McKinsey & Company

IoT & Smart Cities

December, 2020

BOSTON COLLEGE
Woods College of Advancing Studies

Bill Corrigan

Expert AP, Leap & IoT
bill_corrigan@mckinsey.com

Introduction

- Bill is a member of the McKinsey IoT leadership team and McKinsey Leap™ digital business building practice, leading the firm's global efforts on Smart Building and Smart City technologies.

Recent McKinsey Studies

Developing combined IoT + CMP platform for telecom operator

IoT / SaaS product launch for $22B security & tools vendor

IoT/SaaS Product Development for Aerospace & Defense Irvine, CA

IoT technologies for Smart City and Smart Building infrastructure

IoT / Drone / SaaS military base modernization

Digital transformation for global retailer, Dallas, TX

Smart City Strategy for major cloud computing software company

Smart Building - advising global real estate clients on smart building technologies and Covid response / return-to-work

Prior Industry Experience

Microsoft

SharkNinja

Living PlanIT

Agenda

IoT – what is it & why is it important

Smart Cities

Cyber security considerations for IoT / Smart Cities

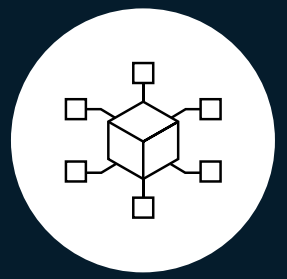
What is IoT?

Sensors and connected devices

+

Software, data, and analytics

=



Improved products, services, operations, and business models

The complete IoT stack is comprised of hardware, software, cloud and analytics

Platform

Layer		IoT industrial automation stack
Enterprise and design (firm level, incl. suppliers)	Cloud	Cloud applications
		IoT/cloud platform
Operations mgmt. (factory level)	"Local" software	Applications
		System solutions
		Connectivity
Control and supervision (line level)	Embedded	Security
		Embedded software
Field (machine level)		Smart Sensors
		Machines/ Hardware

Tech stack		Stack components						
SW infra-structure & apps	Apps	Enterprise & consumer apps	App store	Self-service portal / UI				
		Analytics and visualization	Data orchestration	Hadoop	Machine learning	Rules engine		
	Cloud infra-structure	Data processing	Protocol normalization	Data caching / storing	Data validation	Data logging		
		Data storage	Relational DB	Non-relational DB	Operational data stores	Data backup & DWH	Data indexing	Orchestration & security
	Enablement platform	API management	API publishing and discovery	Tokenization / authentication	API analytics / reporting	Developer tools/ portal		
		App engine	SDK	Search & query	User authentication	Blob management	Algorithms engine	
		Device mgmt	Registration and Pwd mgt	Policy mgt. & Key rotation	Authentication	Log tracking	Configuration mgt	Patching/ Updates
Connectivity		Backhaul	2G/3G/4G/5G LTE	LTE-U	Wired			
		Local	Wifi	BT	NFC	802.15.4 (Zigbee)	Infrared	DSRC
Security		Endpoint protection & IAM	Threat detection	Identity & access mgmt	Anti-virus			
Hardware (and embedded software)		Devices/Packaging						
		On-device software	SDK (incl. libs. message bus)	HDK	RTOS	Firmware, drivers	OS	API
		Board-level components	Processors	Sensors / AFE	Modem	Secure boot loader	Data caching / storing	Actuators

Platform can be hosted on premise, as company-internal service or by 3rd party

We estimate annual impact potential for IoT in 2030 of $6-13 trillion

Cross-sector view of annual potential impact year in 2030

Vehicles
Infotainment, autonomous vehicles and condition-based maintenance
$400-600B

Home
chore automation and security
$400-800B

Cities
public health, safety, transportation
$1.0-1.8T

Offices
security, energy, contact tracing, safety
$200-500B

Outside
logistics and navigation
$600B-1.4T

Factories
Operations, SCO, equipment PDM,
$1.4-3.3T

Human
health and fitness
$800B-1.8T

Retail environments
automated shopping, customized UX
$400-900B

Worksites
operations optimization, health and safety
$400B-1.7T

Impact of

$6-13

trillion by 2030

** Source: McKinsey Global Institute research – summer, 2020*

Examples are not exhaustive

Agenda

IoT – what is it & why is it important

Smart Cities

Cyber security considerations for IoT / Smart Cities

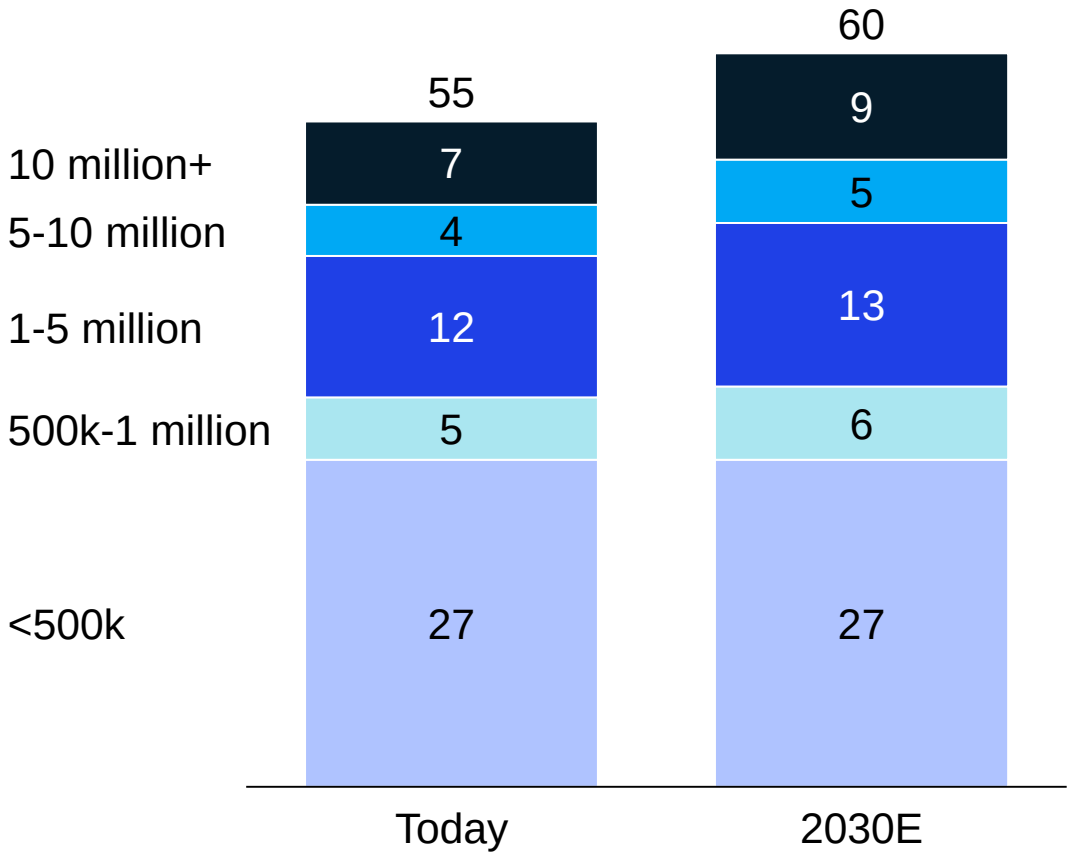
Arundhati Roy
Financial Times
April 2020

Historically, pandemics have forced humans to break with the past and imagine their world anew. This one is no different. **It is a portal, a gateway between one world and the next.**

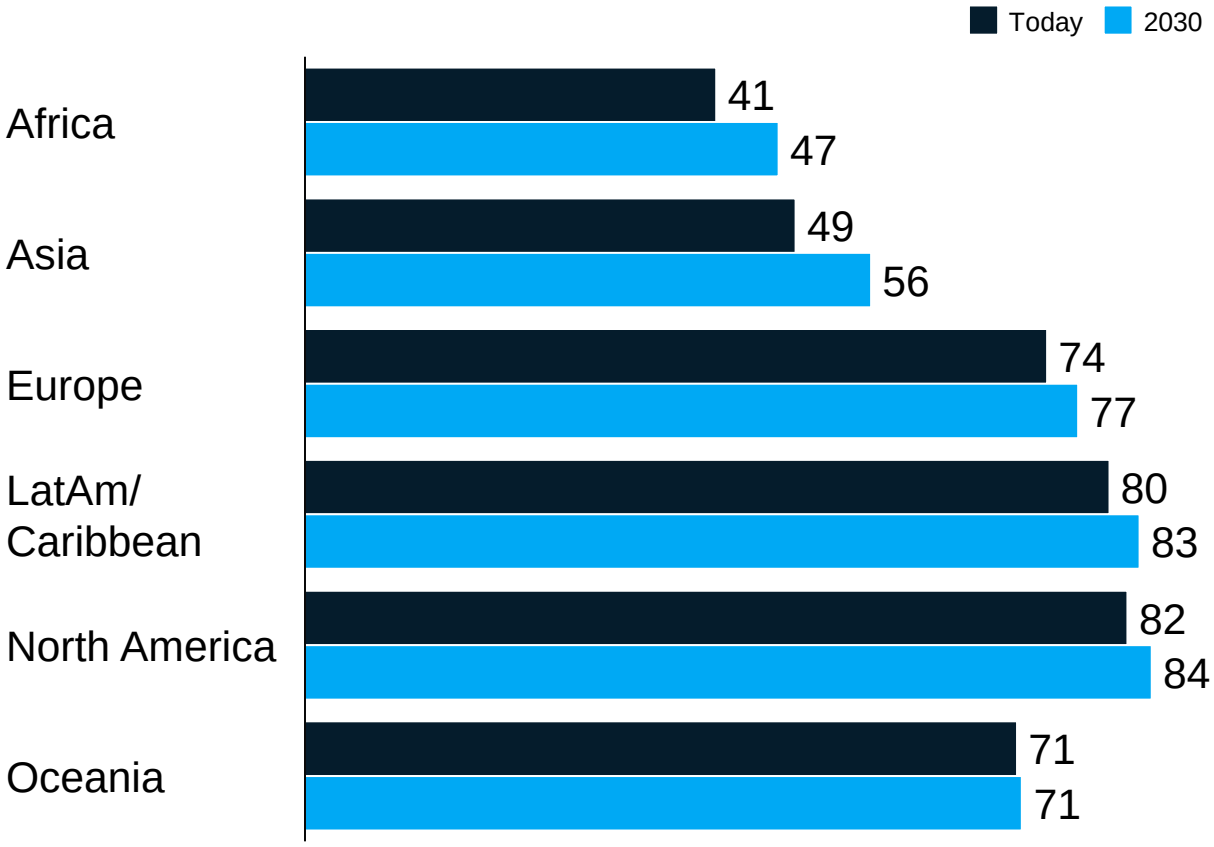
We can choose to walk through it, dragging the carcasses of our prejudice and hatred, our avarice, our data banks and dead ideas, our dead rivers and smoky skies behind us. Or we can walk through lightly, with little luggage, **ready to imagine another world. And ready to fight for it.**

Urban population is projected to grow rapidly, especially in 10M+ cities

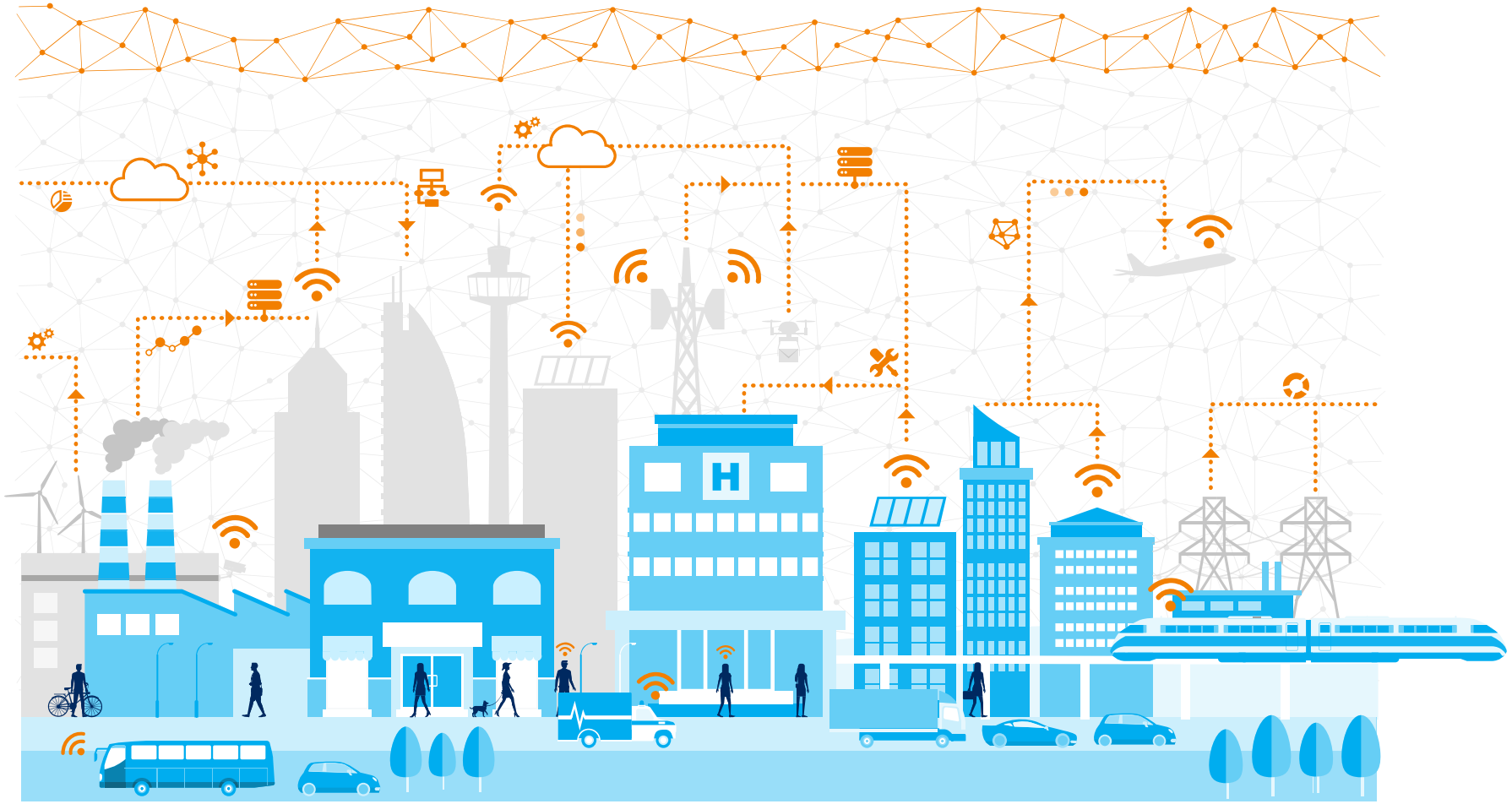
% Total world population in cities



% Population residing in urban areas by region



We define a smart city as one in which different actors use digital technology to solve public problems and achieve higher quality of life



Intelligence Layer
supporting enhanced decision making

Adoption: Changes in behavior

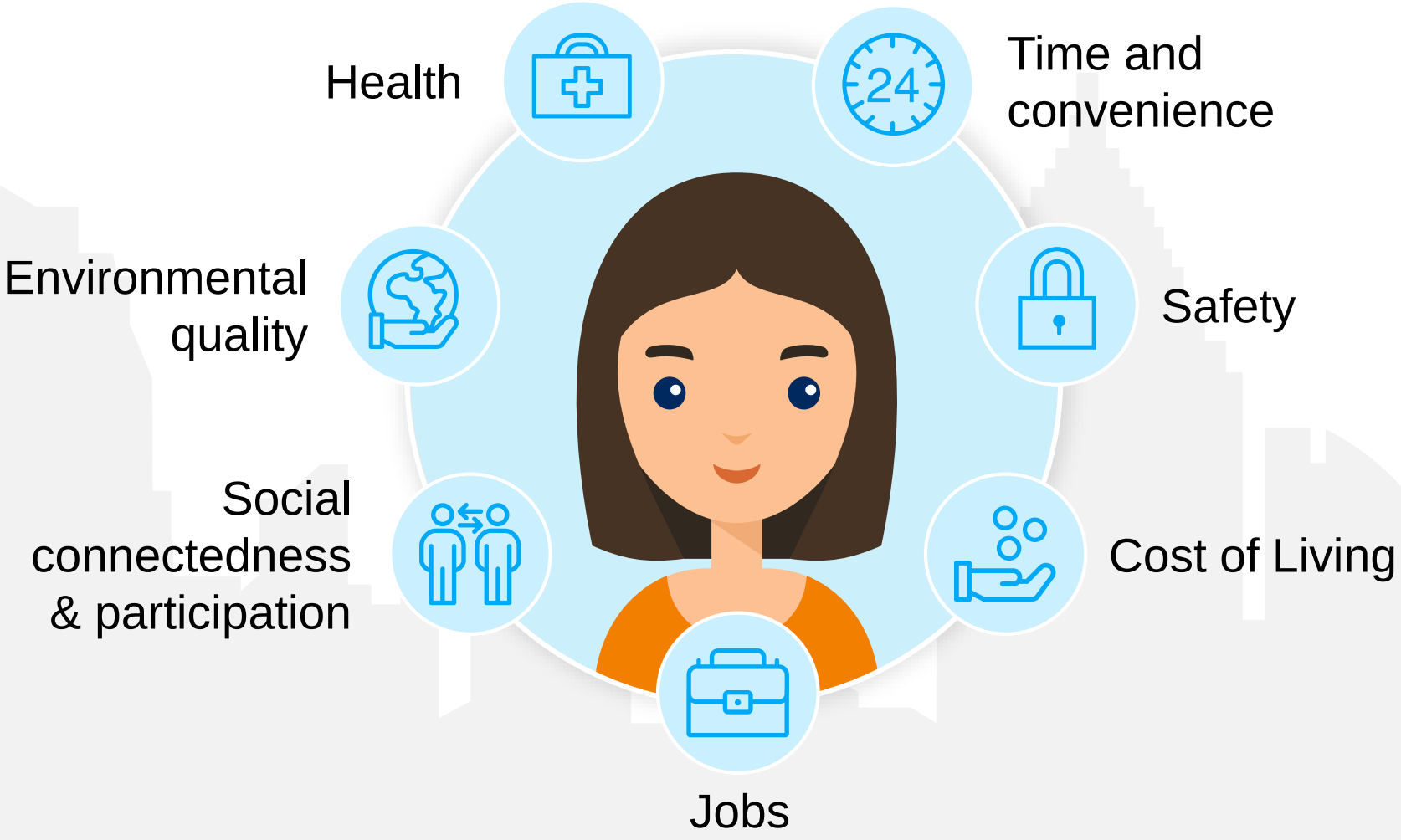
Applications: Data analysis capabilities and applications

Technology base: Network of connected devices and sensors

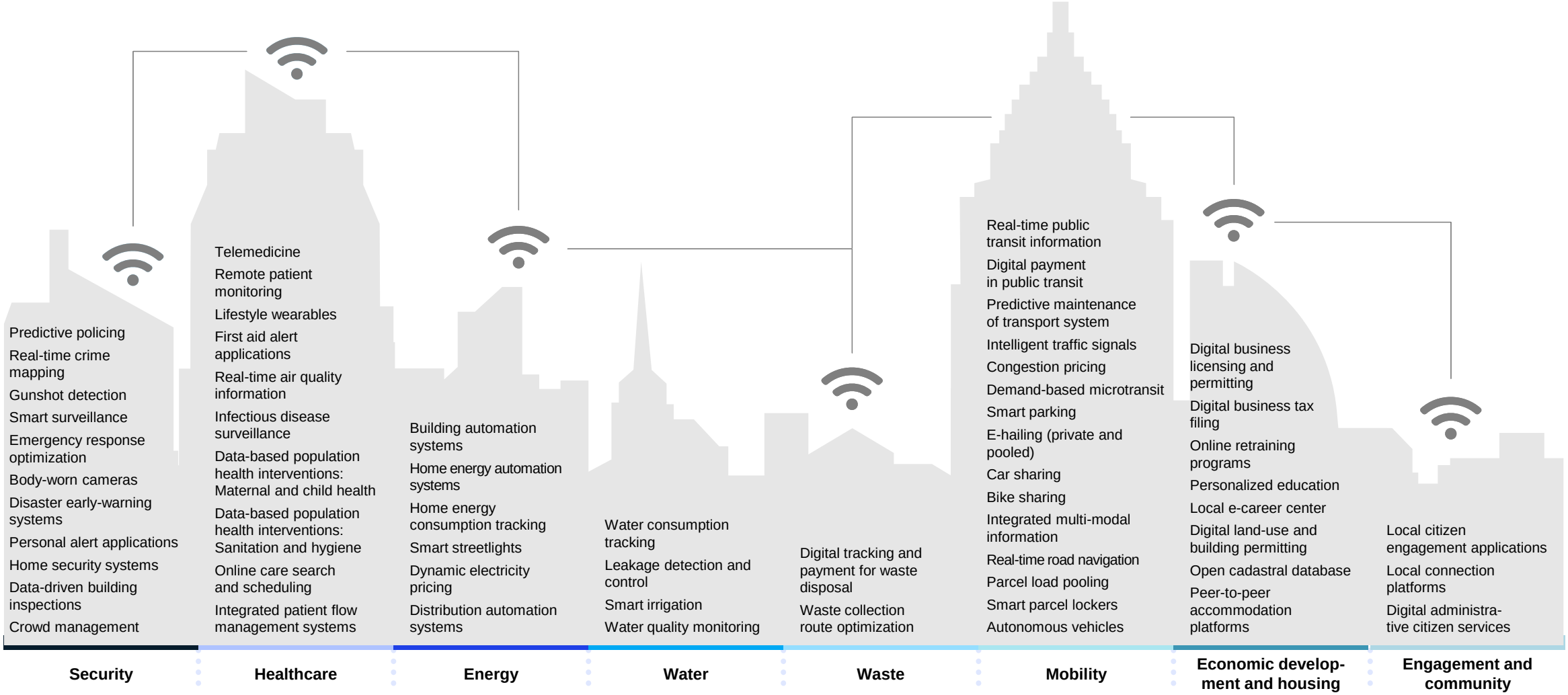
Traditional Infrastructure
(physical and human)
e.g., roads, buildings, doctors

The next era of smart cities will use digital technologies to improve citizen quality of life – we defined 7 relevant outcome dimensions

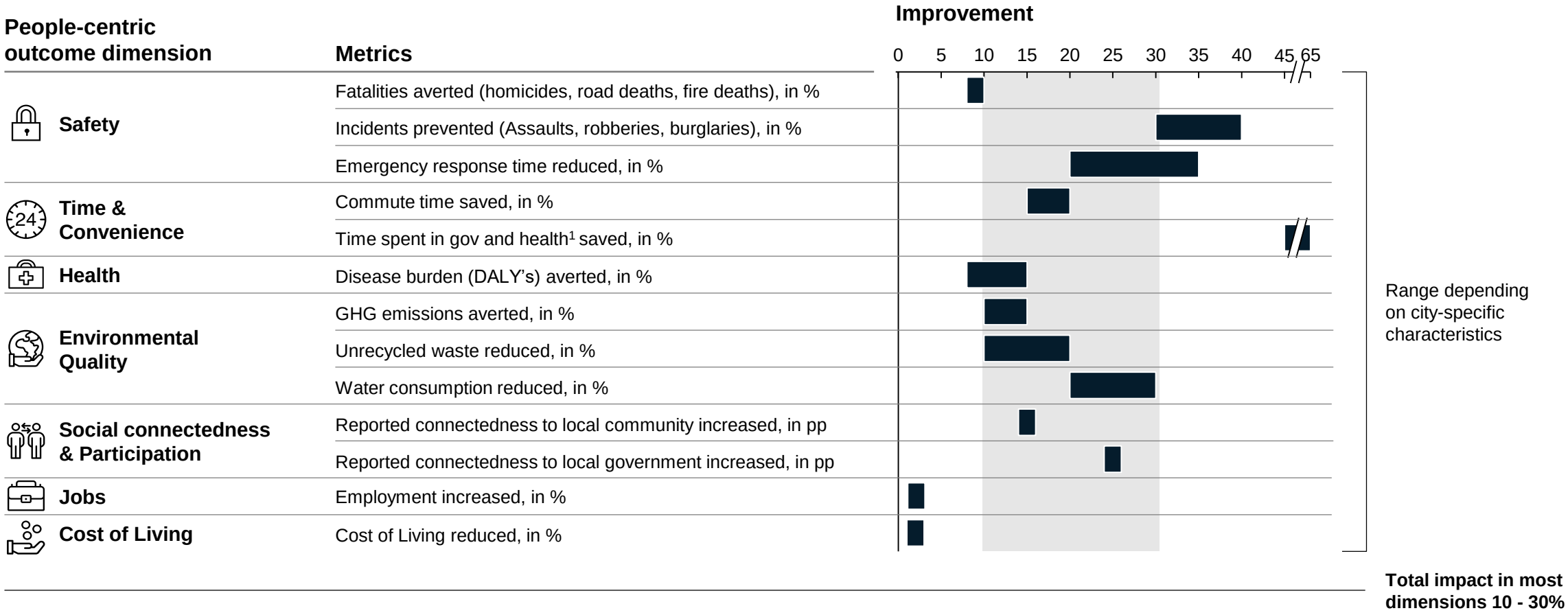
Resident quality of life dimensions for smart cities



Smart cities span multiple domains – our research looked at ~60 applications that will be relevant in the time horizon to 2025



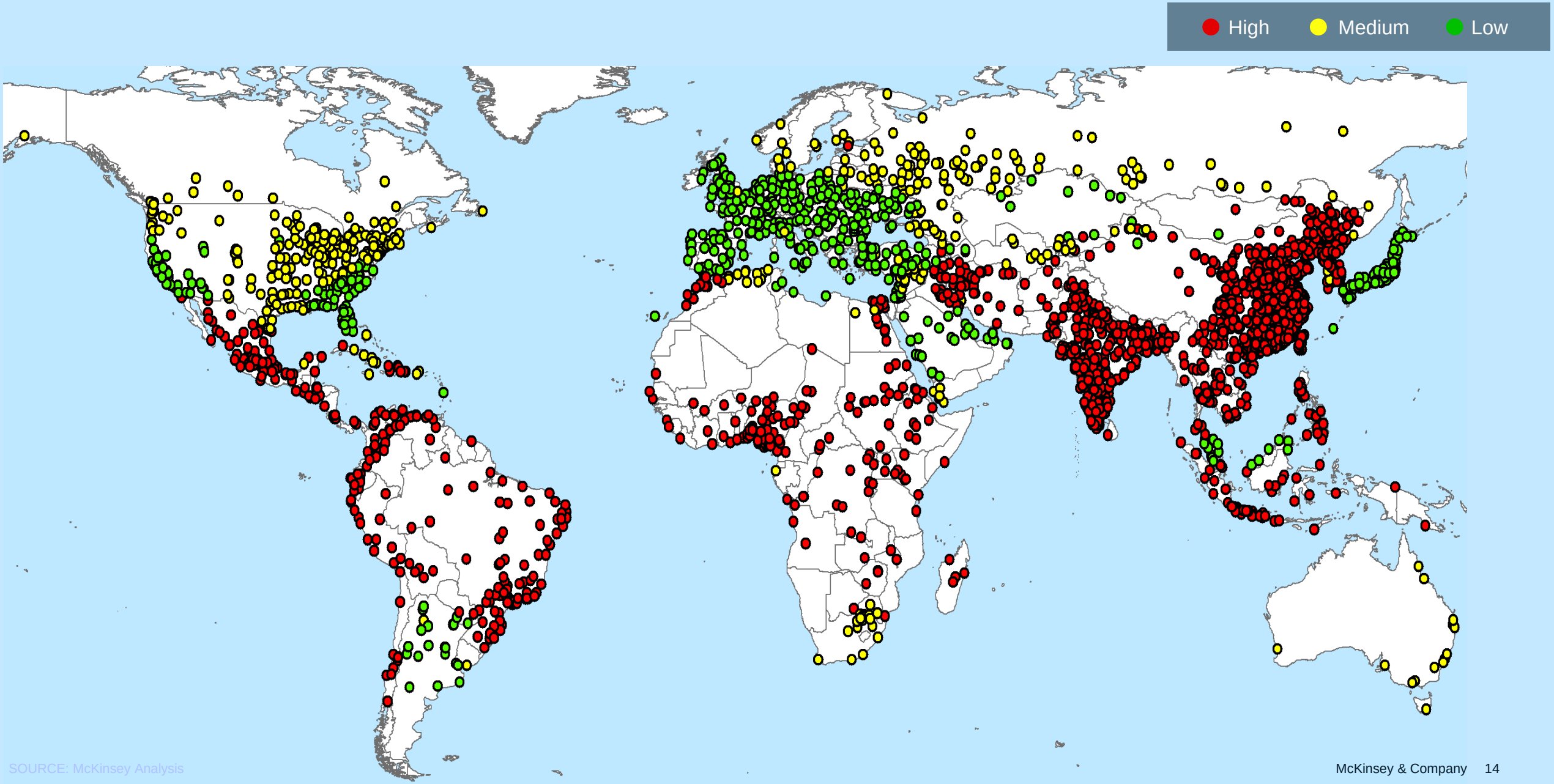
Overall, these applications can improve most dimensions of quality of life by ~10 - 30%, allowing cities to do more with less



1. Includes time in spent in government processes and time spent searching for, traveling to, and waiting for healthcare services
2. 2 DALY = Disability adjusted life years, metric for burden of disease from mortality and morbidity
3. additional jobs per 1,000 working-age citizens. Includes direct job effect as well as approximation for indirect and induced jobs (cross-industry for mid-sized+ cities of 2.2 used)

Source: McKinsey Global Institute

Exposure to natural chronic resource stresses (water, energy, food) by 2025

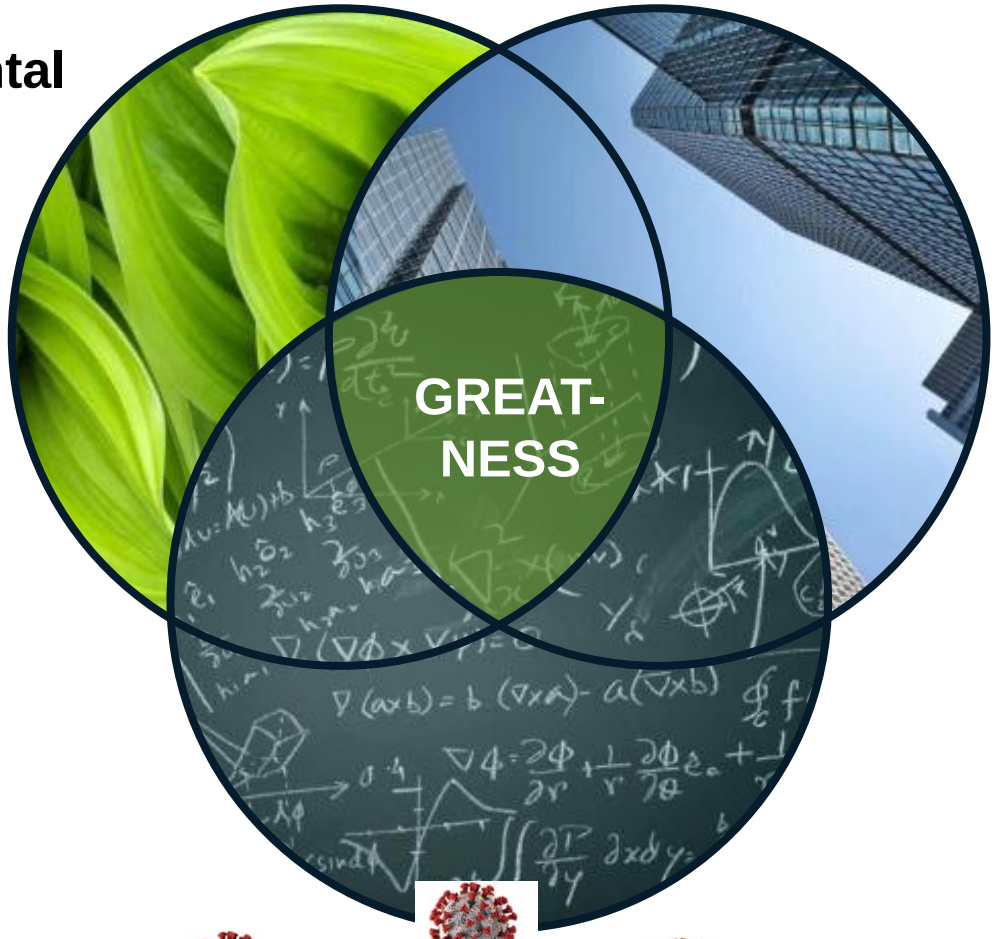


SOURCE: McKinsey Analysis

But great cities must achieve across multiple dimensions which COVID-19 threatens

Environmental protection

Water, emissions, wa biodiversity



Economic wth

Per GD oyme

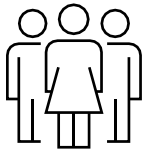
Social progres

hea ucati

SOURCE: Concept from UCN. 2006

Cities are forced to deal with two challenges simultaneously

Cities are the natural owners of the capacity that is needed to respond to the COVID-19 challenge. Around the world, cities are already responding to mitigate the economic and health impacts in urban areas, dealing with two contrasting and often competing interests:



Health

Protect lives
Minimize health impacts by protecting vulnerable populations, enforcing social distancing and facilitating expansion of health systems

Economy

Protect livelihoods
Keep the economy moving by protecting jobs, shoring up businesses and facilitating the continuation of essential urban functionality

Source: Eurocities, National League of Cities

The reimagining menu will be different from previous economic stimulus – we can build back better

From: physical infrastructure, precincts and overseas visitors

To: adaptive reuse and new ways of working

Bridges and tunnels generating construction jobs and increased public transport and commuter travel

Major events, tourism and travel bringing large numbers of visitors from many global destinations to enjoy and work close to arts precincts, culture, sports and amenity

High value manufacturing jobs providing a backstop to innovation industries anchored in rapid easy international travel, migration and study

A commitment to public funding for public works with limited collaborations with the private sector

New sources of construction growth (e.g., refits) focused on stimulating SME sector and targeting new infrastructure sweet spots (digital infrastructure; supply chain last mile/warehousing)

Reimagining neighborhoods and the CBD anchoring work and life in seamless 'distancing in density' ecosystems, embedding **contactless digital defaults** to safely deliver experiences, goods and services

Reskilling and re-energizing people generating jobs in new growth sectors: caring services, localized manufacture, green energy precincts and innovation networks

A 'make it happen' approach to getting funds to flow, crowding in private capital for opportunities of the future

All economic interventions are and will continue to be dependent on the success of public health interventions

COVID-19 will accelerate demand for contactless retail

Amazon's 'just walk out' technology uses computer vision and sensors to remove checkout

Detects products taken or returned to shelves and customers are automatically charged upon leaving

Could potentially reduce store labor by 30% to 40%

Keeps physical distance between staff and shoppers

COVID-19 will reshape in-store experience with interactive technologies to replace contact - Innisfree New Retail Smart Store

Description

- Innisfree smart store in China has a **AR-enabled Magic Mirror** in which customers can try makeup virtually and get directed to corresponding product shelf with light instructions
- **Smart Skin Analyzer** leverages high-precision camera on face and instantaneously generates a detailed report of customers' skin condition and product recommendation
- **Smart Shelf** helps customers self-educate about product information by sensor-equipped shelf. **Cloud Shelf** showcases online and offline inventory to enhance the navigation experience
- **Facial Recognition Payment** improves check-out experience by expediting the process
- **AR Interactive Photo Booth** take photos with celebrity brand ambassadors which attracts traffic in store

Key implications/learning

- People can have contactless experiences of trying new products where previously they would have sat in a chair and had products applied directly
- Customers can easily locate products in-store, find detailed information on items on offer and get personalized recommendations

Impact

- The New Retail store is Innisfree's **500th store** in China and it plans to incorporate 61 more stores in Shanghai and Hangzhou to **T-mall smart New Retail system** to take full advantage of omnichannel data

SOURCE: Press search

Italy taking an opportunity to reduce car use after Covid-19 lockdown

Milan announces ambitious scheme to reduce car use after lockdown

In response to the coronavirus crisis, Milan is to introduce one of Europe's most ambitious schemes reallocating street space from cars to cycling and walking.

Under the nationwide lockdown, motor traffic congestion has dropped by 30-75%, and air pollution with it.

City officials hope to fend off a resurgence in car use as residents return to work.

The city has announced that 35km (22 miles) of streets will be transformed over the summer, with a rapid, experimental citywide expansion of cycling and walking space to protect residents as Covid-19 restrictions are lifted.

Source: The Guardian April 2020

Smart City Architecture at a 30,000-ft view

Applications

Residents and Visitors

Universal App for Residents & Visitors [Focus towards journey based services]

City Administrators

City Management apps

City Command & control centers

Others

Partner ecosystem applications

City Technology Platform

Enablement Platform

Core City Applications

Business Support Applications

Enterprise Integration

Ecosystem Platform

Data & Analytics

Nextgen IT Infrastructure

External Information Exchange Platform

Network & Connectivity

Wired Connectivity
- Optical Fibers
- Leased Line
- Sea Cables

Wireless Connectivity
- City Wi-Fi Network
- End to end connectivity to households

Smart Sensors
- IoT Enabled City Assets
- IoT Enabled Household Assets

Cellular Network
- Cellular Tower (BTS)
- Main switching centre
- MVNO

Cross functional ecosystem

Household and Commercial Areas

Phones, tablets

Vehicles

Private Buildings

Commercial Buildings

Public Services Areas

Water

Parking

Lighting

Waste

Public places

Safety

Traffic

Integrative Areas

GIS

Asset Management

Other data platforms

Security

Agenda

IoT – what is it & why is it important

Smart Cities

Cyber security considerations for IoT / Smart Cities

There are many different archetypes for IoT players' offerings

EXAMPLE PLAYERS

Archetypes with deep dive

Sub-segments		Player archetypes: Horizontal/agnostic	Vertical-focused
Applications		**Application providers** (high number of mostly small players)	
IoT security		(A) **IoT security providers**: FORESCOUT	
IoT platform & Infrastructure	**IoT platform (excl. below)**	(B3) **Horizontal IoT platform providers (agnostic or with some vertical specializations)**: ORACLE, software AG, Cumulocity, SAP, IBM, HUAWEI, Azure, Google Cloud, aws	
	IoT data ingestion & analytics	(B4) **Players with partial IoT platform offering**: Device/ connectivity mgmt.: ERICSSON, Jasper, SIERRA WIRELESS, Telit; Data ingestion & analytics: CRATE.IO, ELEMENT ANALYTICS, influxdata, kafka, StreamSets	(B2) **Vertical IoT platform providers**: relayr, Bosch IoT Suite, ADAMOS, ptc, MindSphere, PREDIX, C3.ai, HITACHI, UPTAKE
	Infrastructure	(B1) **End-to-end horizontal IoT platform providers (incl. infrastructure – cloud services)**: Azure, Google Cloud, aws, Alibaba Group	
Connectivity		**Connectivity service providers**: Traditional MSPs/MNOs: Deutsche Telekom, verizon, vodafone, AT&T, orange Business Services; Alternative MNOs: sigfox, ingenu, MYRIOTA; Mobile virtual network operators: Telit, SIERRA WIRELESS, wireless logic	**Connectivity hardware providers**: NOKIA, SIERRA WIRELESS, CISCO, Hewlett Packard Enterprise, DELL, ERICSSON
"Things"/ devices		**Operating system providers**: aws, HUAWEI, Azure, androidthings; **Component manufacturers**: arm, intel, Qualcomm; **Device manufac-turers/integrators**: FOXCONN, JABIL	
		(C) **Edge integrated solution providers (HW/SW)**	

Vertical end-to-end IoT solution providers[1]

B2B solution providers: KONUX, Particle

B2C IoT gadget providers (with ecosystem): fitbit, amazon alexa, nest

System integrators: accenture (High performance. Delivered.), Capgemini

1 Vertical end-to-end IoT solution providers might integrated several sub-segments from other players (especially connectivity, IoT platform in order to enable their offering, but usually sell an end-to-end, ready-to-use solution

IoT security: overview of market and player archetype

NOT EXHAUSTIVE

Key value proposition and market overview

Securing the **device** through creating **visibility** and **control** mechanisms over device and building in **security measures** in **device** from the **start**

Providing **conventional cybersecurity** solutions for **all levels** in **IoT ecosystem**

Challenges addressed

Diverse requirements to secure IoT ecosystem **end-to-end** due to **heterogeneity** of devices (e.g. capabilities), connectivity protocols and IoT platforms

Difficult to keep track & control of all connected devices to network

IT, **IoT** and **OT** networks now **connected** – **new end-to-end** security **challenges**

Capabilities of **devices insufficient** for **full** device-level **security software**

Solution

Visibility of device location and status to understand operational and security risk

Embedded security-by-design at device-level and physical device security

Conventional cybersecurity (e.g. encryption) at device- (IoT sensors and OT), network-, server-level to ensure end-to-end security solution

Offerings and players

		gemalto	FORESCOUT	Zingbox	armis
IoT security lifecycle mgmt. and device visibility	Device identification, authentica-tion, onboarding, secure firmware updates OTA, decommissioning; real time insights and automated control for IoT, IT and OT	✓	✓	✓	✓
Device HW & SW security-by-design	Toolkit for integration of security functions and hardware during development	✓			
Conventional cyber-security	Measures such as encryption, access control at device-, network-, sever-level	✓			✓

Evaluation

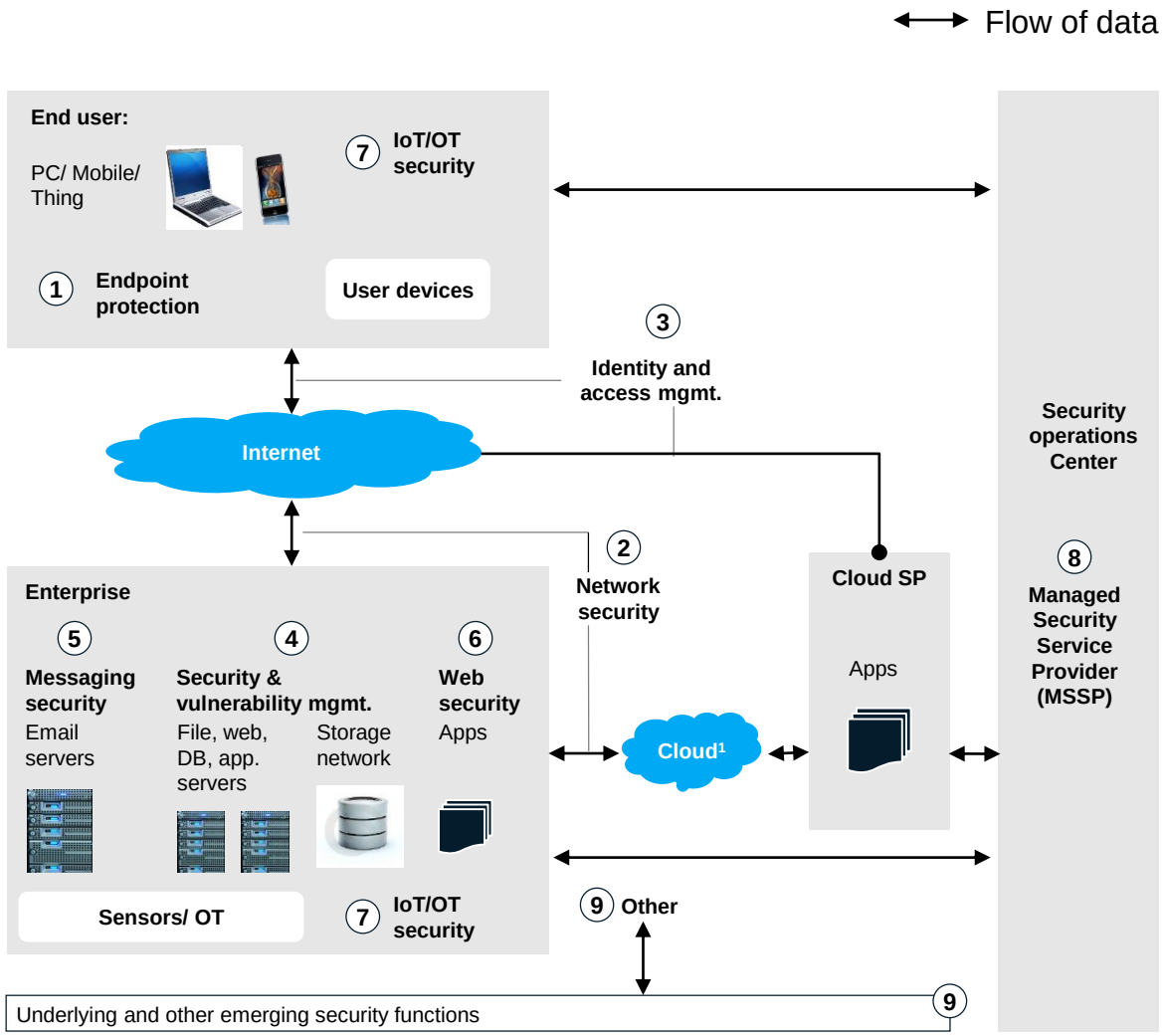
- **Potential** for **high value creation** for technically advanced solution
- **No established end-to-end security players** yet
- **Demand still low** – low awareness & few resources in enterprise security divisions
- **High complexity** to build **E2E security solution** due to heterogeneous HW/SW landscape

Hypothesis on future development

IoT security and **IoT device mgmt.** (as part of IoT platform) **will merge**, because technical requirements and offering are similar (both create transparency over device)

Enabling effective cyber-security requires 9 technology components that tackle distinct needs…

Segment	Description
1 **Endpoint protection**	Provide advanced protection of endpoints (desktops, laptops, smartphones, tablets)
2 **Network security**	Prevent attackers from gaining access to a company's network and infrastructure through NGFW, IPS/IDS, VPN etc.
3 **Identity and access mgmt.**	Provide tools and governance model/ processes to control access to information
4 **Security and vulnerability mgmt.**	Assess current risk, maturity, and vulnerabilities and manage a full spectrum of security operations
5 **Messaging security**	Protect collaborative applications, including email, instant messaging (IM) through URL filtering, content filtering etc.
6 **Web security**	Protect against both inbound (malware) and outbound (data leakage) threats related to web applications
7 **IoT/OT security**	An emerging market for security of factories and other manufacturing/ industrial facilities with multiple nodes, as well as security of individual IoT and connected devices
8 **Managed Security Service (MSS)**	Security Operations Center functions that are outsourced as a managed services contract, including monitoring (L1-L3+), event management, threat intelligence, and incident response
9 **Other services and products**	Includes Security consulting, implementation and HW support as well as underlying functions that do not fit well into above categories e.g. encryption tools, secure OS, specific storage security



1. "Cloud" is included as sub-segments of the 9 categories

Source: McKinsey Cyber Practice

The cybersecurity market is filled with high growth, large attackers

Product segments	Sub-segments	Large attackers within segment		
1 **Endpoint protection**	Access and Information protection (AIP), antimalware, proactive endpoint risk management (PERM), security suites, server security	CYLANCE	Carbon Black.	TANIUM
2 **Network security**	Firewall/UTM, VPN appliances, NGFW, IPS/IDS	Bitglass	paloalto NETWORKS	distil networks
3 **Identity and access mgmt.**	Authentication (including legacy), privileged access, provisioning, single sign-on, OTP solutions	SailPoint	okta	onelogin
4 **Security and vulnerability mgmt.**	SIEM, security device systems management, forensics and incident investigation, policy and compliance, GRC	sumologic	SECURONIX	ALIEN VAULT
5 **Messaging security**	Content filtering, email and messaging security gateways with some DLP functionality	DIGITAL GUARDIAN	ContentKeeper	
6 **Web security**	Web Application Firewalls, URL filtering, web antimalware	zscaler	IMPERVA	iboss
7 **IoT/OT security**	Industrial control systems and OT, individual devices	Bastille	MOCANA	Rubicon
8 **Managed Security Service (MSS)**	Monitoring, threat intelligence, incident response services	MASERGY		
9 **Other services and products**	Security consulting, implementation, HW support, encryption tools and algorithms, security product verification testing, secure operating systems etc.	COALFIRE		

Note: “Cloud” is included as sub-segments of the categories

Source: IDC, Gartner, McKinsey Cyber Market Map

Many companies competing for share in each segment with top 3 vendors on average controlling ~35%

x% 2016-2020 CAGR ✓ Security pure play companies

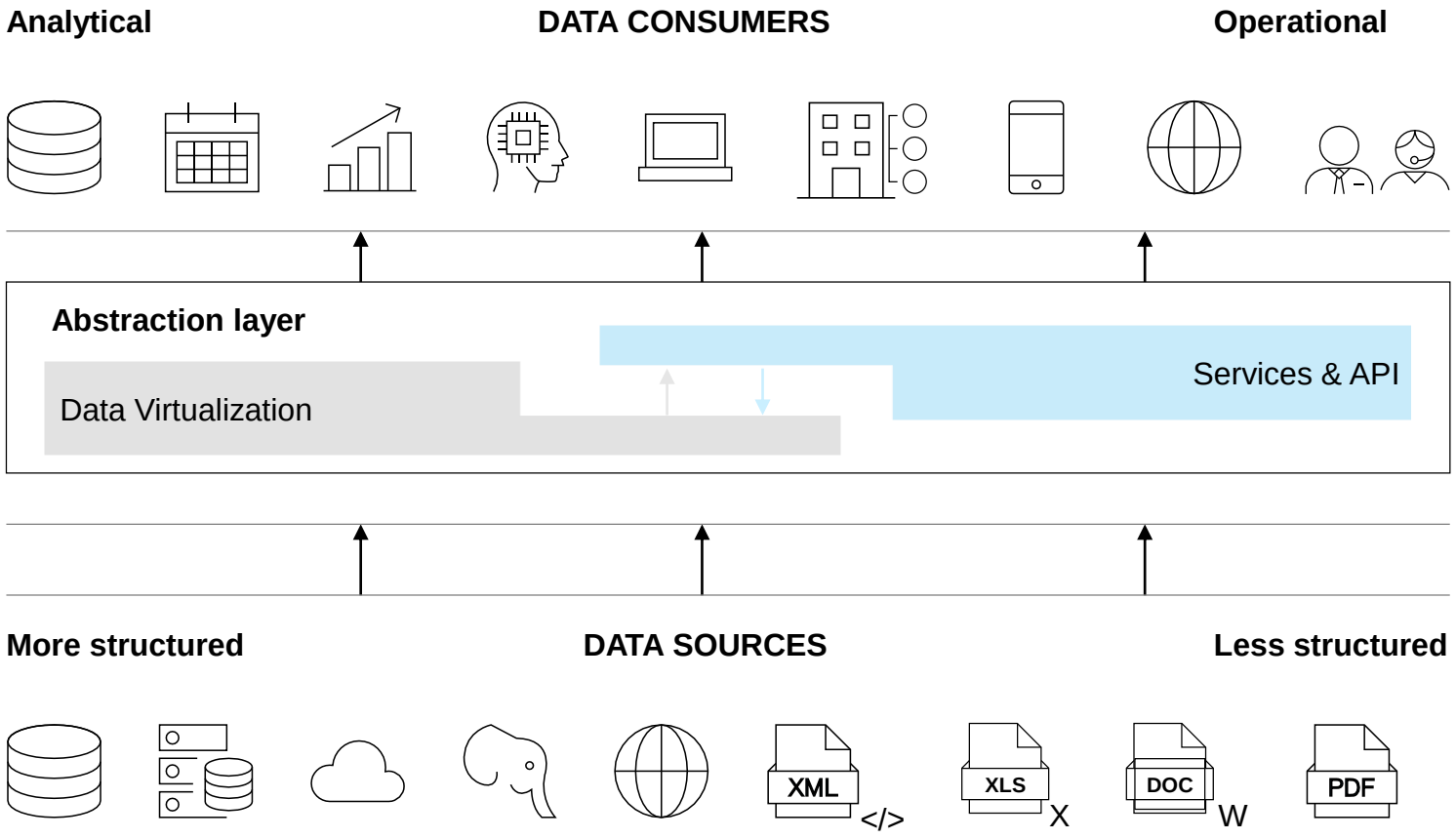
			Top 3 players and their market share, %		Challenger
Products	Endpoint protection	5	Symantec ✓, McAfee ✓, Trend Micro ✓	56	Kaspersky, Bromium, AhnLab, Lookout, MobileIron, avast!, SentinelOne, Infocyte, Cylance, Good, invincea, Microsoft, Tanium, CounterTack
	Network security	9	Cisco, Check Point ✓, paloalto ✓	41	Fortinet, Barracuda, Bitglass, distil networks, CipherCloud, radware, cores, Symantec, Netskope
	Identity and access mgmt.	8	IBM, RSA ✓, Oracle	34	CA, CyberArk, okta, Symantec, covisint, ThreatMetrix, ForgeRock, PingIdentity, Centrify, onelogin, SailPoint, gemalto, SecureAuth, Micro Focus, NetIQ
	Security and vulnerability mgmt.	12	IBM, Hewlett Packard Enterprise, RSA ✓	29	splunk>, sumologic, LogRhythm, Symantec, tripwire, FireEye, Veracode, Securonix, Alien Vault, Optiv
	Messaging security	2	Symantec ✓, Cisco, Trend Micro ✓	36	proofpoint, Barracuda, Forcepoint, McAfee, Digital Guardian, Microsoft, ContentKeeper
	Web security	6	Symantec ✓, Forcepoint ✓, Cisco	47	zscaler, Barracuda, f5, Fortinet, paloalto, Imperva, Check Point, Symantec
	IoT/OT security	13	GE	<~10	Rubicon, Argus Cyber Security, Imubit, ZingBox, Bastille, Mocana, cryptosoft delivering trust in IoT, ARM
Services	MSS[1]	12	IBM, AT&T, Hewlett Packard Enterprise	13	verizon, SecureWorks, BT, NTT Communications, Wipro, Atos, Symantec, DXC.technology, Optiv, Masergy, Trustwave
	Other services and products[2]	8	Deloitte, EY, pwc	37	KPMG, Hewlett Packard Enterprise, protiviti, Booz | Allen | Hamilton, IBM, accenture, Atos, Optiv, AT&T

1. Managed security services (MSS) often bundled with products and requires partnerships between vendors
2. Top players share and challengers are Security Consulting focused

Source: IDC, Gartner

Data access should be granted through an abstraction layer that provides a unified view of data across the company, regardless of the source

Data virtualization



Details

Data access **abstraction** is achieved through a **semantic layer** that allows to retrieve data without knowing the technical details underneath; this semantic layer can be composed of 2 key components:

- **Data virtualization:** virtual data repository (i.e., virtual DWH) accessible by analytical tools and operational applications
- **Data services:** services exposed via APIs to internal and external consumers

Data virtualization, which may or may not exist in the target data architecture, offers **5 key functionalities:**

- Technology, storage and access **abstraction**
- **Virtual data access** from a single point
- **Transform** data for end users
- Data **federation**, combining several sources
- Data **Delivery** by publishing results or even data services

Source: McKinsey Data and Analytics Practice

Backup

5 core elements are accelerating IoT adoption

Ubiquitous Connectivity

Smartphones, tablets, WLAN, 5G/LTE, LPWAN

Commoditized Hardware

Sensors, gateways, cameras, edge devices

Cloud Services & Platforms

Microsoft Azure IoT, AWS, PTC, Google Cloud

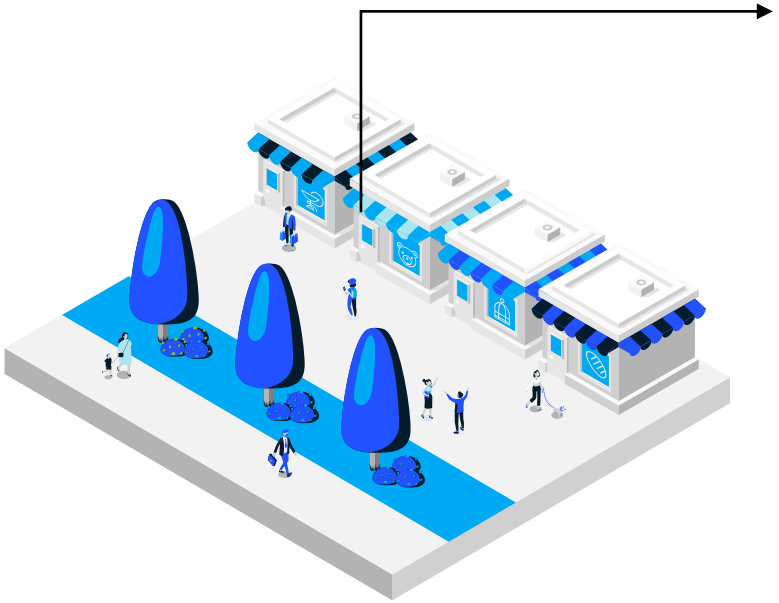
Big Data / Machine Learning

Data lakes, cloud analytics, elastic compute resources

Human – Machine Interfaces

AR/VR headsets, biometric sensors, cobots

1. Sample high-level architecture for smart city recommender system



Azure Cloud Environment

Raw data sources

- **Geolocation** from mobile app
- **Customer sentiment** using computer vision
- **Customer profile/social network**
- **App interaction patterns**

Edge device

- Edge devices installed at stores as the **middle layer** between the various local network devices and the cloud environment

Data ingestion/ processing

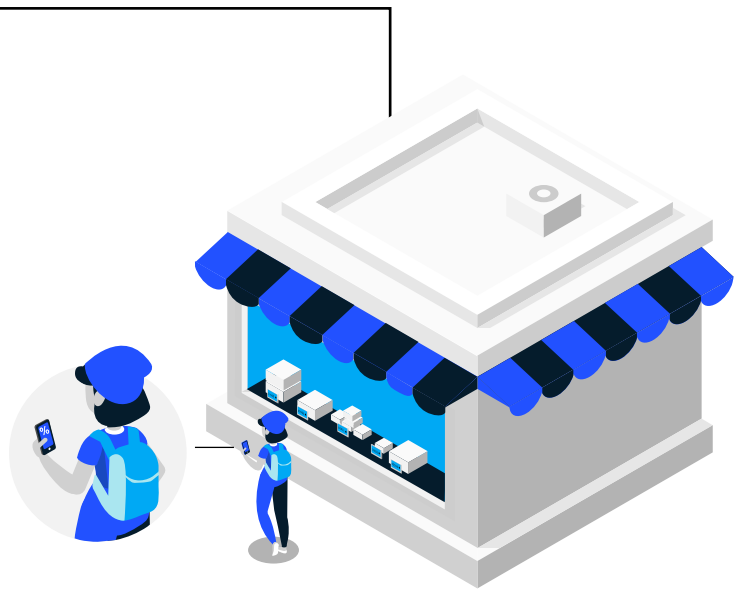
- **Translation from raw data** to normalized, mapped, consistent, data using IoT hub, Data Factory and other Azure IoT data services

Storage

- **Data lake** - data that is accessed infrequently stored as cold storage, data used frequently stored in warm or hot storage in databases

Service/ microservices layer

- **Aggregate and serve data** across machine learning, analytical, and rule based models, and create APIs to communicate data to FE



Mobile application, digital signage, dashboards

- Push notification of a sale/discount sent to customer individualized and based on a model result run on data collected across mobile app, customer sentiment, social network/profile, and app interaction patterns

Many companies competing for share in each segment with top 3 vendors on average controlling ~35%

x% 2016-2020 CAGR ✓ Security pure play companies

			Top 3 players and their market share, %		Challenger
Products	Endpoint protection	5	Symantec ✓, McAfee ✓, Trend Micro ✓	56	Kaspersky, Bromium, AhnLab, Lookout, MobileIron, avast!, SentinelOne, Infocyte, Cylance, Good, invincea, Microsoft, Tanium, CounterTack
	Network security	9	Cisco, Check Point ✓, paloalto ✓	41	Fortinet, Barracuda, Bitglass, distil networks, CipherCloud, radware, cores, Symantec, Netskope
	Identity and access mgmt.	8	IBM, RSA ✓, Oracle	34	CA, CyberArk, okta, Symantec, covisint, ThreatMetrix, ForgeRock, PingIdentity, Centrify, onelogin, SailPoint, gemalto, SecureAuth, Micro Focus, NetIQ
	Security and vulnerability mgmt.	12	IBM, Hewlett Packard Enterprise, RSA ✓	29	splunk>, sumologic, LogRhythm, Symantec, tripwire, FireEye, Veracode, Securonix, Alien Vault, Optiv
	Messaging security	2	Symantec ✓, Cisco, Trend Micro ✓	36	proofpoint, Barracuda, Forcepoint, McAfee, Digital Guardian, Microsoft, ContentKeeper
	Web security	6	Symantec ✓, Forcepoint ✓, Cisco	47	zscaler, Barracuda, f5, Fortinet, paloalto, Imperva, Check Point, Symantec
	IoT/OT security	13	GE	<~10	Rubicon, Argus Cyber Security, Imubit, ZingBox, Bastille, Mocana, cryptosoft delivering trust in IoT, ARM
Services	MSS[1]	12	IBM, AT&T, Hewlett Packard Enterprise	13	verizon, SecureWorks, BT, NTT Communications, Wipro, Atos, Symantec, DXC.technology, Optiv, Masergy, Trustwave
	Other services and products[2]	8	Deloitte, EY, pwc	37	KPMG, Hewlett Packard Enterprise, protiviti, Booz | Allen | Hamilton, IBM, accenture, Atos, Optiv, AT&T

1. Managed security services (MSS) often bundled with products and requires partnerships between vendors
2. Top players share and challengers are Security Consulting focused

Source: IDC, Gartner

A. IoT security: Deep dive on players, offerings and competitive dynamics

NOT EXHAUSTIVE

Key players

Players with IoT security solutions for devices, network and cloud

- **Players specialized on IoT security:** <5 year old startups with security-by-design and IoT security lifecycle mgmt.
- **Generic cybersecurity providers:** Selling endpoint and network security products also to IoT, but not specified
- **IoT platform providers** securing own offering and selling add-on security solutions

Player	Quick facts	
Players with specialized IoT security	THALES + gemalto	Gemalto offers device-level security solutions, such as Cinterion Secure element for storing encryption keys and other sensitive data on device Offers the Trusted Key Manager solutions for smart grids including digital authentication, data encryption and security lifecycle management
	FORESCOUT	Israeli based Forescout offers a IoT security through a NAC-platform – protecting all devices on a certain network by monitoring all devices as they connect to the network
	ZingBox, ordr, armis	Pure specialized IoT security solution providers with IoT device visibility and IoT device lifecycle management (discovery and management, device behavior and risk analysis) focus; automated protection without agent installation, IT/OT/IoT integration
Generic cyber-security providers	BlackBerry + CYLANCE	AI-based cybersecurity solutions for endpoint, detection and response and security optimization Currently launching customized IoT security product range
	FORTINET	Generic cybersecurity solution provider that offers endpoint protection, firewalls, security incident and event mgmt. solutions also for IoT (non-specified)

Further large cybersecurity players active in the field, e.g. Checkpoint, Symantec

Competitive dynamics

Specialized IoT security players and generic cybersecurity players have roughly similar market shares (each ~40%); however specialized players will grow more strongly because of superior offering

While ZingBox, ORDR and Armis are leaders in specialized IoT security, there are hundreds more small IoT security startups

There are no established players with end-to-end IoT specific offering yet – this is a market opportunity

Large players such as Siemens and PTC provide a combination of own security offerings plus partnerships

IoT security lifecycle mgmt. has overlaps with device mgmt. – players from either offering might enter the other

B1. End-to-end horizontal IoT platform providers: Deep dive

NOT EXHAUSTIVE

Short description

Large webscale players with cloud background, building on cloud core to offer agnostic IoT solutions covering most of IoT stack, while providing ecosystem for partners serving specific use cases

Typical offerings

Application marketplace	Open app store or similar where 3rd parties provide use case-specific applications/platform elements
Application enablement	API managed services to enable 3rd party SaaS apps
Device/ connectivity mgmt.	Software to connect, monitor and manage IoT assets at scale, incl. device simulation,
Data ingestion and analytics	Software for data collection & mgmt., ML/AI engines and visualization/dashboards
Edge Intelligence	Software to bring (cloud-based) IoT platform capabilities to devices; e.g. data analytics/ML, workload mgmt., device security, device OS, containerized module deployment
IoT platform infrastructure	Market leaders in IoT cloud services; to other IoT platforms and enterprises

Typical customers

Other IoT platforms that do not have end-to-end capabilities, especially for IoT infrastructure (e.g. C3 IoT)

Enterprises with little use case-specific requirements or with parallel subscription to other IoT platforms and applications

Key players

Player	Quick facts	Indicative IoT platform revenue, $ mn, 2018
aws	Horizontal open IoT platform with strong emphasis on developer environment and commoditizing IoT platform tools at low prices **Portfolio:** Full IoT platform with focus on functionalities and integrations, but not user interface; developers can use AWS tools to build customized platform elements and applications • Special features: IoT device security mgmt.; extensive edge offering (e.g. SW, AI chip, edge OS), dedicated product for data mgmt. from industrial equipment (AWS SiteWise) **Partnerships:** Supplying IoT platform infrastructure to horizontal and vertical platforms	~500
Azure	**Portfolio:** Full IoT platform with typical offerings including very rich set of development tools and advanced analytics, open source tools, ready-to-use apps, manufacturing & connecting MCU-powered devices ("Sphere"), OS support and service ("Windows 10 IoT Core Services"); focus on expanding core capabilities – no extensive set of pre-built applications (yet) **Partnerships:** Supplying IoT platform infrastructure for horizontal and vertical platforms (e.g. PTC) Historically, limited invest in vertical use cases with clients – instead, fully integrating vertically specialized applications and small platforms, that can use Azure value add platform capabilities, e.g. data analytics Recently, moving towards vertical-specific capabilities, i.e. for industrial vertical Natural strength in industrial as most machines run on Windows	~500
Google Cloud	**Portfolio**: Full IoT platform with all typical offerings, offerings enabling end-to-end security, AI chip for the edge **Partnerships:** Device manufacturers providing compatible hardware and software, integration with +20 IoT platforms and applications to provide device/connectivity mgmt., data insights and other value-adding services Weak positioning compared to other webscalers – no awareness in market, weak salesforce	~80

Competitive dynamics

In the past focused on providing infrastructure play and "passively" providing horizontal end-to-end services such as APIs, data ingestion

Recently built up IoT specific capabilities (e.g. device mgmt., IoT security), putting pressure on horizontal IoT platforms

Collaborations with other IoT platform players, particularly to provide IoT infrastructure

Players are building up collaborations and strong partner ecosystem:

- To provide IoT infrastructure to other IoT platforms
- To benefit from vertical-/use case specific platforms elements and applications from other IoT platforms

1 Rough estimate, for IoT platform unit

B4. Partial IoT platform offering (device management-focused): Deep dive

NOT EXHAUSTIVE

Short description

Players with a hardware- and connectivity history that mainly offer device and connectivity management solutions for own and 3rd party hardware, but have ambitions to offer full IoT platform (incl. application enablement, data ingestion/analytics)

Typical offerings

Device management	Open app store or similar where 3rd parties provide use case-specific applications/platform elements
Connectivity management	API managed services to enable 3rd party SaaS apps
Application enablement (some players)	Software to connect, monitor and manage IoT assets at scale, incl. device simulation,
System administration (some players)	Software for data collection & mgmt., ML/AI engines and visualization/dashboards

Typical customers

Enterprises with low vertical specificity requirements

Partially **industrial players** that take technological foundation for closed ecosystem restricted to own company

Key players

XX **Indicative IoT platform revenue, $** mn, 2018

XX **# connected devices,** Million

Player	Quick facts	Indicative IoT platform revenue	# connected devices
Cisco Jasper	**Portfolio:** Network- based IoT platform "Kinetic" (gateway mgmt. , edge and fog processing, data control), IT/OT integration, connectivity mgmt., IoT threat defense **Partnerships with >50 telco service providers: C**onnectivity mgmt. technology for telco IoT offerings (e.g. AT&T) Market leaders with telco customers	~210	~80
Telit	**Portfolio:** Device and connectivity mgmt. as core focus, with some functionalities in data mgmt., system admin. (e.g. billing, access mgmt./security) and application enablement **Partnerships:** Provision of device mgmt. for SAP IoT; interfaces to AWS, Azure, etc. Building China presence through new contract with China Unicom	~40	N/A
Ericsson	**Portfolio:** IoT platform ("IoT Accelerator"), sold in modular fashion (device/data mgmt., orchestration, integration, automation, billing, marketplace and exposure) **Partnerships:** Device manufacturers (to enable zero touch onboarding)	~70	~17.4
Sierra Wireless	**Portfolio:** Device and connectivity management platform ("AirVantage") and to a restricted degree applications for use cases (asset tracking, tank monitoring, offender monitoring) Focus on pre-integrating own hardware and connectivity services, but open to 3rd party (APIs, open source, standards)	~50	N/A

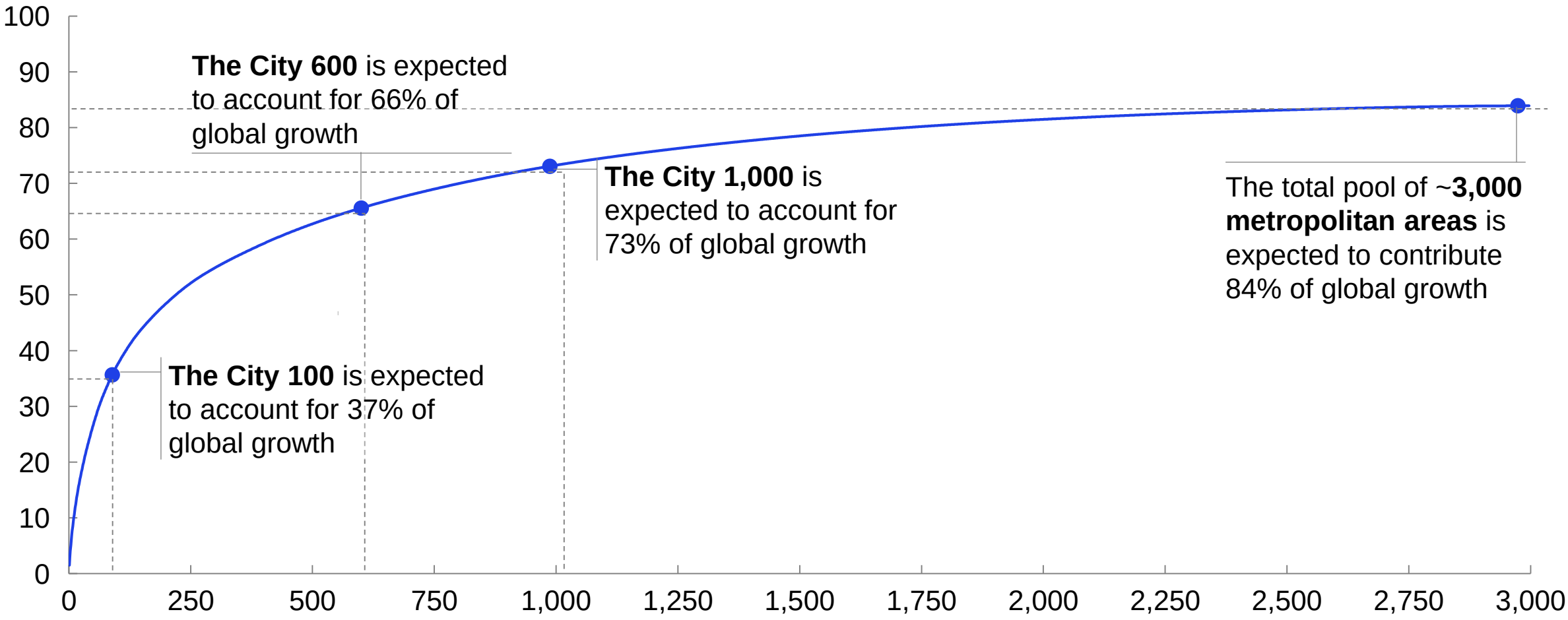
Competitive dynamics

Players "right to exist" is derived from its capabilities in complex connectivity mgmt., which other IoT platforms with cloud-background cannot (yet) handle
Most device/connectivity mgmt. players (e.g. Ericsson, Cisco Jasper) integrate with AWS, Microsoft Azure, IBM Cloud IoT infrastructure; often through partnerships
All players are extending connectivity/device mgmt. offering towards full IoT platform, but are not yet seen as competitors to established IoT platforms

1 Rough estimate, for IoT platform unit

Just 600 cities fuel more than 65 percent of global growth

Projected cumulative contribution to global GDP growth, 2015-2025, %



1 Predicted real exchange rate

SOURCE: McKinsey Global Institute Cityscope 3.0

McKinsey
& Company