BROADCOM SOFTWARE

Symantec
A Division of Broadcom

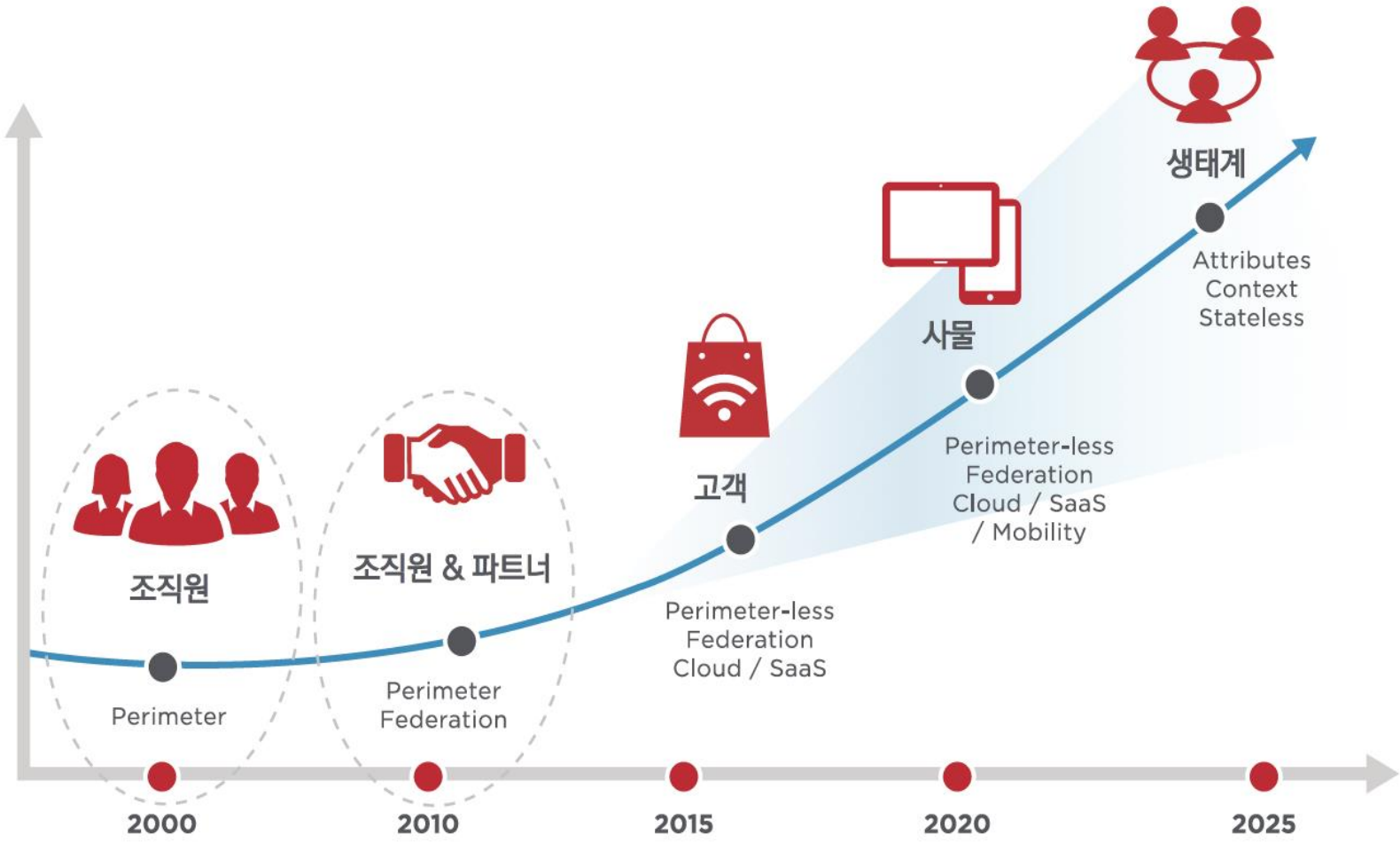
IAM 플랫폼의 미래

엔시큐어㈜, 박 정 만 이사 (park.jm@ensecure.co.kr)

Date: 2023.12.07

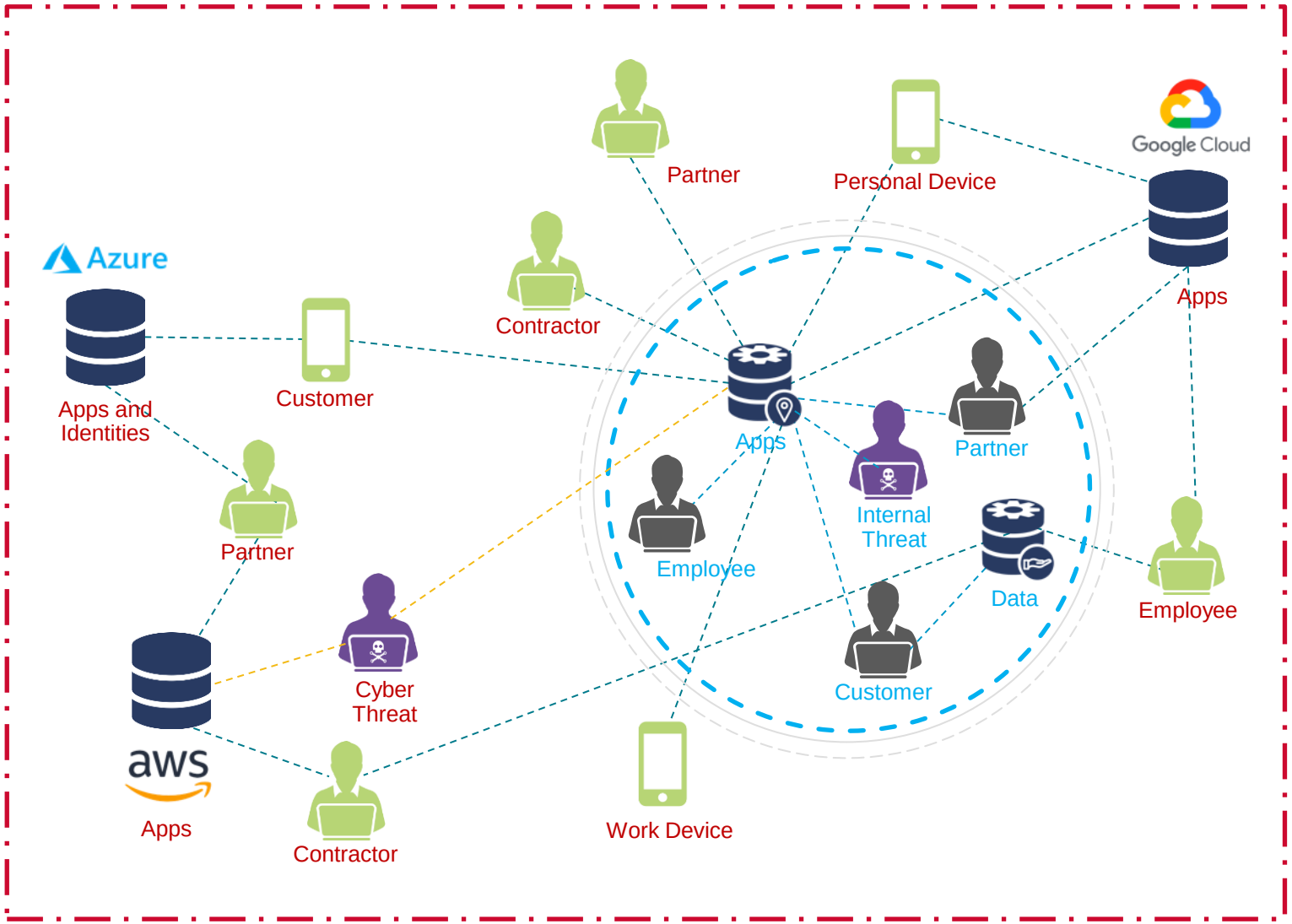
엔터프라이즈 컴퓨팅 환경의 진화

- 경계가 사라진 엔터프라이즈 컴퓨팅

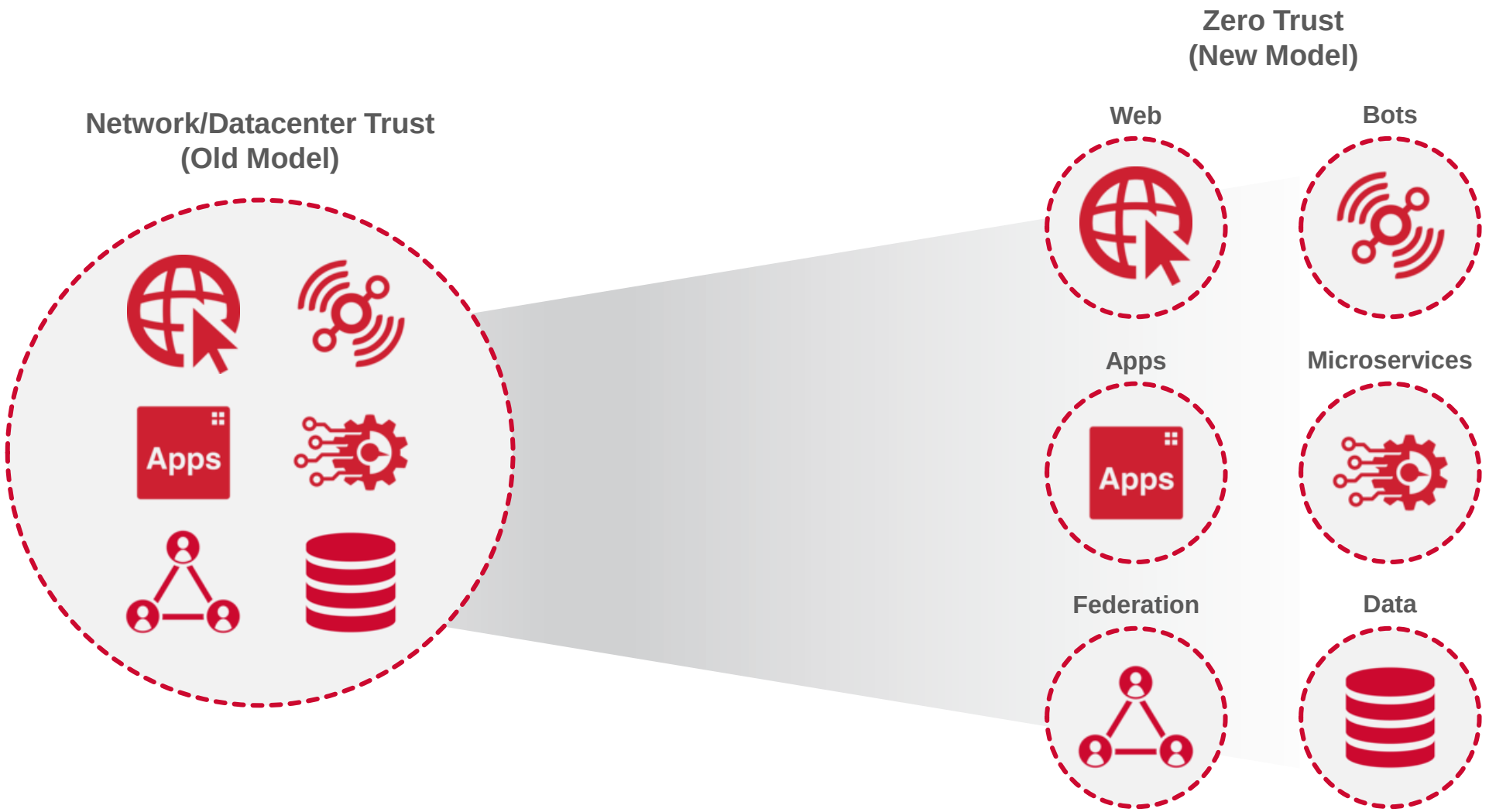


Identity Fabric 요구 증가의 기술적 요인 – 하이브리드 컴퓨팅 확산

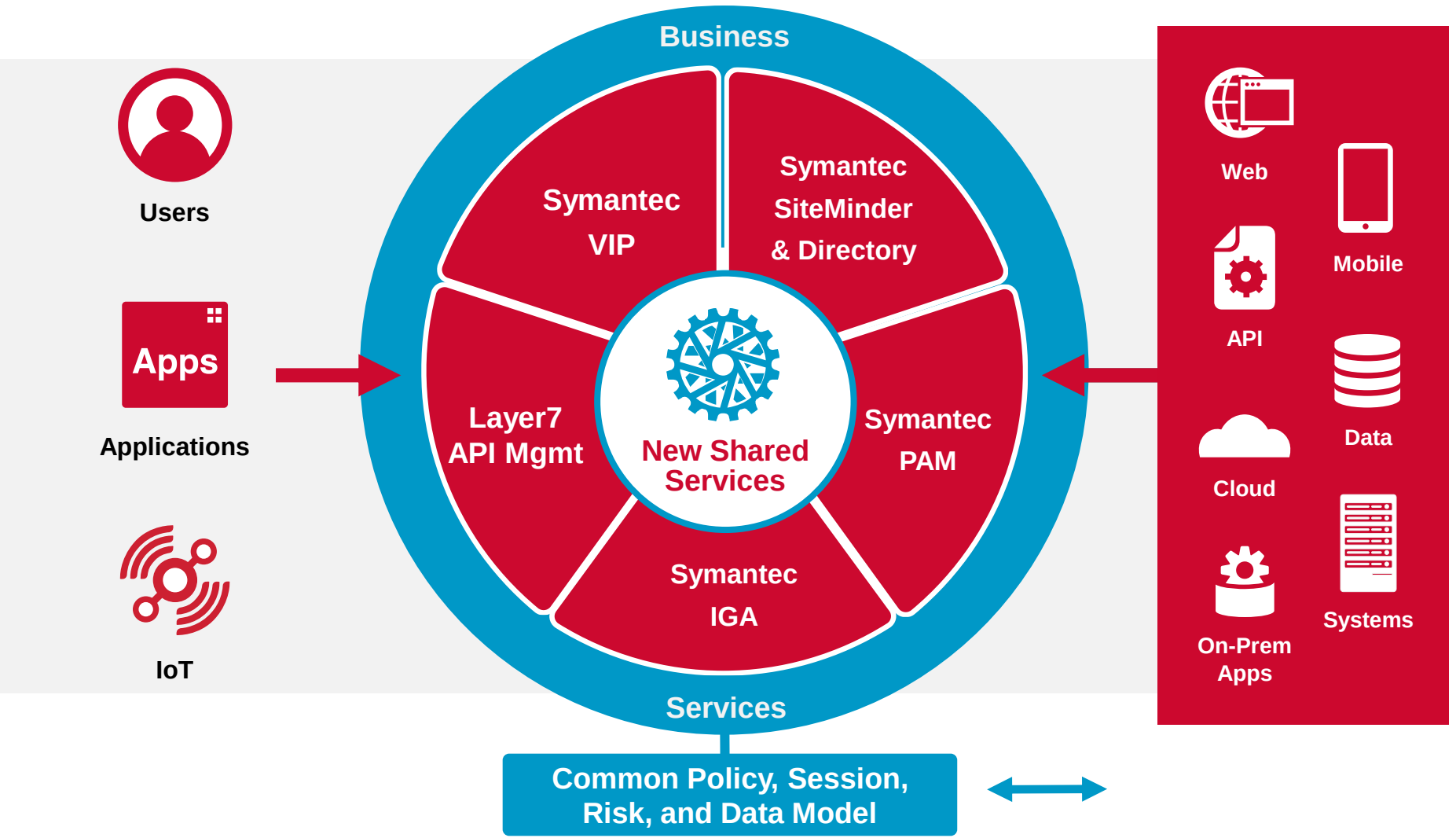
- IT 아키텍처는 **Hybrid**가 대세
  - 앱, Data 및 ID는 기존 기업 경계 밖에 있을 가능성이 많아지고 있음
- **상황**에 따른 액세스
  - 고객, 파트너, 직원 및 기타 사람들은 언제 어디서나 앱과 데이터에 액세스 해야 함
- Identity가 **핵심**
  - 클라우드 및 하이브리드를 채택하려면 신뢰의 토큰화를 기반으로 표준화된 통합 패턴 및 프로토콜이 필요함



Identity Fabric 요구 증가의 비즈니스적 요인 – 디지털 전환(DX) 가속



Identity Fabric의 개념 및 구성 요소



Security Services Platform

Cloud-native platform은 공유 보안 서비스 세트를 지원함

Business Services

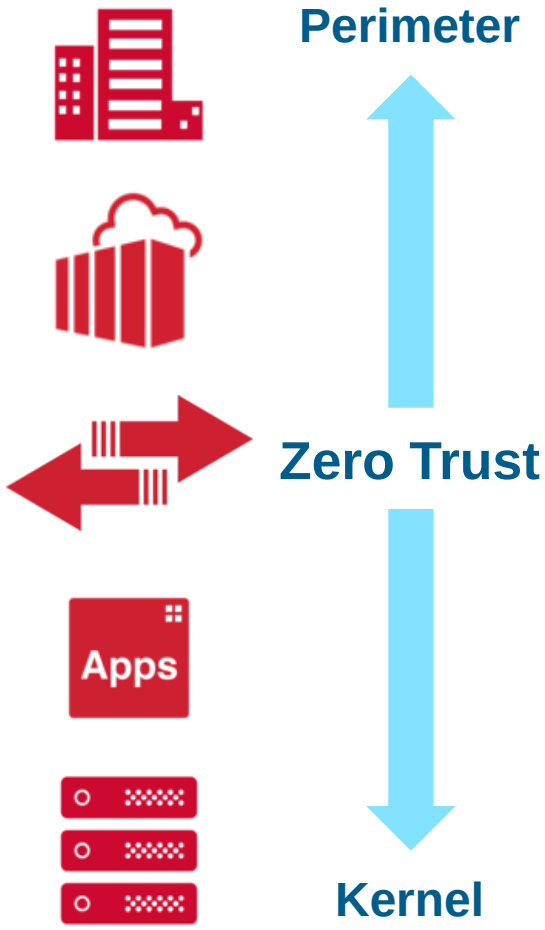
비즈니스 서비스 및 API로 노출되는 핵심 제품의 기능을 확장하여 쉽게 연결 할 수 있음

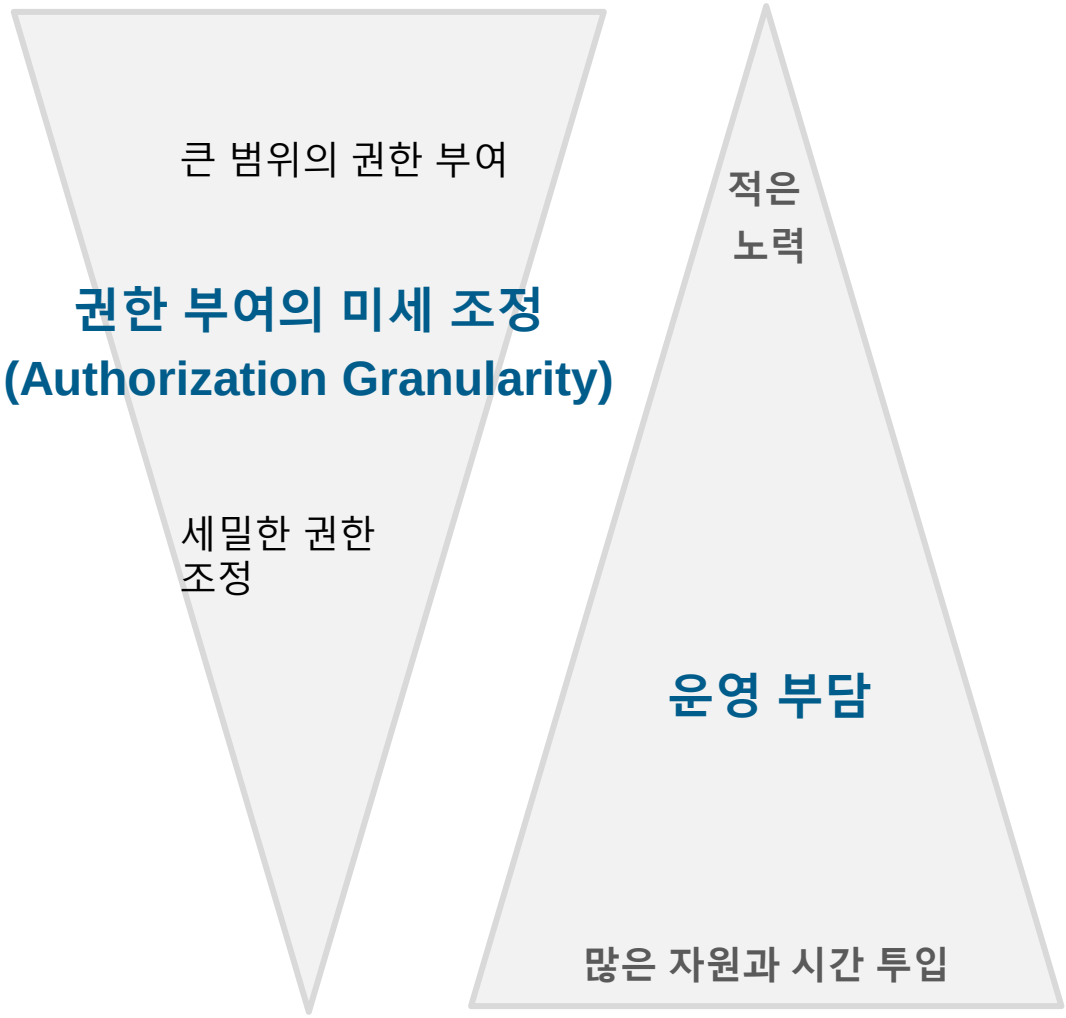
Global Intelligence Network

Security services platform은 Symantec GIN에서 풍부한 데이터를 가져와 real-time risk service를 지원함

미래의 IAM: Zero Trust와 ID 패브릭 간의 연결

- 접근 제어를 통한 데이터센터 보호
- 데이터센터를 온프레미스 환경과 프라이빗 클라우드로 분리
- 통신 및 API 채널 보호
- 앱과 데이터베이스 접근 제어 구현
- 보안을 개별 서버와 컨테이너까지 확장



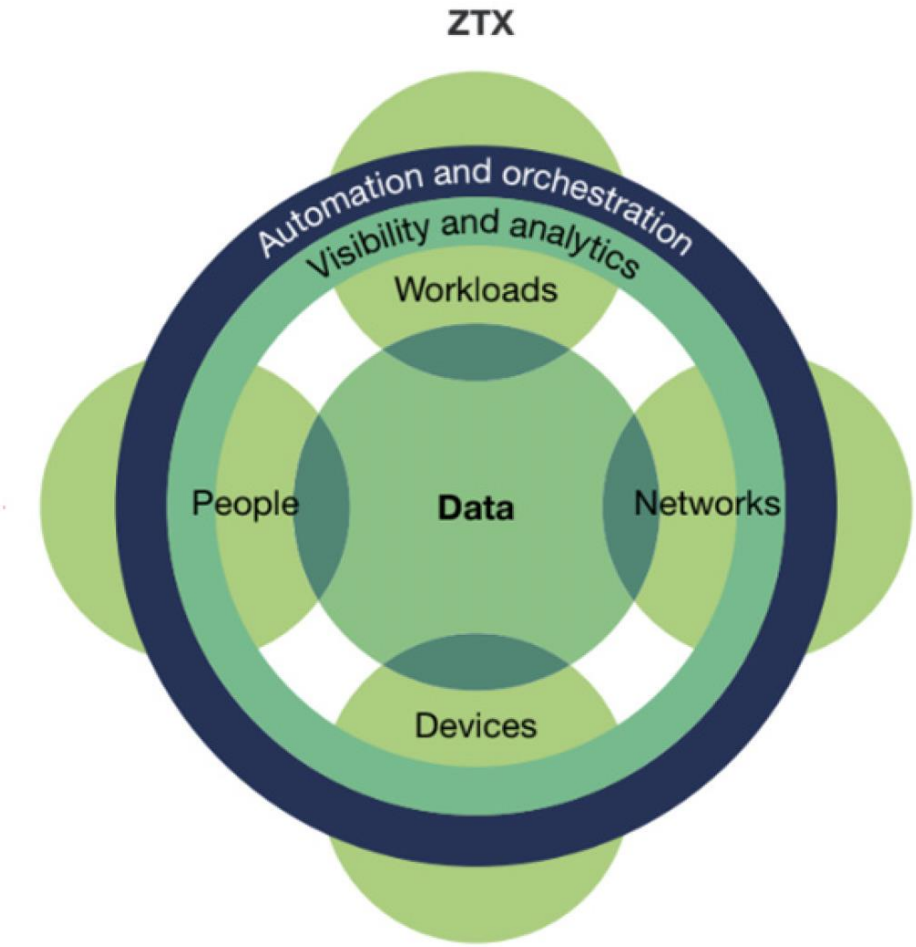


Symantec
A Division of Broadcom

BROADCOM
SOFTWARE

Zero Trust의 핵심 구성 요소

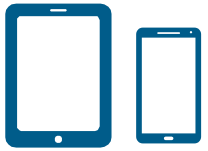
- 2009년 포레스터, 7가지 핵심 요소로 구성한 제로 트러스트 모델 소개
- 중심에는 보호 대상인 '데이터'가 위치
- 주변에는 데이터에 접근하려는 '사람', '디바이스', '워크로드'가 위치
- '네트워크'는사용자와 데이터를 연결
- '자동화와 오케스트레이션'은 데이터 보안 요소로 기능
- '가시성과 분석'은 데이터 접근을 모니터링하고 무단 접근을 차단



Zero Trust 원칙을 토대로 ID 패브릭 구현

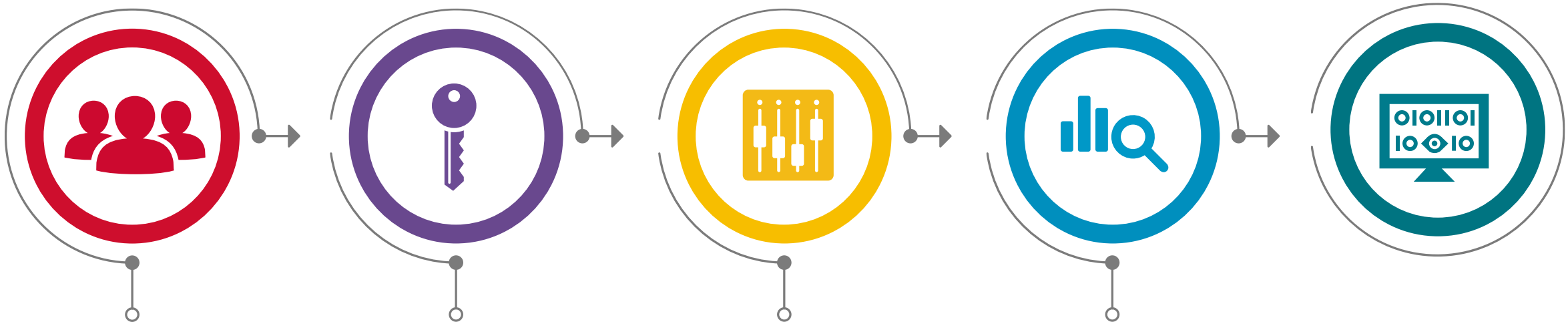
Any Identity

Any Device/Network



Any App

상황과 위험에 기반한 접근 관리



1 AUTHENTICATE
앱 및 데이터에 접근하는 사용자 인증 편의 제공

2 AUTHORIZE
위험도 및 데이터 민감도 기반 인증

3 AUTHORIZE
위험도 및 데이터 민감도 기반 인증을 지속해서 평가 및 조정

4 MONITOR
위험한 접근 패턴 인식 기반 모니터링

5 MANAGE
적절한 접근 수준을 보장하기 위한 권한 관리

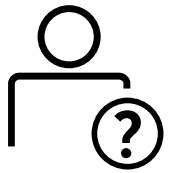
Symantec
A Division of Broadcom

BROADCOM
SOFTWARE

상황과 위험을 토대로 맥락을 파악한다는 것은?

사용자는 어디에 있습니까?

어떤 장치를 사용하고 있습니까?



사용자가 무엇을 하려고 합니까?

행동이 기존의 행동과 일치합니까?

LOCATION

- 위치가 본질적으로 의심스럽습니까?
- 그들은 전에 거기에 있었습니까?
- 그들은 최근 어디에 있었습니까?

DEVICE DNA

- 어떤 종류의 장치입니까?
- 그들은 전에 그것을 사용한 적이 있습니까?
- 마지막으로 사용한 이후로 변경되었습니까?

BEHAVIOR

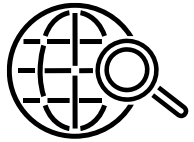
- 이것은 사용자의 일반적인 작업입니까?
- 행동이 본질적으로 위험합니까?
- 이전에 비슷한 조치를 취한 적이 있습니까?

HISTORY

- 지금이 그들에게 일상적인 시간인가요?
- 로그인 빈도가 비정상입니까?
- 현재 조치가 이전 조치와 일치합니까?

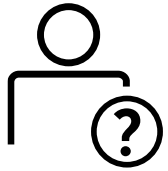
상황과 위험을 고려한 위험도 및 데이터 민감도 기반 인증을 한다는 것은?

Contextual Authentication



사용자는 어디에 있습니까 ?

어떤 장치를 사용하고 있습니까 ?



사용자는 무엇을 하려고 합니까 ?

이전에 하던 행동과 패턴이 일치합니까 ?

상황에 따른 인증

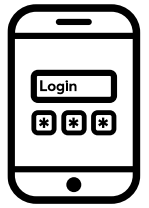
+

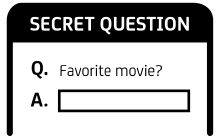
다양한 인증

Versatile Authentication

AUTH ID

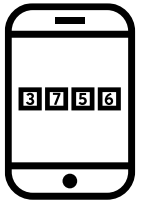
MOBILE OTP





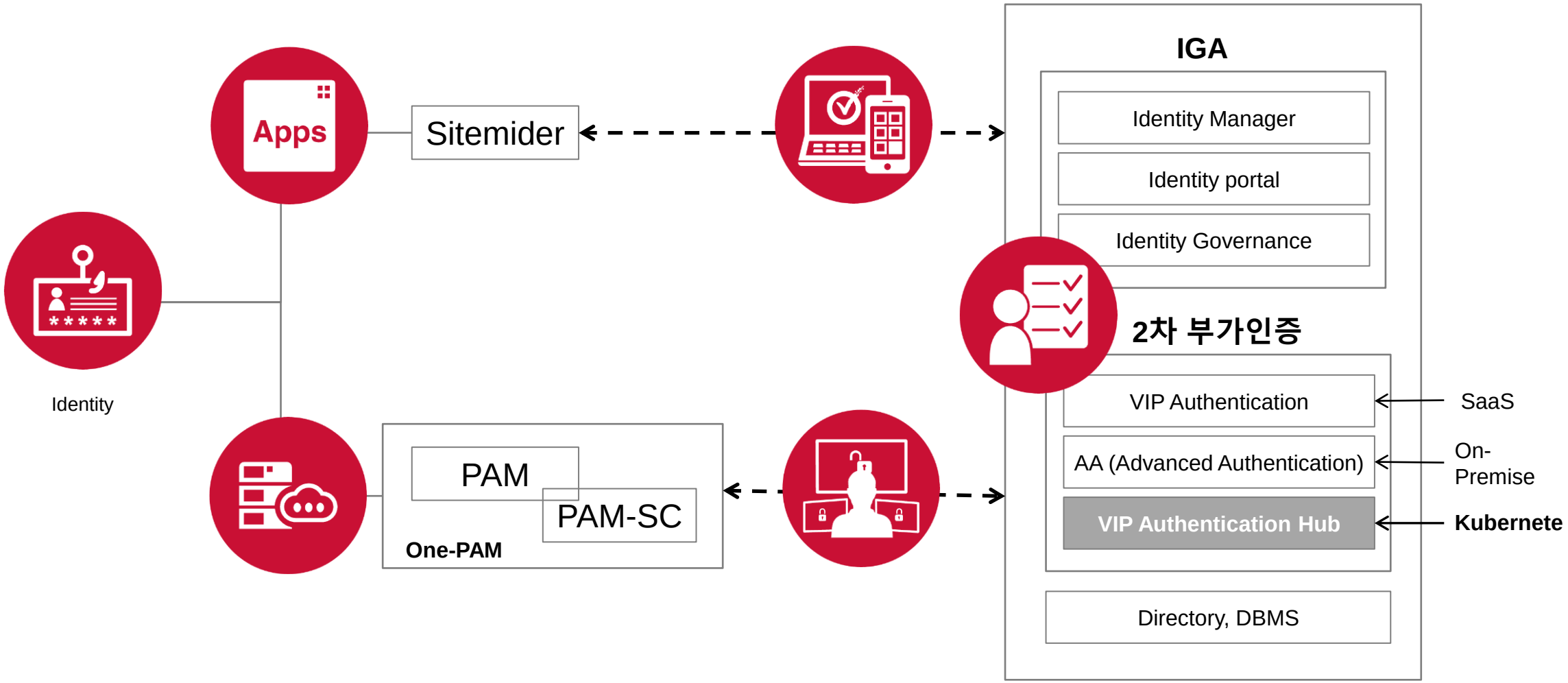
Q&A

OATH TOKENS

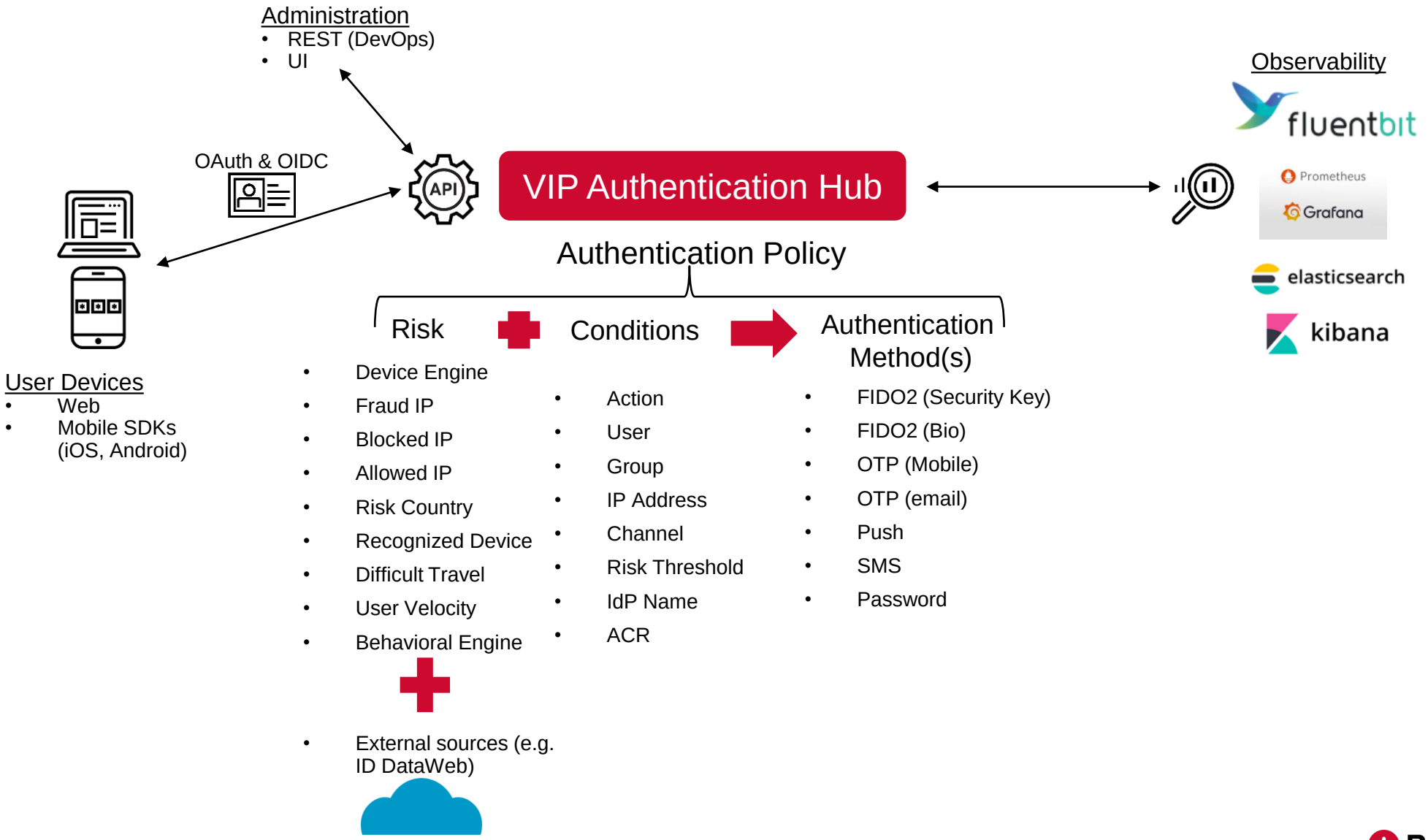


OTP OUT OF BAND

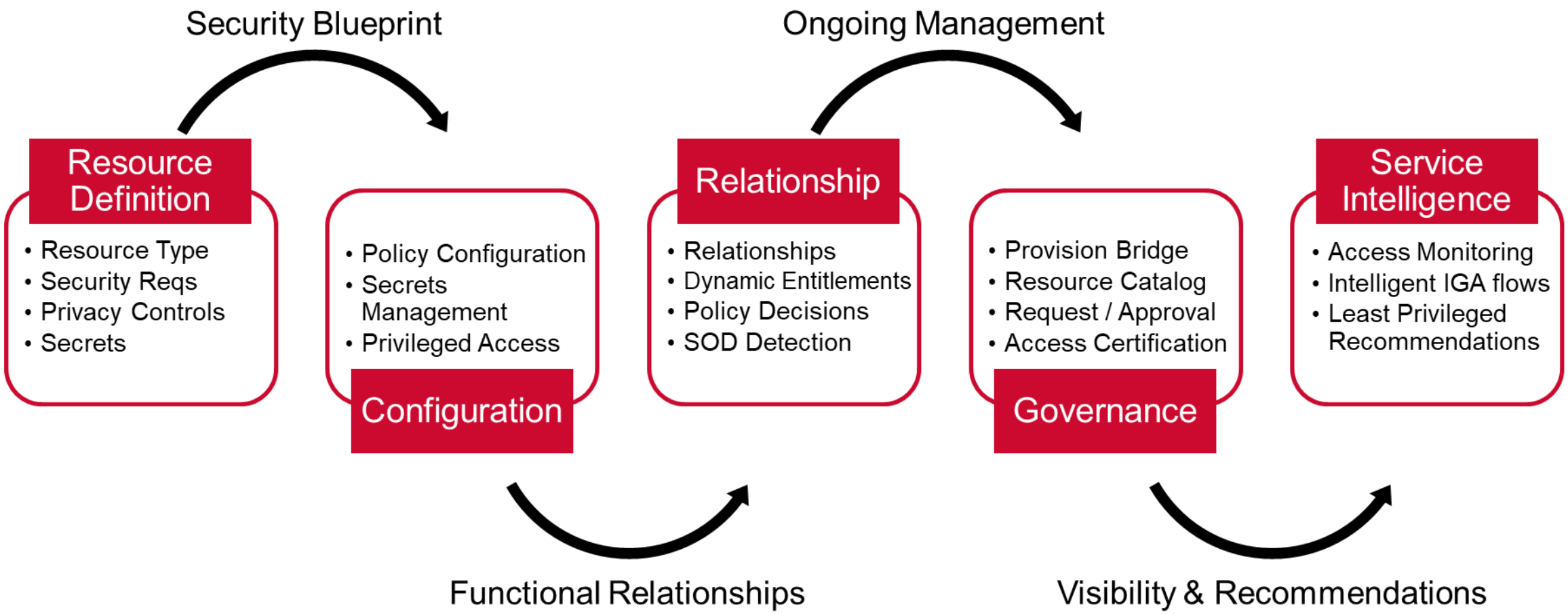
Use Case: Zero Trust 원칙을 토대로 사용자와 장치를 보호하는 ID 패브릭 예



차세대 ID 패브릭의 구심점 VIP Authentication Hub



Use Case: DevOps 파이프라인에 ID 패브릭 적용



Summary: Zero Trust를 향한 ID 패브릭의 진화 방향

1 **Risk-based authentication**
FIDO2 호환 자격증명, 모바일 OTP/푸시, SMS를 포함한 다양한 요소에 대한 지원을 갖춘 위험 기반 인증

2 **Native integration**
SiteMinder, PAM, IGA 및 메인프레임과의 네이티브 통합

3 **API-driven,**
API 기반으로 최종 사용자 경험을 완전히 제어하고 사용자 정의할 수 있음

4 **Intelligence Engine**
위협 인텔리전스 엔진은 위험 분석을 수행하며 외부 위험 서비스에 연결될 수 있음

5 **Standards support**
OIDC, SAML, OAuth를 포함한 표준 지원은 제3자 서비스와의 통합을 단순화함

6 **Cloud-native architecture**
클라우드 네이티브 아키텍처는 몇 분 안에 배포되며, 필요에 따라 확장되고 제로 다운타임으로 업데이트됨

7 **DevOps and Operations friendly**
DevOps 및 운영 친화적인 K8S, Helm 차트, Kafka, Grafana 등


BROADCOM®
SOFTWARE