IoT Implementation and Management — From the Edge to the Cloud: A Gartner Trend Insight Report

Published: 26 April 2018 **ID:** G00350392

Analyst(s): Mark Hung

A coherent Internet of Things strategy is key to the success of an organization's digital business transformation. Successful implementation and management of that strategy involve both new technical and organizational know-how.

Opportunities and Challenges

- Early IoT adopters have by now identified the key internal and external business value of the technology and moved their projects from experimentation to production.
- On the technical front, IoT has exacerbated application integration and data interoperability challenges with a wide spectrum of platforms, applications and protocols.
- From an organizational standpoint, team leadership, staffing, financing and skills development are the most important components to IoT project success. However, one in five IoT projects fail due to deficiencies in these aspects, as reported by organizations participating in the 2017 IoT Strategies Survey.

What You Need to Know

- Security continues to be the most prevalent technical concern, with nearly two in five (39%) of the organizations identifying security as one of their top three technology barriers, as per the participating organizations.
- CRM and ERP are the business applications most likely to be impacted by the implementation of IoT in an organization.
- CEO and CIO involvement is critical to the early phase of IoT adoption, architecture and implementation.

Insight From the Analyst

IoT: Moving From the Lab to Production

Mark Hung, Research VP

Organizations are starting to do more than just talk about IoT: From Gartner's latest CIO survey,[1] 12% of them have deployed an IoT project, and 24% are actively experimenting in IoT. Furthermore, how IoT can deliver value to an organization is better understood — cost reduction and revenue growth are the top drivers for IoT strategy. As per the 2017 IoT Strategies Survey, conducted among adopters of IoT initiatives, those who have or will deploy external IoT initiatives identify monetizing customer data and selling additional value-added products or services as top benefits.[2]

Among these early IoT adopters, however, there is a growing realization of the complexities and challenges involved in both the technical and organizational aspects of IoT. On the technical front, IoT puts a renewed emphasis on the edge architecture, whether it is in the form of compute resources, connectivity, storage, applications or data management and analytics. From an organizational perspective, insufficient financial resources and staff skills are most often cited as the reasons for failure of IoT projects.

In this IoT report, we examine four facets of IoT project implementation and management:

- What are the key enabling technologies for IoT?
- How should organizations be structured for IoT?
- How should IoT be integrated into the existing enterprise architecture?
- What are some of the best practices that other successful organizations have used?

In this latest collection of IoT research, you will find that as IoT starts to permeate throughout an organization, its impact on both your enterprise architecture and organizational structure expands as well.

Executive Overview

Definition

As organizations embark on their digitalization journey, a well-formulated IoT strategy is indispensable. Some choose to focus on IoT's external benefits first, including generating new revenue streams, enhancing customer service and increasing engagement. Others initially target internal benefits, such as optimizing asset utilization and improving worker safety and security. Currently, the internal benefits of IoT is driving its adoption: In Gartner's IoT Strategies 2017 Survey,

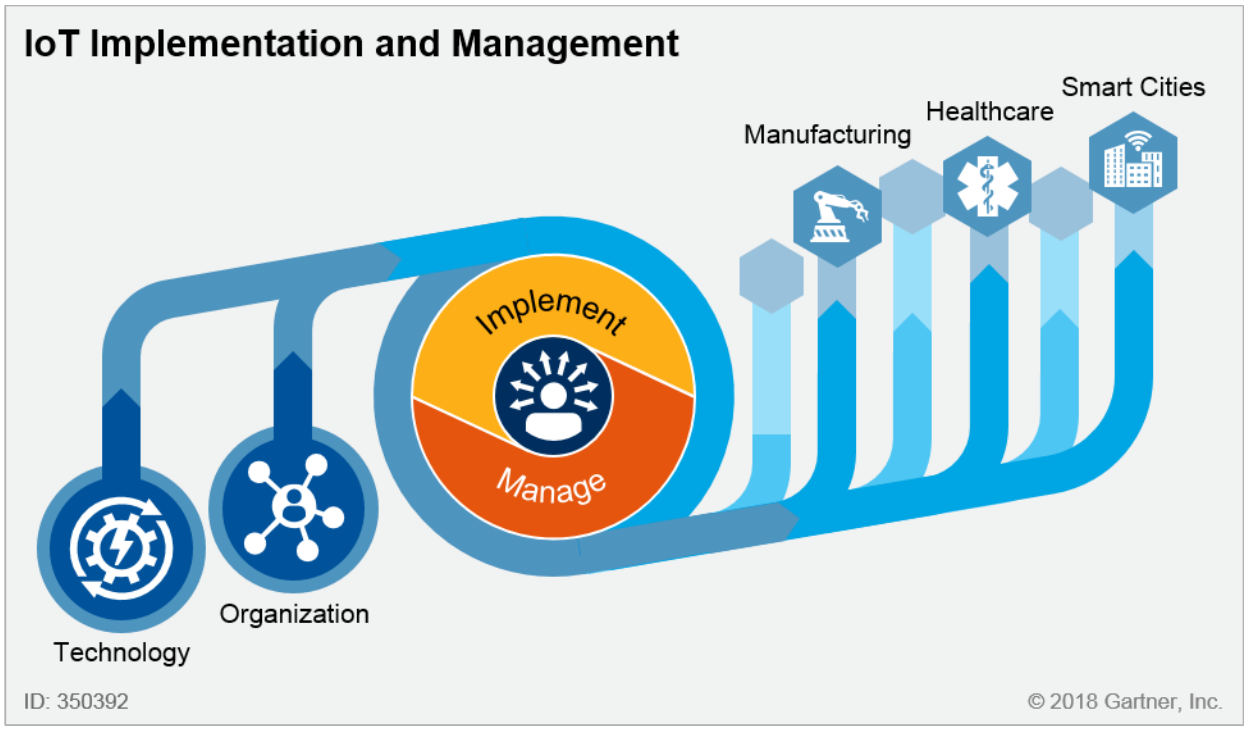
nearly all participating organizations (92%) had internal IoT initiatives in place, while close to half (50%) were deploying external IoT initiatives.

> IoT is a network of dedicated physical objects (things) that contain embedded technology to sense or interact with their internal state or the external environment. This excludes general-purpose devices, such as smartphones, tablets and PCs.

Some common themes, whether technical or organizational, have emerged in these IoT deployments. IoT's initial technical challenges included a lack of common standards, lack of shared infrastructure and poor battery life of endpoints. As these growing pains have started to subside, new ones have emerged: integration challenges, data management and analytics complexity, and continuing security concerns. On the other hand, organizational issues have become a larger concerns as well, such as identifying the most effective leadership for an IoT project, staffing the team, and adequately resourcing the effort from both an external and internal perspective.

In this document, we delve into the technical challenges (in terms of both the building blocks and implementation practices), organizational challenges, and examples from select IoT industries, such as manufacturing, smart cities and healthcare (see Figure 1).

Figure 1. IoT Implementation and Management — From the Edge to the Cloud



Source: Gartner (April 2018)

Research Highlights

Key Technologies Form the Foundation of IoT

When it comes to IoT's enabling technologies, security continues to be the most prevalent technical concern. Nearly two in five (39%) of the surveyed organizations identified security as one of their top three barriers, and this is similar across countries and verticals covered in the study. As IoT implementations and digital ecosystems proliferate, IT competencies, including security governance, planning and organization, become more complex — and the approaches to addressing these security challenges are evolving. While capitalizing on new IoT-fueled information is a key goal of digital transformation, information security is also increasingly mission-critical. Ensuring the privacy and safety of people and the overall integrity of cyberphysical convergence is essential. To do this, cybersecurity governance must evolve and be structured to address these concerns.

As organizations are looking to extract more value out of their IoT data, analytics is moving to the forefront. Engineers have been doing relatively simple OT analytics for decades, but the big data revolution, along with the movement toward ML and AI, is adding complexity and driving engineers to gain more expertise. This is only partly offset by advances in self-service features in modern BI and data science platforms. As a result, most IoT analytics will require a roughly equal collaboration of engineers as SMEs and professional data scientists.

Other key technology building blocks include wireless communications, endpoint technologies (sensors, power management, embedded OSs and processors), edge computing, blockchain, and digital twins.

Related Research

Security

"Securing the Internet of Things": IoT has created a new dynamic linking organizations with society. Securing the IoT will require a thorough understanding of the new actors that have emerged. These new actors include data scientists, external integrators and exposed endpoints.

Analytics

"Managing the Data Tsunami: How AI and Edge Computing Will Enhance IoT Analytics": Enterprise architectures are being threatened by the increasing amount of IoT data being produced. Advances in AI and edge computing will need to be utilized in order to control this growing volume of data.

AI/ML

"Innovation Insight for Artificial Intelligence of Things — Machine Learning in the IoT Era": New industries are being created due to the application of machine learning to the IoT. To remain competitive, Artificial Intelligence of Things strategies will need to be developed and executed.

Wireless Communications

"The Evolution of Wireless Communications and Its Impact on Your IoT Project": How to address the emergence of IoT applications has been one of the key drivers to the rapid advancement of wireless communications technologies. A thorough understanding of multiple wireless communications technologies will provide I&O leaders with knowledge to build successful IoT projects.

"Innovation Insight for 5G: Enabling Emerging IoT, Fixed Broadband and Mission-Critical Applications": 5G wireless access technology will soon arrive; however, enterprise leaders are mostly unaware of the technology's availability, value and cost. This note explores the benefits, uses and risks 5G will have upon its impending arrival.

Endpoint Technologies

"Market Trends: IoT Endpoints Will Need New Technologies to Achieve Scale": The failure rate of IoT projects is set to double by 2021 due to existing technologies failing to overcome challenges of scale. Autonomous technologies will be needed to be integrated in order to build up market share and brand position.

"Indoor Location-Sensing Technologies Enable New Contextual Experiences, 4Q17 Update": The indoor location sensing domain will remain complex and fragmented, with new vendors, technologies and algorithms continuing to emerge through 2022. This note analyzes 29 different ways to detect indoor location and advises on how to choose between them.

"Market Guide for Embedded Operating Systems": Embedded OSs are key enablers for IoT-enabled products. The following technology areas will continue to influence embedded computing: communications, IT/OT alignment, analytics and security.

"Market Insight: Design-In High-Performance Processors to Meet IoT Endpoint Analytics and Security Demands": The need for greater compute power to perform analytics, and to secure IoT endpoints, is driving technology product management leaders to incorporate semiconductors with higher processing performance in their IoT endpoints.

Edge Computing

"Digital Business Will Push Infrastructures to the Edge": I&O leaders focused on edge computing are faced with several challenges, including new technology choices, distributed computing architectures, remote management and edge security. Expanding infrastructures to the edge will be a necessity in order to address this.

"Market Guide for CSP Edge Computing Solutions": Large edge computing deployments can be driven by network optimization, vertical use cases and OTT interworks. This research focuses on providing I&O leaders with a logical upgrade roadmap to keep up with distributed cloud opportunities.

"Emerging Technology Analysis: NB-IoT": Communications service providers are rolling out NB-IoT, a new low-power wide-area communications standard. This report looks at NB-IoT's potential for technology strategic planners and provides market data to size the opportunity.

Cloud

"IoT Is Becoming a Standard Cloud Offering: Time to Think Differently": IoT capabilities from enterprise application software and cloud vendors are rapidly becoming standardized services within cloud platforms, changing how enterprise architecture and technology innovation leaders must make vendor selection decisions.

Blockchain

"Top Applications for Blockchain for IoT in 2018 and 2019": Blockchain for IoT is very immature; however, it will eventually enable radical new business models in many areas. For now, there should be a focus on investments in business applications for blockchain and IoT, which are less likely to be impacted by technology and partner immaturity.

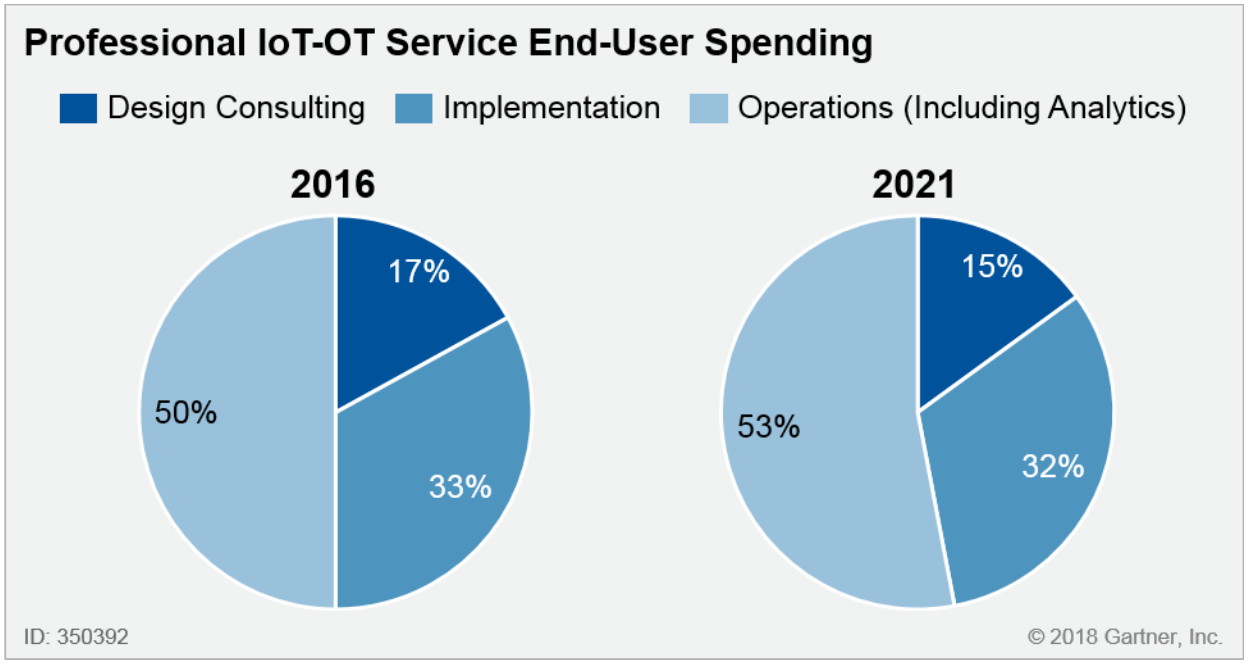
Digital Twins

"Exploiting Digital Twins to Drive Ecosystem Strategies": Digital-twin-enabled collaboration will be utilized to achieve leadership across digital ecosystems. CIOs building and expanding their digital business strategy will need to develop comprehensive digital twin models, analytics frameworks and multiparty collaboration capabilities.

IoT Organizational Challenges Have Emerged

As per the results of the 2017 IoT Strategies Survey, C-level involvement, particularly CEOs and CIOs, is common during this early adopter phase of IoT. In addition, most of the surveyed organizations have core members of their IoT team coming from multiple functional groups and reporting to formally organized teams. IT is the chief source for members of the core team. More organizations also indicated that they involve external providers after the objective and strategy setting phase; their preferred model changes in each stage, becoming more performance-driven as the indicators become more firm. The growth of external providers can be seen in our latest IoT forecast (see Figure 2 and "Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017").

Figure 2. Professional IoT-OT Service End-User Spending, 2016 Versus 2021



Source: Gartner (April 2018)

Resource concerns dominate, with the surveyed organizations selecting cost/funding (38%) and staff skills (36%) as the most prevalent nontechnical barriers. Inadequate budgeting, lack of know-how in the core team and lack of support from other functions were identified as reasons for failure of IoT projects by nearly one in five organizations.

Related Research

"Digital Disruption Profile: IoT Drives Rethinking Business Models, Processes and Skills": As one of the most disruptive trends in the past decade, the IoT is creating an opportunity to enhance or transform business models. In response, CIOs will need to prepare their technology, infrastructure, organization and team skill set capabilities.

"CIOs in Midsize Enterprises Must Align Their IoT Ambitions With Their Capabilities": The potential complexity of IoT creates a particular set of challenges for MSEs. To overcome these challenges, MSEs must choose technologies and partners that complement their capabilities and reduce IoT risks.

"2017 Strategic Roadmap for Successful Enterprise IoT Journeys": Differentiating between IoT, OT and IT is a critical element CIOs must be well-versed in. IT and OT approaches will need to be adjusted for IoT.

"I&O Leaders Must Get Involved With Current or Planned IoT Initiatives": Many I&O leaders are unaware of their organization's ongoing IoT initiatives. To overcome this and avoid stalled IoT projects, I&O leaders must proactively push to become more involved in the identification and tracking of all IoT initiatives.

"IoT: Think Big, Start Small, Move Fast": The deployment of IoT solutions is creating challenges for many firms across all industries. IoT frameworks must be deployed incrementally, while emphasizing business priorities across the enterprise and ensuring scalability, extensibility and flexibility.

"Three Strategies to Achieve Better-Than-Planned Outcomes for IoT Projects": The primary objective of the IoT Strategies Survey was to understand both the practices for IoT strategy development and the execution responsibilities within organizations that have already adopted IoT.

"Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus": As companies increasingly rely on IoT to improve their operations or products, expectations for IoT ROI and scale also increase. IoT investments will need to be increased incrementally, and quick returns will need to be targeted as a hedge against unrealistic or excessively long-term IoT project ROI targets.

"Market Trends: Strategies for Optimizing IoT POCs": The vast majority of POCs run by TSPs for enterprise customers do not result in a recurring paid engagement, particularly outside of the provision of hardware and software products. Efforts must be made to only invest in those clients that are serious about implementation.

"Three Ways to Listen to the Voice of 'Things' in the IoT": By 2020, Gartner estimates there will be 20 billion connected things, and their role and influence is set to dramatically increase over the next 10 years. A team must be established to develop an architecture and governance structure that supports the business unit's "treating things as customers" initiatives.

"Best Practices to Augment Employees With Wearable Technologies": Wearable technologies are capable of providing value; however, organizations are unaware how this value can best be provided.

"Three Key Development Practices to Implement Effective Enterprise Augmented Reality Applications": AR is being used by organizations to improve workflows and business processes. This note provides guidance to application leaders who are driving their organization's mobile and digital application strategies via AR.

"IoT Security Primer: Challenges and Emerging Practices": Increasingly, low-level security incidents are becoming a risk that CISOs must take seriously. This note explains how those incidents are changing, what that change means for security, and how CISOs can position their incident response programs to handle this change.

"The Death of IoT Security as You Know It": An unclear definition has led to confusion around the concept of IoT security. This note examines how security and risk management leaders can refine organization communication, restructure program management and apply new approaches to their IoT projects.

"Field Service Management Processes Must Change to Benefit From the Internet of Things": Maturing IoT elements are transforming FSM applications. Application leaders supporting field service should study this report to learn how to adjust their business model, technology and operational approaches in order to derive cost and customer experience benefits from the IoT.

"Modernize Your Endpoint Classification Systems to Drive Business Value": New kinds of endpoints like IoT sensors and wearables are entering organizations in large volumes, and current ways of classifying them are inadequate. Multiple classifications for endpoints must be used to ensure all relevant information is captured.

How to Integrate IoT Into the Enterprise Architecture

"Survey Analysis: Improve Your IT Competencies to Tackle Expanding IoT Projects," reveals that IoT solutions have moderate to high impact across key functional categories of business applications, with CRM and ERP as the ones most likely to be impacted. No provider is capturing the majority of net-new IoT project spend, but traditional IT vendors are well-positioned to capture significant share. Owner-operators (for example, hospitals, power plants and manufacturers) usually have IoT-enabled products from different manufacturers, which substantially complicates IoT integration. Data security is a top concern at the IoT solution planning stage. However, after implementation, both data security and data quality are key concerns. Finally, organizations are struggling with solution quality assurance (testing and simulation) of end-to-end IoT solutions because IoT solutions are hyperconnected, distributed complex systems. Therefore, even small changes in one part of the system can create significant unintended consequences in other parts of the system. Close to a quarter (23%) of companies surveyed do not perform or plan to perform end-to-end IoT solution testing.

Other key challenges with regard to IoT implementation include the following:

- Lack of focus on end-user experience
- Use of legacy systems
- Lack of data protocol standards
- Legal, regulatory and rights issues
- Availability of network coverage
- Power consumption
- Cost of sensors and equipment

Related Research

General

"Survey Analysis: Recommendations to Help You Scale IoT Implementations": IoT projects are evolving, and now adopters of these technologies are moving from simpler, experimental projects to more complex early stage production. This note highlights the IT competency investments that are needed to overcome scaling challenges.

"A Guidance Framework for Developing an IoT Proof of Concept": Developing a POC is a critical step in building an IoT system, but it is challenging because of the lack of vendor-neutral methodologies. This note provides a step-by-step procedure for technical professionals based on a small-scale IoT POC.

"A Guidance Framework for Architecting the Internet of Things Edge": Technical diversity and integration complexity are two of the challenges that are associated with the architecting of the IoT edge. This analysis provides an in-depth look into designing an IoT edge architecture.

"A Guidance Framework for Testing IoT Solutions": There are harsh consequences when IoT solution problems arise and failures occur. This note provides the key steps and priorities necessary to overcome the testing challenges of IoT solutions.

"Market Guide for IoT Integration": IoT project implementers cite integration as a top technical challenge. To help ensure successful deployment of IoT projects, application leaders must understand that IoT integration capabilities vary widely and seek providers with integration capabilities that fit their needs.

"Market Guide for IoT Service Providers": Fragmentation and challenges identifying best-fit providers have led to difficulties for buyers in the IoT service provider market. This research aimed at CIOs provides an overview of the various types of IoT service providers in the market today.

"'Zombie' Vendors and Other Pitfalls for CIOs Created by Oversupply in IoT": There is a very real threat of the emergence of a set of "zombie" vendors that has obligations to support a set of customers. A strict evaluation criteria must be developed for vendor selection, in particular when selecting vendors with large tent-pole clients that will all but guarantee ongoing support.

"Decide If You Should Use Containers for Your IoT Project": The possibility of using containers as a mechanism to deploy IoT systems is a strategy IoT architects have begun to evaluate. This research note details this strategy and informs I&O leaders that not all IoT applications are suitable for containerization.

Communications

"Enterprises Must Have a Device Communications Strategy for IoT": Enterprises deploying IoT devices are encountering disruptions due to inadequate vendor information about IoT device communications capabilities. Device connectivity policies must be enforced to ensure alignment between IoT performance requirements, devices and network functionality.

"When and Why Enterprises Should Implement RFID to Track Critical Assets": Many types of technologies are considered "RFID." Enterprises that use the wrong technology either will get suboptimal outcomes or will fail. This note explores the need for the business processes to be redesigned first to determine the value that implementing RFID will provide to the overall solution.

Data Management

"Ten Critical Data Management Implications for Your Internet of Things Initiatives": There are a number of data-related implications that now affect organizations due to the rise in IoT initiatives, technologies and architectures. The 10 most critical impacts data and analytics leaders will face are discussed in detail in this research note.

"How Data Sovereignty Will Kill Your IoT Strategy and What You Can Do About It": With the explosion in IoT devices, a huge amount of personal data is being gathered that will be in breach of sovereign privacy legislation. Distributed data storage strategies must be deployed for countries that restrict the geographic storage of data where collection of personal data is essential for service.

"Avoid Being Crushed by the Avalanche of Connected Car Data": The amount of data generated by connected vehicles could dramatically exceed most automakers' storage, handling and analytics capabilities. A plan must be created for gathering data by determining what concerns the company is trying to address, and then there must be a focus on filtering vehicles and gathering data.

Security

"Five Disturbing Trends in IoT Security for 2018, and What You Can Do About Them": As IoT deployments increase, security and risk management leaders should make note of key IoT security trends caused by these deployments, and of resulting actions needed.

"How to Create Privacy, Safety and Reliability Through Internet of Things Security Architecture": The scale and diversity of IoT technology pose a sizable security challenge. Strong practices and architecture, focusing on the IoT edge in particular, are critical to managing digital business risk.

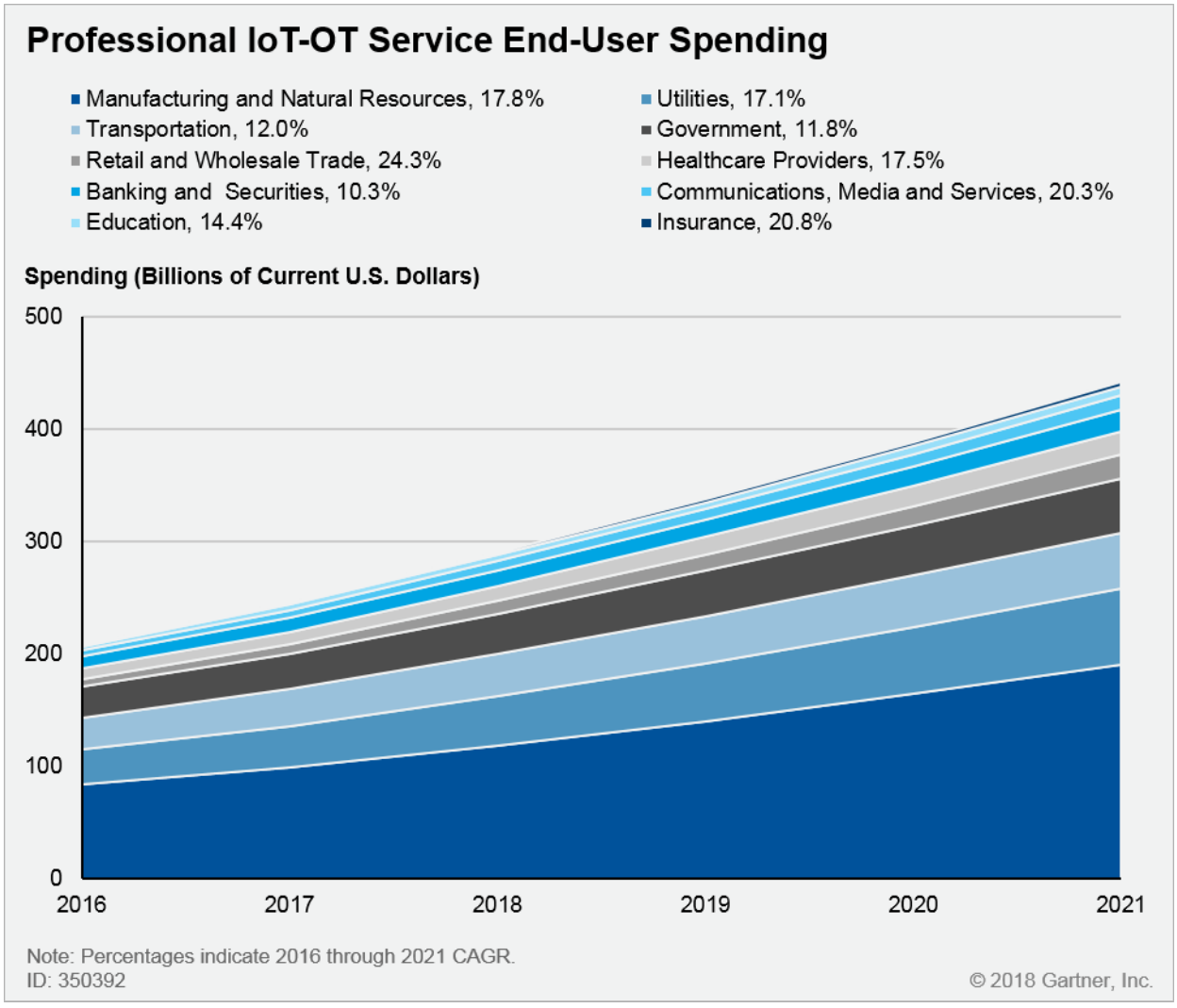
"Key IAM Considerations for IoT Platforms": IoT platforms are the hub of most IoT deployments and are a risk aggregation point. A personalization process must be implemented that establishes trust

when registering devices, regardless of whether the devices are personalized at the factory or in the field.

IoT Best Practices in Key Industries

According to Gartner's latest forecasts, there will be 25.1 billion IoT endpoints deployed by 2021. In addition, IoT services spending is poised to grow to almost $450 billion per year by 2021 (see Figure 3).

Figure 3. Professional IoT-OT Service End-User Spending by Industry (CAGR), 2016-2021



Source: Gartner (April 2018)

As shown in Figure 3, some of the key industries that will experience healthy growth over the next few years include manufacturing, government (smart cities) and healthcare. For example, in manufacturing, some of the key trends that we have identified include the following:

- Most of the companies are looking to upgrade or introduce modern IoT capabilities to improve manufacturing operations in the next 12 months.
- The top technology focus for improvement in manufacturing operations through IoT is process control and automation.
- Automation of many manufacturing operations is expected in the future, with the key objectives of cost reduction and efficiency.

Related Research

"IoT Project Metrics (KPIs) Help Ensure Your Industrie 4.0 Outcomes": When it comes to implementing supporting IoT solutions, there are often difficulties aligning IoT projects with the business objectives defined in an organization's Industrie 4.0 initiatives. This note examines the need for CIOs to apply measurable KPIs to help improve their IoT project planning and monitoring outcomes.

"Market Trends: Predictive Maintenance Drives IoT in Manufacturing Operations": Innovative manufacturers are leading the way with IoT for improved asset management, operational efficiency and cost reductions. There should be an emphasis on standardizing integration products and services, as well as building domain expertise.

"Plan Intelligent Manufacturing Aligned With the 'Made in China 2025' Policy": China's "Made in China 2025" policy is leading many organizations with plants in the country to consider using IoT and AI technologies to develop intelligent manufacturing to comply with this policy. There should be adequate planning and collaboration with multiple stakeholders in order to succeed.

"Debunking Myths and Misconceptions About Industrie 4.0": The vision of Industrie 4.0 is being hindered by misunderstandings, false perceptions and prejudices. This research examines the need for CIOs to test and validate three "myth conception" assumptions against their current initiatives to generate maximum business value from Industrie 4.0.

"Market Trends: China's Smart City Construction Enters a New Phase: Will You Be Ready?": The Chinese government's "New-Type Smart City" initiative aims to guide future smart city projects in areas of standardization, government engagement, and financing and delivery models. This research explores the need for technology strategic planners at IoT platform vendors to realign their strategies to address these concerns.

"Go-to-Market Lessons for IoT Vendors From Four Smart City Projects in Asia/Pacific": This document sets out the lessons collected from interviews with key officials in smart city planning departments in Singapore, Taiwan, China and India. The coverage was deliberately selected to represent Asia/Pacific countries that were at various stages of maturity in their smart city implementations.

"Market Insight: Healthcare IoT in 2018 — Sell to CEOs and Set Realistic User Expectations": Currently, the adoption levels of IoT across health systems is uneven and confusing for sellers to

understand. This note provides guidance to technology strategic planners who are seeking to improve their vertical go-to-market effectiveness in the healthcare industry.

"Market Insight: Wearables in Healthcare Ecosystems Get Rolling in 2018": Gartner estimates smartwatches and wrist-based tracker sales totaled 155.4 million units in the past two years. This note examines the need for technology product management leaders to reconsider their product roadmaps for B2B and B2B2C applications.

"Three-Step Plan for Insurance CIOs to Build an Effective IoT Initiative": Most insurance CIOs have not had enough evidence of the value that IoT data can deliver to key areas of insurance business. This research summarizes the practical experience of several insurance IT leaders from around the world that apply IoT data to manage their product and service portfolios.

Related Priorities

Table 1. Related Priorities

Priority	Focus
Succeeding With Semiconductor-Based Technology	This initiative enables technology providers to improve their competitiveness by using products and services out of the semiconductor and electronics industry, and investing in emerging technologies.
Delivering Effective Identity and Access Management Capabilities	The delivery of effective IAM capabilities involves tools and best practices that manage identity, privileges, access and trust to facilitate security, risk management and business imperatives.
Building and Expanding a Digital Business	Digital business is the creation of new business designs by blurring the digital and physical worlds. Digital business involves the interaction of people, businesses and intelligent "things."
Supply Chain Strategy, Leadership and Governance	Designing strategy, optimizing networks, developing the organization and managing performance must work interdependently to execute an efficient demand-driven supply chain.

Source: Gartner

Gartner Analysts Supporting This Trend


Nathan Nuttall, Research Director


Emil Berthelsen, Research Director


Denise Rueb, Research Director


Aapo Markkanen, Research Director


Peter Havart-Simkin, Research Director


Sanjit Ganguli, Research VP


Paul DeBeasi, VP Distinguished Analyst


Ted Friedman, VP Distinguished Analyst

Related Resources

Webinars

"Securing the Internet of Things: An Architectural and Risk-Driven Approach"

"AI on the Edge: How AI and IoT Will Catalyze New Digital Value Creation"

"How to Architect the IoT Edge"

"IoT for Midsize Enterprises"

"Maximizing the IoT's Potential in Manufacturing"

Articles

"Wearables Hold the Key to Connected Health Monitoring"

"How to Listen to the Voice of 'Things' in the IoT"

"The Emergence of the IoT Architect"

"Prepare for the Impact of Digital Twins"

Acronym Key and Glossary Terms

AI	artificial intelligence
AR	augmented reality
B2B2C	business to business to consumer
BI	business intelligence
CAGR	compound annual growth rate
CISO	chief information security officer
FSM	field service management
I&O	infrastructure and operations
IoT	Internet of Things
KPI	key performance indicator
ML	machine learning
MSE	midsize enterprise
NB-IoT	NarrowBand IoT
OT	operational technology
OTT	over-the-top
POC	proof of concept
SME	subject matter expert
TSP	technology and service provider

Evidence

[1] **2018 Gartner CIO Survey**

This survey was conducted online from 20 April through 26 June 2017 among Gartner Executive Programs members and other CIOs. Qualified respondents were the most senior IT leader (CIO) for their overall organization or a part of their organization (for example, a business unit or region). The

total sample is 3,160, with representation from all geographies and industry sectors (public and private). The survey was developed collaboratively by a team of Gartner analysts, and it was reviewed, tested and administered by Gartner's Research Data and Analytics team.

[2] **Gartner IoT Strategies 2017 Survey**

Results presented are based on a Gartner study conducted to gain insight about trends among adopters of IoT. The research was conducted online from June through August 2017 among 717 respondents in four countries: Germany, Japan, the U.K. and the U.S. All respondents were screened for active employment in organizations with more than 500 employees who were currently using IoT— either in their internal operations (internal IoT) or touching their customers or suppliers (external IoT), or both. The respondents were from a good representation of industries under manufacturing, retail, healthcare providers, transportation, utilities, and natural resources and agriculture-related verticals. Respondents also were required to have a high level of responsibility in IoT decisions related to determining business objectives, setting the IoT strategy, and measuring or determining how to measure ROI/effectiveness of IoT initiatives. Quotas were established by country to ensure a good representation in the sample. The survey was developed collaboratively by a team of Gartner analysts who follow the market, and it was reviewed, tested and administered by Gartner's Research Data and Analytics team. The results of this study are representative of the respondent base and not necessarily the business/market as a whole.

Gartner IoT Solutions Implementation Trends Study

This study was conducted to collect information on best practices for IoT deployments and strategies for developing IoT solutions. The research was conducted using computer-assisted telephone interviewing and online methodology during June and July 2017 among 202 respondents in the U.S., Germany, China and Japan.

Participating organizations were screened to have already delivered IoT solutions or have working projects in progress. All industries qualified, except technology vendors, business consulting services and investment services. The largest industry representation was from manufacturing (25% of the sample).

Respondents were required to have involvement/roles in IoT implementation within organizations with annual revenue greater than $100 million.

The survey was developed collaboratively by a team of Gartner analysts who follow IoT. It was reviewed, tested and administered by Gartner's Research Data and Analytics team.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp