





IoT 를 위한 Azure Sphere 활용

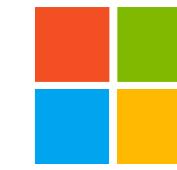
- 윤기석 부장
- 마이크로소프트
- kiyun@microsoft.com





CLOUDMATE
Azure Expert Group

CLOUDZEN

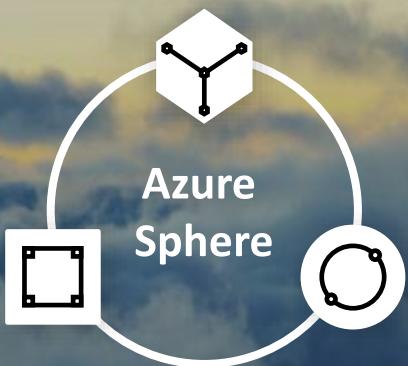


Microsoft

Global Azure Virtual 2020 는 클라우드메이트, 클라우드Zen, 마이크로소프트의 후원을 받아 진행되고 있습니다.

Microsoft's intelligent edge offering

Azure Sphere



Cloud Security
Secured MCU
Secured OS

Azure IoT Edge



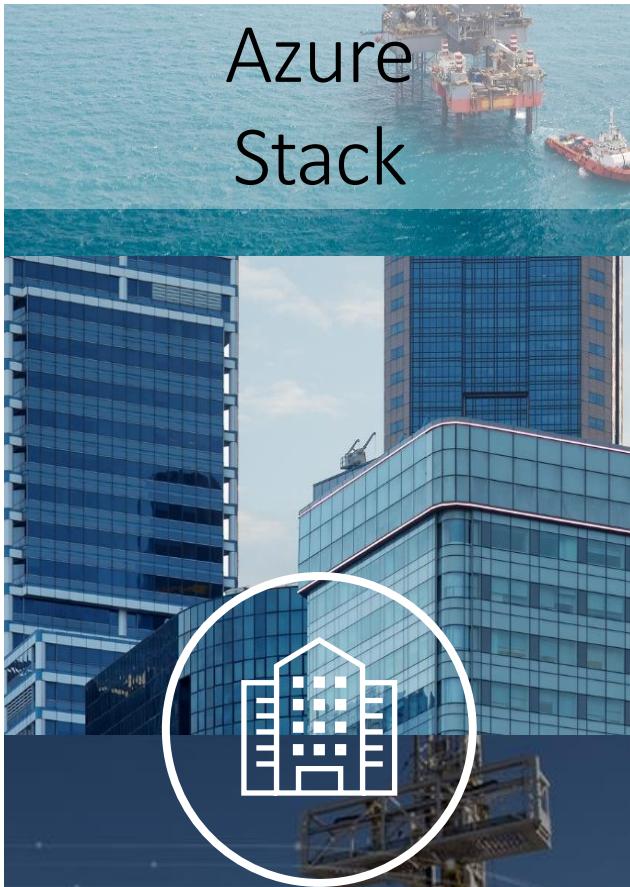
Open Source
Azure IoT Edge Runtime
Windows SDK and Commercial
Drone Solutions

Windows IoT



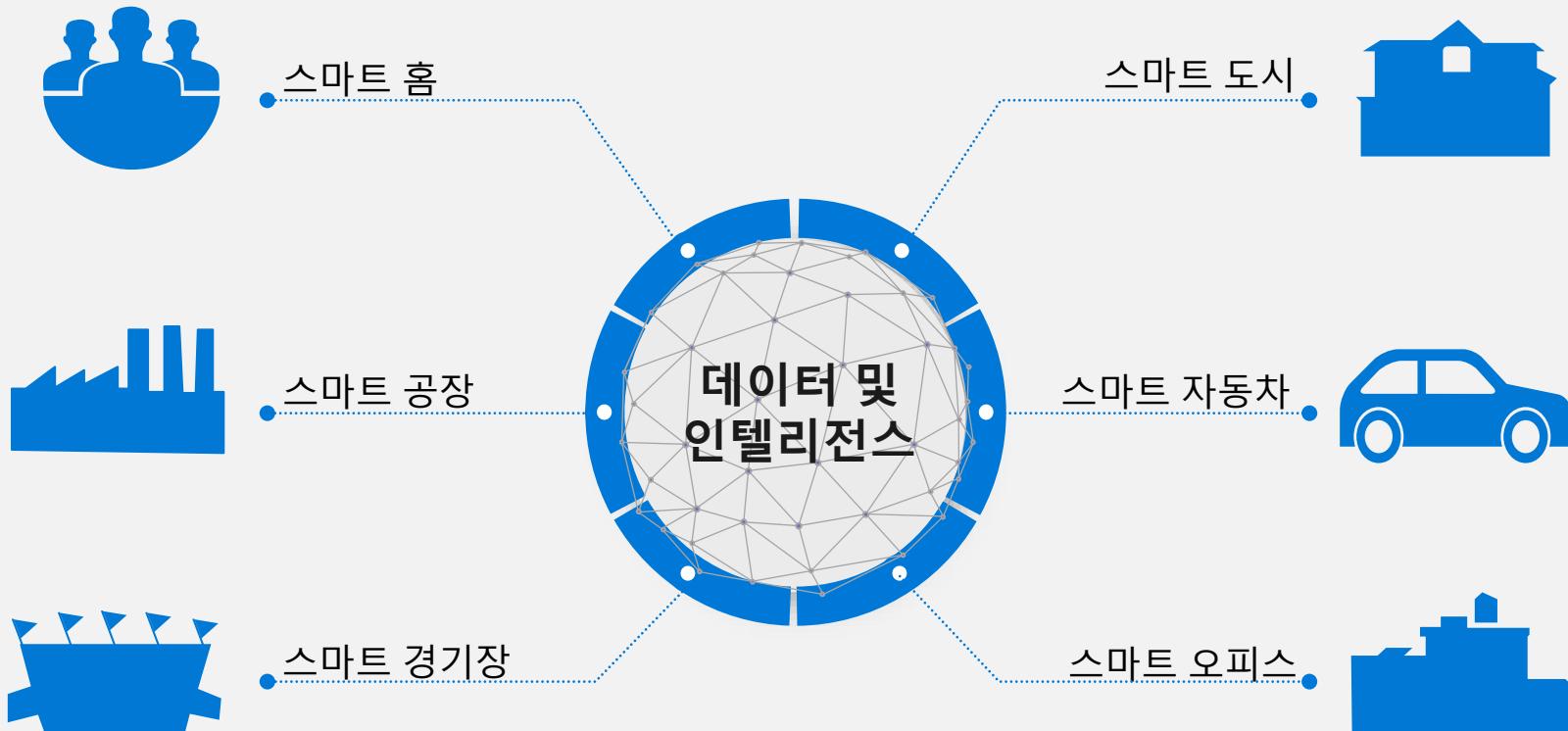
Intelligent security
Faster time to market
Smarter devices

Azure Stack



On-premises,
cloud consistent

IoT를 활용한 디지털 혁신 추진



"2020년 말까지 연결된 디바이스 수는 200억 개까지
늘어날 전망"

Gartner

416억 개

2025년까지 생성될 것으로 전망되는 연결된 "사물"의 용량(데이터 79ZB 생성)

미화 1,300억 달러

IoT 관련 디바이스로 인해 창출될 것으로 전망되는 신규 수익원

80%

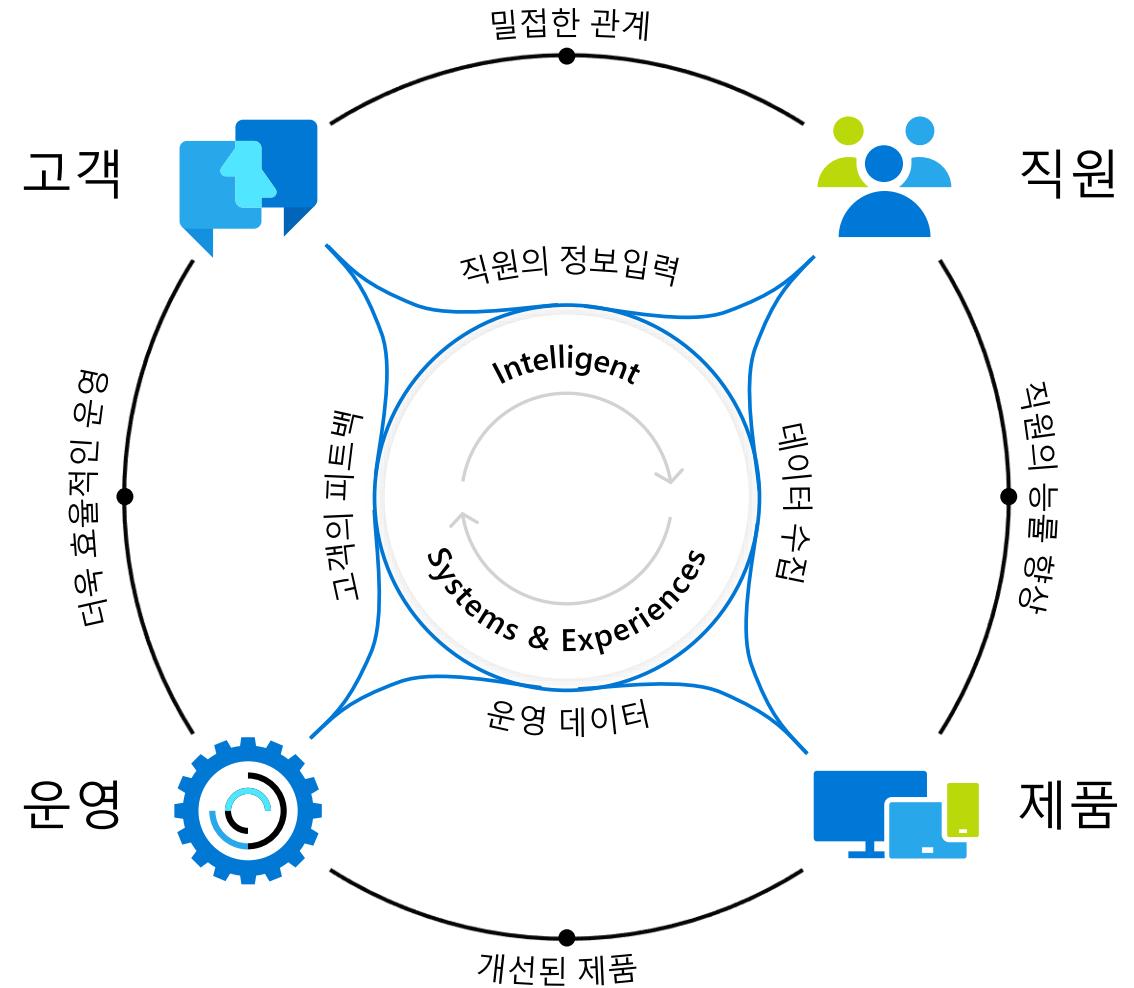
IoT 구현의 결과로 매출이 증가한 업체의 비율

미화 1억 달러

디지털 혁신 추진율이 가장 높은 기업의 평균 운영 수입 증가액(평균 8%)

디지털 피드백 순환(Digital Feedback Loop)

- ① 데이터: 모든 비즈니스에 걸쳐 디지털화된 신호를 수집
- ② 통찰력: 데이터의 연결과 분석
- ③ 실행: 업무의 개선과 결과물 도출





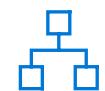
비용 감소



고객 만족도 개선



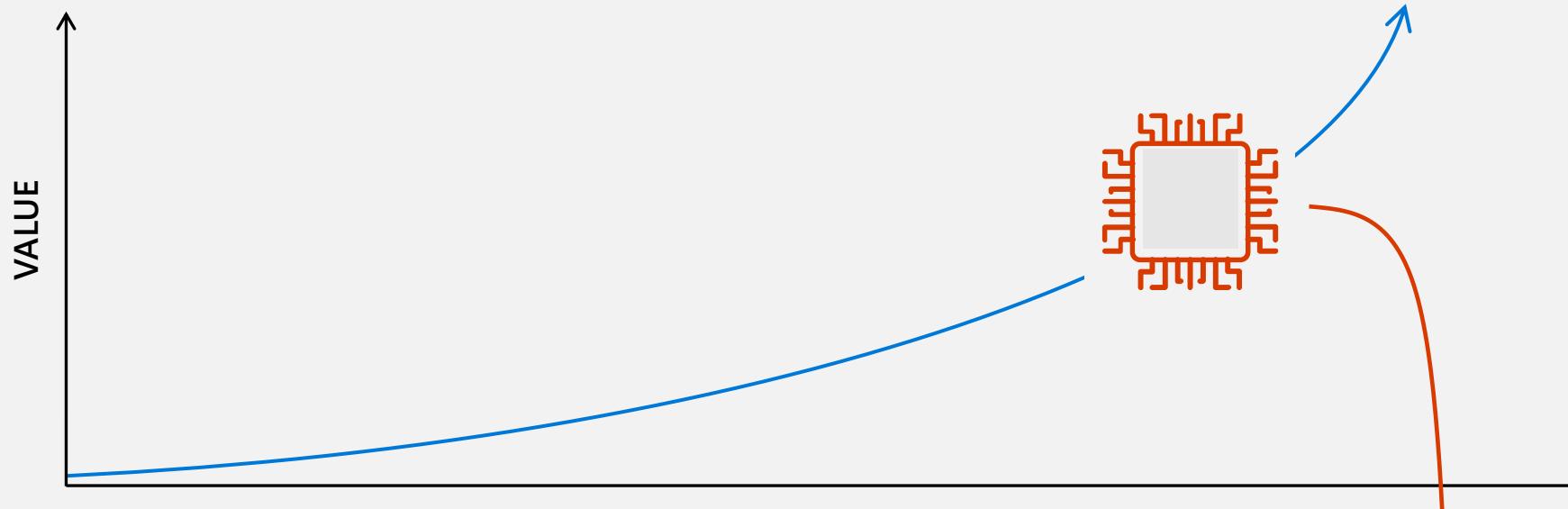
원활한 운영



신규 비즈니스 모델 작성



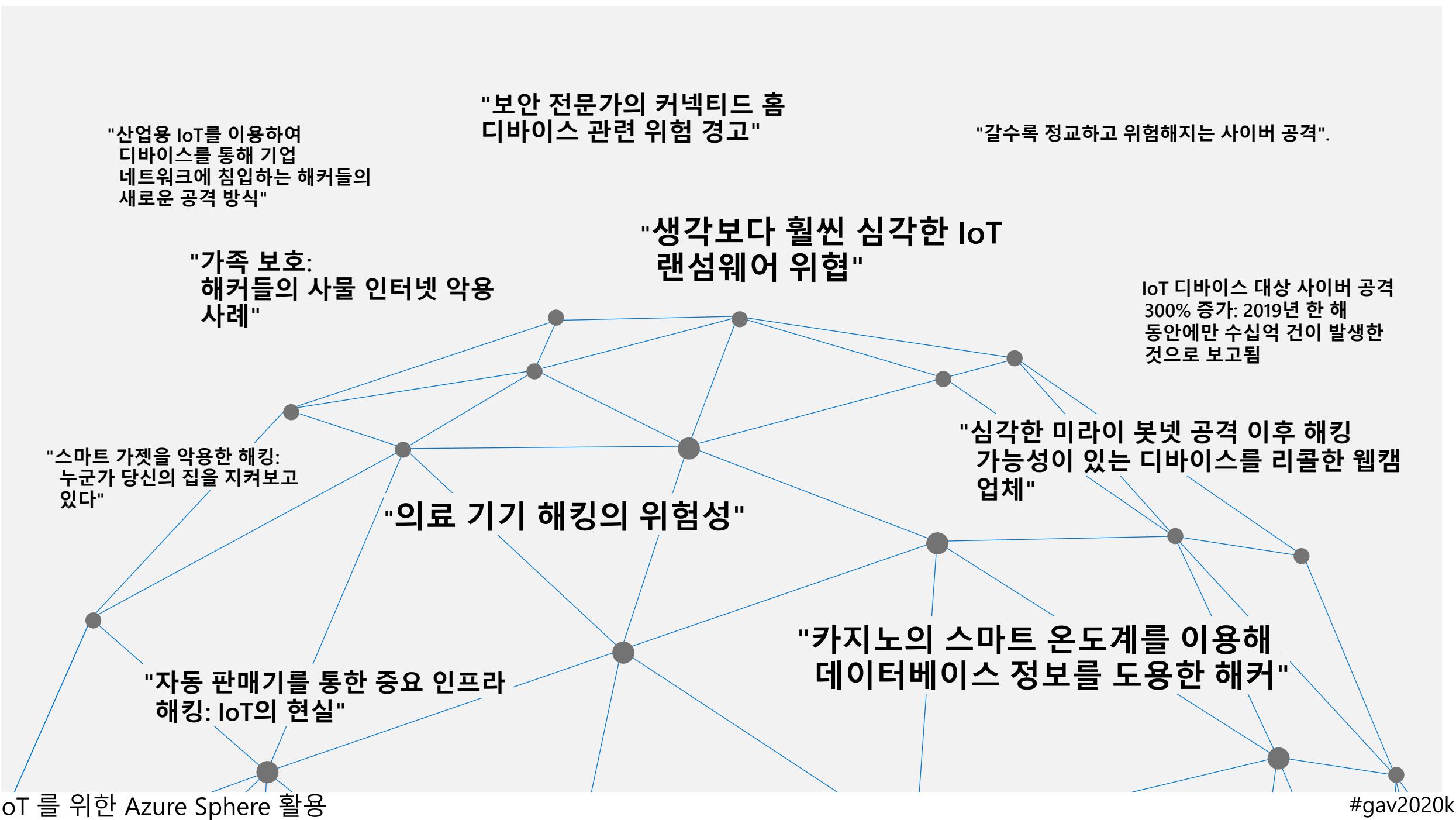
IoT 배포 계획



PoC 단계
가치 상승

프로덕션 배포
실제 비즈니스 가치 제공

반복
디지털 피드백 루프를 통해 더욱
빠르게 가치 창출



인터넷 보안 유지를 위한 노력.





정부 차원의 조치

USA

주 정부 법안 통과(캘리포니아, 오리건, 뉴욕, 일리노이, 메릴랜드)
의회에 여러 법안 제출
NIST의 규정에 따라 보안과 관련한 여러 기준을 정의해야 함

유럽/영국

EU 사이버 보안법에 따른 보안 인증
영국 행동 규범에서 ETSI 표준 제시
영국 내에서 다양한 소비자 레이블 테스트

APAC

싱가포르의 보안 지침 정의
일본의 소비자 기기 해킹 위험성 홍보 캠페인

디바이스 수준 공격 표면

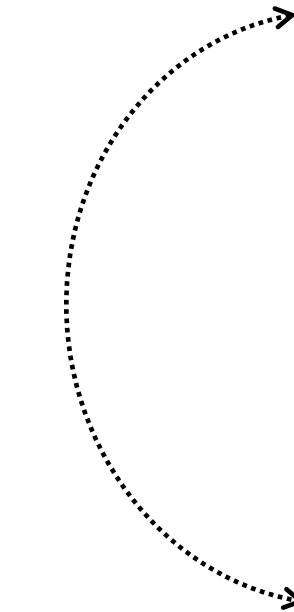
애플리케이션

네트워크 통신

네트워크 스택

OS/플랫폼

하드웨어





디바이스 작동을 중지시키거나 잠그고 금전 요구

완화 전략 및 기능:

심층 방어 | 스토리지 액세스를 제어하는 여러
방어 계층

구획화 | OS의 여러 측면에 대한 액세스 제한

차단 하드웨어 | 칩에서 통신 흐름을 제어하는
MMU 등

OTA(무선) 업데이트 | 디바이스의 보안을 간접하여
공격 성공 기회 제한

모범 사례: 모든 기능이 연동되어 있으며 포괄적으로 함께
갱신되는 수직 통합 시스템





디바이스를 악의적 용도에 사용

완화 전략 및 기능:

사설/공개 키 쌍 (신뢰할 수 있는 암호 및 프로토콜 포함)
| 신뢰할 수 있는 통신 보장

보안 부팅 | 디바이스가 최신 상태의 정품 소프트웨어만 실행하도록 설정

앱 컨테이너 및 권한 제한 | 물리적 제어권 액세스
권한 제한

스택 카나리 | 디바이스의 보안을 갱신하여 공격 성공
기회 제한

OS 기반 앱 매니페스트 | 적절한 작업 정의/앱 동작
제어





데이터 및 비즈니스 인사이트 손상

완화 전략 및 기능:

위조 불가능한 고유 ID | 실리콘에 포함

상호 인증 | 서버와 클라이언트의 인증 보장.

증명 | 신뢰할 수 있는 소프트웨어를 실행하는 정품 디바이스만 서비스에 연결 가능하도록 설정

서명/암호화된 통신 | 전송 중인 데이터와 패킷의 손상 방지

모범 사례: 프라이빗 키가 보안 환경의 디바이스를 통해 생성된 다음 HW 신뢰 루트를 통해서만 액세스할 수 있는 키 자격 증명 모음에 저장됩니다.



보안 수준이 높은 디바이스의 7가지 속성

디바이스의 보안 수준이 높습니까, 아니면 일반적인 보안 기능만 포함되어 있습니까?



하드웨어 신뢰 루트

디바이스의 ID 및
소프트웨어 무결성이
하드웨어를 통해
보호됩니까?



심층 방어

보안 메커니즘이
손상되어도 디바이스의
보호 상태는 유지됩니까?



신뢰할 수 있는 소규모 컴퓨팅 기반

디바이스의 보안 적용
코드가 애플리케이션 코드의
버그로부터 보호됩니까?



동적 구획

배포 후에 디바이스의
보안을 개선할 수
있습니까?



인증서 기반 인증

디바이스가 인증서를
사용해 자체적으로
인증을 합니까?



오류 보고

현장에서 파악할 수
있도록 디바이스가
오류를 보고합니까?



갱신 가능 보안

디바이스
소프트웨어가
자동으로
업데이트됩니까?

<https://aka.ms/7properties>

까다롭고 비용이 많이 드는 7가지 속성 통합 작업

포괄적인 솔루션 설계 및 빌드



취약한 링크가 있으면
전체적인 보안 수준은 낮아집니다.
보안 격차가 없는 전체 솔루션에 개별
보안 구성 요소를
통합해야 합니다.

기술

새롭게 등장하는 위협 인식 및 완화



위협은 지속적으로 발전합니다.
새롭게 등장하는 위협을 완화하는데
필요한 업데이트를 파악하고 작성할
수 있는 보안 전문 지식을 상시
보유하고 있어야 합니다.

TALENT

전 세계적으로 업데이트 배포 및 적용

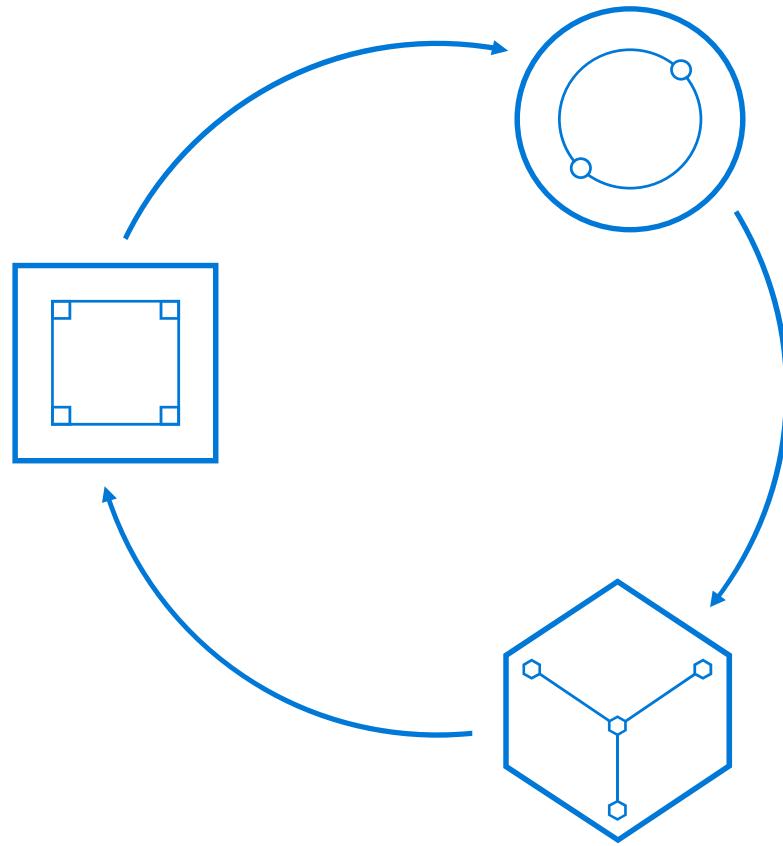


업데이트 효율성을 높여야 합니다.
몇 시간 이내에 전 세계의 전체
디바이스 집합에 업데이트를
제공/배포할 수 있는 효율적인
인프라, 물류 및 운영 체계가 있어야
합니다.

전술

Azure Sphere 는 MCU 디바이스를 보호하기 위한 end-to-end 보안 솔루션입니다.

Azure Sphere 인증 MCUs, 반도체
파트너, 마이크로소프트에서 만든
하드웨어 신뢰의 바탕.

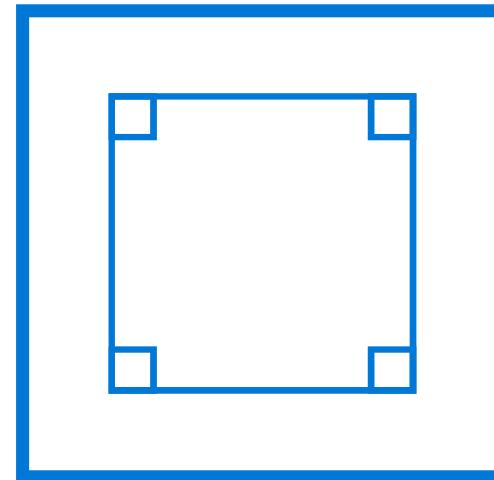


Azure Sphere 운영체제, 지속적인
업데이트를 통한 마이크로소프트 보안의
소프트웨어 플랫폼.

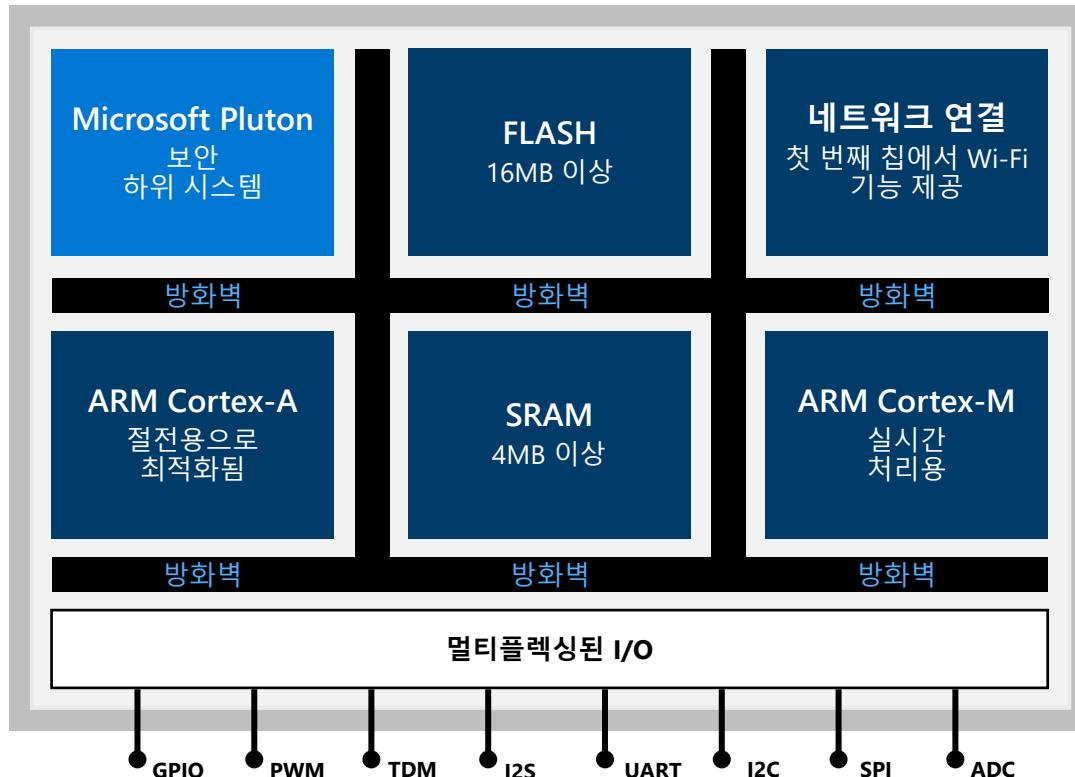
Azure Sphere 보안서비스, 모든 Azure
Sphere 장치를 보호.
신뢰, 대규모 위협 감지, 그리고 장치 보안
갱신의 증개역할

10년 이상 개선되어 온 보안 및 OS 업데이트가 Microsoft에서 각 디바이스에 직접 제공됨

Azure Sphere 인증 칩
내장된 hardware root of trust
3세대에 걸친 Xbox 콘솔의 보안 경험을 바탕



커넥티드 방식의 지능형 에지 디바이스용 보안 신뢰 루트를 생성하는 Azure Sphere 인증 SoC



연결

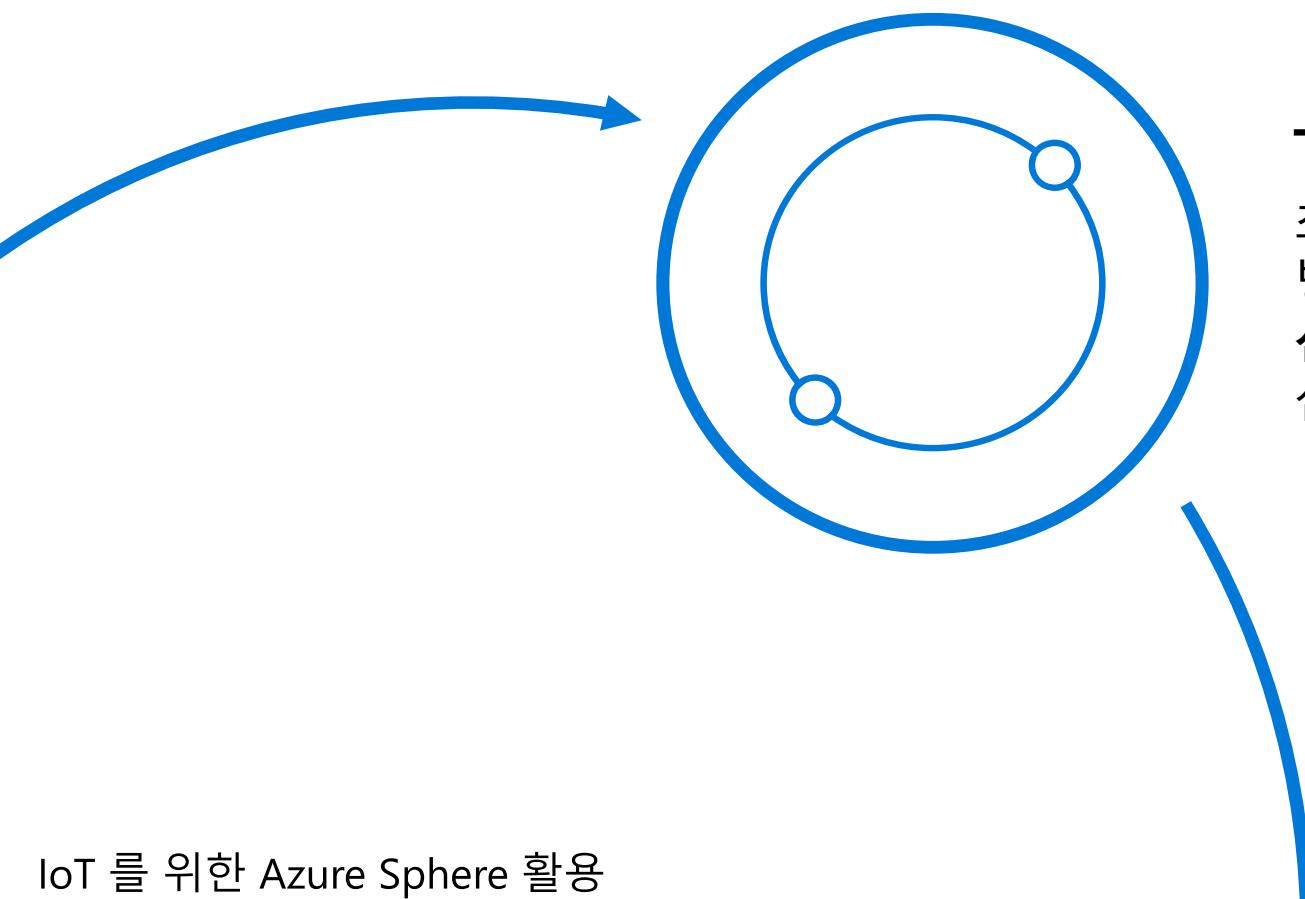
기본 제공 네트워킹 기능 사용

보안

Pluto 보안 서브 시스템을 비롯한 기본 제공 Microsoft의 보안 IP 기술 적용

크로스오버

사상 최초로 MCU 및 크로스오버 SoC에서 Cortex-A 처리 기능 제공



The Azure Sphere 운영체제

최고의 Microsoft 및 OSS 기술을
병합하여 새로운 IoT 환경을 위한
신뢰할 수 있는 플랫폼을 만드는 다층
심층 방어 OS

IoT/보안 유지/빠른 속도 제공을 위해 최적화된 Azure Sphere OS

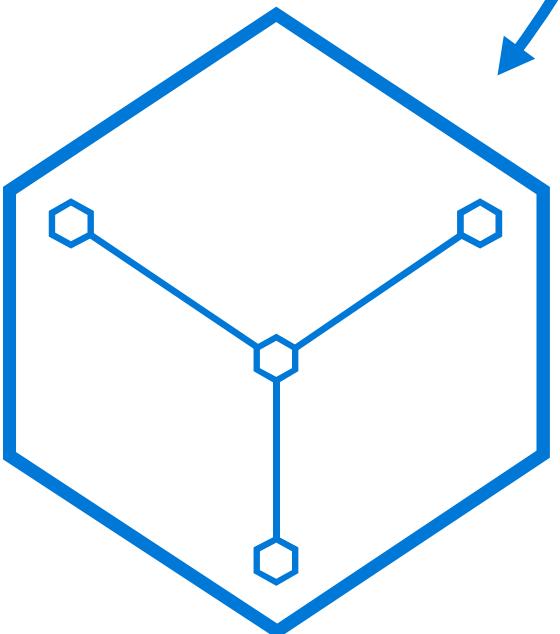


보안 애플리케이션 컨테이너
속도, 안정성, 보안 개선을 위해 코드 구획화

온칩 클라우드 서비스
업데이트, 인증 및 연결 기능 제공

Customized Linux 커널
빠른 반도체 개선 및 코드 재사용 가능

보안 모니터
중요 리소스 액세스 및 무결성 보호



The Azure Sphere 보안 서비스
모든 Azure Sphere 장치를 보호합니다. 신뢰를
증명하고, 새로운 위협을 탐지하며, 장치
보안을 업그레이드합니다.

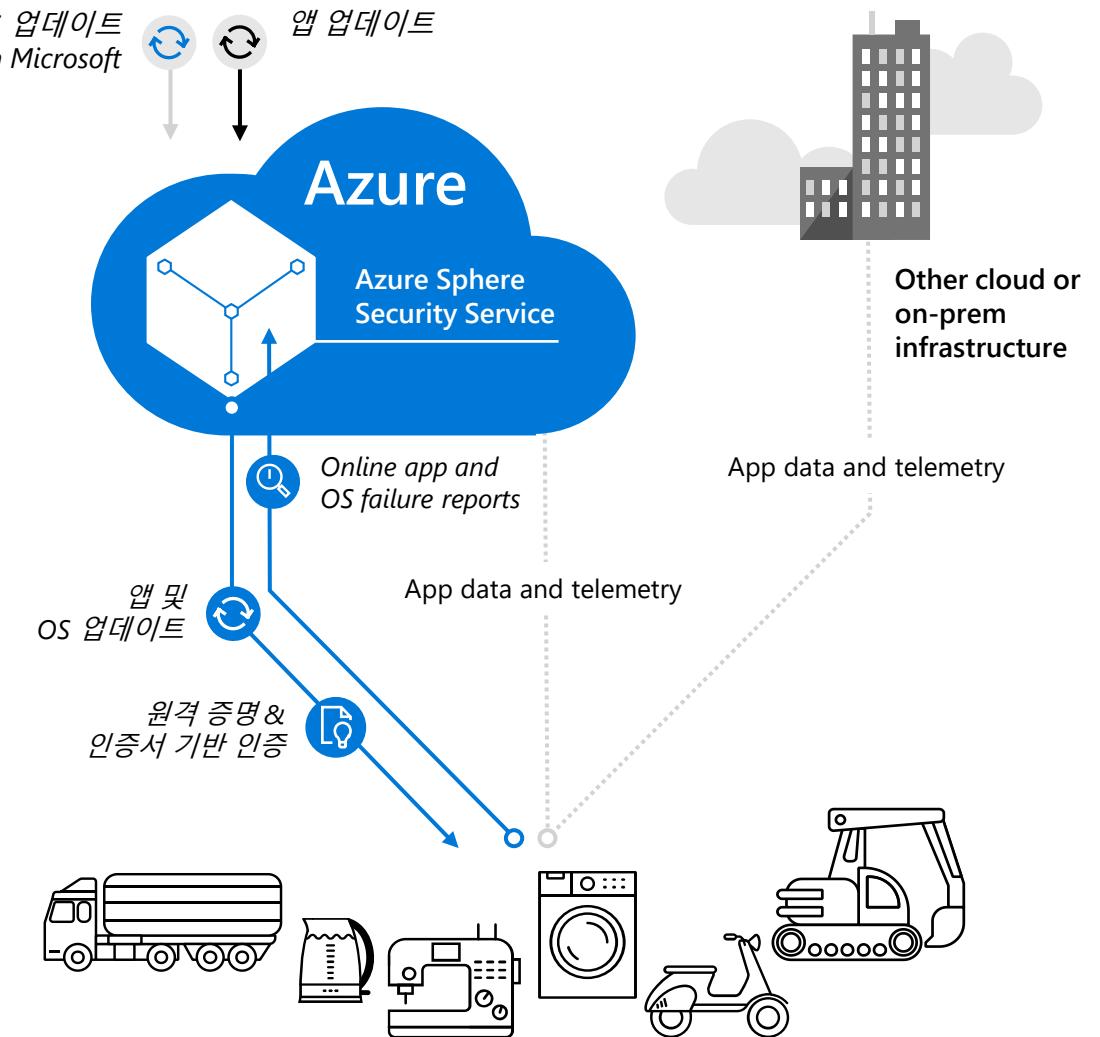
Azure Sphere 보안 서비스는 모든 Azure Sphere 장치를 연결하고 보호합니다.

보호 장치는 모든 통신이 인증서 기반 인증을 통함

검지 장치 오류의 자동화된 처리를 통한 새로운 보안 위협

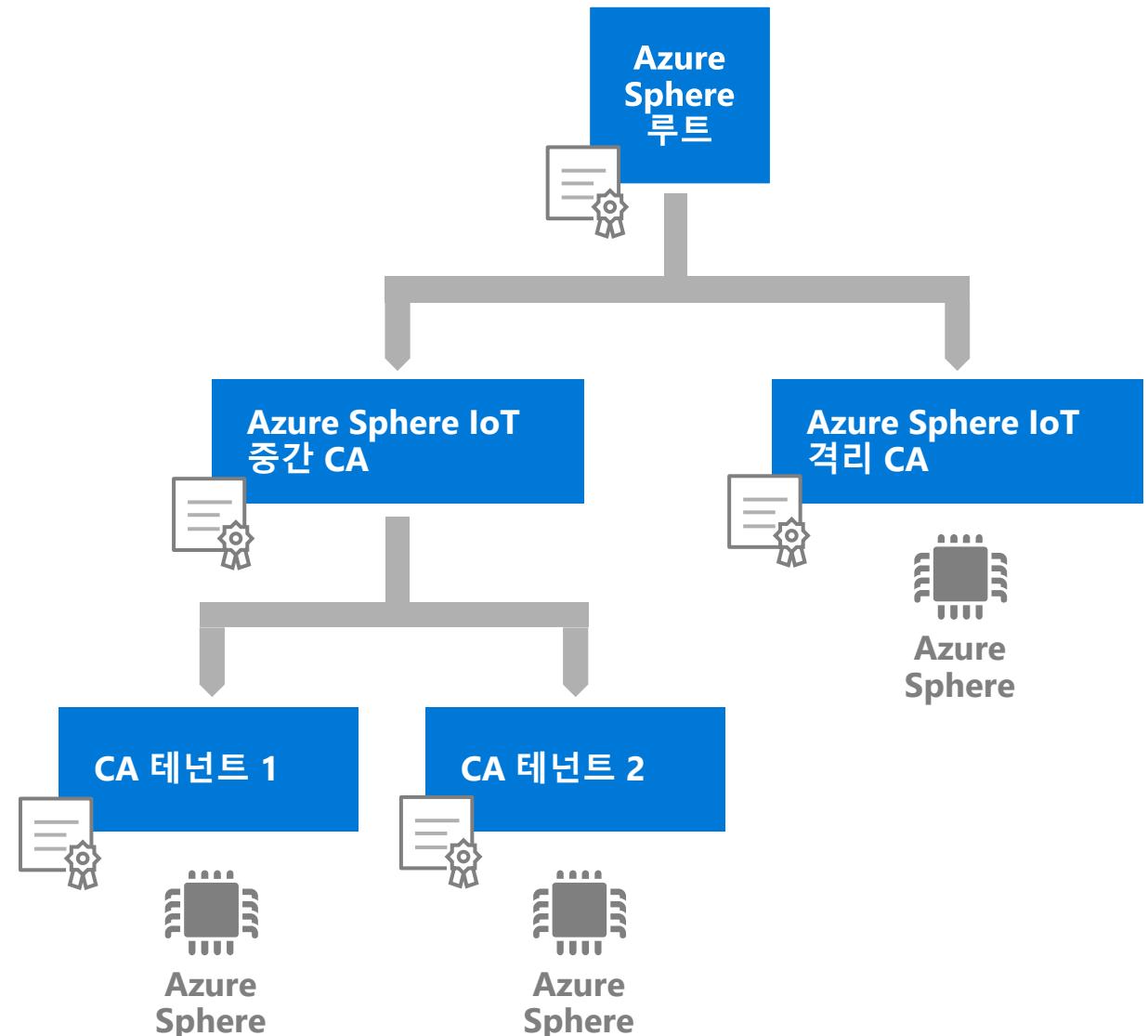
응답 OS의 완전 자동화된 온디바이스 업데이트로 위협에 대처하기

허용 Azure Sphere 장치에 소프트웨어 업데이트를 쉽게 배포할 수 있습니다.

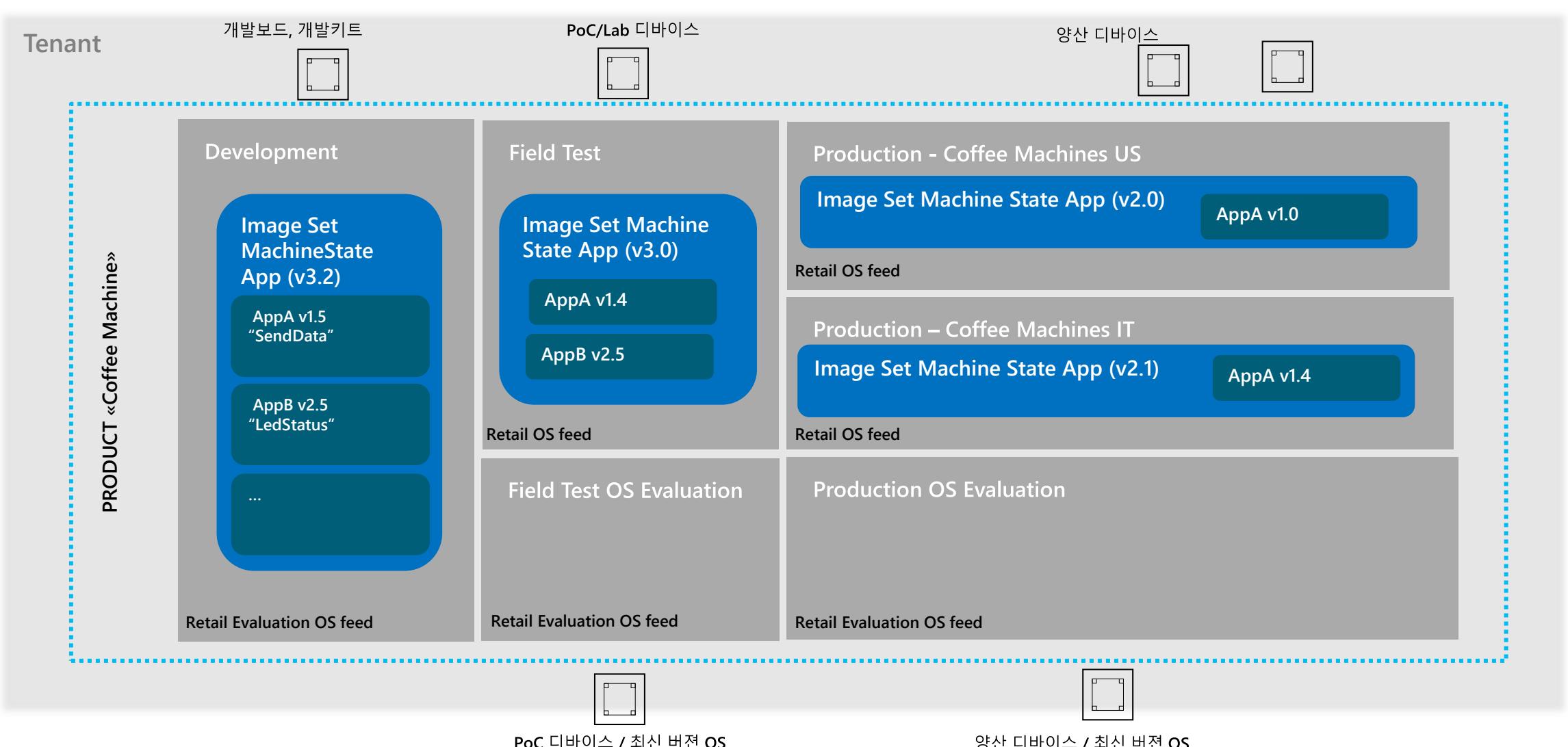


DAA PKI: 인증서 발급

- Azure Sphere Security Service에서 Azure Sphere 테넌트는 디바이스 그룹을 나타냅니다.
- 테넌트는 디바이스 관련 정보를 포함할 뿐 아니라, 이러한 디바이스 관리를 위한 격리 경계도 제공합니다.
- 테넌트는 각 디바이스 포함된 고유 ID를 "클레임"합니다.
- DAA 인증서 서비스는 테넌트별로 작동합니다.
- 테넌트에 등록된 각 디바이스는 테넌트별 체인 내에서만 유효한 인증서를 수신합니다.



Azure Sphere 보안 서비스 : 디바이스 관리





Microsoft 보안 전문가가 모든 Azure Sphere
디바이스에 OS 및 보안 업데이트를 지속적으로
제공합니다.

실리콘 에코시스템



즉시 구매 가능

MT3620

MCU 품 팩터
Wi-Fi 사용 가능



출시 예정

i.MX8 제품군에 포함됨

최고의 성능과 기능을 제공하도록
최적화:

더욱 다양한 기능이 포함된 환경

AI(인공 지능)
그래픽
비디오



출시 예정

칩 세부 정보 공개 예정

언제 어디서나 연결 가능하도록 제작됨:

셀룰러 사용 가능
초절전 시나리오 지원

지속적으로 확대되는 하드웨어 에코시스템 파트너 네트워크(OEM/IDH)



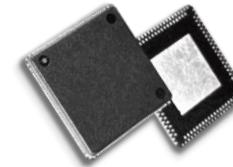
개발 키트: 조직의 신속한 원형 작성 지원
모듈: 디바이스 제조업체의 제품 출시 시간 단축
보호 모듈: 안전한 재생 IoT 지원

지속적으로 확대되는 HW 파트너 에코시스템



Azure Sphere 인증 MCU

칩 제조업체 에코시스템의 지속적 확대를 통해
Microsoft의 실리콘 기반 구축



개발 키트

조직의 신속한 원형 작성 지원



모듈

디바이스 제조업체의 제품 출시 시간 단축



보호 모듈

안전한 재생 IoT 지원

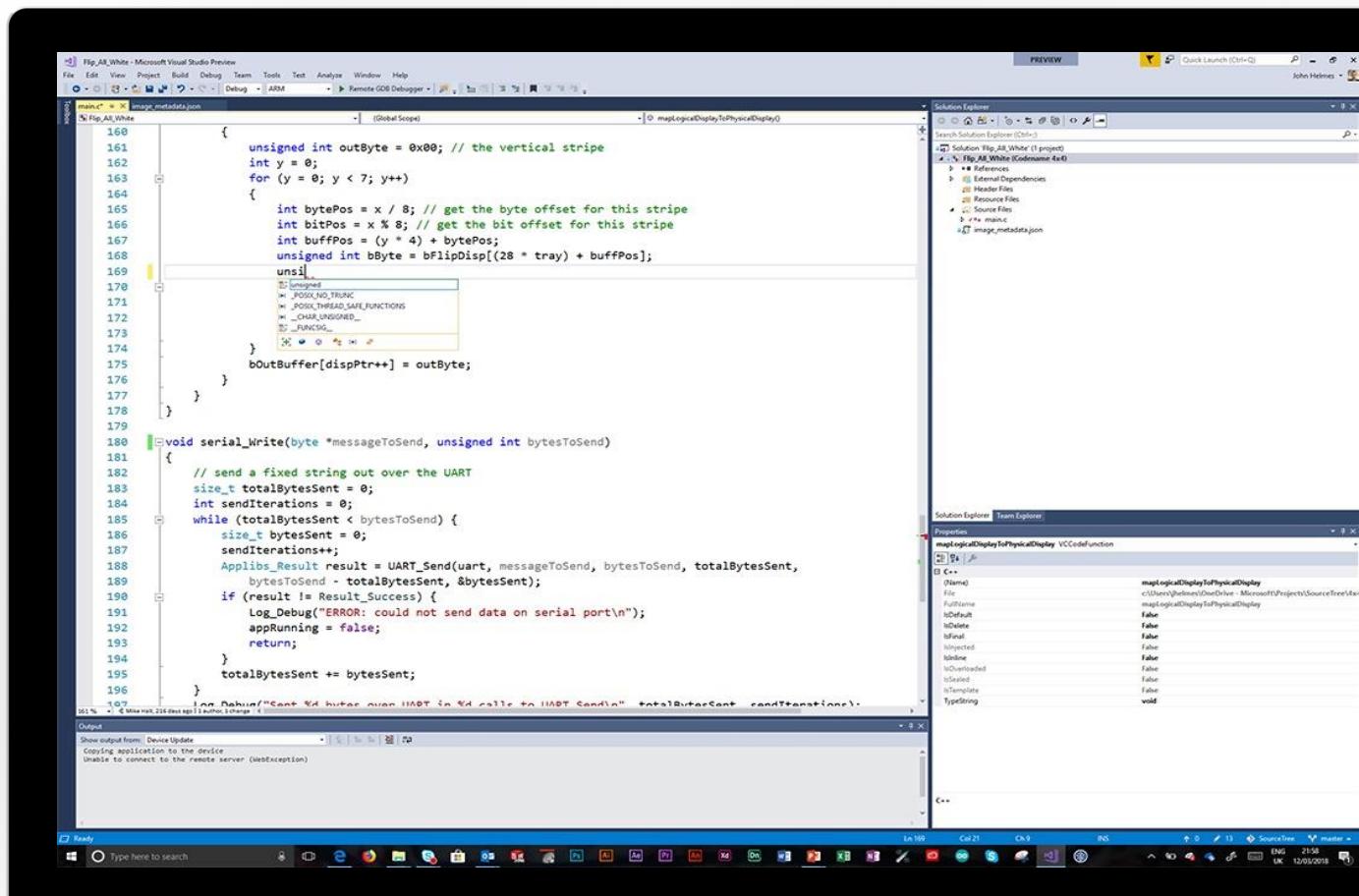


Azure Sphere와 Visual Studio로 MCU 개발 과정 현대화

개발 작업 단순화
창출하려는 가치에 맞는
디바이스 개발 작업 집중 수행

원활한 디버깅 진행
디바이스와 클라우드 전반에서
상황을 인식하는 대화형 디버깅 수행

팀 전체에서 공동 작업 가능
전체 개발 조직에
도구를 통해 지원되는 공동 작업 방식 적용



두 가지 구현 유형

재생
기존 디바이스/장비

일반 사용 사례:
요식업 | 냉장 |
산업 장비 | HVAC 컨트롤

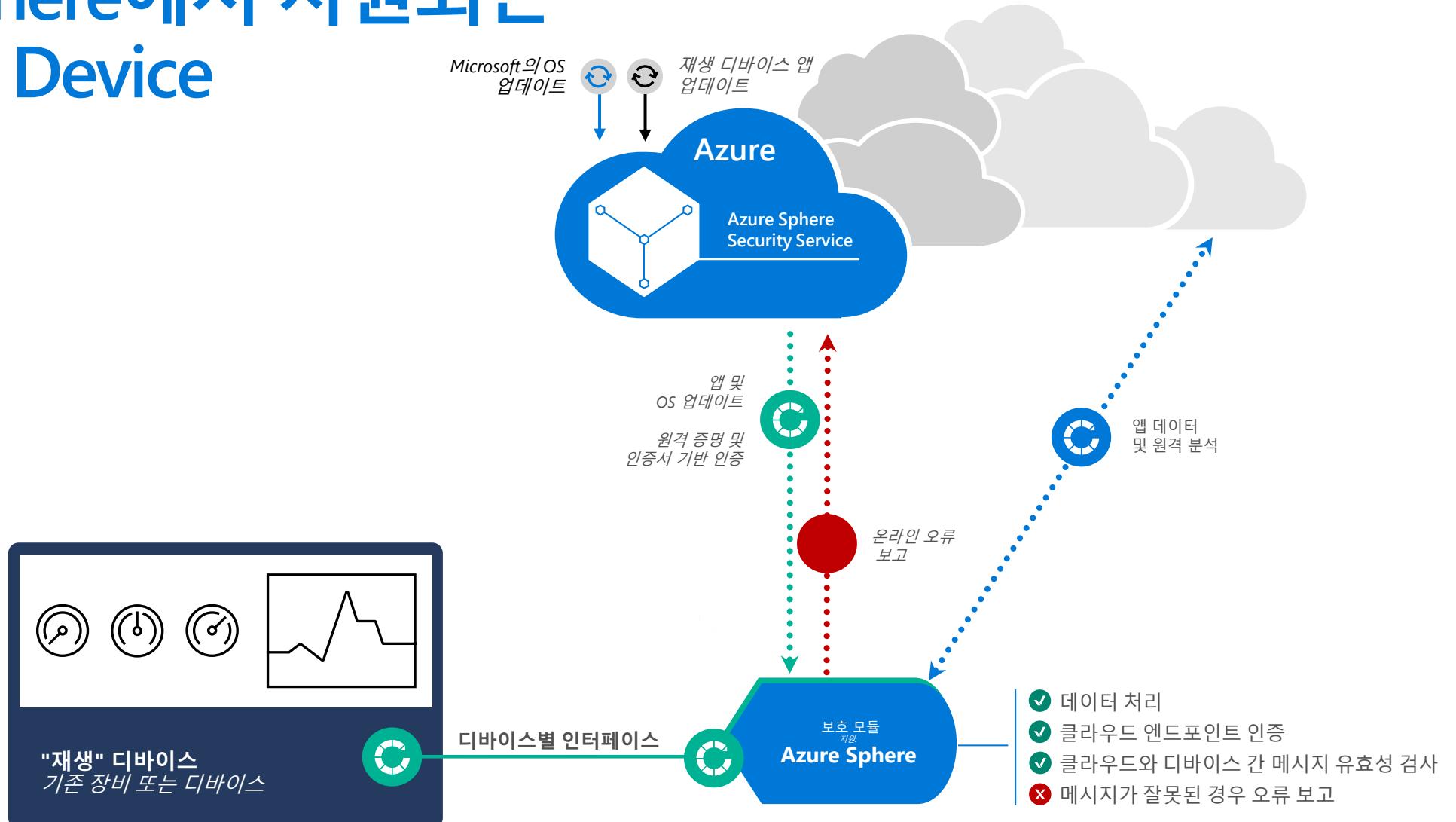
IoT 를 위한 Azure Sphere 활용

신규
새 디바이스/장비

일반 사용 사례:
실제 위치에서 통합 설계 보증 | 교체 주기
조정 | 안전하게 연결된 엔드포인트 디바이스

#gav2020kr

Azure Sphere에서 지원되는 Guardian Device





STARBUCKS

Azure Sphere를 통해 IoT를 도입한 Starbucks

"Starbucks는 클라우드로 직접 프로비전되는 여러 하드웨어 및 소프트웨어 보안 수준을 제공하는 유일한 IoT 에지 솔루션인 Azure Sphere를 선택했습니다."

Venkat Venkatakrishnan(Starbucks 엔지니어링 부문 VP)

고객 환경: 매번 최고의 커피 제공

운영 효율성: 기계에 조리법 직접 다운로드

비용 절약: 불필요한 유지 관리 출장 횟수 감소



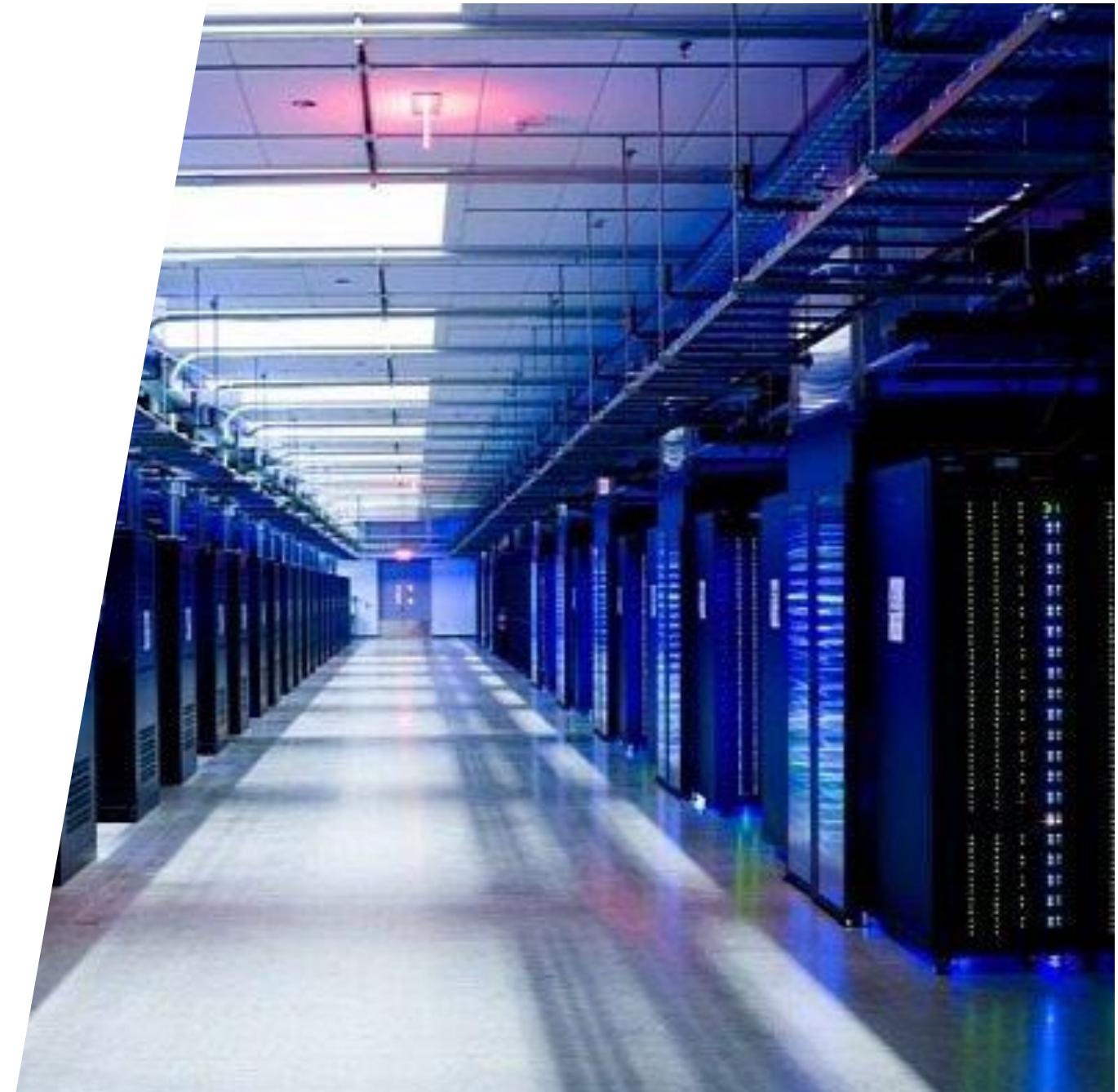
104mm x 84mm x 34mm



Azure Data Center: Azure Sphere를 통해 중요 인프라 보호

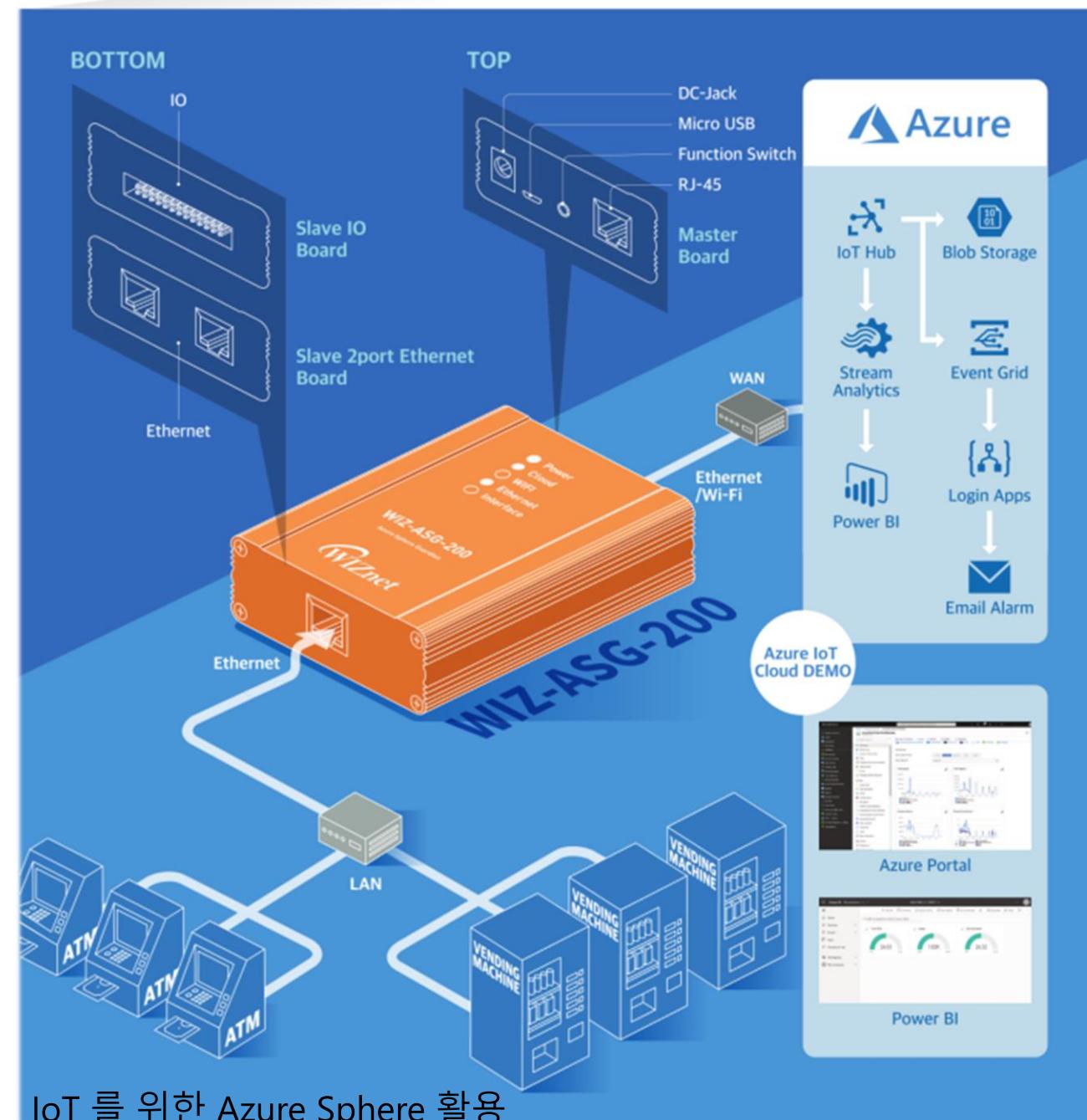


IoT 를 위한 Azure Sphere 활용

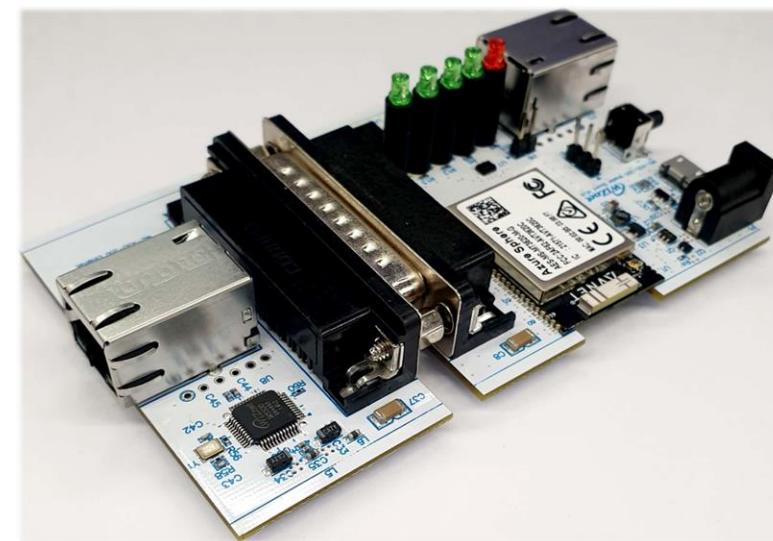


#gav2020kr

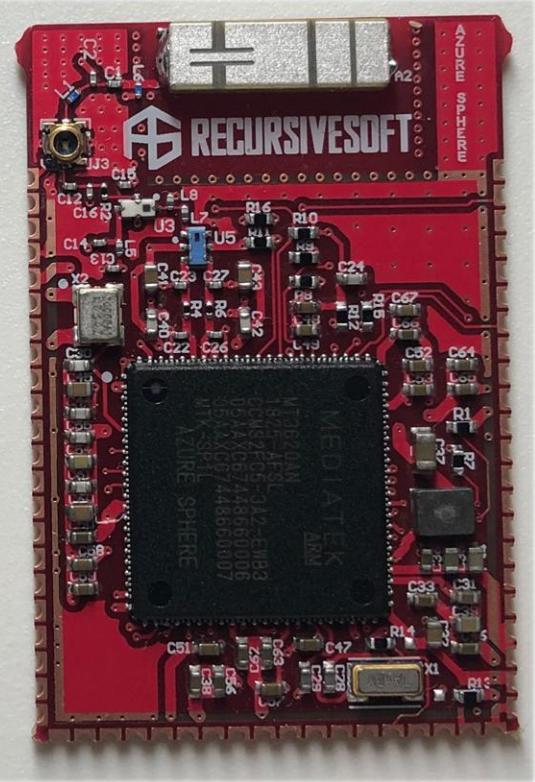
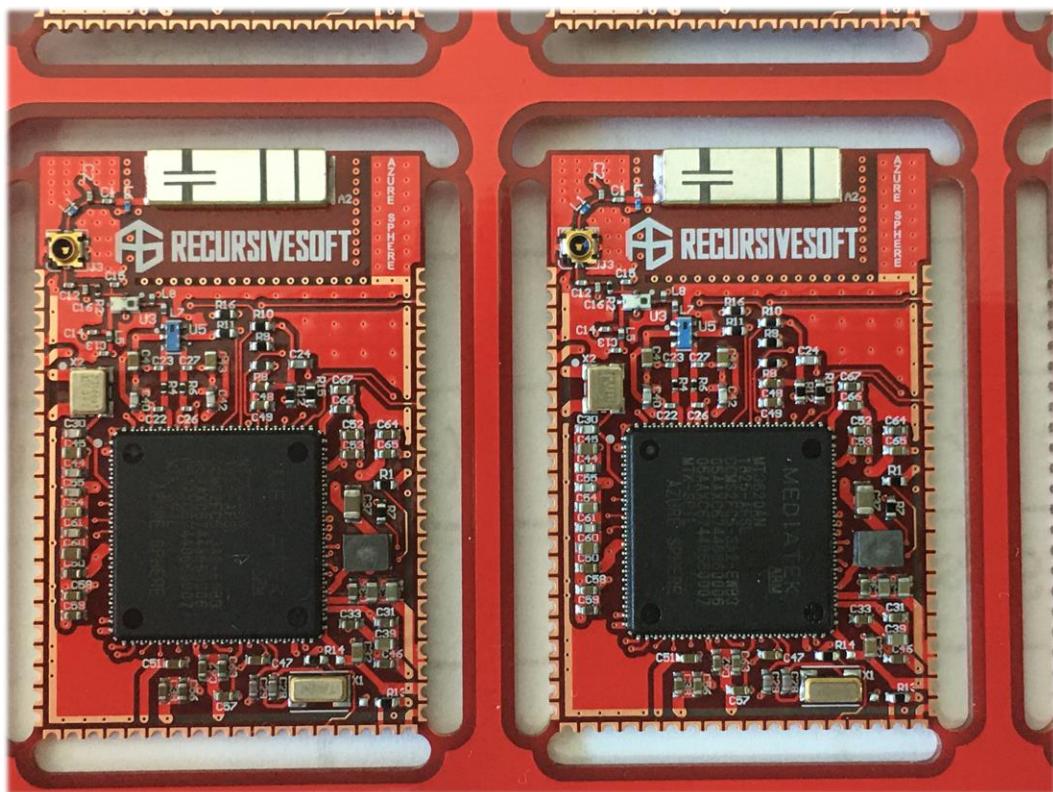
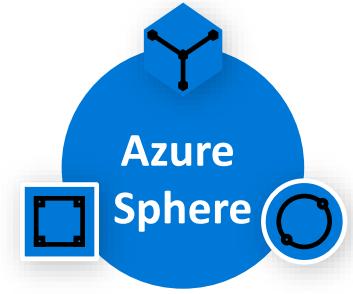
2-port Ethernet and Wireless EDGE module



WIZnet Dual Ethernet Guardian Device



Azure Sphere 모듈



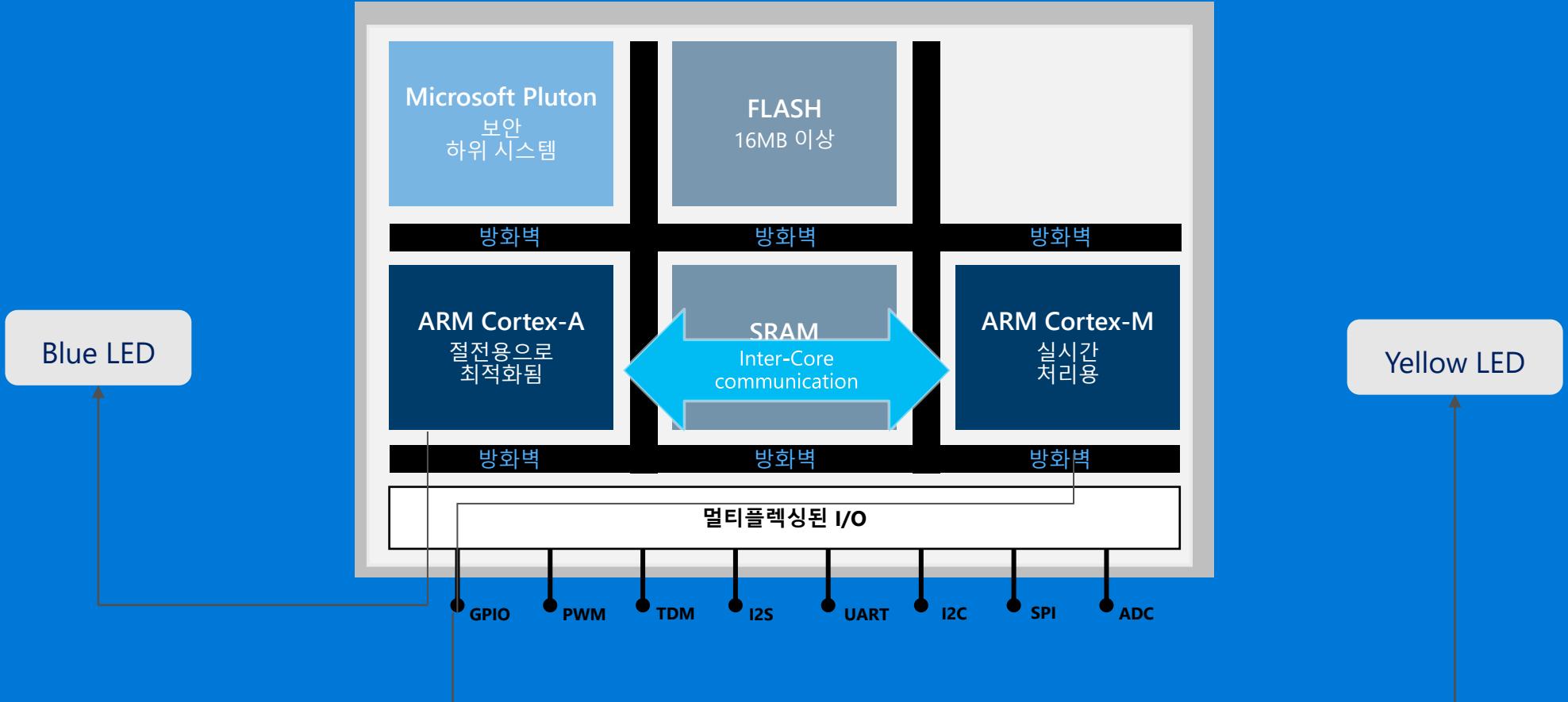


Multi-Core 및 손쉬운 OTA 데모



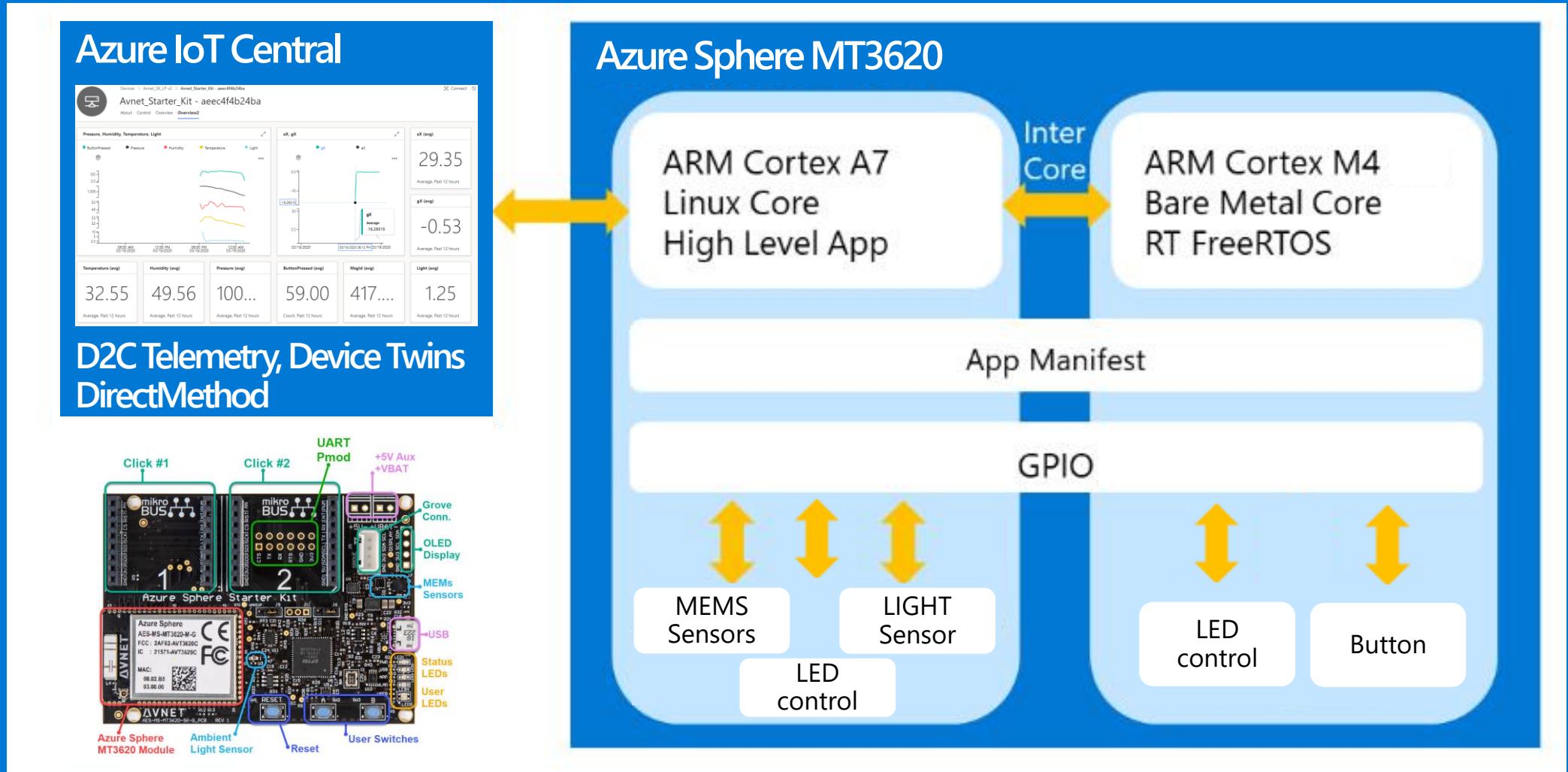
데모

2개의 Application 을 OTA 업데이트



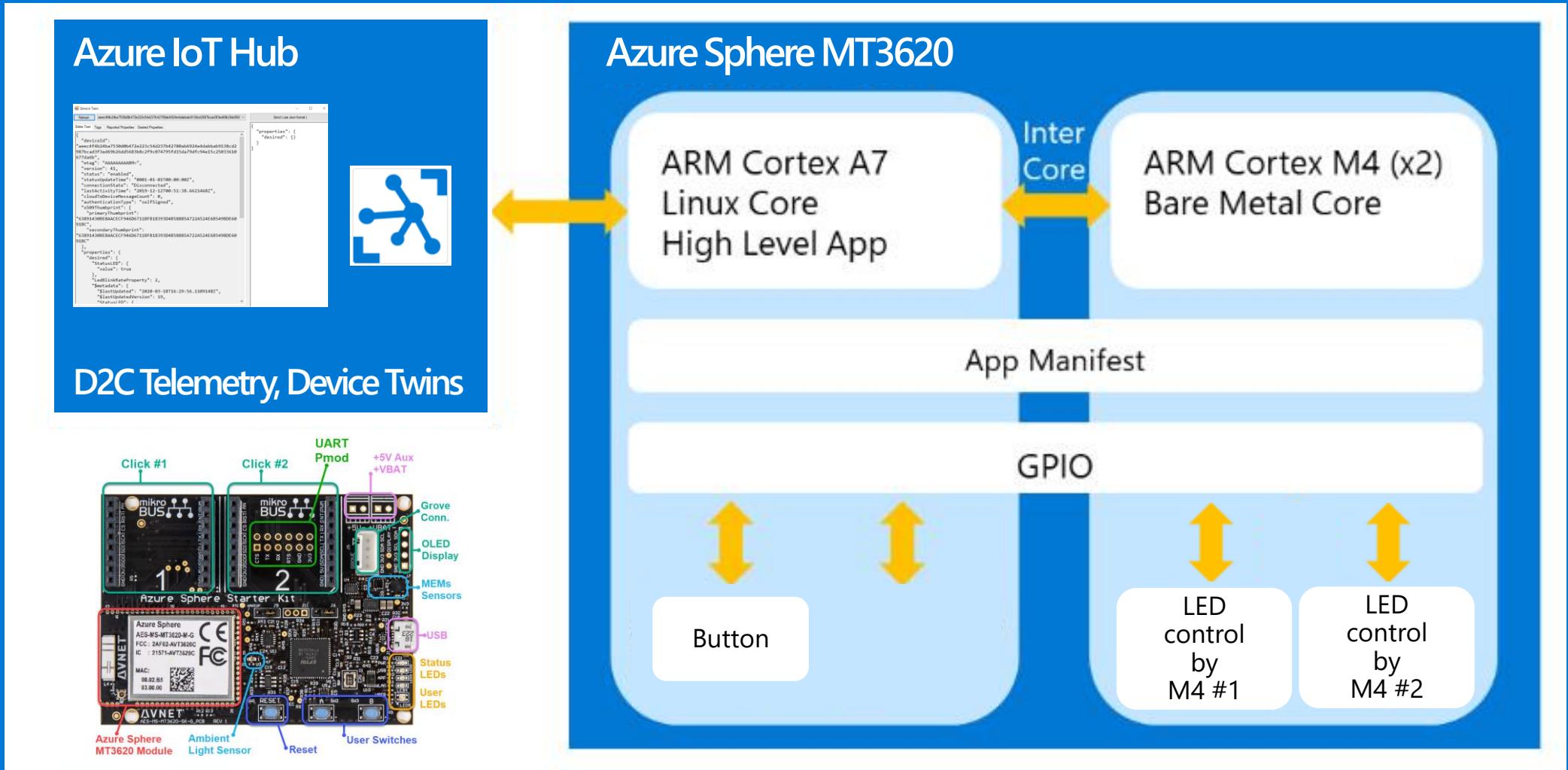
데모

2개의 Application 을 OTA 업데이트 + Azure IoT Central 과 연동



데모

3개의 Application 을 OTA 업데이트 + Azure IoT Hub 와 연동



안전한 미래 지향적 플랫폼.



SECURED FROM THE SILICON UP

당신의 목소리를 들려주세요!

Global Azure Virtual 2020는 여러분의 목소리를 기다립니다.
가감 없는 목소리가 발표자 분에게 매우 큰 힘이 됩니다.
앞으로 더 좋은 행사가 될 수 있도록 목소리를 내주세요.
감사합니다!

세션에 대한 목소리:

<https://sv.kazure.com/session-c4>

파트너사 행사:

<https://bit.ly/2RvJQzR>

