IoT Technology Disruptions: A Gartner Trend Insight Report

Published: 15 June 2017 **ID:** G00331334

Analyst(s): Sanjit Ganguli, Ted Friedman

IoT's rapidly evolving technologies have ushered in innovative disruptions at a breakneck pace. This report highlights Gartner research that covers these IoT technical disruptions in five key areas: security, artificial intelligence, data and analytics, communications, and endpoint technology.

Opportunities and Challenges

- The unique volume, variety and velocity characteristics of IoT data present scalability and integration challenges to harness and gain business insights, and may require an architectural realignment.
- Communication and endpoint IoT technologies are rapidly evolving to support new and disruptive IoT use cases, with numerous competing and fragmented standards and protocols.
- The deployment of IoT technology introduces a multifaceted "attack surface" that must be secured.

What You Need to Know

- Advances in artificial intelligence algorithms, advanced analytics like deep learning and new data management approaches enabled by abundant computational power can successfully expedite the delivery of business outcomes promised by IoT.
- IoT communications networks should be implemented to balance network efficiency and compatibility, based on an understanding of evolving standards, protocols and implications to existing enterprise networks.
- IoT's multifaceted attack surface can be secured with new and innovative approaches in IoT security, including advanced asset discovery, identity management, authentication, visibility and security analytics.

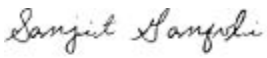
Insight From the Analyst

Technology Evolving to Turn IoT Hype Into Reality

 Sanjit Ganguli, Research Director

 Ted Friedman, Vice President, Distinguished Analyst

The Internet of Things (IoT) has seen years of growing interest among enterprises and service providers with the promise of enabling new digital business initiatives and unlocking operational efficiencies. Practically, much of this interest has been rooted in the discovery phase of IoT, where CIOs and CTOs wondered, "What is IoT?" and "Why do I need to care?" Today, as demonstrated in our published research and observed in our client interactions, this has transitioned to the implementation phase, where executives are asking, "How do we get started with IoT?" (see the Evidence section). This shift is largely fueled by the disruptions in IoT technology that have occurred, enabling a feasible and achievable path to creating business value.



Theme

Advances in artificial intelligence, data and analytics, security, communications and endpoint technology have been critical IoT enablers. Their applicability and state of the art are evolving rapidly, and organizations planning and deploying IoT solutions need to know what is new and emerging in these technology areas, and answer the questions:

- How will these IoT technology disruptions impact my ability to drive new digital business and become more operationally efficient?
- How will these technology developments disrupt my current IoT initiatives?
- Will these technology disruptions in IoT eventually disrupt traditional IT and other areas of the business?

In this IoT Trend Insight report, we highlight the Gartner research that analyzes these very disruptions. This research will highlight Cool Vendors that are innovative and game-changing,

market trends in evolving technology areas, best practices for enabling these technologies, and vertical-industry-specific use cases.

This collection will be organized into the five disruptive technology areas, as shown in Figure 1:

- Sensing: IoT Endpoints
- Communicating: IoT Communications
- Securing: IoT Security
- Understanding: IoT Data and Analytics
- Acting: IoT Artificial Intelligence

Figure 1. Five Areas of IoT Technology Disruption

Source: Gartner (June 2017)

Executive Overview

Definition

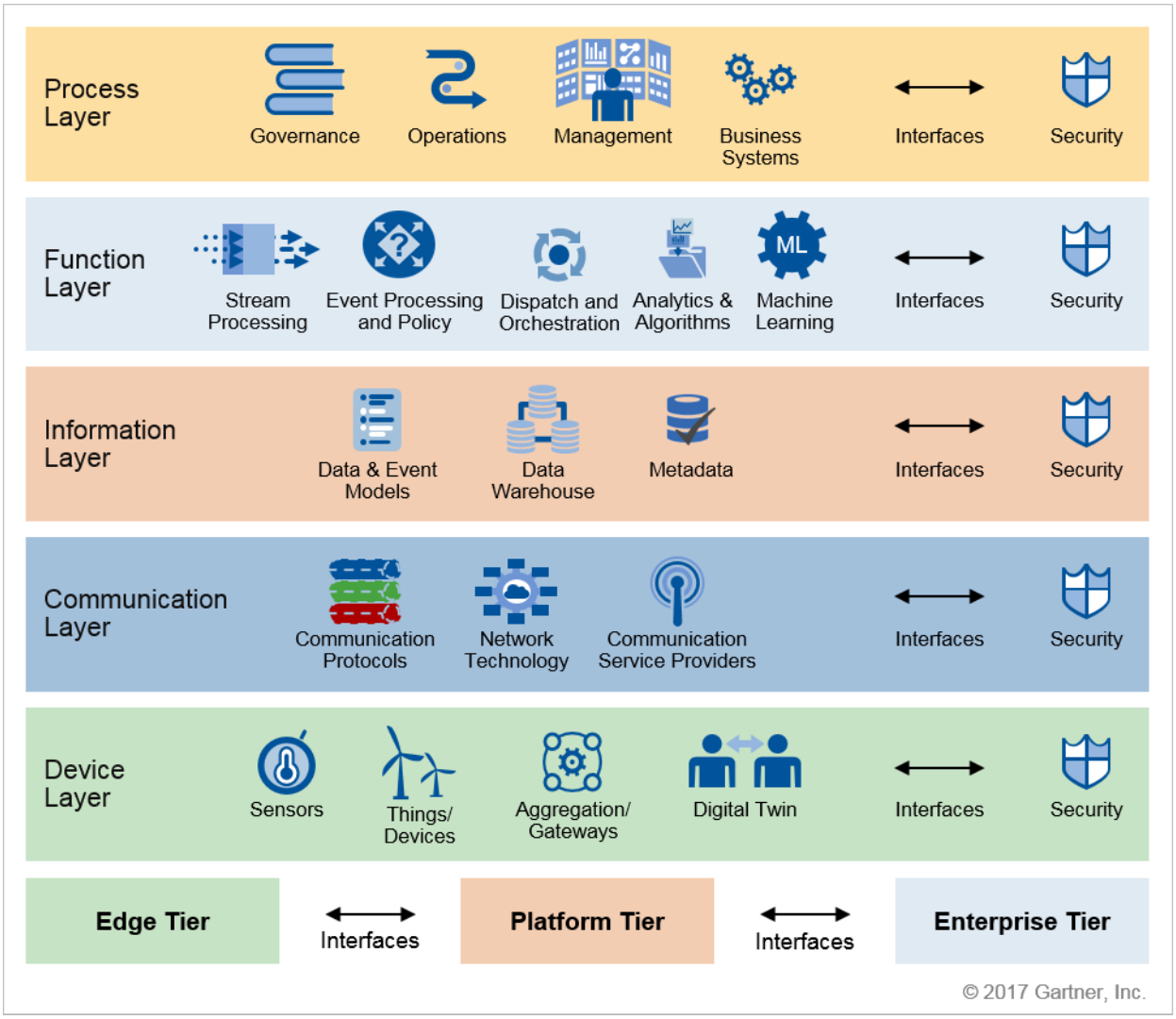
The Internet of Things is defined as:

> 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.

The various technology disruptions discussed in this research fall into different layers of the IoT Reference Model (see Figure 2). In the model, the layers define what capabilities an IoT component, function or process must possess, while the tiers define where a component, function or process operates in the IoT architecture. The interfaces define how data and control flow into, out of and through the system.

Endpoint technology inhabits the Device Layer; communications technology comprises the Communication Layer; data and analytics reside in the Information Layer; and artificial intelligence exists on the Function Layer. Security technology, as it is pervasive in its nature, touches each of these layers (see "Architect Your Internet of Things System by Using the Gartner IoT Reference Model"). Understanding the interaction and interdependence of each technology area with the IoT system as a whole will enable a better understanding of their impact.

Figure 2. Gartner IoT Reference Model at a Glance

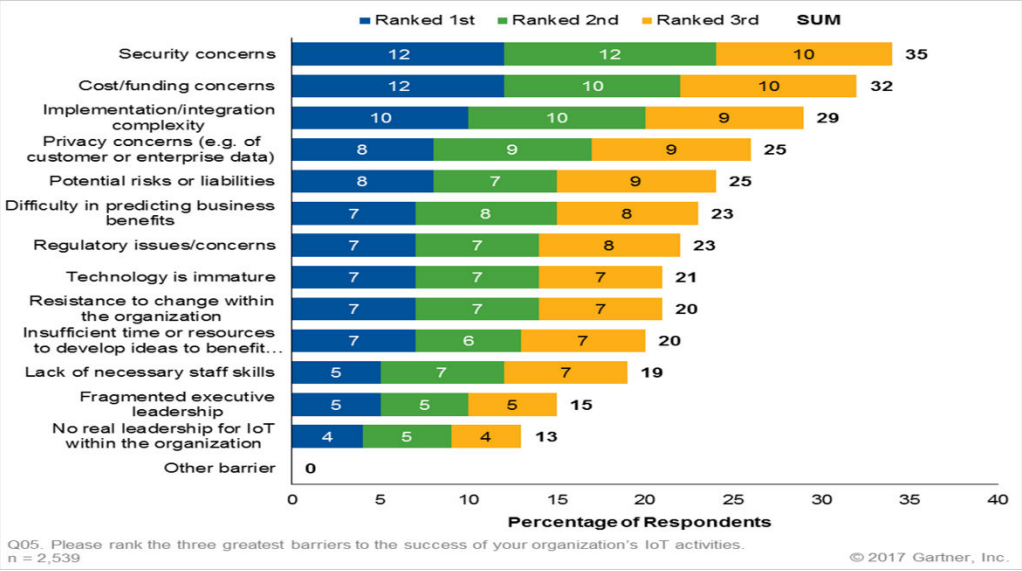


Source: Gartner (June 2017)

Finally, it is important to not think of these technology disruptions as trends that will only impact IoT initiatives. Instead, consider their impacts within the larger context of IT and digital business. New IoT communications technologies will likely have a major influence on how enterprise networks are architected in the future, with enhancements in wireless networking and edge computing. Similarly, data analytics and artificial intelligence (AI) technologies, which will enable the harvesting of knowledge from the massive amounts of IoT data, can be applied to traditional enterprise IT or business data to enable new digital business initiatives. Furthermore, the increasing miniaturization, dynamism, mobility and modularity of traditional IT systems will, over time, resemble many of the characteristics of IoT systems.

Given all of the promise of IoT technology, there remain significant perceived barriers to IoT success in the minds of CIOs and CTOs. While their perception of IoT has changed after their initial investigations, much of their concern is based on the current deficiencies of IoT systems. In fact, Gartner's latest Internet of Things Backbone Survey showed that security was cited as the top barrier to IoT success (35% of respondents), with privacy concerns (25% of respondents) and potential risks and liabilities (25% of respondents) all in the top five. Additionally, the complexity of implementation and integration ranked third with 29% of respondents, and 21% felt that the technology itself is immature (see "Survey Analysis: 2016 Internet of Things Backbone Survey" and Figure 3). The ability to stay abreast of IoT's technology disruptions and influence IoT initiatives to make best use of them will be paramount to ensuring success of future IoT projects and overcoming these barriers.

Figure 3. Barriers to IoT Success



Source: Gartner (June 2017)

Research Highlights

Sensing IoT Endpoints

Endpoints of the Internet of Things will grow at a 32.9% compound annual growth rate (CAGR) from 2015 through 2020, reaching an installed base of 20.4 billion units. With this massive growth in the number of endpoints come major technology disruptions in sensor, device, gateway and digital twin technologies. This is coupled with the growth of edge computing technologies, where computing and analytics move closer to the endpoint to enable more real-time use cases. Understanding these technology disruptions can help minimize the complexity involved in selecting, deploying, managing and operating these IoT endpoints. The research highlighted here discusses many of these disruptions.

Related Research

"Cool Vendors in 'Thingification', 2017" focuses on desktop development tools that enable CIOs to create IoT prototypes and small-run projects within existing resources. Cool Vendors in this research each provide unique technologies that can enable new business models with minimal investment.

"Cool Vendors in the Internet of Things, 2017" provides recommendations for CIOs looking to enable disruptive IoT solutions and business outcomes. These include supporting the business unit's IoT cost optimization or operational building projects by establishing a team to build an IoT requirements checklist and impact assessment. Key elements of the checklist and assessment include IoT architectural elements such as gateways, platform, security and integration into enterprise solutions.

"Cool Vendors for Smart City Applications and Solutions, 2017" provides CIOs with advice on how integrated smart data with cool software solutions containing multiple functionalities is vital for smart building, multimodal mobility and collaboration.

"Cool Vendors in Enterprise Wearable and Immersive Technologies, 2017" explores how I&O leaders struggle to build a complete platform to support wearable devices in the enterprise. It highlights innovative tools that go beyond hardware and addresses issues key to a successful enterprise wearable device strategy.

"Cool Vendors in Personal Devices, 2017" shows how new device categories like virtual personal assistant (VPA)-enabled speakers are evolving, going beyond voice UIs and integrating multimodal interactions (i.e., via cameras and displays) to create more contextualized and personalized experiences.

"Market Guide for Edge Computing Solutions for Industrial IoT" demonstrates that the edge computing solution vendor landscape is rapidly evolving. Most vendors in the IoT market have recognized that edge computing is an integral part of an IoT solution. Not all data needs to be sent to the cloud or core data center, as that is cost-prohibitive, bandwidth-intensive, has performance implications or is not practical, as in the case of remote locations. Therefore, it is imperative to have data aggregation and processing deployed at the source of data generation as an aid to rapid decision making using real-time analytics.

"Market Trends: The Connected Home, 2017" highlights how 2017 promises to be an exciting year for the connected home. We fully expect big-brand virtual personal assistant (VPA)-enabled speakers, such as Amazon Echo and Google Home, and home ecosystems, such as Works with Nest, Apple HomeKit and the growing number of Alexa-enabled devices, to breathe new life into the connected home market, thanks to both the novelty and the network effect. But it is not just these giants that are likely to proliferate in the market.

"Market Trends: The Need for Real-Time Insights Offers Market Opportunities in Edge Computing" demonstrates how edge computing provides alternative design elements that can be used, depending on the specific application requirements. In edge computing, cloudlike functionalities, such as compute, storage and networking (including applications of virtualization and software-

defined data center technologies), are pushed to the edge of the network — where IoT data is generated by sensors and other IoT endpoints. Edge computing serves as the decentralized extension of cloud at the edge of the campus networks, at the edge of the data center networks and at the edge of the cloud.

"Emerging Technology Analysis: Energy Harvesting Enables Autonomous IoT Endpoints" shows that IoT deployments face significant and increasing battery management costs as networks scale up and move to battery-operated endpoints for increased autonomy and lower installation costs. Gartner forecasts between 2 billion and 2.5 billion battery-operated endpoints by 2020. However, battery management issues are often underestimated, resulting in delayed IoT initiatives and overbudget IoT costs.

"Architect Your Internet of Things System by Using the Gartner IoT Reference Model" describes the Gartner IoT Reference Model and three-step process. The reference model provides a framework that enables technical professionals to define their system architecture. The three-step process provides a methodology to guide technical professionals toward this goal. Organizations can use the model and process irrespective of what technology they use, which vendors they select or what business outcome they are trying to achieve.

"Cool Vendors in IoT Edge Computing, 2017" explores the growing need for real-time insights closer to the point of IoT data generation. IT leaders responsible for IT/OT alignment face an increasing urgency to deploy decentralized, scalable and secure computing technologies at the edge of data center, cloud and campus networks.

"Use the Internet of Things in Smart Buildings to Achieve Work-Life Ambience" focuses on smart buildings, which have gained the attention of real-estate and facilities management leaders under pressure to reduce operational costs, meet sustainability goals and improve the employee experience. CIOs can use this research to plan how to work with their colleagues to achieve all three.

Communicating: IoT Communications

The IoT communications space is in the midst of a standards and protocol battle, with far-reaching implications in the technology choices that IoT end users make. Readers should consider the varying technologies across a wide range of coverage, including:

- PAN — 802.11ad, Bluetooth 4, Near Field Communication (NFC)
- LAN — 802.11n, ZigBee, Thread, Bluetooth 5
- WAN — LoRa, Sigfox, narrowband IoT (NB-IoT), LTE-M

Selecting the correct network architecture to address the IoT application requirement requires an understanding of the network's ability to address performance, scalability, security, interoperability and device connectivity. Research highlighted here discusses the benefits and weaknesses of these communications technologies and their broader implications on networking architecture.

Related Research

"Market Trends: LoRa Offers Low-Risk, High-Reward LPWA Opportunity" describes how Sigfox, Random Phase Multiple Access (RPMA), LoRa and NB-IoT are competing for market share, but have different business model risks. This research highlights the options for technology strategic planners at semiconductor companies who risk missing market opportunities by wasting investment in inappropriate wireless technologies for IoT solutions.

"The Role of the Alarms and Notifications Platform in the Real-Time Health System" explores how alarms and notifications (A&N) platforms acquire, filter, manage and deliver clinical alarms and event data from patient monitors and medical devices. As a key enabler of the real-time health system, healthcare provider CIOs will need to familiarize themselves with the A&N platform value proposition. As more systems and devices are engaged in the delivery of care, at least one A&N vendor is positioning its platform as an IoT platform.

"2017 Strategic Roadmap for IoT Network Technology" highlights Gartner research that has identified four basic IoT network architecture domains, each with its own communication technologies, as well as network architecture dependencies and opportunities. Selecting the wrong network architecture for the desired outcome means reducing the network's ability to address performance, scalability, security or device connectivity to address the IoT application requirements. Unfortunately, it typically also means throwing everything away and starting from the beginning for Round 2 to provide network communication for the IoT project.

"The Top Three Impacts of IoT on Networks" highlights the regular failure of IT to identify and remediate the IoT implementation's impact on network elements, creating headaches for networking leaders.

"Automaker CIOs Should Move Quickly to Implement Over-the-Air Update Capability" focuses on over-the-air (OTA) capability as an absolute requirement for the automotive industry to begin using new technology and to try out different business models. Despite the fast-spreading connectivity of vehicles, automakers have been slow to add this capability, and have limited it mostly to noncritical entertainment functions. The pace of introductions of the capability will increase.

"Emerging Technology Analysis: Time-Sensitive Networking" looks at time-sensitive networking (TSN) as an IoT wireless and wired solution that can overcome the weaknesses of Wi-Fi and Ethernet. Technology strategic planners focused on the IoT and enterprise connectivity must develop an aggressive pricing strategy by limiting functionality premiums to entice organizations to upgrade to TSN capabilities as part of normal switching refresh cycles.

"Innovation Insight: How CIOs Can Leverage the IoT to Break Down Building Management Silos" is recommended for business leaders looking to boost their green credentials. According to Energy Star, the average building wastes 30% of its energy through inefficiencies. Much of this energy can be conserved by using the IoT and IT infrastructure to enable communication between the different building management systems.

"How to Realign ITOM Product Offerings for IoT Use Cases" explores how, while it may seem that marketing and selling IT operations management (ITOM) products for IoT use cases may be an easy

and natural extension, the reality is that the vast majority of vendors don't have the vertical-specific capabilities or expertise to viably participate in the IoT market. Many of these vendors also lack an understanding of whether the data collected can assist in solving the vertical market business problem.

Securing: IoT Security

IoT security is cited as the top barrier to IoT success, as the explosion of varying types of IoT endpoints creates an attack surface that has never before seen. IoT-security-related technology disruptions have been broad in their scope and can be broken down into the following security methods:

- Asset discovery, profiling and tracking
- Authentication
- Network-based protection
- Secure software development
- Visibility through monitoring, detection and response

The integration of these IoT security technologies with traditional IT and operational technology (OT) security infrastructures and practices remains a challenge, and is exacerbated by the specific vertical and use-case nature of IoT systems. Research covered here highlights both technology-specific and vertical-industry-specific trends in IoT security technology.

Related Research

"Cool Vendors in IoT Security, 2017" describes vendors that bring notable approaches to software composition analysis, enterprise mobility management and asset discovery. Security and risk management leaders should see these offerings as leading indicators of emerging priorities in IoT utilization.

"Semiconductor Design, Key Management and In-Situ Updates Will Enable Secure IoT Solutions" considers how the widespread deployment of IoT endpoints amplifies the possibility for major security risks. Technology product management leaders at semiconductor vendors that fail to integrate security features and processes into their IoT-targeted products will lose design-ins and suffer brand devaluation.

"Top 10 Strategic Technology Trends for 2017: Adaptive Security Architecture" drives home the fact that security considerations must be factored in from the earliest stages of solution design. Existing blocking and prevention capabilities are insufficient — comprehensive protection requires an adaptive process to predict, prevent, detect and respond to security breaches.

"Market Trends: Grow Your IoT Security Business by Investing in Real-Time Discovery, Visibility and Control" focuses on the chief information security officer's (CISO's) concern that security and risk management leaders in the consumer and industrial IoT verticals don't know what assets they have,

whether or not assets are connected to the internet, and whether protection is required. This is due to a lack of network and device visibility; discovery is a prerequisite to IoT security.

"Healthcare Provider CIOs Need to Address IoT's Security Risks Now" shows that the widely varied data from almost every aspect of daily operation in a healthcare facility is a security risk. This data includes specifics such as how the facility is performing physically (heating/cooling/lighting) and patient condition — both within the hospital and at home — with many more use cases to be discovered, all of which must be protected.

"Don't Let Your IoT Projects Fail: Use the Right IoT Security Pattern to Protect Them" shows that security and risk management leaders must recognize that IoT projects have security risks and that they must do something about them today, including identifying the security controls and technology needed for the IoT pattern used for the project.

Understanding: IoT Data and Analytics

Data from things and the insights derived from that data fuel the business value and transformative nature of IoT. Many existing data and analytics capabilities can be applied to IoT initiatives and IoT data, but organizations need to modernize in three key areas:

- Styles of analytics (expanding into predictive)
- Styles of integration (diversifying and adding real-time and virtualized)
- New data persistence models (cloud and NoSQL)

Research highlighted here exposes critical technology developments in data and analytics that are directly applicable to IoT.

Related Research

"Competitive Landscape of IoT Platform Vendors" highlights that there is no dominant provider of IoT platforms. In fact, the market is extremely crowded with a very broad range of companies, with a mix of startups, big industrial players, system integrators and traditional IT companies all competing to provide solutions in the space. In addition, a significant number of vendors are adding IoT capabilities to their portfolios, making the landscape unclear.

"Align Data Integration and Data Quality to Strengthen IoT Solutions" looks at the rapid evolution toward digital business, where IoT projects create significant data management challenges for integration and quality. A process for sharing and certifying IoT data requires technologies such as data quality tools that must work alongside data integration activities.

"Cool Vendors in Internet of Things Analytics, 2017" profiles innovative vendors in IoT analytics. These vendors focus on some of the hottest areas of IoT — visibility into the manufacturing process, enabling new analytics users, and device diagnostics, repair and maintenance — to help data and analytics leaders increase the value of IoT projects.

"Use Master Data Management Principles for Identity Management in the Internet of Things" considers that complex digital business initiatives include IoT devices which can involve hundreds of thousands or even millions of "entities" — digital identifiers of people, devices, applications or subsets of those entities. The means to identify, label and manage those entities can already be found in multiple management systems and technologies.

"A Guide to Deploying IoT Analytics, From Edge to Enterprise" shows how, for successful digital transformation, technical professionals must establish new ways to leverage and monetize IoT data by embedding analytics throughout the IoT architecture. This report offers guidance on deploying analytics across IoT solutions, from edge to enterprise.

"Innovation Insight for Digital Twins — Driving Better IoT-Fueled Decisions" considers how exploiting the digital-twin concept is becoming an important innovation that enables stakeholders to monitor and make informed decisions about the state of the actual physical things, their context and the required action needed to optimize their future state.

"Market Guide for Energy Management Systems, IoT" shows that as IoT-based systems emerge, energy management systems (EMSs) have evolved into platforms that monitor and manage all energy use in a building, including the HVAC system, lights, major equipment, renewable energy and plug load. Consequently, EMSs not only enable energy management, but also create an environment of energy economics, sustainability and operational efficiency.

"The Impact of Event-Driven IT on API Management" explains how digital business trends — including the IoT, real-time decision making and microservice architecture — are driving application leaders to focus on event-driven IT.

"Embrace Your Bias to Enable Analytics Clarity" shows that bias is inherent in the development of analytic models, data selection and the associated algorithms. The bias continuum provides a discussion template to data and analytics leaders for transparently exposing statistical bias to ensure real business impacts.

"Harness Streaming Data for Real-Time Analytics" warns analytics leaders that stream processing compute platforms are the core of serving data for real-time analytics, especially for the IoT systems, yet mastering these platforms requires a mental shift toward treating data as dynamic, not static.

Acting: IoT Artificial Intelligence

AI will be used to render new insights, transform decision making and drive improved business outcomes. The complexity, speed and distribution of IoT solutions and the data they generate may obviate traditional decision-making techniques, both manual and automated. Advances in AI, in the form of new algorithms, increasing computational power and breakthroughs in deep learning, will enable transformative IoT solutions that would otherwise be impossible. This research highlights key trends in AI and critical connections to the IoT.

Related Research

"Develop Your Artificial Intelligence Strategy Expecting These Three Trends to Shape Its Future" looks at the three major trends to affect AI during the coming years, including better communication, deeper integration and richer ecosystems.

"AI on the Edge: Fusing Artificial Intelligence and IoT Will Catalyze New Digital Value Creation " describes how AI and the IoT are symbiotic technologies that will be the foundation of a new platform for digital business value creation. CIOs engaged in IoT initiatives should leverage these capabilities for strategic advantage.

"Market Guide for Conversational Artificial Intelligence in China" explores how the technology is progressing in China with a wide range of solutions, as the market remains immature and challenging.

"Market Trends: How AI and Affective Computing Deliver More Personalized Interactions With Devices" shows how current platforms for detecting and responding to emotions are mainly proprietary and specialized in a few isolated use cases. We expect Google, Apple, Facebook and Amazon to disrupt the emotion-sensing digital device market by offering tools that will enable affective computing for broader use cases.

"Market Guide for Augmented Reality" highlights how augmented reality solutions are poised for rapid growth, empowered by the IoT, digital business and next-generation smartphones. Enterprise architecture and technology innovation leaders must carefully evaluate providers as the market consolidates around platforms.

"Preparing and Architecting for Machine Learning" explains the business value machine learning (ML) provides, the basics of the architecture, process and skills needed for ML, and what steps should be taken to get started in ML.

"Top 10 Strategic Technology Trends for 2017: Artificial Intelligence and Advanced Machine Learning" focuses on the key drivers for IoT and machine learning that will impact all businesses.

"Prepare for Big Changes in Software and SaaS Pricing, Driven by AI and IoT" considers the upheaval in negotiations and software evaluation from changing service types.

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

Mark Hung

Alfonso Velosa

Benoit Lheureux

Earl Perkins

Saniye Burcu Alaybeyi

Eric Goodness

Tim Zimmerman

Svetlana Sicular

Whit Andrews

Related Resources

Webinars

"Cool Vendors for 2017: The Digital Nail Gets Hammered, So Be the Hammer"

"The IoT Roadmap for the Digital Business"

"Rapidly Architect Your IoT System With the IoT Reference Model"

"Digital Twins: The Future of Better IoT Fueled Business Decisions"

"The Gartner Top 10 Strategic Technology Trends for 2017"

"Preparing and Architecting for Machine Learning"

Articles

"Let Machine Learning Boost Your Business Intelligence"

"Navigating the Security Landscape in the IoT Era"

"Gartner Reveals 2017 Cool Vendors That Can Help Keep Pace With Digital Innovation"

"How to Address Threats in Today's Security Landscape"

"Digital Has Changed the Security Landscape"

"5 Steps to Address IoT Integration Challenges"

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Internet of Things Primer for 2017"

"IoT Communications Architecture Demystified"

"Hype Cycle for the Internet of Things, 2016"

"IoT's Challenges and Opportunities in 2017: A Gartner Trend Insight Report"

"Hype Cycle for IoT Standards and Protocols, 2016"

"Ready-for-Development Semiconductor Solutions Massively Reduce Drone Market Entry Barriers"

Evidence

The analysis and advice provided in this document are built from constant scanning of the market, as well as from the aggregation of analysts' experience and ongoing interactions with end users and technology and service providers. We used a range of sources to feed our perspective on the topics discussed in this document:

- Gartner customer inquiry and conversations, which has shown an average of 40% year-over-year increase in inquiry volume from IT leaders
- Discussions between Gartner analysts with expertise in key technologies or relevant vertical markets
- Previous Gartner analysis of digital business, IoT and related technologies

Gartner analysts also leverage secondary sources of information, including government agencies, standards organizations and so forth.

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