Predicts 2020: As IoT Use Proliferates, So Do Signs of Its Increasing Maturity and Growing Pains

Published: 16 December 2019 **ID:** G00463441

Analyst(s): Benoit Lheureux, Alfonso Velosa, Katell Thielemann, W. Roy Schulte, Avivah Litan, Barika Pace

As Internet of Things implementations proliferate, evidence of IoT's increased maturity (and some growing pain) is emerging. Application leaders should factor these predictions regarding the evolving state of blockchain, digital twins and security into their IoT implementations.

Key Findings

- Companies are increasingly experimenting with combined Internet of Things (IoT) and blockchain projects, and most use cases are to help achieve cost optimization.
- To help scale up their proliferating digital twin deployments, IoT implementers will increasingly acquire digital twins via marketplaces, as an alternative to other sourcing options.
- IoT security capabilities will increasingly be delivered via IoT platforms and general-purpose security products, rather than via stand-alone IoT security solutions.

Recommendations

Application leaders responsible for IoT should take these actions:

- Invest in combined IoT and blockchain projects particularly where a trusted, multiparty audited trail of data and events originating with IoT-connected "things" support desired outcomes.
- Leverage marketplaces as an open, consistent approach to acquiring digital twins to supplement other (more proprietary) sourcing approaches, to help scale digital twin use.
- Factor long-term viability of stand-alone IoT security providers into your IoT security solution evaluation, considering the likely volatility of the IoT security provider landscape.

Table of Contents

List of Figures

Strategic Planning Assumption(s)

By 2024, 75% of combined blockchain and Internet of Things (IoT) projects will have been implemented to help achieve improved cost optimization.

By 2024, over 100,000 digital twin models will be available via marketplaces.

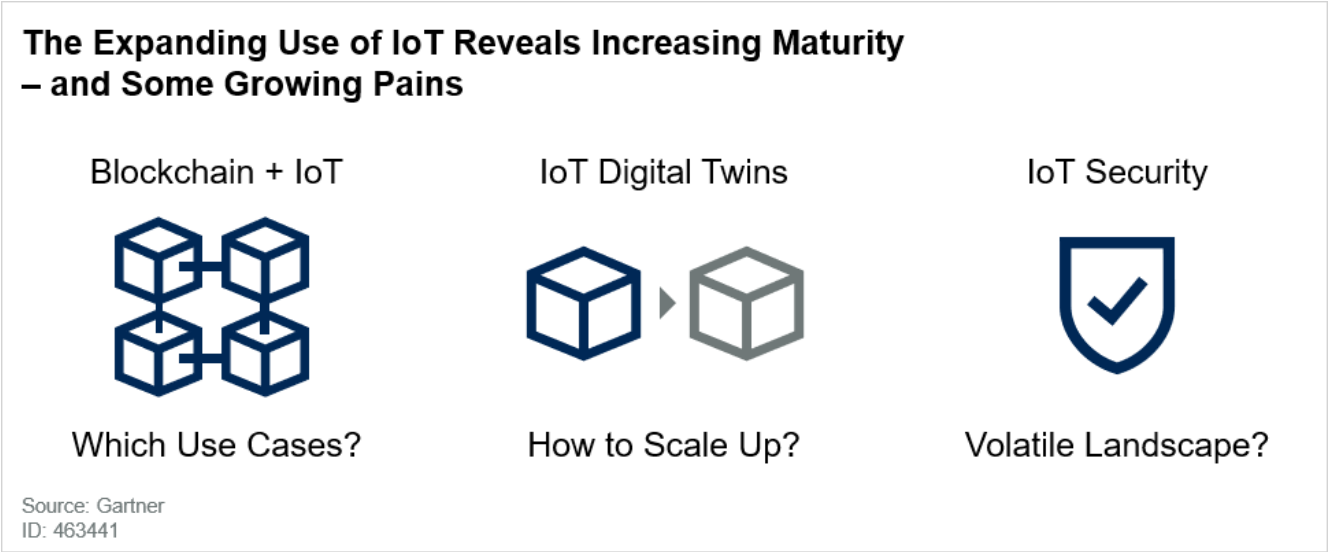
By 2023, IoT implementers will have to rearchitect their security solutions because 70% of current providers will have rebranded, repositioned, been bought, or disappeared.

Analysis

What You Need to Know

While IoT implementations proliferate and scale up, various IoT-enabling technologies and the associated provider landscape continue to evolve and mature. This dichotomy of expanding IoT use and the changing technology provider landscape reveals IoT's increasing maturity and a few growing pains (see Figure 1).

Figure 1. The Expanding Use of IoT Reveals Increasing Maturity — and Some Growing Pains



Notable signs of IoT's increasing maturity and growing pain include:

- Blockchain is beginning to be used in conjunction with IoT implementations, and this requires a relatively complicated mix of two already individually complicated technologies. Despite this challenge, early indications from project implementers is that the majority of combined IoT and blockchain use cases are associated with improving cost optimization.
- Digital twin adoption is increasingly synonymous with IoT adoption, and the proliferation of dozens, hundreds, or even thousands or millions of digital twins will tax many organizations' ability to scale up their digital twin development. Thus, as a supplement to custom development and other approaches, they will increasingly acquire digital twins via marketplaces.
- Security is considered one of the most challenging technical problems faced by IoT implementers, who have been turning to IoT-focused security technology and service providers for help. But over time IoT implementers will increasingly acquire IoT-related security features as an extension to their general-purpose security products or IoT platforms.

Application leaders should factor the following predictions related to these examples of IoT's increasing maturity and growing pains into their IoT strategy and implementation solution planning.

Strategic Planning Assumptions

Strategic Planning Assumption: By 2024, 75% of combined blockchain and Internet of Things (IoT) projects will have been implemented to help achieve improved cost optimization.

Analysis by: Avivah Litan, Benoit Lheureux

Key Findings: Blockchain networks have emerged as a promising innovation to affirm the integrity of data shared among constituents in multiparty process collaboration. IoT has emerged as a method for bridging the gap between resources (e.g., things) and their associated business processes. Integrating IoT and blockchain has the potential to support trusted multiparty processes that bridge physical world things to business process computing environments. The combined environment enables an immutable audit trail of key IoT data and related business events that is shared across multiple participants and which can be independently verified by each party.

In the technical architecture, IoT digital twins provide the visibility and monitoring of things and related events (e.g., using IoT devices to automatically capture the origin of a product), and blockchain enables the shared single version of truth as to the state of these things across their life cycles and associated business events — see "Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes." From a commercial point of view there are numerous potential use cases for combined IoT and blockchain projects, such as ensuring the origin and condition of goods or products in supply chain. For example, increasing confidence in the origin of high-quality, organic beef from a specific producer (important to consumers, who desire confidence in the quality of the meat they consume), or the accurate tracking and temperature control of blood as it moves from blood donor to patient (to help ensure patient safety).

Auditable tracking of product origin and proper handling in supply chain are good examples of how to improve cost optimization; because fraudulent or tainted products affect producers, transportation companies, distributers, consumers, insurers and other business ecosystem constituents. This is because of the impact of product wastage, dissatisfaction and liability, as well as damage to reputation. In a recent survey we asked implementers of combined IoT and blockchain projects to rank their top two benefits of blockchain and cost optimization was the most cited benefit.[1] Thus, we believe over the next few years that cost optimization will be a primary use case for combined IoT and blockchain projects.

Market Implications:

IT projects that combine IoT and enterprise blockchain are still quite immature. Technical implications of implementing such combined IoT and blockchain projects include:

- Most IoT devices don't have adequate computational or networking resources to act as full nodes in a blockchain so must rely on proxies or gateways. In any event, it's best to keep IoT devices physically separated from blockchain nodes.
- The relative volatility of blockchain implementations involving protocol and data format changes may be a challenge for long-lived IoT devices.
- Some blockchain implementations struggle to scale to the transaction rates that can be generated by large numbers of connected "things."

We expect the combination of IoT and blockchain to eventually to help enable innovative devices and business models, but the necessary evolution in both blockchain and IoT will take five to 10 years to achieve maturity.

Commercial implications of combined IoT and blockchain projects include:

- Relatively high cost and complexity of implementing both IoT and blockchain. Implementing end-to-end IoT business solution projects is nontrivial and requires many IT competencies and technologies to ensure success — see "Use the IoT Platform Solution Reference Model to Help Design Your End-to-End IoT Business Solutions."
- Rapidly evolving technical IoT/blockchain integration alternatives will mean that you must plan to periodically upgrade the combined platform over the next five years to support greater scalability, security and seamless bridges between things, devices and business events.
- Because of relatively high cost of the IT solution, likely combined IoT and blockchain solutions will be more applicable to higher margin products, and scenarios where the benefits of the innovative technologies help to offset the technical implementation.

Recommendations:

- Consider combined IoT and blockchain projects particularly where a trusted, multiparty audited trail of data and events originating with IoT-connected things supports desired outcomes.
- Because the cost and complexity of combined IoT and blockchain projects is relatively high, prioritize projects where there's a significant potential ROI.
- Establish KPIs (e.g., reduce in-transit product spoilage) to measure clearly defined business outcomes to be achieved by combining your IoT and blockchain networks.
- Explore use cases where the immaturity and rate of change of the technology isn't an impediment, and be prepared to migrate to different platforms.

Related Research:

- "Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes"
- "Survey Analysis: U.S. IoT Adopters Embrace Blockchain"
- "Assessing the Optimal Blockchain Technology for Your Use Case"

Strategic Planning Assumption: By 2024, over 100,000 digital twin models will be available via marketplaces.

Analysis by: Alfonso Velosa, Benoit Lheureux

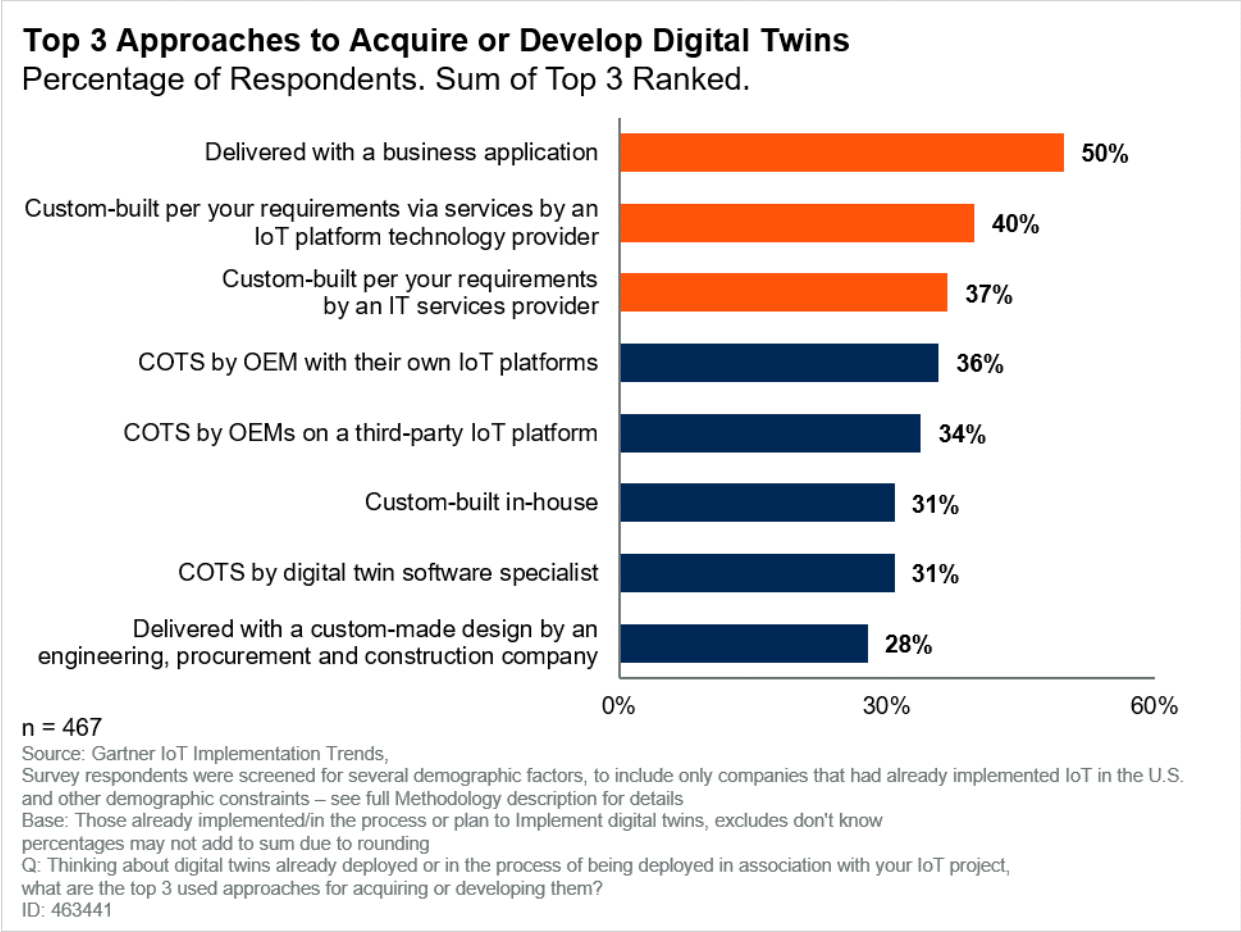
Key Findings:

Digital twins (DTs) are an enterprise software design pattern that represents an asset (e.g., equipment or process). Its objective is to understand the asset's state, its state changes, and how to use that improved situation awareness to improve business operations (see Definitions section). Digital twins are being deployed by companies implementing IoT at a very high rate — 85% of IoT implementers have already implemented, are currently implementing, or will have implemented digital twins over the next year — see "Survey Analysis: IoT Digital Twin Adoption Proliferates Across Many Sourcing Options." Those survey results revealed that many digital twins will be

acquired as part of new business applications, or often custom-developed (in-house or via a system integrator). But we believe that in order to scale up the deployment of digital twins, companies will at times also need the option of acquiring commercial off-the-shelf (COTS) digital twins that are pre-certified to work, or digital twin models that can be configured to work, with specific types of IoT connected products, equipment and assets.

Digital twins are increasingly available via a variety of sources, including from OEMs, IoT platform vendors and from digital twin software specialists. In a recent survey we asked IoT implementers, "*Thinking about digital twins already deployed or in the process of being deployed in association with your IoT project, what are the top three used approaches for acquiring or developing them?"* Respondents could pick their top three approaches. The results, illustrated in Figure 2, revealed that companies broadly source their digital twins from multiple sources, including bundled with business applications, as delivered with OEM products, delivered by IoT platform vendors, and custom built via several different approaches.

Figure 2. Top 3 Approaches to Acquire or Develop Digital Twins



Obtaining digital twins when delivered as part of a specific IoT-connected product, IoT-enabled application, or when delivered as part of a specific IoT-related technology offering (e.g., IoT

platform) can be a viable approach, but there will be times when doing so does not best align with your needs. For example, a power utility or oil and gas industry company that uses IoT-connected industrial pumps and valves from a dozen or more different OEMs faces an extraordinarily complex commercial and technical problem when acquiring digital twins for products or equipment from many different OEMs or technology providers — see "Five Approaches for Integrating IoT Digital Twins." As an alternative, sourcing digital twins from one (or just a few) marketplaces has the potential to simplify the complexity of acquiring, operating and integrating the technology.

The notion of digital twin marketplaces is currently nascent. In fact, there are no generally available digital twin marketplaces that can be easily browsed to find and download needed digital twins. But the various precursor offerings that have emerged have the potential to evolve into digital twin marketplaces. Technology vendors such as Uptake Technologies, GE Digital, ANSYS, and IBM are working on digital twin models, portfolios, and marketplaces.

Market Implications:

On the one hand we believe that there is a commercial opportunity for some TSPs to emerge or evolve into the role of digital twin marketplaces, but on the other hand we also recognize that there are potential challenges to the commercial viability and potential success of this approach.

Drivers for digital twin marketplace emergence:

- Reducing the OEM supply chain "friction" that is currently associated with delivering digital twins for relatively common and unsophisticated (but often mixed-OEM and heterogenous) IoT-connected product and asset classes (e.g., commercial refrigerators and industrial pumps).
- Owner-operators that would prefer to "single-source" digital twin software in a manner similar to how they single-source other kinds of business software.
- OEM "channel masters" (e.g., large manufacturers, producers, etc.) that may collaborate around digital twin standards to help lower commercial and technical barriers to digital twin adoption.
- IoT technology and service providers that perceive a revenue opportunity and an opportunity to differentiate themselves in the IoT/digital twin market by becoming a digital twin "broker."

Inhibitors to digital twin marketplace emergence:

- Immaturity and limited customer demand for the digital twin marketplace concept.
- Commercial barriers (e.g., unproven pricing, intellectual property protection and liability) that could make OEMs reluctant to "publish" product-related digital twins to a third-party digital twin marketplace as an alternative to offering digital twins on their own IoT platform or other delivery model.
- OEM technical challenges associated with "publishing" digital twins in a manner that allows them to run on multiple IoT platforms and other forms of platform middleware such as application platform as a service (aPaaS). More realistically, most OEM digital twins will only be

able to run on one, two or perhaps three platforms, which could inherently limit the value of a platform-neutral digital twin marketplace.

- Increasing availability of many digital twins as an embedded feature of evolving business applications, IoT platforms, system integrators, digital twin specialists and system integrators.

Recommendations:

- Companies with large portfolios of high-value assets (e.g., manufacturers, utilities and refineries) that are considering and purchasing IoT-connected products and equipment should ask OEMs for alternative digital twin delivery models (such as marketplaces) as an alternative to only delivering digital twins on their own software or other middleware.
- Companies that design and manufacture IoT-connected products and equipment should adopt a flexible digital twin delivery model to lower barriers to adoption, such as offering digital twins via marketplaces, rather than only offering digital twins via their own, proprietary, delivery model.
- Users of digital twin marketplace should plan a contingency strategy (e.g., rights to possession of relevant digital twins via an alternative delivery model) to offset the risks associated with first generation digital twin marketplaces and the nascent digital twin marketplace market segment.
- Engage partners in your vertical market to develop digital twin marketplaces that can provide you with both a range of templates, as well as other forms of business value.

Related Research:

- "Survey Analysis: IoT Digital Twin Adoption Proliferates Across Many Sourcing Options"
- "What to Expect When You're Expecting Digital Twins"
- "Market Trends: Software Providers Ramp Up to Serve the Emerging Digital Twin Market"

Strategic Planning Assumption: By 2023, IoT implementers will have to rearchitect their security solutions because 70% of current providers will have rebranded, repositioned, been bought, or disappeared.

Analysis by: Katell Thielemann, Barika Pace

Key Findings:

As security, privacy, and safety concerns remain a key priority, IoT implementers in all verticals and geographies continue to be bombarded by vendors professing to help solve a whole host of IoT security problems. Most vendors present what they believe are unique point solutions to detect connected assets and ensure data feeds' confidentiality, integrity and availability. And most are less than 10 years old, having gravitated to the field following the promise (and premise, when pitching to Venture Capital firms) that billions of connected devices needing to be secured would be waiting for them. Others rushed in when they discovered that most early IoT adopters pointed to security as a major driver of IoT "pilot purgatory" when efforts failed.

What these vendors failed to realize is that security and risk management leaders in implementing organizations do not live in a generic IoT world and are not charged with securing marketing concepts. They live in a world where increased instrumentation of assets and deployment of connected devices are a reality driven by concrete business needs, and anchored to concrete vertical industry business models, regulatory frameworks and risk profiles. They are now dealing with cyber-physical systems that are engineered to orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). These systems face risks, threats and vulnerabilities across the entire cyber and physical spectrum. And IoT implementers are not building their security strategy and technical solutions from scratch just because of IoT — they usually have a baseline strategy and technical solution in place. IoT implementers and the security and risk management leaders on their teams, faced with real world problems to solve, do not have time to educate security startups on these realities. As a result, generic IoT security marketing and positioning efforts fail to fully address the more nuanced reality of combined non-IoT and IoT solution-focused security needs.

For those vendors targeting consumer IoT devices, widespread apathy is the norm, and burgeoning regulations will target embedding security into product development, and security features will be added to home Wi-Fi systems as additional features, so that stand-alone offerings won't be appealing.

Market Implications:

The vendor landscape is becoming more volatile.

Companies like C3, for instance, started as C3IoT and have already rebranded to C3.ai, to play up its software and analytics credentials — see "Market Insight: Act Before Convergence Kills Your Stand-Alone OT/IoT Security Product Solution."

Some are repositioning in various ways:

- An increasing number of vendors (e.g., CynergisTek, Armis and Senrio in medical device security) are using early wins in specific industries to develop targeted solutions, positioned specifically to serve the unique needs of those verticals.
- Some are taking a page out of traditional cybersecurity vendors by researching specific exploits and partnering with OEMs to secure them. Such is the case for Armis, for instance, and the Urgent 11 VxWorks notifications.
- Others are getting better aligned to IoT implementers and their security and risk management leaders' needs — see "Market Guide for Operational Technology Security." They are starting to realize that they have had enough of stand-alone point solutions, and are working on developing features that can be fed into existing SIEM or SOC solutions, for instance.

Some vendors will be bought to add an additional, IoT-targeted security capability to existing security vendors' portfolios. Such is the case of Zingbox, which was recently acquired by Palo Alto Networks for a modest $75 million. Several firms that saw an infusion of VC or Private Equity capital in the last five years will likely quickly find themselves in a similar situation.

As illustrated above, there are many ways to avoid the generic IoT security solution trap, but vendors who fail to realize these trends or react too late will retrench into an increasingly illusive market or disappear altogether.

Recommendations:

- Inventory the current IoT security vendor landscape to identify the most important and strategic security products and services the organization relies upon today and for future IoT implementation plans.
- Engage with these strategically important vendors to understand their market positioning, growth trajectory, viability, technology roadmaps, convergence plans with IT security products, and partner ecosystem.
- Assess which IT security vendors currently used by the organizations have plans to expand into IoT security either organically, via mergers and acquisitions, or through acqui-hires.
- Revisit the organization's go-forward IoT security strategy as a result of these efforts, and rearchitect IoT security solutions accordingly.

Related Research:

- "Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT"
- "How to Develop a Security Vision and Strategy for Cyber-Physical Systems"
- "Market Insight: Act Before Convergence Kills Your Stand-Alone OT/IoT Security Product Solution"

A Look Back

In response to your requests, we are looking back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2016 Prediction — By 2020, more than half of major new business processes and systems will incorporate some element, large or small, of the IoT (see "Predicts 2016: Unexpected Implications Arising From the Internet of Things").

The prediction was triggered by the observation that costs of instrumenting physical devices with sensors and connecting them to systems in the cloud or on-premises were dropping so that applications that were previously impractical were becoming practical. Organizations that can incorporate current information from the physical world have better situation awareness and can make more-precise and effective decisions about what to do. A key point was that the IoT would have a substantial impact even in information-centric, record-keeping business processes, such as those commonly found in insurance, banking, government, education and marketing. It was already clear before this prediction that the IoT was changing manufacturing, supply chain, mining and transportation operations that had used "operational technology" (OT) for decades to make machines smarter.

Since this prediction, we have seen the IoT penetrate consumer, corporate and industrial processes on a broad scale. The IoT ranked fourth on the list of game-changing technologies in the Gartner 2019 CIO survey (2,835 respondents).[2] Furthermore, in a separate survey, 383 respondents who had implemented IoT and tracked their spending reported a 12% increase in IoT investments in 2019 over 2018.

Legacy IT systems and business processes always linger because of the cost of change, including new software and devices and introducing new ways of working to a company. However, the prediction, which was aimed at *new* processes and systems, has held up well. All things considered, we believe our 2016 prediction was correct and the trend will continue for the foreseeable future.

Missed: 2018 Prediction — Through 2018, half the cost of implementing IoT solutions will be spent on integration (see "Predicts 2016: Rising to the Challenge of Building IoT Solutions").

One of the factors in our original prediction is that the problems that device, data and process integration address are nontrivial, often involving extraordinary heterogeneity (that is, multiple types of devices, data and systems to integrate), distribution (that is, devices are often remotely located by distance and geography), and performance (that is, large numbers of devices, high API throughputs, and large volumes of data). Another factor is that end-to-end IoT business solutions, overall, involve integrating with many IoT endpoints, one or more IoT platforms, various back-end applications and systems, and with external business partners in your business value-chain ecosystem. At that time, our current understanding of the cost of integration was based on the estimate that, "More than 50% of the cost of implementing 90% of new large systems was spent on integration" (see "Predicts 2013: Application Integration."). Given that IoT adds to any new application system's integration complexity, we projected a similar level of cost for integrating IoT solutions.

Since this prediction our understanding of the cost of integrating IoT solutions has evolved in two ways. First, the difficulty of integrating IoT endpoints is lower than we originally expected because the IoT platforms themselves have matured and increasingly automate IoT device provisioning and connectivity, therefore do not as substantially add to the integration burden as we expected. Second, during the last few years since we originally published this research doing integration between the IoT platforms and other applications and systems has become easier. One reason is that the increasing availability of APIs for both IoT platform-based applications as well as the back-end applications to which they are integrated has simplified (though not eliminated) the integration development effort. At the same time the most commonly used integration tool — integration platform as a service (iPaaS) — used to do IoT platform to back-end system integration (see "Choose the Best Integration Tool for Your Needs Based on the Three Basic Patterns of Integration") emphasizes ease-of-use and the availability of prebuilt connectors for applications that are commonly integrated in IoT projects (e.g., CRM, EAM, FSM). This downward trend for the cost of doing integration is further supported by a recent survey which found that companies that have implemented new ERP and CRM application projects indicate that, on average, they spend about 20% of their implementation budget on integration (from the 2019 Gartner Business Application Integration survey). All things considered, we believe that while integration continues to be a significant task associated with implementing IoT solutions, based on factors (such as simplified IoT

device connectivity, API-capable IoT platforms, and a reduced burden integrating back applications) we now estimate that the cost of integrating IoT solutions is 25%, versus our original estimate of 50%.

Gartner Recommended Reading

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

"Choose the Best Integration Tool for Your Needs Based on the Three Basic Patterns of Integration"

"Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT"

"Survey Analysis: IoT Digital Twin Adoption Proliferates Across Many Sourcing Options"

"Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes"

Definitions

Digital Twin: A digital twin is a virtual representation of an entity such as an asset, person or process and is developed to support new or enhanced business objectives. The three types of digital twins are discrete, composite and organizational. Required elements to meet business objectives are model, data, a one-to-one association, and monitorability, optional elements are analytics, control and simulation. For details see "Hype Cycle for the Internet of Things, 2019."

Evidence

Digital Twins Are Acquired as COTS in Addition to Other Sources

[1] Results presented are based on a Gartner study of companies that implement IoT. We sought to better understand what kinds of business benefits IoT delivers, how companies organize IoT to best deliver on those benefits, and how they overcome the technical challenges of implementing complex IoT projects. The primary research was conducted online from 15 May through 27 June 2019, among 511 respondents from the U.S.

Companies were screened for having annual revenue less than $100 million. They were also required to have completed or plan to complete deployment of at least one use case or project of IoT by year-end 2020.

Respondents were required to be at manager level or above and should have a primary involvement and responsibility for making decisions in IoT implementation.

The study was developed collaboratively by Gartner analysts and the Primary Research Team.

Disclaimer: Results of this study do not represent the market as a whole but are a simple average of results for the targeted country, industries and company size segments covered in this survey.

[2] The 2019 Gartner CIO survey was conducted online from 17 April through 22 June 2018 among Gartner Executive Program members and other CIOs. Qualified respondents are the most senior IT leaders (CIOs) for their overall organization or a part of their organization (e.g., a business unit or region). The total sample is 3,102, with representation from all geographies and industry sectors (public and private). The survey was developed collaboratively by a team of Gartner analysts and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Predicts 2020: Barriers Fall as Technology Adoption Grows — A Gartner Trend Insight Report

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