◆People- centric

## ■ Hyperautomation(초자동화)

다수의 머신러닝, 패키징 된 소프트웨어, 자동화 툴을 결합시켜 업무를 수행하는 것이다.

초 자동화는 감지, 분석, 설계, 자동화, 측정, 모니터링, 재평가 등을 포함하는 자동화 자체의 모든 단계를 아우르는 개념이다.

현재 RPA, IBPMS, 디지털트윈 등이 대표적이다.

## ■ Multiexperience(다중 경험)

사용자 경험은 2028년까지 디지털 세상에 대한 사용자들의 인식, 상호 작용 방식에 있어 VR,AR,MR 등을 통해 크게 변화할 것이다. 가트너의 부사장은 "사람이 기술을 이해해야 했던 모델에서 기술이 사람을 이해하는 모델로 변화할 것”이라며, “따라서 의도를 파악해야 하는 역할은 사용자에서 컴퓨터로 넘어갈 것"이라고 말했다. 이어 "다양한 인간적 감각을 활용해 사용자들과 소통하는 능력은 모호한 정보를 전달하는 데 있어 보다 풍부한 경험을 제공할 것"이라고 덧붙였다.

## ■ Democratization(전문성의 민주화)

전문적인 교육 없이도 광범위한 영역에서 비즈니스 프로세스, 경제 분석 등 전문 분야에 접근 가능한것을 말한다.

가트너는 2023년까지 민주화의 4가지 핵심 요소가 가속화될 것으로 예상했다. 데이터 및 분석의 민주화, 개발의 민주화, 설계의 민주화, 지식의 민주화가 이에 해당한다.

## ■ Human Augmentation(인간 증강)

인간 증강은 기술이 어떻게 인간의 인식과 신체의 향상을 제공할 수 있는지를 탐구한다.

과거에 안경, 보청기, 임플란트 등이 인간의 능력을 보완시켰다면, 향후에는 새로운 기술, 제품들이 인간의 능력을 강화하며 새로운 기회를 창출할 전망이다.

## ■ Transparency and Tracebility(투명성 및 추적성)

많은 소비자가 개인 정보의 가치를 인식하고, 이에대한 통제를 요구한다. 기업들은 정보 관리의 위험이 증가하고 있음을 자각하고 있으며, 정부는 이를 확실히 하기위해 규제를 시행하고있다.

기업들은 투명성과 신뢰 관행을 구축하면서 인공지능 및 머신러닝 영역, 개인 데이터 보호, 소유 및 제어 영역, 윤리적 설계의 영역 등 세 가지 영역에 초점을 맞춰야 한다.

◆Smart spaces

## ■ Empowered Edge(자율권을 가진 엣지)

엣지 컴퓨팅은 소비자 디바이스 가까운 곳에 정보소스, 저장소를 배치하여 정보를 처리하고 콘텐츠를 수집 전달하는 토폴로지다.

점점 정교하고 전문화된 컴퓨팅 리소스와 데이터 스토리지로 엣지 컴퓨팅이 강화되면서 폭넓은 사업에 중요 요소로 자리매김 하고 있다.

신속한 데이터 처리와 소통이 필요한 로봇, 드론, 자율주행 자동차 등에서 확산중이다.

## ■ Distributed Cloud(분산형 클라우드)

퍼블릭 클라우드 서비스가 다양한 장소에 배포되는 것이다. 외부에서 서비스를 제공하지만 운영, 유지관리 및 업데이트 등은 여전히 퍼블릭 클라우드 제공 업체의 소관이다.

대부분의 퍼블릭 클라우드 서비스의 중앙화 모델에 상당한 변화를 주며, 새로운 클라우드 컴퓨팅 시대를 견인할 것이다.

## ■ Autonomous Things(자율 사물)

인간이 수행하던 기능들을 자동화 하는 데 AI를 활용하는 디바이스다. 대부분 로봇, 드론, 자율주행차, 자율행선, 가전제품등의 형태로 구현된다. 이는 엄격한 프로그래밍 모델들이 제공하는 자동화를 뛰어넘는 수준으로, AI를 활용하여 주변 환경 및 사람들과 자연스럽게 상호 작용하는 고급 행동을 구사한다.

## ■ Practical Blockchain(실용적 블록체인)

신뢰 구축, 투명성 제공, 비즈니스 생태계 간 가치 교환 구현, 잠재적 비용 절감, 거래 합의 시간 단축, 현금 흐름 개선 등을 통해 산업을 재구성할 수 있는 잠재력을 가진 기술이다. 자신의 출처를 추적할 수 있기 때문에 위조품 사기의 가능성이 낮아진다. 식품관리, 신원확인, 등 여러 분야에서 혁신및 잠재력을 가지고 있기 때문에 기업들은 빠른 시일 내에 블록체인 기술을 도입하지는 않더라도, 기술에 대해 검토하기 시작해야한다.

## ■ Ai Security(인공지능 보안)

초연결 스마트 공간에서 사이버 공격 노출이 증가하면서 AI기반 시스템과 프로세스 역할이 증가할 것이다. 보안 및 위기관리를 위해 AI 기반 시스템 보호, AI를 활용한 보안 방어 향상, 공격자의 범죄 목적AI 사용 예측 등 주요 영역에 초점을 맞춰야 한다.