



Why RSA

RSA 인증 솔루션 소개



Long History for 50 years

Time Sync OTP
RSA SecurID

SW Token for Windows
SW Token for BlackBerry
SAML2.0

Approve Auth.
Apple Touch ID

The image displays ten authentication methods arranged in a 2x5 grid. Each method is represented by a square icon with a light gray background and a rounded corner. The icons are as follows:

- Push:** A smartphone icon with a checkmark and a thumbs-up gesture.
- Mobile OTP:** A smartphone icon with a hand entering a code.
- Biometrics:** A hand being scanned by a fingerprint sensor.
- Proximity:** A circular icon with a stylized 'd' and a signal wave.
- Wearable:** A smartwatch icon with signal waves.
- HW Token:** A physical security token icon.
- SW Token:** A software token icon with a key and a code.
- FIDO:** A USB security key icon.
- SMS:** A smartphone icon with an 'SMS' bubble.
- Voice Call:** A telephone handset icon with a speech bubble.

Risk Base Authentication for B2E
SW Token for iOS & Android
Credential: SanDisk, Broadcom,
Intel, IronKey, Upek
Enterprise Mobile Management:
VMware, BlackBerry

Identity
Assurance
Apple Face ID
Apple Watch

Windows Hello
Azure AD MFA

Unified Identity Platform

1977 - 2013

2014 - 2023

RSA SecurID
SW Token

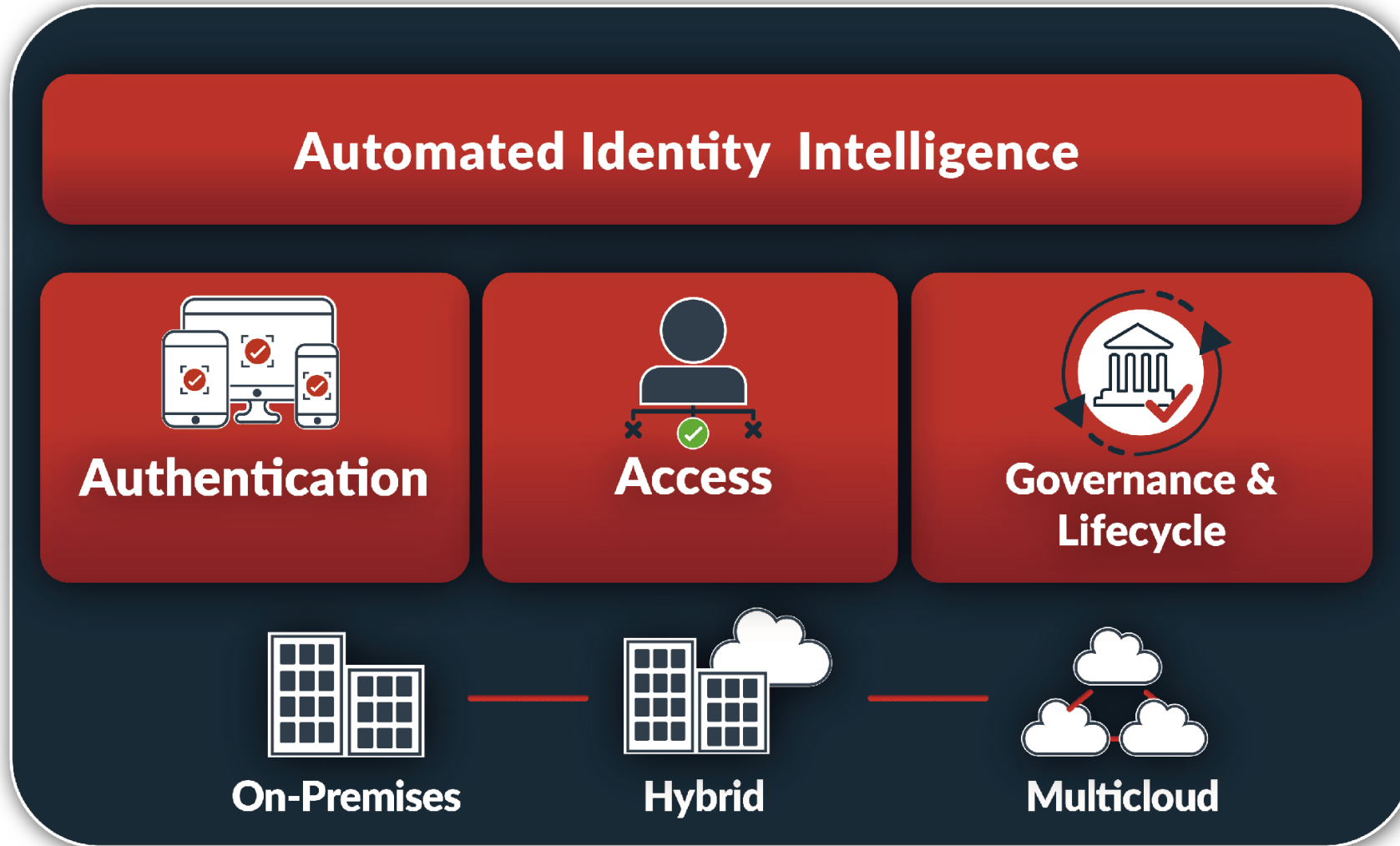
Transaction Signing
Adaptive Authentication
FraudAction
PIV/FIPS201

SMS Auth.
SW Token for Palm Pilot
SW Token for Windows Mobile

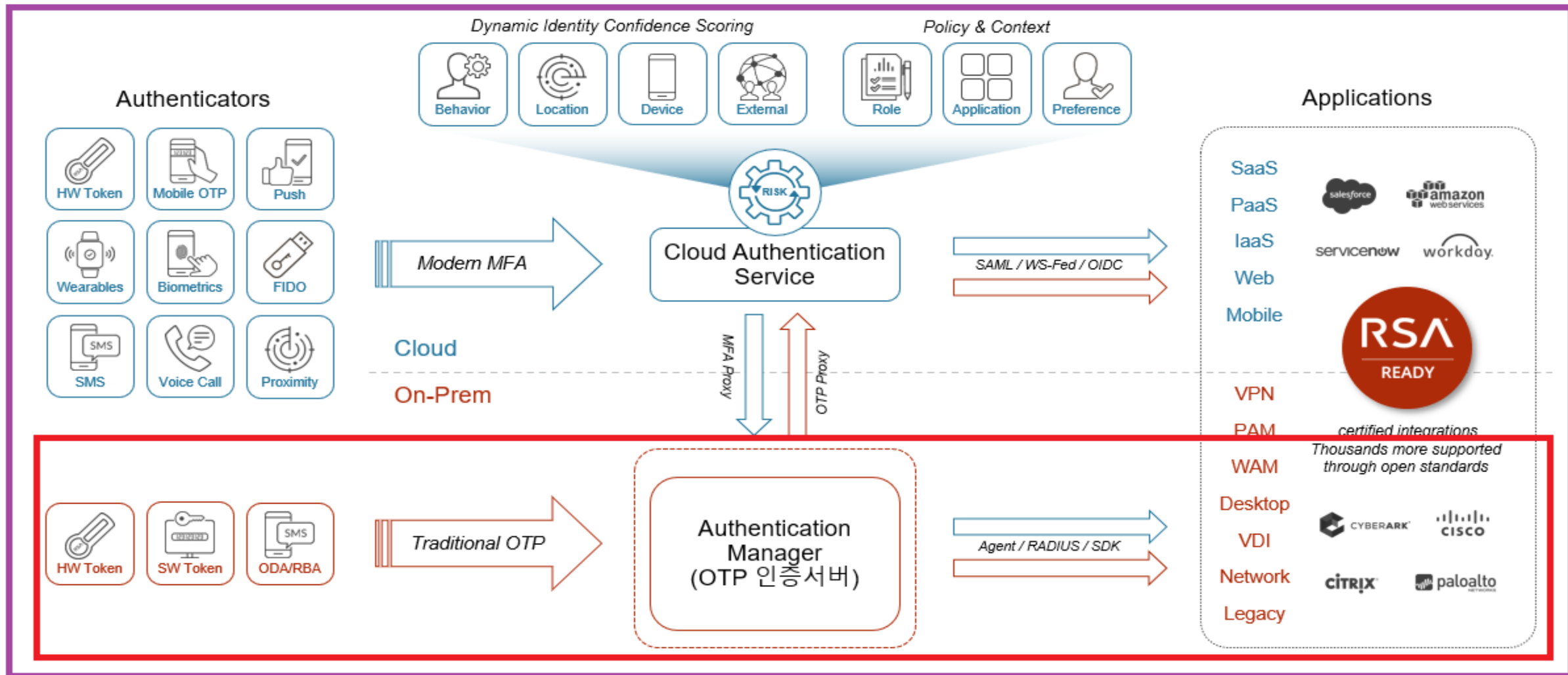
Proximity MFA for Windows
Samsung Fingerprint Auth.
FIDO U2F

Passwordless
 FIDO2
 Yubico

RSA Unified Identity Platform



OTP vs ID Plus 인증 범위



WHY RSA ID Plus

하이브리드 인증

단일 라이선스로 On-Prem,
Cloud, Hybrid 환경 지원

중단 없는 인증

온프레미스와 결합된
하이브리드 구성으로 파일오버
대책 마련, 업무 연속성 보장
오프라인, 비행기 모드에서도
인증

Passwordless

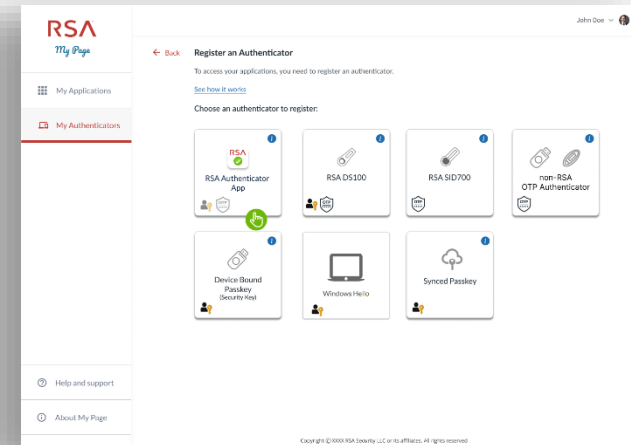
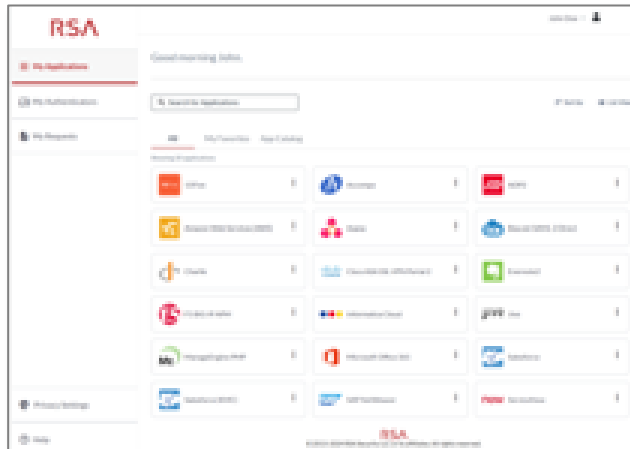
OTP, 생체인증, QR코드 등
다양한 인증 수단 지원
피싱 공격에 강하고 FIDO
인증을 받은 Passkey로
안전하고 비밀번호 없는
인증을 실현

연동 호환성

API, SAML, OpenID 등
다양한 방식으로 연동
다양한 응용 프로그램에
연결할 수 있는 연동 가이드
제공

보안 신뢰성

1977년 RSA Algorithm을
시작으로 한 50년 이상의
보안 전문회사
암호화 키를 타사에 맡기지
않는 기업용 암호 키



Single Sign-On

OFFICE

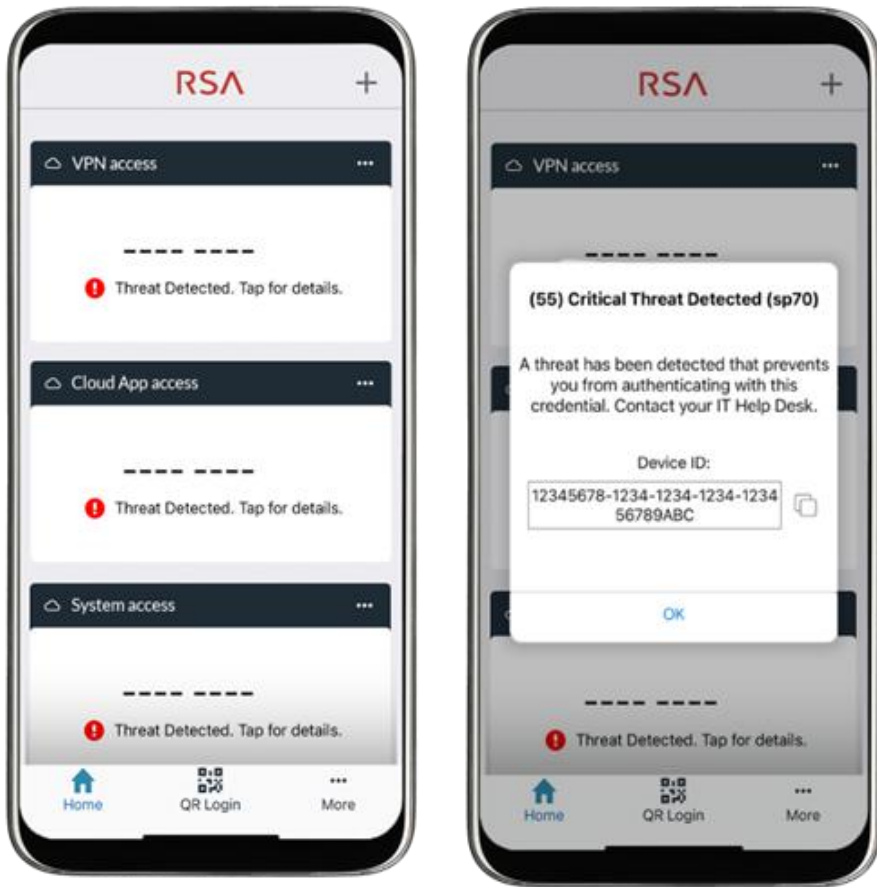
REMOTE

Self-Service

HYBRID

ID Plus_ MFA and More

1. MFA + Malware 방지



RSA Mobile Lock

BYOD 시대의 새로운 대안



- RSA 인증 앱 작동 시마다 사용자의 모바일 기기를 검색하여 위협을 자동 감지하고 위협이 감지된 경우 즉시 사용자와 IT 부서에 경고를 보내 조직의 시스템이나 데이터에 대한 액세스를 중지
- 사용자의 모바일 기기에는 RSA 인증 사용 기능만 일시 중단하여 기타 장치 기능 사용 기능은 유지함으로써 사용자의 불편을 최소화
- iOS 및 Android용 RSA 인증 앱과 통합되어 별도의 설치가 필요하지 않음

ID Plus_ MFA and More

2. MFA + 피싱 방지



RSA iShield Key 2 Series
powered by Swissbit



엣지 장착형 터치 센서

RSA iShield Key 2 Series

Passwordless 인증 방식 중 가장 강력한 인증

- Swissbit에서 제공하는 FIDO2 RSA iShield Key 2 시리즈를 RSA ID Plus와 통합함으로써 최고 수준의 보안 표준을 충족
- 피싱 방지 인증(M-22-09)에 대한 미국 연방 요구 사항을 충족
- FIPS 140-3(레벨 3) 검증된 암호화 모듈을 최초로 출시하여 산업 규제 요구사항 준수
- AAL3 호환(NIST SP800-63B에 따른 최고 수준의 인증)
- 100% 표준 기반: 클라이언트 소프트웨어 필요 없음
- 펌웨어 현장 업그레이드 가능: 교체나 재발급 없는 유연성 제공

ID Plus_ MFA and More

3. RSA+ MSFT Entra ID 사용자를 위한 제안 ID Plus M1

Microsoft Entra ID는 클라우드 환경을 지원하지만, 대부분의 고객은 여전히 레거시, 온프레미스 또는 하이브리드 인프라(예: 데이터 센터, AD, VPN)를 사용하고 있습니다.

RSA 제안:

RSA ID Plus는 Microsoft만으로는 불가능한 유연한 인증방법을 활용한 하이브리드 배포를 지원합니다.
기존 사용하는 **MSFT Entra ID** 를 그대로 사용하면서 **RSA**를 추가하여 온프레미스 사용자까지 함께 인증하는 하이브리드 인프라를 구축하세요.



RSA + Microsoft: 중요사항

Passwordless



모든 사용자를 위한 광범위한 옵션

휴대전화 접근이 제한된
사용자를 위한 FIDO2 인증기
제공



Microsoft를 넘어 Passwordless 확장

- Data center
- Mainframes
- Legacy applications
- macOS



Microsoft와 결합한 강력한 MFA 옵션

- AD-joined machines
- Window 10
- Windows Server
- RADIUS



규제 산업을 위한 최고의 규정 준수

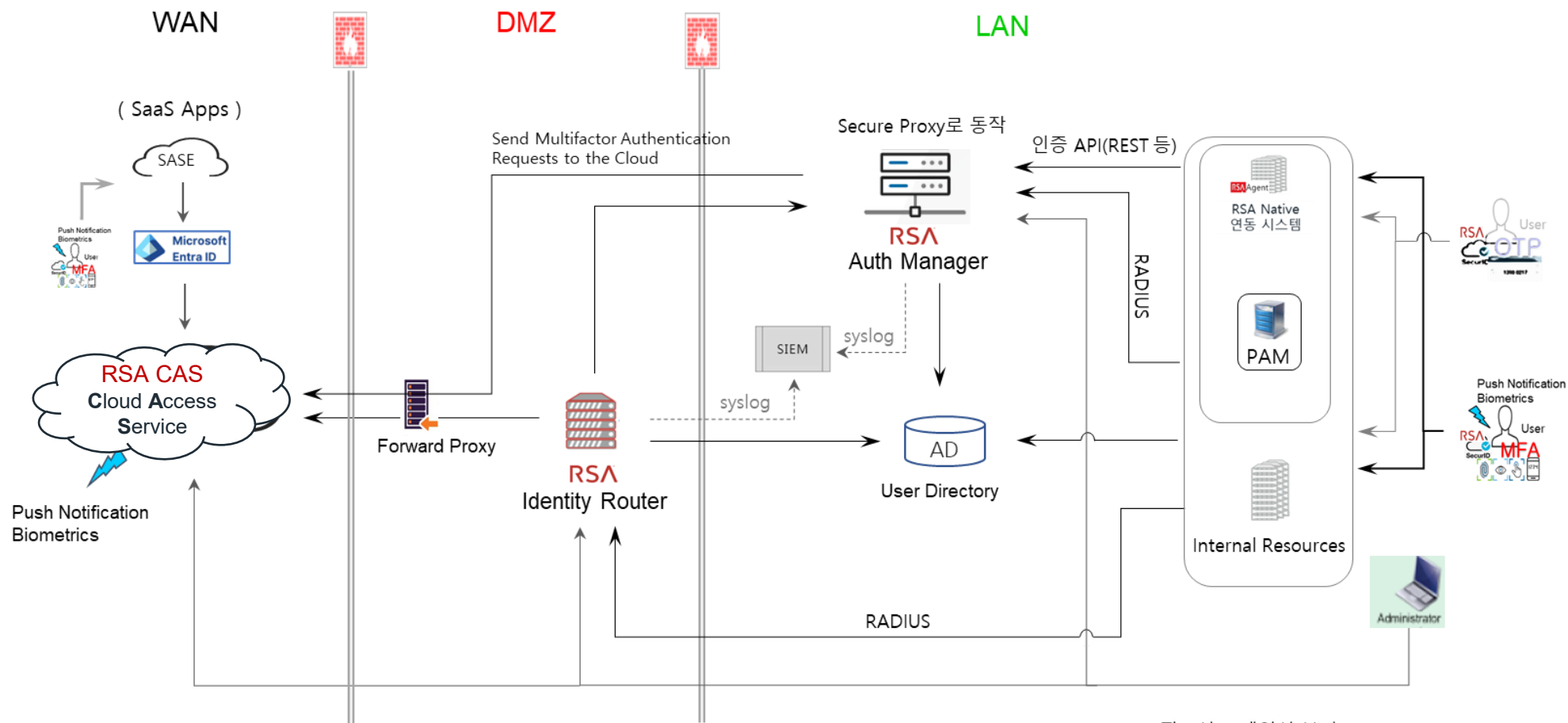
- Hybrid 복원력
- Dedicated security layers
- Data sovereignty
- Air-gapped networks

Why RSA – 특징점 정리

구분	RSA	경쟁사	확인 사항
유연성	단일 라이선스로 On-Prem, Cloud, On-Prem+ Cloud (Hybrid) 환경 지원	On-Prem, Cloud 환경을 별도 지원	- 현재 OTP/MFA 적용 범위가 어디인가요? - 각각의 환경에 별도의 OTP/MFA를 사용하고 있으신가요?
모바일 폰 사용불가 시 대안	모바일 폰 이외의 별도의 데스크탑 S/W토큰, H/W토큰, FIDO2 인증 등 추가 옵션 제공	스마트폰을 외의 인증 수단 제공이 제한적	모바일 폰 사용이 제한적인 사용자가 있나요? (예_서버실, 연구실 등)
Hybrid Failover 가용성	- 클라우드 및 사내 인증을 통합하여 중단 없는 인증 및 검증 기능을 보장할 수 있는 시장 유일의 하이브리드 인증 플랫폼 - Cloud의 예기치 않은 운영중단시 지속적인 보안 및 액세스를 보장	제공하지 못함	클라우드 운영 중단이나 on-prem 장애 발생시 Failover 대책이 마련되어 있습니까?
오프라인 인증	사용자가 인터넷/회사네트워크에 연결되지 않은 시간에도 동일한 인증 토큰으로 접속환경 제공	오프라인 지원 제한	인터넷 사용이 불가한 상황에서의 인증 대안이 있습니까? (예_비행기모드, 오프라인 환경)
모바일 폰 위험 감지, 인증 제한	사용자 모바일 폰의 중요한 위험을 탐지하고 위험 문제가 해결될 때까지 사용자의 인증 기능을 제한 함으로서 해킹 위험 방지 (Mobile Lock)	사용자의 모바일 폰 관리의 허점이 발견되는 경우 해킹 위험에 노출	개인의 모바일 폰을 사용하는 BYOD 상황에서 모바일 폰을 해킹하여 회사망에 침투하는 위험을 검토해 보셨나요?
연동 호환성	- 다양한 응용 프로그램에 연결할 수 있는 연동 가이드 제공 - API, SAML, OpenID 등 다양한 방식으로 연계 가능	연동가이드가 없는 경우 추가개발 필요	새로운 어플리케이션 도입 시 현재사용중인 OTP/MFA 과의 연동을 어떤 방식으로 진행하시나요?
신뢰성	1977년 RSA Algorithm 을 시작으로 한 보안 전문회사로 보안에 특화	2022,2023년 해킹에 노출되며 고객파일 노출	해외 사업장이 있는 경우 Global standard 인증이 필요하지 않을까요?

MFA 적용사례 - 보험사

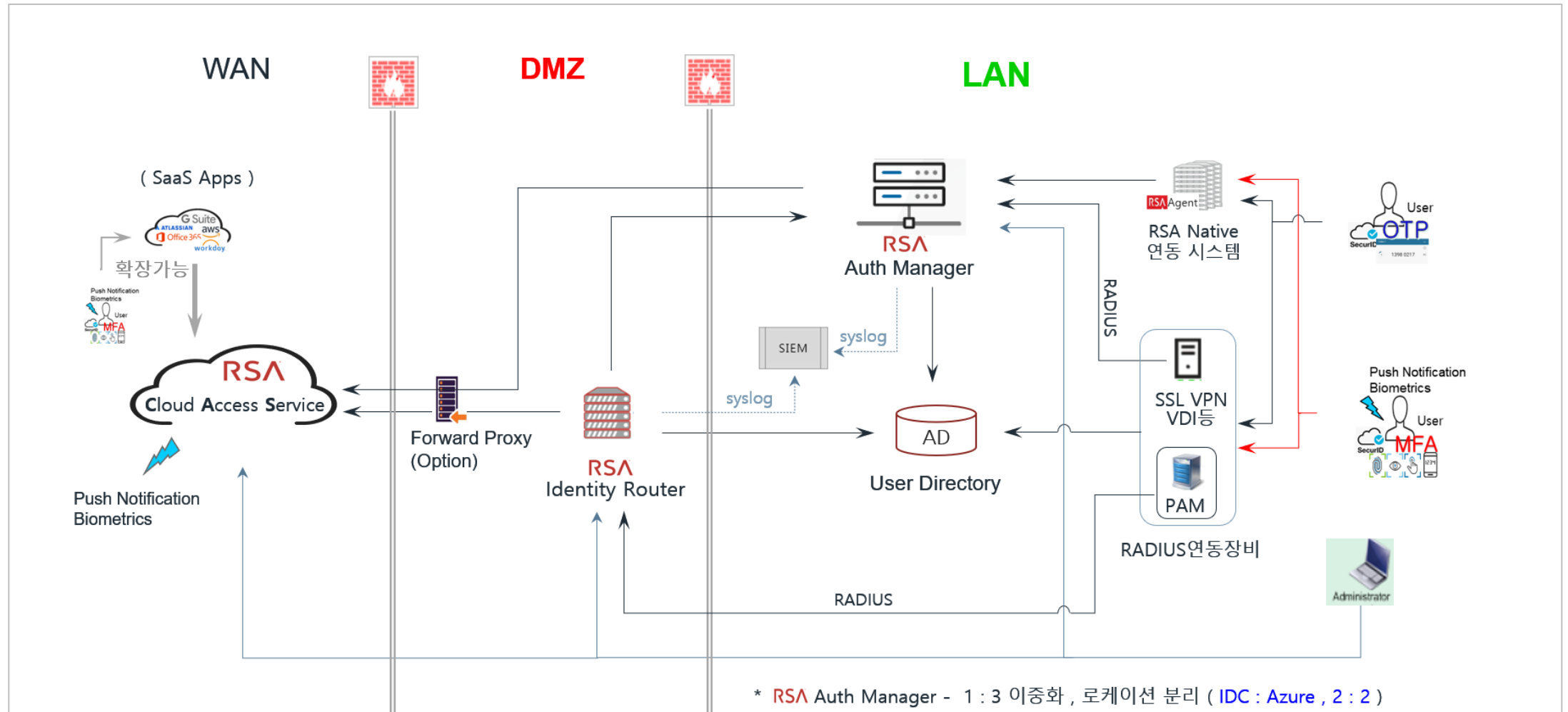
- Hybrid 구성 (On-Prem + Cloud) , ID Plus E1 License+ Option (SMS + Mobile Lock) since 2024
- PAM, SSL VPN, MS Entra ID, SASE 인증 등에 활용



- RSA Auth Manager - 1 : 1, Active : Active (필요시 로케이션 분리)
- RSA Identity Router - 1 : 1, Active : Active (필요시 로케이션 분리)
- Forward Proxy^(*) - 제안솔루션의 구성요소는 아니며 고객내 기 운영중인 시스템

MFA 적용사례- 온라인 쇼핑몰

- Hybrid (On-Prem + Cloud) , ID Plus E2 License+ SMS option since 2021



감사합니다