백서

관련 사물 인터넷 (THE INTERNET OF RELEVANT THINGS)

IOT 컨텍스트 및 데이터와 비즈니스 목표 사이의 격차를 해소하여 전략적 목표 달성하기

aruba
a Hewlett Packard Enterprise company

목차

교수와 나무꾼

수년 전, 예일 대학의 한 산업공학과 교수는 다음과 같이 말했습니다. "만약 문제를 해결할 수 있는 시간이 딱 한 시간 주어진다면 그중 3분의 2는 문제를 정의하는 데 사용할 것입니다."[1] 같은 맥락에서, 한 나무꾼이 다음과 같은 질문을 받았습니다. "나무를 벨 수 있는 시간이 5분밖에 없다면 어떻게 하시겠습니까?" 나무꾼은 대답했습니다. "먼저 2분 30초 동안 도끼를 날카롭게 갈 겁니다."[2] 어떤 업종에 종사하든 먼저 준비를 철저히 하고 목표를 신중하게 정의하고 이를 달성하기 위해 필요한 도구를 선택하는 것이 중요합니다.

그러나 안타깝게도 유독 사물 인터넷(IoT) 프로젝트에서는 이러한 원칙이 간과되는 경우가 많습니다. 그것이 IoT라는 개념이 주는 매혹 혹은 IoT에 대한 오해 때문이든, 경쟁사들로부터 뒤처지게 될 수 있다는 두려움 때문이든, 아니면 무엇인가 새로운 것을 해야 한다는 압박감 때문이든, 기업들은 자주 목표와 가치 제안 또는 도구 적합성을 명확하게 정의하지 않은 채 IoT 프로젝트에 무모하게 뛰어들곤 합니다. 그 결과 수많은 IoT 프로젝트가 쓰디쓴 실패를 맛보고 고객들은 환멸을 느끼게 되었습니다.[3]

이렇게 되는 원인 중 하나는 바로 '사물 인터넷'이라는 용어가 오해를 불러일으키고 현혹되기 쉽기 때문입니다. '사물 인터넷'이란 용어는 원래 상호 연결된 기계들로 구성된 에코 시스템을 설명하기 위해 사용되었으나, 오늘날에는 말 그대로 모든 장치가 인터넷에 연결된다는 의미로 받아들여지고 있습니다. IoT의 중대한 목표는 기업의 모든 장치를 네트워크에 연결하는 것도, 존재하는 모든 장치를 인터넷에 연결하는 것도 아닙니다. IoT 장치는 컨텍스트와 데이터가 담긴 용기에 불과하며, 그중에서 관련성이 높은 정보와 장치만 활용할 수 있어야 합니다.

그렇다면 어떤 정보가 관련성이 높고 어떤 정보가 관련성이 낮은지 어떻게 판단할 수 있을까요? 관련성은 기업의 전략적 목표와 이를 달성하기 위한 비즈니스 목표, 그리고 상황에 따라 동적으로 활용할 수 있는 일시적인 고객 관련 기회(Gartner는 이를 "비즈니스 순간"이라고 칭합니다)가 하나의 사슬처럼 엮여서 발생하는 것입니다.[4] 비즈니스 순간이란 기업의 전략적 목표와 이를 제대로 활용했을 때 고객의 행동, 태도 및/또는 감성을 긍정적으로 변화시키는 관련성 있는 IoT 컨텍스트 및 데이터(그림 1)가 융합되는 지점을 가리킵니다.

비즈니스 순간이 고객에게는 즉흥적으로 발생하는 것처럼 보일 수 있으나, 기업에서는 이를 신중하게 조율할 줄 알아야 합니다. 성공은 관련성 있는 IoT 컨텍스트 및 데이터와 이를 비즈니스 순간으로 전달하는 IoT 아키텍처로 이루어진 또 다른 사슬에 좌우됩니다. 예컨대 IoT 아키텍처가 관련 정보를 제대로 추출하지 못해서 이 사슬이 제대로 작동하지 않는 경우에는 비즈니스 순간이 도래하더라도 별다른 성과를 얻지 못하거나 부정적인 감성을 불러 일으켜 오히려 전략적 목표에 해가 될 수 있습니다.

여기서 다시 교수와 나무꾼의 이야기가 떠오릅니다. 기업이 IoT 프로젝트에 착수할 때 가장 먼저 할 일은 달성해야 할 전략적 비즈니스 목표를 정의하는 것입니다. 전략적 비즈니스 목표가 정의되면 성공적인 비즈니스 순간에 의해 좌우되는 일련의 구체적인 목표가 도출됩니다. IoT 아키텍처는 이러한 전략적 목표에 도움이 되는 방식으로 고객의 행동, 태도, 행위를 유도할 수 있도록 관련성 있는 IoT 컨텍스트와 데이터를 추출하고 활용하기 위한 도구입니다.

먼저 비즈니스 목표가 정의된 다음에만 어떤 IoT 아키텍처와 관련 장치를 사용해야 하는지 알 수 있게 됩니다. 남들이 다 사용하기 때문에, 혹은 보기에 좋아서 IoT 솔루션을 선택한다면 이는 아무런 도움이 되지 않을 수 있습니다.

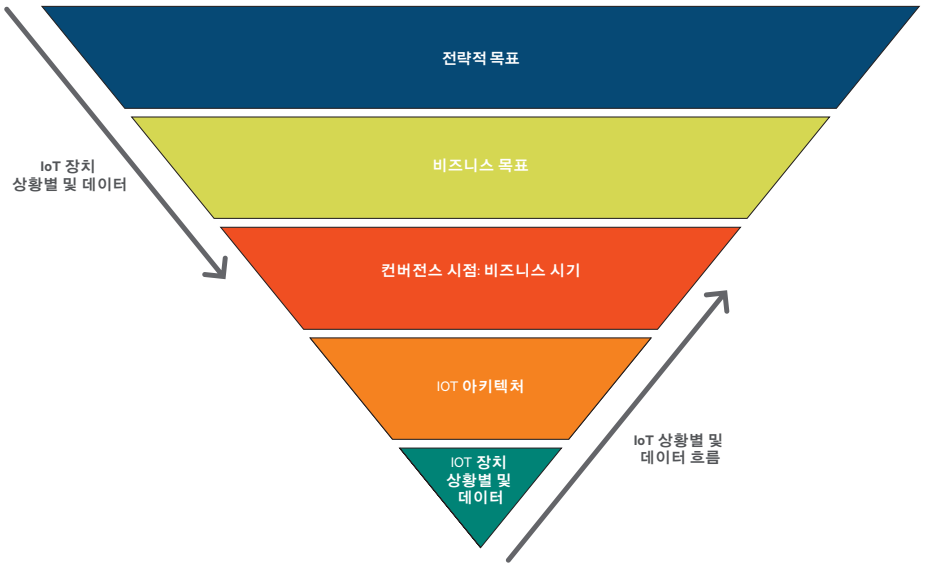


그림 1: IoT 전략 구조

다리 놓기

이 모든 과정에 길잡이 역할을 하는 프레임워크가 없다면 비즈니스 목표와 이를 달성하기 위해 필요한 IoT 아키텍처 사이에 다리를 놓는 작업이 무척 어려워집니다. 각 사업부의 관계자들은 기업의 목표에 맞춰 개별적인 과제를 포기해야 할 수 있습니다. 경영, 제품, 엔지니어링, IT, 운영 조직 사이에도 새로운 차원의 협업이 요구됩니다.[5] 보다 관련성 있는 대안을 위해 몇몇 프로젝트와 기술을 폐기해야 할 수도 있습니다. 신규 공급업체들이 더욱 관련성 높은 솔루션을 온보딩할 수 있도록 하려면 오랜 벤더 관계를 청산해야 할 수 있습니다.

IoT 가치 사이클(그림 2)은 비즈니스 목표를 가시성, 보안, 혁신, 수익성이라는 네 가지 주요 요소로 분해함으로써 이러한 프레임워크를 제시합니다. 가시성과 보안은 비즈니스 목표에 부합하는 컨텍스트와 데이터를 추출하는 IoT 인프라와 관련이 있으며, 혁신과 수익성은 이러한 컨텍스트와 데이터를 활용하는 비즈니스 순간을 정의합니다. 모든 관계자들이 협력하여 이 네 가지 요소를 올바르게 정의하고 구현한다면 IoT 솔루션을 바탕으로 유의미한 비즈니스 순간에 대응할 수 있으며, 궁극적인 비즈니스 목표를 충족할 수 있습니다.

가시성은 "충분히 연결되어 있는가?"라는 질문에 대한 답을 제공하는데 이는 장치, 기계, 그리고 관련 프로세스, 비즈니스, 고객 관련 컨텍스트 및 데이터 사이의 인터페이스를 구축함으로써 달성됩니다. 이를 구현하는 데 필요한 인프라는 애플리케이션에 따라 달라집니다. 자동차 애플리케이션에는 셀룰러 텔레매틱스가 필요하며, 감시 제어 및 데이터 취득(SCADA, Supervisory Control And Data Acquisition) 시스템에는 LAN과 메시 무선이 필요하고, 해외 원유 플랫폼에는 클래스 1 디비전 1 방폭 Wi-Fi 인프라가 필요할 수 있습니다.

관련성 있는 장치의 물리적 위치를 불문하고 신뢰할 수 있는 출처에서 신뢰할 수 있는 데이터만 보고 사용할 수 있어야 합니다. 그에 따라 IoT 데이터의 전체 라이프 사이클에 걸쳐 이동 중과 저장 중에 이를 보호하고 관리해야 합니다. 또한 외부 사용자와 내부 사용자의 무단 조작으로부터 장치, 운영 체제, BIOS 및 인프라를 보호해야 합니다. IoT 솔루션을 설치하고 관리하는 사람들과 이들이 사용하는 도구 또한 안전하게 관리되어야 합니다. 애플리케이션과 시스템의 무중단 가동을 보장할 수 있어야 하며, 항시 데이터 사용 현황에 대한 적절한 거버넌스가 실행되어야 합니다. 끊임없이 변화하는 사이버 보안 환경에서 신뢰는 순식간에 사라져 버릴 수 있습니다. 따라서 항시 최신 보호 방책을 구현하기 위해서는 IoT 프로젝트의 전체 라이프 사이클에서 "완벽하게 보호되고 있는가?"라는 질문을 끊임없이 던져야 합니다.

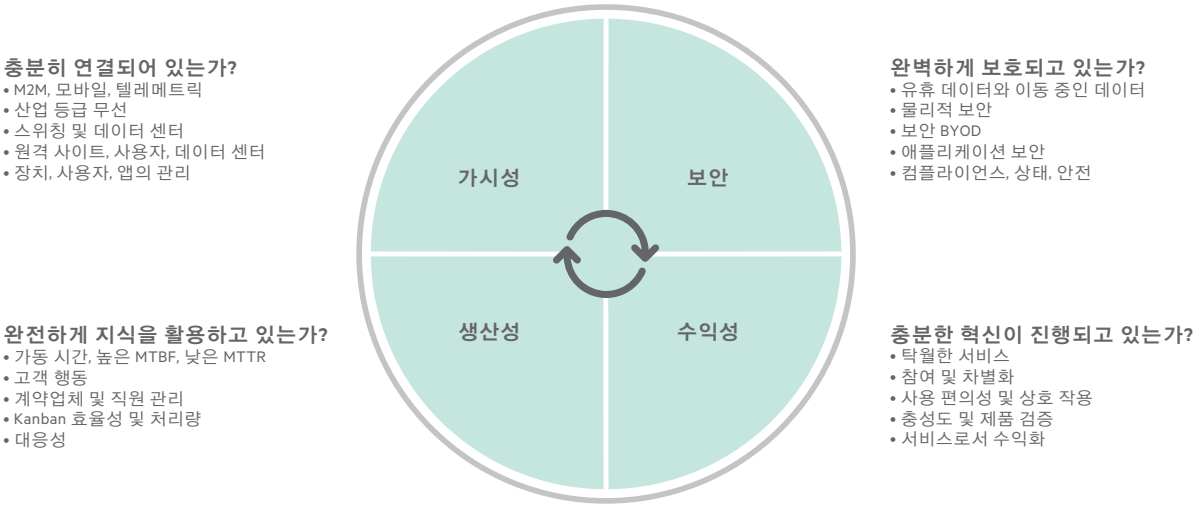


그림 2: 사물 인터넷 가치 사이클

이렇듯 데이터 소스에 액세스하고, 신뢰를 확립하고, 추출된 정보의 라이프 사이클을 관리하기 위해서는 가시성과 보안을 바탕으로 IoT 아키텍처를 구축해야 합니다. 결과적으로 가시성과 보안은 IoT 전략 구조의 두 번째 레이어를 정의합니다.

IoT 전략 구조의 기본이 되는 레이어에서는 액세스 용이성과 신뢰가 IoT 장치에 의해 생성되고 그에 포함되는 관련성 있는 컨텍스트와 데이터에 부합하도록 해야 합니다. 관련성에 대한 고려 없이 모든 장치를 활용하려고 하면 불필요한 비용이 상승하게 됩니다. 연결을 구축하기 위해 장치 비용이 발생하며, 가시성과 보안을 확장하기 위해 노동력과 자본이 투입되고, 추출된 데이터를 처리 및 저장해야 하며, 가치 있는 것과 그렇지 않은 것을 구분하기 위해 리소스를 소모하게 됩니다.

관련성을 충분히 고려하고 특정 IoT 장치에 주력하기 위한 지침은 수익성과 생산성 요소에서 찾을 수 있습니다. 수익성은 고객에게 더 나은 서비스를 제공하고, 고객이 필요로 하는 제품과 서비스를 개발하고, 비즈니스에 이로운 방식으로 고객의 행동과 태도를 변화시킴으로써 매출을 증진하거나 비용을 절감할 때 달성될 수 있습니다. "충분한 혁신이 진행되고 있는가?"라는 질문은 탁월한 서비스를 제공하고, 고객과의 관계를 강화하고, 경쟁사와 차별화하고, 상호 작용을 간소화하고, 충성도를 높이며, 제품 성능의 유효성을 검증하고, 서비스로부터 수익을 창출하는 방법을 이끌어내기 위한 관문이 됩니다.

IoT 가치 사이클의 마지막 요소인 생산성은 효율성을 극대화하는 방식으로 인적 자원과 자본 자산에 주력하는 데 중점을 둡니다. 생산성은 가동 시간을 극대화하고, 중단 시간을 최소화하고, 영업 및 지원 프로세스를 간소화하고, 고객과 직원들을 더 효율적으로 관리하고, 자산 관리 및 프로세스 처리량을 최적화하고, 요구 사항과 변화에 보다 민감하게 대응함으로써 달성할 수 있습니다. "지식을 충분히 활용하고 있는가?"라는 질문은 효율성을 개선하기 위해 IoT 컨텍스트와 데이터를 활용하는 방식을 도출하기 위한 첫걸음입니다.

가시성, 보안, 수익성, 생산성은 대상 고객에 따라 다르게 나타납니다. 특정 업종에 국한하여 보더라도 모든 경우에 적합한 전천후 IoT 솔루션이란 존재하지 않습니다. 기업의 목표가 조금만 달라도 이를 달성하기 위한 솔루션은 극명하게 달라질 수 있습니다. 경쟁사의 솔루션을 참고하는 것이 의미가 있을 수는 있지만, 자사의 목표와 비즈니스 순간이 경쟁사와 동일하지 않다면 경쟁사에서 사용하는 솔루션이 유용하지 않을 수 있습니다. 경쟁사를 맹목적으로 따라가는 것이 현명한 대처가 아닐 수 있습니다.

IoT 전략 구조와 IoT 가치 사이클을 겹쳐 놓고 보면(그림 3) 목표와 아키텍처 사이에 다리를 놓는 데 도움이 될 수 있습니다. 수익성과 생산성은 컨텍스트와 데이터를 추출할 관련성 있는 소스를 파악하는 데 도움이 되고, 가시성과 보안은 이러한 소스로부터 데이터를 추출하기 위해 필요한 아키텍처와 인프라를 결정하는 데 도움이 됩니다.

이러한 다리 놓기 과정은 예시를 통해 구체적으로 시각화할 수 있습니다. 이후 섹션에서 리테일을 비롯한 여러 업종의 시나리오를 검토하기 전에 먼저 보안에 대해 살펴보겠습니다.

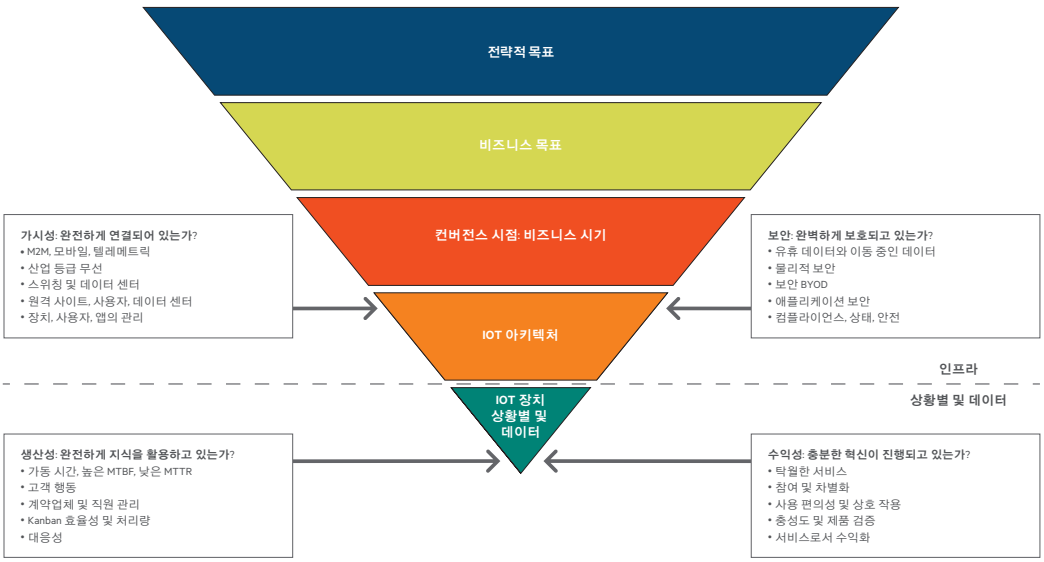


그림 3: 아키텍처 및 IoT 컨텍스트/데이터와 비즈니스 목표 사이에 다리 놓기

내부와 외부의 보안

IoT 네트워크 침입과 데이터 침해는 원자력, 리테일, 의료, 소비자 등 분야를 막론하고 모든 업종에서 일반적인 현상이 되었습니다. 그 이유는 간단합니다. 대부분의 IoT 장치와 환경은 보안 방책이 구현되지 않았거나 구현되었더라도 그 수준이 미비하여 신뢰할 수 없기 때문입니다. IoT 장치를 설계하는 엔지니어들은 프로세스 안정성과 애플리케이션별 아키텍처에 주력합니다. 이는 제품들이 가능한 한 오랫동안 안정적으로 가동되게 하는 운영 기술(OT) 영역에 속합니다. 반면 사이버 보안 전문가들은 정보 기술(IT) 엔지니어와 협력합니다. IoT 제품 및 시스템을 설계할 때 OT와 IT가 긴밀하게 협업하지 않으면 결과적으로 신뢰할 수 없는 솔루션이 구축됩니다.

의도적으로 또는 부주의에 의한 무단 조작의 위험이 있는 IoT 정보와 프로세스를 사용하는 것은 바람직하지 않습니다. 우리가 사용하는 정보는 뛰어난 무결성과 신뢰성에 바탕을 두어야 하는데, 이를 위해서는 IoT 장치에서부터 애플리케이션에 이르기까지 엔드-투-엔드(end-to-end)로 신뢰가 구축되어야 합니다. 이렇게 하려면 새로운 IoT 장치에 보안 기능을 적용하고 레거시 장치를 보호망으로 감싸, 신뢰할 수 있다고 판명되지 않은 장치나 사용자로부터 이러한 장치를 보호할 수 있는 방어 프레임워크를 구축해야 합니다. 이러한 프레임워크는 다양한 소스로부터 추출된 컨텍스트 정보를 바탕으로 사용자와 장치가 접속하기 전후에 이들의 보안 상태를 면밀히 살펴볼 수 있어야 합니다.

Aruba의 IoT 보안 프레임워크인 Connect-and-Protect에는 다음과 같은 보호 메커니즘이 적용되어 있습니다.

- 소스/대상 장치의 인증 및 센서 입력과 버스를 비롯한 트래픽 패턴 모니터링
- 상용 암호화 표준과 해당하는 경우 정부 암호화 표준을 사용한 데이터 패킷 암호화
- 보안 터널 내부의 패킷이 원래의 목적지로 전송되도록 보장하기 위한 패킷 엔벨로핑
- IoT 장치가 신뢰할 수 있는지, 신뢰할 수 없는지 또는 알려지지 않았는지 확인하기 위해 지문 감식/액세스 및 네트워크 서비스를 제어하는 적절한 역할 및 컨텍스트 기반 정책의 적용
- 애플리케이션 방화벽과 맬웨어 탐지 시스템으로 종단 트래픽을 검사하여 동작 모니터링 및 관리
- 정책 위반 발생 시 엔터프라이즈 모빌리티 관리(EMM), 모바일 애플리케이션 관리(MAM), 모바일 장치 관리(MDM) 시스템을 사용하여 동작 모니터링 및 다른 장치 보호

그림 4: 연결 및 보호 IoT 보안 메커니즘

이때 특히 주목해야 할 것은 IoT 장치 프로파일링, 아이덴티티 및 포스처에 있어 Aruba ClearPass Policy Manager가 수행하는 역할입니다. 프로파일링 기능은 IoT 장치가 접속을 시도하면 지문을 감식하고 분류하여 여러 장치 유형을 구분하고 정체를 가장한 장치를 가려냅니다. 아이덴티티 기능은 위치, 시간, 요일, 보안 포스처 등 IoT 장치의 접속 시점 및 접속 방식을 확인함으로써 더욱 세밀한 역할 기반 액세스 제어를 수행합니다. 포스처는 알려진 취약성, 활성 포트, 운영 체제 버전, SNMP 보안 등을 확인하는 상태 점검 기능입니다. 컴플라이언스를 보장하기 위해서는 포스처의 유효성을 규칙적으로 확인해야 하며, 포스처가 기준에 미치지 않는 경우 신뢰할 수 있는 장치라도 액세스가 거부될 수 있습니다.

ClearPass는 프로파일링, 아이덴티티, 포스처 기능을 사용하여 IoT 장치가 신뢰할 수 있는지, 신뢰할 수 없는지 또는 알려지지 않았는지 판별한 다음 그에 따라 조치를 취합니다. 프로파일링 데이터는 특정 장치의 작동 모드가 변경되었는지 또는 다른 IoT 장치로 가장하고 있는지 여부를 가려내고, 이 정보를 바탕으로 ClearPass가 장치의 인증 권한을 자동으로 변경합니다. 예를 들어, 특정 PLC(Programmable Logic Controller)가 Windows PC로 가장했다면 즉시 네트워크 액세스가 차단됩니다.

정책의 효과는 정책을 구성하는 데 사용된 정보와 정책을 보호하는 데 사용할 수 있는 시행 도구에 따라 달라집니다. 보안에 체계적으로 접근하면 IoT 위협 벡터와 이에 대처하는 데 필요한 보안 기술을 효율적으로 파악할 수 있습니다.

IoT의 궁극적인 목표는 IoT 장치에 방치되어 있는 무궁무진한 데이터를 활용하여 비즈니스 혁신을 촉진하는 것입니다. 기초부터 탄탄하게 수립된 올바른 보안 방책을 적용하면 IoT 솔루션 전반에서 신뢰를 구축할 수 있습니다. 이렇게 하면 신뢰할 수 있는 IoT 아키텍처를 사용하여 전략적 목표에 다리를 놓는 작업에 더욱 집중할 수 있게 됩니다. 이번에는 다리 놓기 작업이 어떻게 진행되는지 예를 통해 살펴보겠습니다.

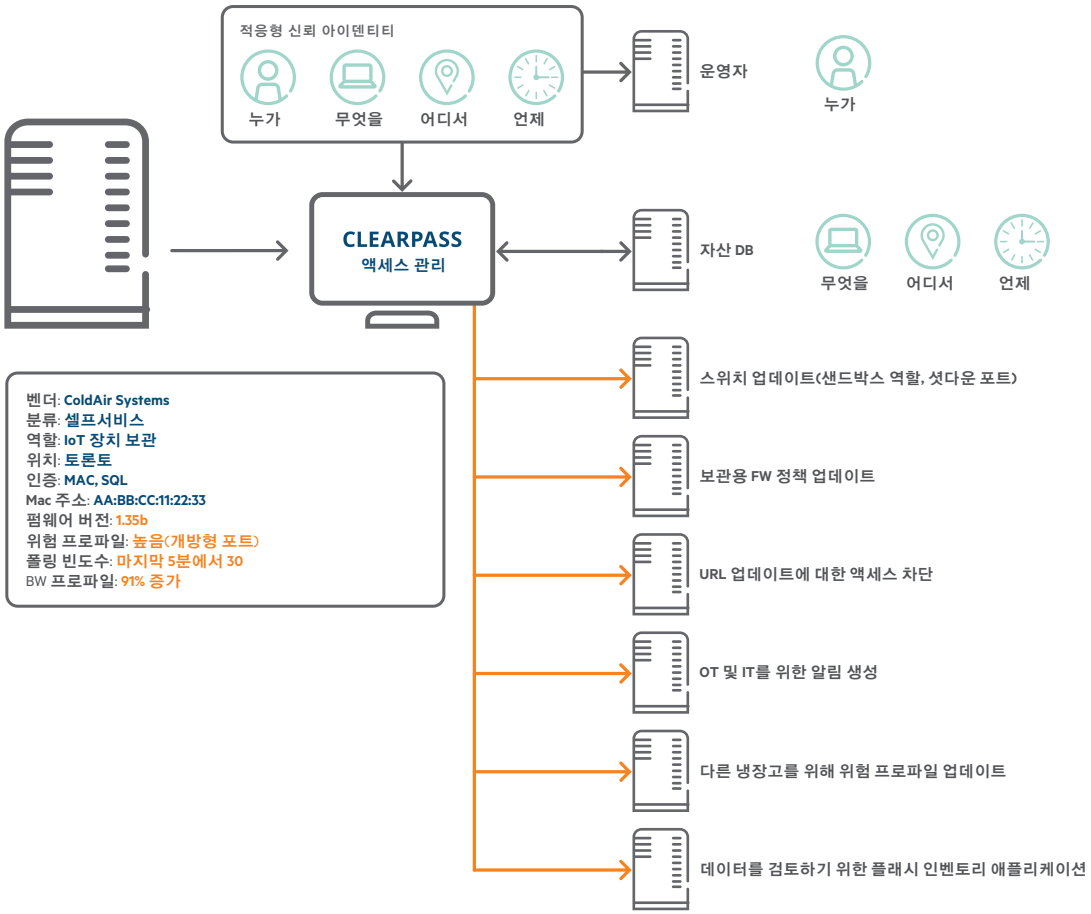


그림 5: ClearPass IoT 장치 보안 위반 워크플로우

업종별 사례: 리테일

전국구 규모의 한 리테일 업체가 다음 해에 목표 매출을 달성하기 위해서는 고객이 매장을 1회 방문할 때 구매하는 양(basket size)을 10% 늘리고 매장 이탈률을 절반으로 줄여야 합니다. 이와 같은 목표를 달성하기 위해서는 보다 몰입도 높은 고객 환경이 제공되어야 하는데, 여기에서 몇 가지 세부 목표가 도출됩니다. 첫째, 고객이 불만족을 느끼면서 매장을 나서는 일이 없도록 하려면 고객의 소비 규모에 해당하는 가격의 원하는 제품을 손쉽게 찾을 수 있어야 합니다. 둘째, 실물은 매장에서 확인하고 실제 구매는 최저가 검색을 통해 온라인에서 수행하는 고객들이 매장에서 구매까지 완료할 수 있도록 해야 합니다. 이 경우 모종의 적극적인 개입이 필요합니다. 마지막으로, 필요한 제품을 빠르게 찾지 못한 고객이 있다면 매장을 나서기 전에 재빨리 대응해야 합니다. 이를 위해서는 직원 1인당 고객 비율을 신중하게 산출해야 합니다.

고객, 직원, 재고가 모두 모바일이라는 특성을 갖기 때문에 가장 적합한 도구는 바로 백엔드 CRM, PoS, 재고 애플리케이션과 함께 작동하는 IoT 위치 기반 서비스입니다. 위치 서비스는 다음과 같은 질문에 대한 답을 제공합니다.

- "지금 내가 있는 곳은 어디인가?"
- "지금 고객이 있는 곳은 어디인가?"
- "지금 제품이 있는 곳은 어디인가?"

이러한 리테일 애플리케이션에 대해서는 다음과 같은 비즈니스 목표를 달성해야 합니다.

- 매장에 들어오는 고객의 과거 구매 행위와 웹 행위를 파악하여 고객이 지금 관심을 가질 만한 혜택을 실시간으로 제공
- 고객이 스마트폰으로 재고를 조회할 수 있도록 지원하고 구매 예산을 늘릴 수 있도록 상향 판매 기회를 극대화하는 경로를 통해 고객이 매장을 돌아다닐 때 재고가 있는 제품과 대체 제품에 대한 안내 제공
- 고객이 자유롭게 웹 서핑을 할 수 있도록 무료로 Wi-Fi 제공하여 리테일 업체는 고객이 어디에서 어떤 애플리케이션을 사용하는지 확인 가능. 예를 들어, 고객이 쇼루밍(showrooming) 행위를 할 경우 리테일 업체는 전광판을 업데이트하고 인터넷 가격을 알려주는 푸시 메시지를 전송하고 동일한 메시지가 매장 직원에게도 전송되어 고객이 매장에서 구매를 완료하도록 유도
- 모든 고객에게 서비스가 제공되도록 고객의 위치와 직원 1인당 고객 비율 모니터링

비즈니스 목표를 파악했으면 다음 단계로는 적절한 IoT 도구를 선택해야 합니다. 아래 표에는 Aruba의 다양한 IoT 위치 기반 서비스 옵션이 나와 있습니다. 솔루션 선택은 개략적인 질문에 대한 답을 찾는 것에서 시작하여 구체적인 IoT 도구 권장 사항이 도출되는 것으로 끝납니다.

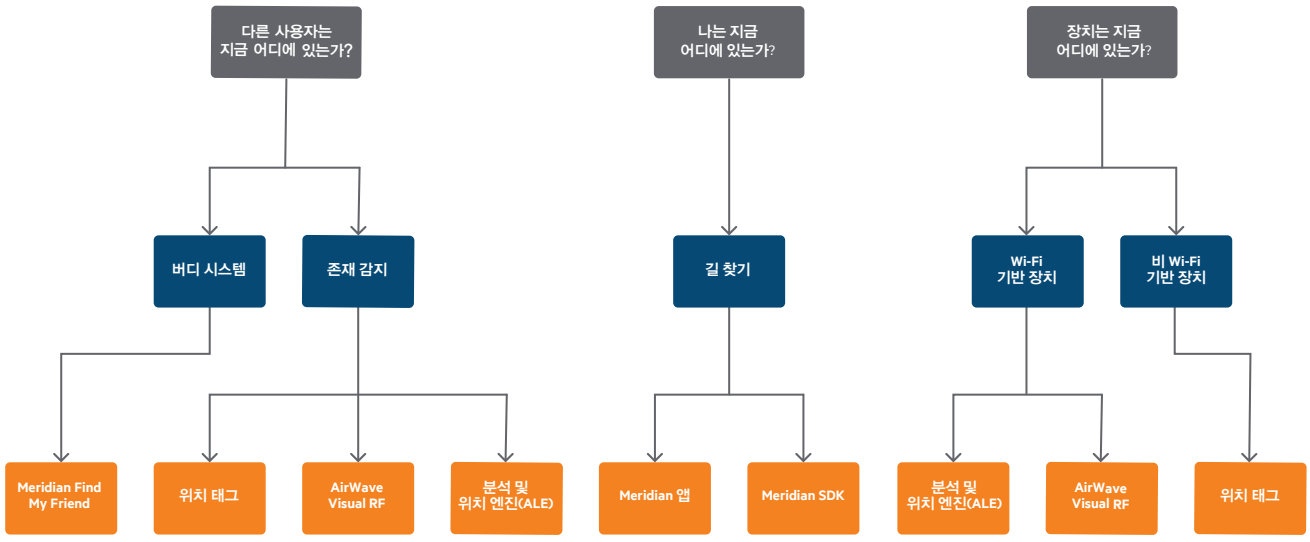


그림 6: 위치 기반 서비스 옵션

파악한 비즈니스 목표를 달성하기 위해서는 다음 네 가지 유형의 위치 도구가 필요합니다.

- 길 찾기(Wayfinding): 고객이 실내 GPS와 유사한 서비스를 사용하여 스스로 위치를 찾을 수 있도록 지원하고, 고객이 지오펜스 경계로 들어오면 알림을 제공하고, 고객에게 직접 푸시 메시지 제공
- 프레즌스(Presence): 언제 어떤 고객이 있는지, 온라인에서 무엇을 하는지, 지오펜스 경계로 들어왔는지 여부 파악
- 버디 시스템: 전체 매장에서 도움을 줄 수 있는 직원의 위치 안내
- 비Wi-Fi 기반 자산 추적: 자산, 팔레트, 상품의 위치 안내

고객의 몰입도를 극대화하기 위해서는 실시간으로 바뀌는 직접적인 상호 작용이 수반되어야 합니다. 즉, 고객의 스마트폰이나 태블릿에서 실행되며 길 찾기, 푸시 메시지, 지오펜싱 기능을 직접 제공하는 애플리케이션이 필요합니다. Aruba Meridian 서비스는 하나의 애플리케이션으로 이러한 세 가지 핵심 서비스를 모두 제공합니다. Meridian 솔루션은 실내 GPS와 유사한 길 찾기 환경을 통해 고객에게 턴바이턴(turn-by-turn) 안내를 제공하고 지도 상에 실시간 위치를 표시해 줍니다. 매장 관리자는 Meridian의 Find A Friend(친구 찾기) 기능을 사용하여 매장 내 직원들의 위치를 곧바로 파악할 수 있습니다. 또한 지오펜스 기능을 사용하여 필요에 따라 특정 동작과 애플리케이션을 실행할 수 있습니다.

Meridian은 고객 관계 관리(CRM), PoS, 기타 백엔드 애플리케이션 및 비즈니스 규칙 엔진과 인터페이스하여 복잡한 부울(Boolean) 조건 처리를 구현할 수 있습니다. 푸시 메시지 기능을 통해 즉각적인 피드백, 오퍼, 업데이트를 제공할 수 있습니다. 리테일 업체에서 자체적인 애플리케이션을 보유하고 있는 경우에는 Meridian SDK를 사용하여 해당 애플리케이션으로 이와 같은 서비스를 제공할 수 있습니다.

길 찾기에서 쇼루밍 감지로 나아가려면 고객이 Amazon과 같은 온라인 쇼핑 서비스를 사용하는 시점을 파악해야 하기 때문에 복잡한 기술이 요구됩니다. Aruba ALE(Analytics & Location Engine)는 매장에 있는 고객 중 해당 서비스에 동의했으며 Wi-Fi를 지원하는 장치를 갖고 있는 고객의 x/y 위치를 계산하고, Wi-Fi 네트워크를 통해 URL 서핑 행위를 모니터링합니다. ALE를 백엔드 분석 엔진과 함께 사용하면 고객의 쇼루밍 패턴을 파악하여 더 많은 기회를 매장 내 판매로 연결할 수 있습니다.

ALE의 x/y 모니터링 기능은 백엔드 또는 클라우드 애플리케이션과 함께 사용하여 직원 1인당 고객 비율을 모니터링할 수도 있습니다. 직원 1인당 고객 비율이 기존에 설정한 값 아래로 떨어지면 매장 관리자와 직원들에게 알림이 전송됩니다. ALE의 위치 처리 기능은 부가적인 장점도 갖고 있습니다. 즉, 매장을 지나가는 유동 인구와 매장에 유입되는 인구를 모니터링하여 지나가는 고객 중 몇 퍼센트가 매장에 들어오는지 알려줍니다.

그림 5를 보면 리테일 업체의 전략적인 목표가 비즈니스 순간으로 어떻게 연결되는지, 그리고 그러한 비즈니스 순간을 파악하기 위해 IoT 인프라와 장치 데이터가 어떤 식으로 작동하는지 알 수 있습니다. 이 예에서는 개략적인 목표에서 성공적인 비즈니스 순간을 도출하는 구체적인 IoT 도구로의 흐름을 보여줍니다.

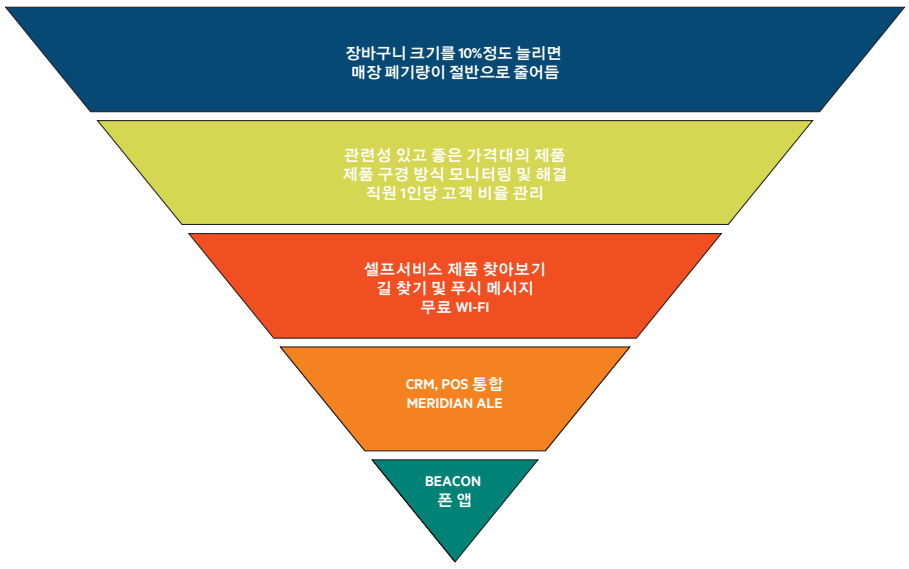


그림 7: 리테일 업체의 전략적 목표에 부합하는 IoT 인프라

목표와 도구가 합치되지 않으면 IoT 프로젝트는 방향을 잃게 됩니다. 예를 들어, 프레즌스 분석만을 사용하여 고객의 위치를 수동적으로 추적하면 고객의 행동에 대한 사후 파악만 가능합니다. 즉, 고객이 어디로 이동했는지 사후에 파악할 수는 있으나 고객의 구매 행위를 실시간으로 바꿀 수는 없습니다. 단지 기존 Wi-Fi 인프라에 구축하기 쉽다는 이유만으로 많은 프레즌스 분석 프로젝트가 진행되고 있지만, 결과적으로 프레즌스 분석을 판매로 연결할 방법이 없기 때문에 별다른 성과가 도출되지 않습니다. 여기서 얻을 수 있는 교훈은 명확합니다. IoT 프로젝트에 착수하기 전에 비즈니스 목표와 긴밀하게 합치되는 IoT 솔루션을 찾아야 합니다.

업종별 사례: 보건의료

이번에는 리테일 예에서 알아본 몇 가지 위치 기반 서비스를 사용하는 의료 분야의 예를 살펴보겠습니다. 수십 개의 병원과 클리닉을 보유한 한 관리형 의료 기관은 차기 회계연도에 부동산, 인력, 초과 근무 급여를 늘리지 않고 수익으로 이어지는 환자를 10% 늘리겠다는 목표를 세웠습니다. 환자 및 직원 만족도 설문 결과에 따르면, 현재로서도 환자-의사 대면 시간이 지나치게 낮아 진료 시간을 단축하는 것은 어려운 실정입니다. 또한 진료 예약 시간이 준수되지 않아 환자와 직원들의 불만족이 높은 상황입니다. 환자들은 병원이 커서 방문할 곳을 쉽게 찾을 수 없고, 비영어권 환자와 노약자들은 지도를 읽을 수 없으며, 진료 당일 해당 진료실이 변경되더라도 예약 알림이 업데이트되지 않아 불만을 갖고 있습니다. 한편 직원 및 의사들은 환자들이 약속된 시간에 방문하지 않아 오전 진료 예약이 준수되지 않는데 비해 오후에는 정해진 업무 시간이 초과되는 경우가 많아, 방문한 환자들이 진료를 받지 못하고 예약을 다시 해야 하는 경우가 발생하여 불만스러운 상황입니다.

이 의료 기관의 목표를 달성하기 위해서는 영어권 환자와 비영어권 환자가 모두 병원에서 쉽게 방문할 곳을 찾아 진료 예약 시간을 준수하게 함으로써 진료 지연이 발생하지 않게 해야 합니다. “지금 내가 있는 곳은 어디인가?”, “지금 고객이 있는 곳은 어디인가?”, “지금 제품이 있는 곳은 어디인가?”라는 맥락에서 위치 서비스를 고려해 보면 다음과 같은 목표가 도출됩니다.

- 고객이 예약된 진료 시간에 병원에 도착하면 예약 시간과 정확한 진료실 번호가 포함된 메시지를 고객이 선호하는 언어로 전송
- 예약 장소나 시간이 변경되는 경우 업데이트된 메시지 전송
- 고객이 들어오는 병원 정문이나 주차장 등을 고려하여 턴바이턴(turn-by-turn) 안내와 진료 예약 시간 안내
- 방문 의료진과 임시 의료진이 쉽게 길을 찾아 예약된 진료를 간편하게 수행할 수 있도록 위와 동일한 메시지와 길 찾기 기능 제공
- 환자가 늦는 경우 직원들이 전화로 안내할 수 있도록 직원들이 병원 내 환자들의 위치를 추적할 수 있는 기능 제공

위와 같은 목표를 달성하기 위해서는 다음 세 가지 범주의 도구가 필요합니다.

- 환자, 직원, 의료진이 병원 내 시설을 손쉽게 찾을 수 있도록 선호하는 언어로 안내를 제공하는 길 찾기 애플리케이션
- 환자가 병원으로 들어와 진료 예약 시스템을 사용하기 시작하면 지오펜싱이 트리거되어 환영 메시지와 함께 예약 시간 및 장소 안내
- 직원들이 예약 시간보다 늦는 환자와 방문 의료진을 추적할 수 있는 개인 추적 시스템

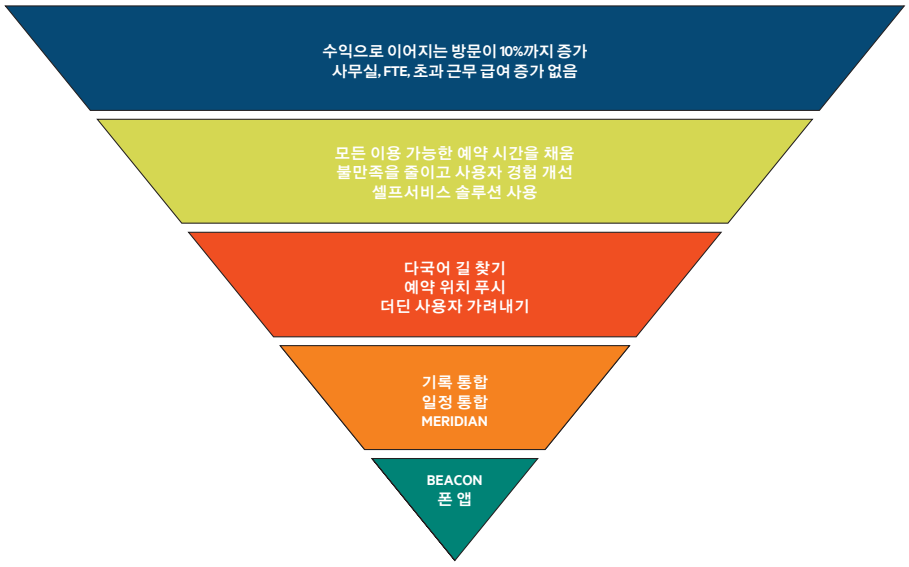


그림 8: 의료 기관의 전략적 목표에 부합하는 IoT 인프라

위에서 언급한 Aruba Meridian 서비스는 셀룰러와 Wi-Fi에서 모두 작동하기 때문에 셀룰러 및/또는 Wi-Fi가 작동하지 않는 주차장과 사각 지대에서도 서비스를 제공할 수 있습니다. Meridian은 Wi-Fi 네트워크에 종속되어 있지 않으므로 Aruba Wi-Fi 시스템과 타사 Wi-Fi 시스템에서 모두 작동합니다.

이 솔루션을 사용하려면 환자 기록, 어카운팅, 직원 개인 시스템과 연동되어야 합니다. 따라서 초기에는 많은 작업이 필요하지만 구현이 완료되면 시간 및 동작 최적화, 부동산 부지 활용, 주차장 가용 공간 알림 등의 다양한 부가가치 서비스를 제공하는 플랫폼으로 활용이 가능합니다.

이러한 목표를 수립하면 기준에 부합하지 않는 솔루션을 제공하는 벤더도 가려낼 수 있습니다. 예를 들어, 위치 서비스를 사용하여 이메일이나 문자를 제공하는 것은 실시간 길 찾기 애플리케이션에 비해 훨씬 시간이 많이 걸리고 비효율적임을 알 수 있습니다. 다중 언어로 지도를 지원하려면 초기 구성이 더 많이 필요하지만, 환자나 보호자들이 자신에게 맞는 언어를 선택할 수 있어 훨씬 효율적입니다. 실시간 업데이트가 제공되면 직원들은 예약을 더욱 효율적으로 관리하고, 최소한의 노력으로 환자들에게 길 안내를 제공할 수 있습니다.

업종별 사례: 석유 및 가스

이번에는 위치 기반 서비스와 에지 분석을 모두 사용하는 산업용 IoT의 예를 살펴보겠습니다. 25,000개의 잭 펌프와 15,000명의 계약직 직원을 보유하고 있는 한 석유가스 기업이 차기 회계연도에 생산량을 그대로 유지하면서 펌프 중단 시간을 10%, 직원 급여를 10% 줄이고, 예비 부품 사용량을 25% 줄이겠다는 목표를 갖고 있습니다. 이 기업은 이론상의 펌프 장애율에 맞춰 펌프 가동 일정을 계획했지만, 결과는 효율적이지 못했습니다. 그 결과 펌프 중단이 빈번하게 발생하여 생산량 매출 감소로 이어졌습니다. 뿐만 아니라 펌프 예비 부품 및 파이프가 분실 또는 도난되어 비용이 증가하고 장비의 적기 수리가 지연되었습니다. 재고 유출의 책임이 누구에게 있는지 정확히 파악되지 않고 있으며, 도난이 문제인지 잘못된 기록이 문제인지 여부도 알 수 없는 상황입니다. 마지막으로 하청업체 송장을 실제 작업량에 맞추는 작업도 무척 까다롭습니다. 계약직 직원이 너무 많은데다 회계 담당자의 수가 충분하지 않기 때문입니다.

이 기업이 목표를 달성하려면 실시간으로 펌프를 모니터링하고 비정상 가동에 대한 관찰을 바탕으로 장애를 예측할 수 있어야 합니다. 펌프는 국지적인 폐쇄 회로 제어로 연결되는 센서 및 액추에이터로 가동되는데, 이로부터 유용한 통찰력을 이끌어낼 수 있는 데이터 마이닝이 실행되지 않고 있습니다. 가동 중인 펌프가 너무 많고 전 영역을 포괄하는 셀룰러 네트워크의 비용이 가변적이기 때문에, 모든 펌프 데이터를 원격 분석 시스템으로 전송하는 데 소요되는 비용이 너무 큽니다. 그 대신 잭 펌프에서 로컬로 분석을 실행하고 비정상 작동이 감지된 경우에만 모니터링 센터로 알림을 제공하는 것이 훨씬 경제적입니다. 이 경우 펌프 현장에 센서 데이터가 보관되어 있다는 가정 하에 모니터링 센터에서는 추가적인 센서 데이터를 요청하면 됩니다. 또한 과거의 가동 데이터를 기준으로 펌프 제조사 데이터베이스를 분석하여 비정상 작동에 어떻게 대처하는 것이 가장 좋은지 판단할 수 있어야 합니다.

계약직 직원들이 현장과 물류장에 도착하고 떠나는 시간을 추적하고 이를 어카운팅 애플리케이션에 공유하면 청구 금액과 실제 작업 시간을 직접 비교할 수 있습니다. 수동 프로세스로 인한 추가적인 노동 비용이 발생하지 않도록 보고 작업 방식도 자동화되어야 합니다. 서비스에 대한 급여를 지급받으려면 모든 계약직 직원이 참여해야 한다는 계약 변경 사항도 필요합니다.

현장에서 계약직 직원을 모니터링하는 추적 솔루션을 물류장에서도 사용할 수 있습니다. 위치 데이터를 액세스 제어 및 CCTV 솔루션으로 공유하면 사이트에 출근한 계약직 직원이 누구인지 파악하여 재고가 누락된 경우 의심되는 사람이 누구인지 알 수 있게 됩니다.

이 기업의 비즈니스 목표는 다음과 같습니다.

- 잭 펌프가 잭 펌프 제어 시스템에서 생성된 아날로그 및 디지털 데이터를 처리하고 비정상 작동을 보고하도록 설정
- 전체 현장의 데이터 수집 시스템을 관리하고, 펌프 데이터에 대한 메타 분석을 수행하고, 과거의 장애 데이터를 예측형 분석 애플리케이션에 통합하는 원격 모니터링 센터 구축
- 펌프 현장이나 물류장에 도착하거나 이를 벗어날 때마다 위치가 보고되도록 모든 계약직 직원이 위치 서비스 애플리케이션을 탑재하도록 의무화. 정규 직원이 아닌 계약직 직원이므로 개인 정보를 보호하기 위해 애플리케이션은 해당 기업의 시설에 도착하거나 시설을 벗어나는 경우에만 작동해야 함(상시 가동형 GPS 추적 시스템은 사용할 수 없음)

위와 같은 목표를 달성하기 위해서는 다음과 같은 몇 가지 범주의 도구가 필요합니다.

- 잭 펌프로부터 센서 및 액추에이터 데이터를 수집하고, 데이터를 처리하는 분석 애플리케이션을 실행하고, 처리 결과를 원격 모니터링 센터로 전송하는 WAN을 제공하는 게이트웨이
- WAN을 관리하고, 집계 데이터를 바탕으로 자체적으로 분석을 실시하고, 서비스 기록이나 제조업체 데이터베이스 등과 같은 기타 데이터 리포지토리와 인터페이스되는 원격 모니터링 시스템
- 직원들이 펌프 현장과 물류장에 도착하거나 여기에서 벗어나면 직원 스마트폰 또는 태블릿에서 애플리케이션을 트리거하는 지오펜스
- 직원들이 현장에 도착하거나 현장에서 벗어날 때 직원 ID 데이터와 날짜/시간이 전송되는 액세스 제어 및 비디오 감시 애플리케이션과의 인터페이스. 특정 시설에 대한 액세스 권한이 없는 직원이 액세스를 시도하는 경우 액세스 제어 시스템에서 액세스 차단

예측형 장애 감지 시스템에는 다양하게 조합하여 여러 가지 구현 요구 사항을 충족시킬 수 있는 몇 가지 기본적인 구성 요소가 필요합니다. 이러한 구성 요소로는 IoT 지능형 IoT 장치, 액세스 장치, 통신 매체, IoT 컨트롤러, IoT 비즈니스 및 분석 애플리케이션, 시스템 관리 도구 등이 있습니다.

이 경우 기업이 파악해야 하는 아날로그, 디지털 및/또는 제어 네트워크 데이터를 생성하는 잭 펌프가 지능형 IoT 장치가 됩니다. 액세스 장치는 IoT 장치와 인터페이스 역할을 수행하고, 데이터를 제공하고, 로컬에서 조치를 취하거나, 원격 모니터링 사이트에 있는 IoT 컨트롤러로 데이터를 전송합니다.

액세스 장치에는 게이트웨이와 컨버지드 IoT 시스템이 있습니다. 게이트웨이는 IoT 장치에서 생성된 데이터 스트림을 사용 중인 네트워크와 호환되는 안전한 형식으로 변환합니다. 게이트웨이는 IoT 장치가 네트워크(LAN, 셀룰러, Wi-Fi)와 안전하게 통신할 수 없거나, 보안 원격 액세스를 위한 로컬 VPN 클라이언트를 실행할 수 없거나, WAN과 호환되지 않는 직렬, 아날로그 또는 독점적 입출력(I/O) 프로토콜이 적용되어 있는 경우 사용됩니다.

그림 10: Aruba Edgeline 게이트웨이 액세스 장치

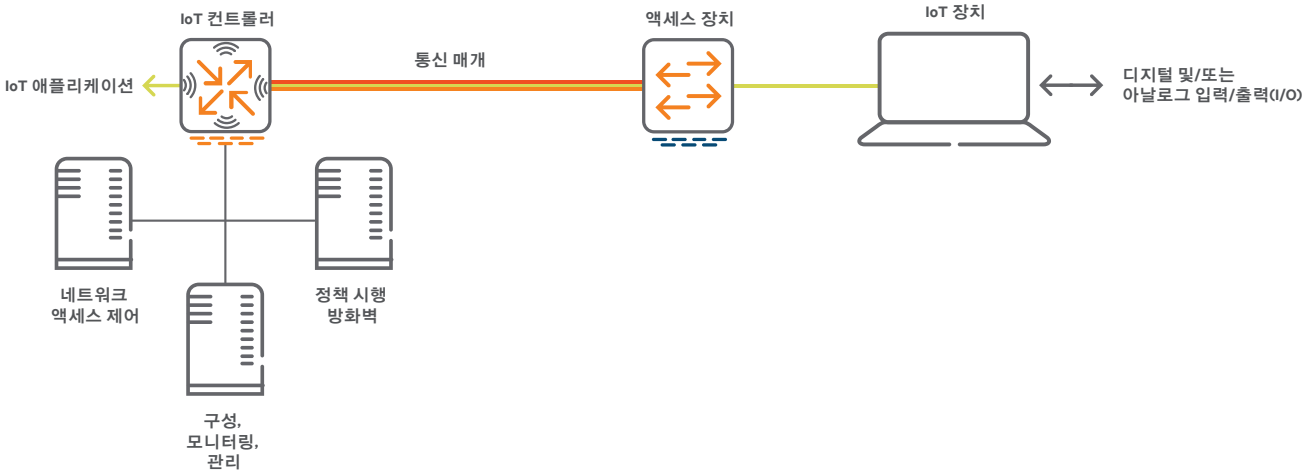


그림 9: 예측형 장애 모니터링 구성 요소

컨버지드 IoT 장치는 IoT 장치에서 생성된 데이터를 로컬로 처리하는 데 필요한 I/O 인터페이스와 컴퓨팅 기능을 갖추고 있습니다. 이 솔루션은 처리 지연 시간을 줄이고, 전역 데이터 통신 트래픽의 양을 줄이고, 로컬 IoT 활동을 처리 및 저장하고, 원격 데이터 센터에 로컬 IoT 활동에 대한 요약을 전송하는 데 사용됩니다. 컨버지드 IoT 장치는 로컬에서 머신 러닝 및 데이터 분석 엔진을 실행하여 이러한 작업을 수행하며 강력한 컴퓨팅 엔진, 아날로그/디지털 센서 데이터와 제어 버스 트래픽 입력 기능, 원격 관리 기능을 구비하고 있습니다.

그림 11: Aruba 컨버지드 IoT 시스템 액세스 장치

이 석유가스 기업의 경우 WAN 비용을 최소화하기 위해 로컬 인사이트가 필요하므로 컨버지드 IoT 시스템이 보다 적합한 액세스 장치입니다. 이 시스템은 통신 매체로서 셀룰러 텔레포니를 사용하여 구축 시간을 단축하는 데, 셀룰러 시스템은 단일 타워가 중단되는 경우 높은 복원력을 보여주기 때문입니다.

셀룰러 비용은 기계 모니터링 애플리케이션 등 낮은 대역폭의 IoT 애플리케이션에 대해 사전 합의를 바탕으로 가입 비용이 경제적인 Hewlett Packard Enterprise의 MVNO(Mobile Virtual Network Operator) 서비스를 통해 대폭 줄일 수 있습니다. 컨버지드 IoT 시스템과 분석 소프트웨어를 사용하여 현장에서 IoT 데이터를 사전 처리하게 되면 셀룰러 통신 트래픽과 비용을 대폭 줄일 수 있습니다.

Aruba의 VIA VPN은 잭 펌프와 모니터링 센터 사이의 데이터를 암호화 및 터널링합니다. VIA는 AES 256+비트 키 암호화를 지원하며 네트워크 수준 피어 인증(network-level peer authentication), 데이터 발신 인증(data origin authentication), 데이터 무결성 및 재생 보호를 제공합니다. 정부 기관용 IoT 애플리케이션의 경우 VIA는 Suite B 타원형 암호화와 함께 제공되어 일급 기밀 정보까지 안전하게 보호합니다.

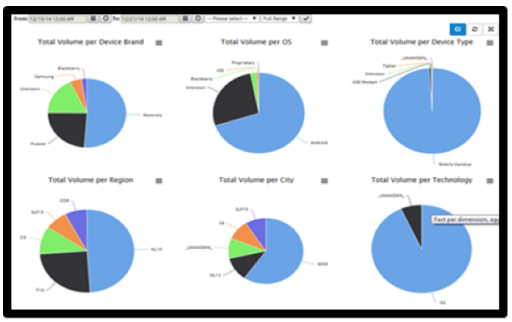
VIA VPN은 이 석유가스 기업 데이터 센터의 IoT 컨트롤러에서 중단됩니다. 컨트롤러는 네트워크 암호화와 인증을 관리하며 방화벽, 네트워크 액세스 제어, 그리고 애플리케이션 레이어 보안/패킷 우선 순위/액세스 규칙을 적용하는 정책 관리 애플리케이션과 인터페이스됩니다. 프라이빗 및 퍼블릭 클라우드 애플리케이션의 하드웨어 컨트롤러 대신 컨트롤러 소프트웨어 인스턴스를 사용할 수 있습니다.

그림 12: Aruba 컨트롤러

분석 애플리케이션은 컨버지드 IoT 시스템과 모니터링 시스템에서 모두 실행됩니다. 분석 애플리케이션은 IoT 데이터를 바탕으로 수학, 통계, 머신 러닝 및/또는 예측형 모델링을 사용하여 비정상 작동을 표시하고 펌프 벤더, 내부 서비스 기록, 심지어는 다른 회사의 사이트에서 생성된 데이터 풀을 마이닝하여 장애를 예측합니다. 이와 같은 애플리케이션에는 HPE Vertica, SAP HANA, GE Predix, Schneider Wonderware가 있습니다.

잭 펌프 사이트는 다양한 IoT 장치 모니터링 전용 서비스로 구성되는 강력한 애플리케이션 제품군인 HPE의 UIoT(Universal IoT) Platform 애플리케이션으로 모니터링됩니다. 이러한 서비스에는 다음과 같은 내용이 포함됩니다.

- 클라이언트 애플리케이션에서 데이터를 사용할 수 있도록 지원되는 API
- 신규 애플리케이션, 마이크로 서비스 및 알고리즘을 신속하게 도입할 수 있도록 지원하는 디지털 서비스
- Aruba 게이트웨이와 컨버지드 IoT 플랫폼에서 생성되는 데이터 수집 및 오픈 소스 메시지 중개를 통한 IoT 프로토콜
- 셀룰러 인터페이스 관리
- 사전 구성된 알고리즘과 즉시 사용할 수 있는 템플릿이 제공되는 강력한 예측형 분석
- oneM2M 또는 동급 데이터 구조 표준 준수/일반적으로 사용되는 제어 프로토콜을 위한 내장 프로토콜 라이브러리
- 장치 및 가입 관리를 비롯해 개방형 표준 메시징 버스를 통한 메시지 큐



FEATURES	CORE BASELINE	OPTION	MODULE
Managing devices and services	Yes		DSM
Uplink and downlink data acquisition	Yes		NIP
Data acquisition and validation	Yes		DAV
APIs exposure	Yes		SGF PRM
Advanced dashboard	Yes		Console
Relational database	Yes		EDB
Dashboard designer		Yes	Console designer
Analytic columnar database		Yes	Vertica
Alarms handling and correlation		Yes	TeMIP/UCA
Micro service design and execution		Yes	SIS

그림 13: UIoT IoT 장치 모니터링 시스템

UIoT는 oneM2M 업계 표준에 맞게 IoT 장치에 대한 지원을 제공하며, 동시에 다양한 IoT 애플리케이션 및 프로세스를 지원합니다. 동일한 프라이빗 또는 하이브리드 클라우드 플랫폼의 장치 검색, 구성, (기존 음성 및 데이터 트래픽에 더해) IoT 트래픽 제어 등 신규 애플리케이션이 대규모로 신속하게 실행될 수 있습니다.

UIoT는 Meridian 플랫폼과 마찬가지로 기존의 전략적 목표를 달성하는 데 필요한 서비스이며, 다양한 부가가치 서비스의 기반으로 작동합니다. UIoT는 지상 모바일 텔레매틱스 애플리케이션을 지원하고 LoRa 및 Sigfox 장거리 무선 시스템과 인터페이스되며 기타 모니터링, 보고, 감사 애플리케이션과의 인터페이스를 지원하는 다양한 API를 갖추고 있습니다.

Aruba의 Meridian 지오펜싱 및 푸시 메시지 서비스를 통해 직원들에 대한 위치 서비스가 제공됩니다. 잭 펌프 현장과 물류장에 Aruba BLE Beacon을 구현하면 펌프 서비스 및 저장 공간 경계에 지오펜스가 적용됩니다. 지오펜스의 규모는 각 현장에 따라 달라집니다. 직원의 스마트폰이나 태블릿이 지오펜스를 넘나드는 순간, 어카운팅 애플리케이션으로 지오펜스 트리거의 신원, 시간 및 위치가 푸시됩니다. Meridian에서 해당 활동을 정확하게 기록했다는 메시지가 해당 직원에게도 푸시될 수 있습니다. 작업에 대한 급여를 지급받기 위해서는 각 직원이 Meridian 애플리케이션을 사용하도록 강제함으로써 해당 기업은 컴플라이언스를 제대로 준수할 수 있습니다.

Meridian에는 위치 데이터를 어카운팅, 액세스 제어, 비디오 감시 워크플로우 등의 다른 애플리케이션과 공유할 수 있는 API도 포함되어 있습니다. 따라서 잭 펌프에서 사용되는 동일한 비콘(Beacon)과 애플리케이션을 물류장에서 보안 시스템을 트리거하는 데도 사용하여 물류의 도착과 출발 작업을 카드 액세스 및 비디오 감시 데이터와 연동할 수 있게 됩니다. 특정 직원의 활동으로 인해 재고가 감소된다는 사실이 감지되면 해당 직원의 신원이 보안 기록의 주요 구성 요소로 기록됩니다.

이 예에서는 석유가스 기업이 펌프 가동 시간, 계약직 직원의 비용 관리, 재고 유출 감소라는 개략적인 목표에 따라 이러한 목표를 달성하기 위한 구체적인 분석, 보고 및 위치 기반 서비스 IoT 도구를 도출하는 방법을 살펴보았습니다.

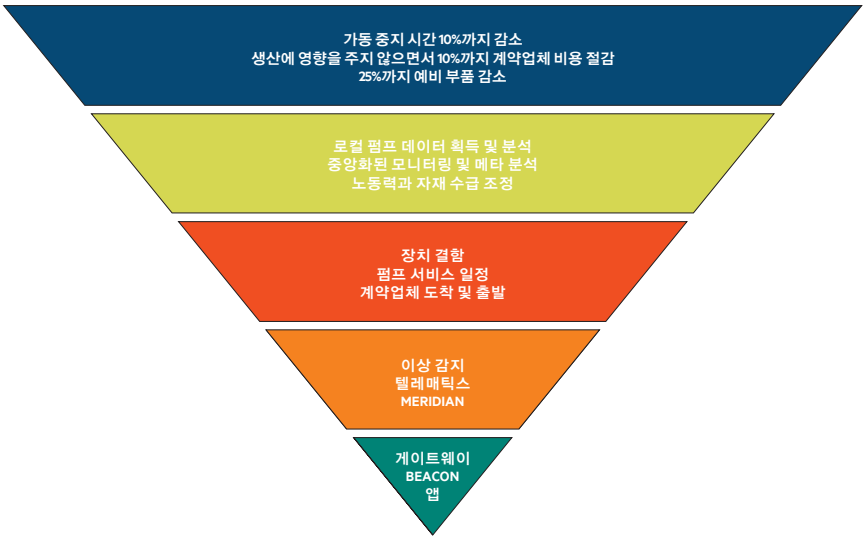


그림 14: 석유가스 기업의 전략적 목표에 부합하는 IoT 인프라

IoT 전환 여정의 첫 번째 단계

IoT 도구는 미래의 비즈니스 목표를 달성하는 플랫폼으로 기능하기 위해 확장성을 갖추어야 합니다. 위에서 살펴본 세 가지 사례에서 Aruba와 UIoT 솔루션은 다양한 사용 사례에 따라 뛰어난 확장성을 보여줍니다.

비즈니스 목표와 IoT 아키텍처 사이에 다리 놓기라는 기술적인 과제는 조직 내의 목표 합치라는 정치적인 난관보다 상대적으로 쉽게 극복될 수 있습니다. 기존의 목표와 진행 중인 프로젝트는 전략적인 목표와 비즈니스 목표를 다른 방식으로 해석하여 서로 경합하게 될 수 있습니다. 각 사업부의 관계자들은 프로젝트 및 목표에 대한 주도권을 쟁취하기 위해 싸우는 과정에서 자신의 비전이 추구되지 않는 경우 자금과 지원을 제공하지 않겠다고 협박하는 경우도 발생할 수 있습니다.

경영, 제품, 엔지니어링, IT, 운영 조직 사이에서 고도의 협업을 실시하기 위해서는 중립적인 제3자의 개입이 필요할 수 있습니다. HPE의 기술 서비스 컨설팅 조직은 이를 위해 IoT 프로젝트에 대한 통합적인 비전을 정의하고, 주요 관계자들 사이에서 합치된 의견을 도출하고, 전략적인 목표와 성공을 가려내기 위해 설계된 IoT 워크샵을 준비했습니다. 자세한 내용은 https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-7269ENW.pdf를 참조하십시오.

결론

IoT의 중대한 목표는 바로 기업의 전략적 목표와 관련성 있는 IoT 컨텍스트 및 데이터를 융합하여 성공적인 비즈니스 순간을 도출하는 것입니다. 성공적인 비즈니스 순간은 빠르게 지나가는 고객 관련 기회를 동적으로 활용할 수 있도록 신중하게 조율되어야 합니다. 고객의 행동, 태도 및/또는 감성을 기업에게 유리한 방향으로 변화시키기 위해서는 IoT 컨텍스트 및 데이터가 중요한 역할을 수행해야 합니다.

이를 위해서는 IoT 컨텍스트 및 데이터에서 IoT 아키텍처에 이르는 일련의 사슬이 제대로 가동되어야 합니다. 본 백서에서는 IoT 구조의 각 요소 사이에 효율적으로 다리를 놓고, IoT 장치로부터 관련성 있는 컨텍스트와 데이터를 추출하고, 이를 활용하기 위한 효율적인 아키텍처를 구현하는 방법에 대해 설명했습니다. 신중한 준비, 목표의 정의, 그리고 효율적인 도구의 선정과 더불어 조직의 목표에 대한 합의가 도출되면 크나큰 성과를 이룰 수 있습니다. 그리고 그 결과 까다로운 비즈니스 목표를 달성할 수 있게 됩니다.

참조 자료

1. William H. Markle, “The Manufacturing Manager’s Skills”, The Manufacturing Man and His Job, Robert E. Finley and Henry R. Ziobro, American Management Association, Inc., New York 1966
2. C. R. Jaccard, “Objectives and Philosophy of Public Affairs Education”, Increasing Understanding of Public Problems and Policies: A Group Study of Four Topics in the Farm Foundation, Chicago, Illinois 1956
3. Alfonso Velosa, W. Roy Schulte, Benoit J. Lheureux, Hype Cycle for the Internet of Things, 2016, Gartner, 2016년 7월 14일
4. 비즈니스 순간은 사전에 결정된 결과가 아닌, 합의된 결과를 도출하는 사람, 비즈니스, 사물 사이에 빠르게 변화하는 컨텍스트 기반 상호 작용을 가리킵니다(예: 위치, 시간, CRM 데이터를 바탕으로 리테일 업체가 제공하는 맞춤형 혜택). Frank Buytendijk, Digital Connectivism Tenet 4: We Do Not Differentiate Between People and Things, Gartner, 1 2016년 11월 참고.
5. Dale Kutnick, Saul Brand, Exploit Enterprise Architecture to Guide IoT Deployments at Scale, Gartner, 2016년 12월 15일

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | 전화: 1.408.227.4500 | 팩스: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com WP_InternetOfRelevantThings_011817