in die Cloud

Erkenntnisse aus Risikobewertung zur
kontinuierlichen Verbesserung nutzen

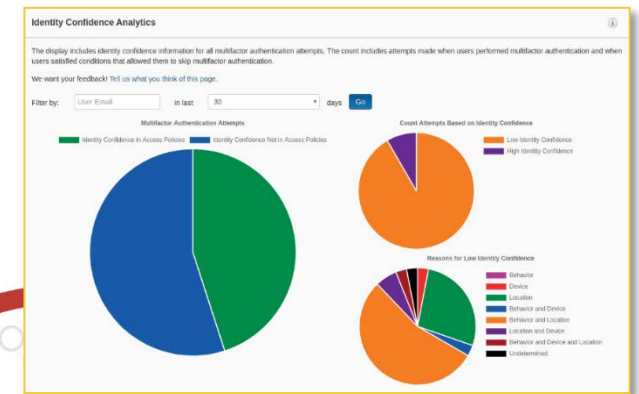
Risk Intelligence von Identity Management bis
Access Management

Risk Insights & Intelligence: The Next Frontier for Zero Trust

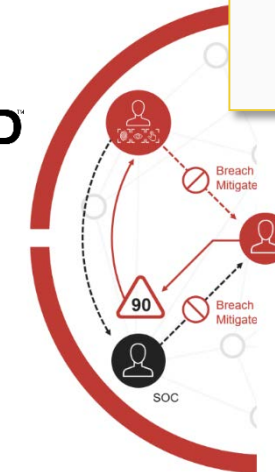


Governance Risk Dashboards

Access Risk Engine Dashboard



SIEM



Threat Aware Authentication

Final Takeaway: Warum SecurID?



- 1** Eine Identity Lösung, die in einzigartiger Weise in der Lage ist, **Identity & Access Assurance** durch die Kombination von branchenführender, intelligenzbasierter **Authentifizierung** und **Governance** zu gewährleisten.
- 2** Eine **hybride Plattform**, die am besten geeignet ist, um die Anforderungen komplexer, sicherheitssensibler Unternehmen auf dem Weg von **On-Premise zu Hybrid, zu Cloud** und darüber hinaus zu erfüllen.
- 3** Ein **modernes und überzeugendes Erlebnis** für jeden User, das den richtigen Zugang für die richtigen User zur richtigen Zeit gewährleistet.

Vorstellung von ID Plus

ID Plus bietet drei Editionen von Cloud-Lösungen, die allen Anforderungen an das Identitäts- und Zugriffsmanagement gerecht werden. Alle können flexibel in der Cloud, On-Premise oder Hybrid eingesetzt und können leicht an Ihre Bedürfnisse angepasst werden.

Eine
Lizenz für
User und
Token

Skalierbar
für Ihr
Unterneh-
men

3 Editionen,
anpassbare
Pläne

ID Plus Packaging

	ID Plus E1	ID Plus E2	ID Plus E3
Use Case	Cloud only Minimaler Support	Zusätzlicher Schutz, angepasste SSO, mehr Support	Dynamische Zugangskontrolle, höchster Support Level
Inhalt	<ul style="list-style-type: none"> MFA und Software Token Single Sign-On & Web Portal bis zu 10 Apps 9x5 Support, Telefon/Email/Chat Static access rules 	<ul style="list-style-type: none"> MFA und Software Token SSO, angepasstes SSO Portal, unbeschränkte Anzahl an Apps Authentication Manager / Cloud Console Conditional rule-based, adaptive access controls (Filter für Länder, vertraute Netzwerk und Lokationen) Customer Success Manager Option abhängig von Umsatz <ul style="list-style-type: none"> Jährliche Business Reviews Halbjährliche CS Meeting 24x7 support, Telefon/Email/Chat Enterprise Skalierbarkeit <ul style="list-style-type: none"> 15 Replicas AMBA 	<ul style="list-style-type: none"> MFA und Software Token SSO, angepasstes SSO Portal, unbeschränkte Anzahl an Apps Authentication Manager / Cloud Console Conditional und Dynamic risk-based authentication und access controls (Filter für Länder, vertraute Netzwerk und Lokationen + künstliche Intelligenz) Customer Success Manager Option abhängig von Umsatz <ul style="list-style-type: none"> Quartalsweise Business Reviews Monatliche CS Meetings 24x7 support, Telefon/Email/Chat Enterprise Skalierbarkeit <ul style="list-style-type: none"> 15 Replicas AMBA
Add-on Optionen	<ul style="list-style-type: none"> SecurID Hardware Authenticators SMS/Voice Credits G&L Cloud 	<ul style="list-style-type: none"> SecurID Hardware Authenticators SMS/Voice Credits G&L Cloud 	<ul style="list-style-type: none"> SecurID Hardware Authenticators SMS/Voice Credits G&L Cloud
	\$2 pro User pro Monat	\$4 pro User pro Monat	\$6 pro User pro Monat

OWN YOUR
IDENTITY.

Fragen?

OWN YOUR
IDENTITY.

RSA[®]