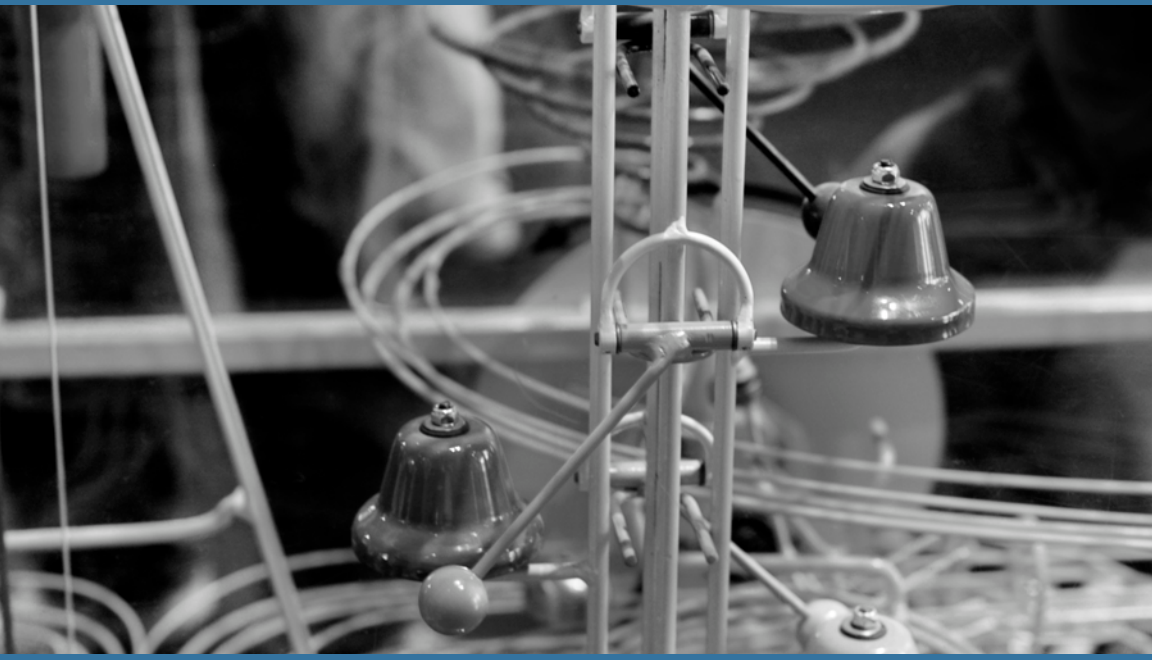
O'REILLY®

Compliments of thingworx®

Evaluating and Choosing an IoT Platform



Matthew J. Perry

ThingWorx is purpose-built for the Internet of Things, with tools, APIs, and marketplace extensions that lower costs, increase developer productivity, and speed time-to-market.

With the ThingWorx IoT Platform, you have access to a powerful development engine and a broad set of innovative technologies that extend the power of the IoT:

- CONNECT to any Thing
- CREATE Apps for all Users
- ANALYZE Machine Data
- EXPERIENCE all Things through Augmented Reality

Learn more about how the ThingWorx IoT Platform is the right choice to power your organization's digital transformation.

thingworx.com/go/SelectTheRightIoTPlatform

ptc

Evaluating and Choosing an IoT Platform

Matthew J. Perry

Beijing · Boston · Farnham · Sebastopol · Tokyo O'REILLY®

Evaluating and Choosing an IoT Platform
by Matthew J. Perry

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editor: Jeff Bleiel

Interior Designer: David Futato
Cover Designer: Randy Comer

January 2016: First Edition

Revision History for the First Edition
2016-01-12: First Release

978-1-491-95203-0

[LSI]

Table of Contents

Evaluating and Choosing an IoT Platform

1. Is an IoT Platform Necessary?

As the Internet of Things (IoT) continues to saturate the world of business and consumer-facing applications, it is all too easy for rational decisions about its adoption to be complicated by the latest bells, whistles, and trends. Every business is determined to be current, or even better, aligned with the future of its industry ecosystem. Over the past decade, purveyors of Internet connectivity, the "plumbing" that welds together existing layers of a business (and thereby creates new layers) have described this future in glowing terms. Every year, millions more devices and things will become "smart," with individual IP addresses that enable the transmission and receipt of data.

The IoT promises to transform how we do business and even the very nature of that business. The challenge today is to know where to begin. Should IoT be phased in, adopted in increments, or is it necessary for companies to invest in the most sophisticated and complete IoT platforms as soon as possible?

Opinion is heavily divided, and as with any new technology, there is as much hype to cut through as there is hard information to harness. Estimates for the expansion of IoT technology vary widely—billions of connected devices, trillions in market sales—but how does this apply to day-to-day operations?

The imperative to modernize applies to almost all businesses that feel the heat from competition and the pull of research that high-

lights the benefits of going to market in many new ways. It may seem like a time to rush, but choosing wisely among the array of choices presented by IoT technology is still critical. This is especially true since business imperatives demand looking beyond today's best solutions. Whatever solutions are implemented, they must last. There will always be upgrades and the need for maintenance, but the essential technology network should be in operation for the foreseeable future. A "future-proofed" tech network will be receptive to the improvements without being erased or obviated by them. It will endure even as it undergoes necessary upgrades and enhancements.

Since IoT is not one technology, but the interplay of many, its relevance to industry and business is not uniform. Each business, even those occupying a single vertical, will determine its needs for the future in a unique way. The only conclusion that likely can be held in common is that some iteration of an IoT platform will be part of how business is done—and how it grows—for the foreseeable future. Beyond that general observation, the combinations of needs and capabilities will be as varied and numerous as the connections between things and people facilitated by the Internet at large.

What Is an IoT Platform?

An IoT platform facilitates communication, data flow, device management, and the functionality of applications. A platform is not the application itself, although many applications can be built entirely within an IoT platform framework. It links machines, devices, applications, and people to data and control centers. It is not confined to brick-and-mortar central command: ideally, it can be accessed and managed from many different locus points. It employs better, quicker search engines and data storage systems with the capacity and sophistication to handle volume far beyond what has brought industry to the present moment. Most of its elements are cloud-based and running on wireless connectivity, which may be established via third-party providers, application programming interfaces (APIs), cellular capabilities, or—most likely—a combination of these technologies.

Through dashboards, APIs, data engines, and algorithms, a platform enables elements and sectors of a business network to connect, monitor, and communicate with each other with far greater speed and flexibility than we have yet seen. Data from an ever-expanding ecosystem can be collected, sorted, and harnessed

entirely online. The platform also can enable data prioritization, a feature of critical importance at a time when machines, sensors, and other objects are beginning to generate new floods of information.

It will provide ample security features, scalability, and abundant capacity for pulling in, storing, and analyzing data. It may connect machines, people, applications, or all three. Like any intelligent network, it provides innate predictive qualities that use data for the purposes of maintenance and troubleshooting. The user interface is intuitive and extensible, allowing for the future development of application extensions and the necessary scalability to track an increasing number of connected devices, people, and data sources.

Essentially, a platform allows for greater concentration of resources in value-add applications. Instead of requiring companies to focus on the lower levels of the technology stack, which are essential but not value-positive, attention can be paid to application development; a smarter, more integrated company ecosystem; and intelligent data generation. Applications can be sent to market faster, and with better support. Connectivity and data management—which historically have required huge investments in time and development costs—should be "givens" on the IoT platform, as reliable as electricity generation, and just as liberating to users.

The root of the IoT is connectivity: more things, more people, and the matrix of connections that springs up between them. Yet in less than a decade, the technology has moved far beyond this fundamental consideration. Where many companies may have believed it was advantageous to build out a platform internally, it is becoming clear that much of the technology stack can now be implemented with out-of-the box tools and effective engagement with vendors.

2. Look Before the Leap: The Key to Smart Platform Investment

Businesses preparing to launch IoT platforms must have strategic goals clearly defined in advance. They also must consider the hazards of launching unstable platforms and underdeveloped applications. In this climate, in which so much technology is new and its uses are still being analyzed, it is possible to jump into a solution that creates more problems than it solves. "Look before you leap" is a phrase to remember when assessing the elements of a platform

that are essential to competitive differentiation, and which can be left alone.

A thorough review of technology needs and strategies will also help to assess vendors. There are many who simply can't provide the comprehensive, distinctive services and products your industry might need. Since the track record for even the most experienced platform vendors is only as long as the technology itself, it can be difficult to determine which can be the best partner and technology provider.

The stakes are high, particularly for companies that depend on IoT technology for growth, funding, and legitimacy. The best defense against failure is a thorough review of what IoT has done for your industry already, and selecting the verticals where it can make the most difference, before a vendor is engaged.

Platforms are complicated, and a great deal of their functionality rests below the application level. Unless a company has reserves of talent that already built out technology stacks, the DIY model is inadvisable in terms of cost: most of the technology stack provides no immediate value-add, and it is expensive. Time and resources are better applied to the identification and development of applications that help the company stand out among the competition and better serve its market.

The following general categories are important jumping-off points for analysis of a company's IoT platform needs:

- **The scalability of the enterprise.** An IoT platform must not just support the needs of today. How many new applications might be added to a company's product suite? How many devices might plug into the application over time? If an enterprise can expect to grow at a pace comparable to the projected expansion of the IoT, the platform must be sufficiently robust and extensible to support future deployments.
- **The extent of legacy architecture.** A great deal of existing IoT connectivity is agnostic, designed to work within a variety of infrastructure systems. There should be a detailed analysis of which legacy elements of a company's infrastructure are indispensable and which can be phased out over time. The efficiency of an IoT platform solution will depend on how new generations of technology can interlock with the old.

- **How a feedback loop can aid outcomes.** An increase in rich data—perhaps an overwhelming increase—is one of the key payoffs of IoT investment. Industries must consider what types of data will make the most difference to performance outcomes, revenue streams, and communication networks. There should be benchmarks in place, projected outcomes that can serve as guidelines for selecting data management systems and the security infrastructure supporting them. Determining where the new data and analysis can make the greatest difference should inform the choices that define the function and reach of the platform.
- **How IoT can affect business-customer interactivity.** By extending on- and offline engagement, IoT platforms can strengthen the connection to real-time customer experience. Mapping out standards that will enhance satisfaction and lock in profitability for later generations of products will help developers distinguish which features their platforms should have.
- **Data management strategies.** Since the digital universe, like the physical one, is now in a state of constant expansion, data storage is perhaps the most critical tool of all. Buying more storage capacity may seem like an obvious answer, but it's a shortsighted one. Storing bytes of data at orders of magnitude beyond what is actually needed is expensive, and the storage methods can quickly become unwieldy.

  Industry experts must evaluate priority data streams and determine who will access them and when. If mobile applications are important to the business model and data volume will be high, data providers will have to be built to scale. Hybrid cloud models (a blend of private and third-party services that can promote scalability at lower cost than storing all data in private, more expensive servers) may be a smart option for industries that must store massive amounts of data, not all of which is proprietary.
- **Your own expertise.** IoT platform vendors should be able to tell you a great deal about how new technology can develop and how to refine your business models. But however transformative IoT can be to your business practices, it will not transform your industry at large. Intelligent IoT vendors will remind you that no one knows your business better than the team you have

in place. Businesses should expect to grow and learn with new technology, not to be replaced by it.

3. A Key Distinction: Consumer- and Industrial-Grade Platforms

It is impossible for one report to provide a complete overview of the IoT platform options and requirements. Each industry vertical—healthcare, manufacturing, energy, and banking, to name a few—will present its IT and OT specialists with particular conditions and problems to solve. Municipal police and fire departments, for example, will depend on a platform that ensures communication between field operations and command centers. Energy and transportation companies will search for ruggedized solutions that will protect field assets from harsh environmental conditions. Banking IoT platforms will demonstrate robust encryption and security features that protect internal and consumer communications and transfers.

One primary division in the IoT delivery ecosystem is between consumer and industrial grades. Both will be important drivers of economic activity in coming decades. Each will produce goods, services, and infrastructure support that will be indispensable to users over time, but for the purposes of this report, we can make a distinction between indispensability based on convenience (which describes the consumer side) versus indispensable as a synonym for necessity (i.e., on the industrial side, when the system fails, there is a crisis).

The focus of this report is industrial IoT (IIoT), rather than consumer-facing devices (such as smart phones, thermostats, fitness wearables, etc.). Our discussion focuses on industries that employ large numbers of devices, sensors, and workers who operate in a wide variety of environments. Many industries rely on subsets of machines on the edges of networks, whose primary purpose is to run remotely without generated data: energy grid routers, signage, automated factory machines, etc. A basic principle of the IoT is that even the machines in these networks will one day be assigned IP addresses and begin to add their accumulated bytes of data to the big data processors on the other end of the platform. But this doesn't reflect the present reality of many legacy assets that were not

designed to accumulate and transfer data; the upgrade will be time-consuming and expensive, and in some cases, it will be unnecessary.

On the other hand, there are many industrial assets that are absolutely dependent on bi-directional, reliable, and robust IoT platform support. MRI scans, military drones, and smart grids depend on a connectivity that provides a conduit for collected data and remote access and control capability. By contrast, a smart home appliance can operate as specified without IoT infrastructure on the back end.

The following table provides general functions of consumer and industrial IoT platforms.

	Consumer IoT	Industrial IoT
Examples	Wearables, devices, B2C (business-to-consumer) products	Automotive, agriculture, aerospace, military, manufacturing, automated factory
Primary value	Contained to the physical product	Embedded software, apps, generated data, and responsiveness
Availability and scalability	Low concern	High concern
Security and reliability	Moderate concern	High concern
Connectivity	Unidirectional, data to cloud; low frequency	Bidirectional for data transmission/remote access control/automation; high frequency

4. What IoT Functionality Is of Paramount Importance to Your Industry?

The divide between consumer and industry IoT is just the first important distinction. Within the industry IoT, there are many subsets of solutions and protocols to be implemented—in energy, medicine, banking, mining, and many other verticals. The IIoT platform will be customized to work with existing business models, along these general guidelines:

- Each industry will utilize a distinct set of applications.
- The means of monetization and metrics for ROI will vary for each industry vertical, and often for competitors within that subset.
- Each industry will require a particular set of tools and communication protocols, which will create a distinct grid of interactivity and monitoring.
- Each industry will prioritize data according to the needs of the business model and will attempt to meet the challenge of containing the data footprint.
- Security and proprietary access features will protect different data sets.
- The degree of ruggedization will vary, depending on the conditions under which industry assets operate.

IoT platforms can be customized for a focus on systems, operations, applications, and products:

- Smart, connected *systems* serve industries that create large systems with components that often run remotely, e.g., cooling units for HVAC systems, refrigeration compressors for food storage, and street lamps on a municipal energy grid. Data capture and predictive maintenance are the key to this model: both can extend the life of expensive products and employ an "evergreen" design that is adaptable, with upgrade capacities embedded.
- Smart, connected *operations* enhance intelligence and connectivity throughout an ecosystem or supply chain, or within a community of linked devices. This has particular relevance to M2M manufacturing (machines making other machines or things). Predictive maintenance, shutting down idle or unnecessary equipment, increasing usage capabilities during peak times, and refining security features can both increase productivity and reduce waste, creating a leaner system that does more with less energy and oversight.
- Smart, connected *applications* can be purpose-built and mounted on an IoT platform to provide interactive user experiences that benefit both the provider and customer. An IoT platform that supports a municipal smart traffic plan will host apps used

by citizens (to locate vacant parking spaces, thus reducing one of the greatest contributors to urban traffic congestion), workers (sensors that indicate when garbage receptacles of full and that work with apps that reroute collection trucks), and system managers (collecting data from the ecosystem and evaluating congestion solutions). Apps can also deliver data and direction to many service or production operations: farming, energy delivery, transportation networks, and medical observation, to name a few.

- Smart, connected *products* are prominent in IoT solutions, and they will be important parts of industrial-grade solutions. Smart products, whether RFID-tagged aircraft components (seats, vests, generators); portable products for emergency personnel that detect life-threatening situations via scans; or sophisticated, ruggedized communication equipment for maintenance workers in the field can be game-changers in terms of efficiency, safety, and return on investment. Energy, medical devices, public safety, and transportation are just a few sectors that are evaluating the impact of new devices and products on how business gets done, and by whom.

Again, there is no need to focus on applications, operations, or products to the exclusion of other elements. In theory (and increasingly in practice), the IIoT applies to all of these components. What is important is prioritization. As companies review their options for building out IoT platforms, they should analyze the costs, functions, and revenue potential of all facets of the business ecosystem and target the areas where the greatest gains can be realized.

5. Key IoT Platform Features

Reliability, rather than innovation, is the name of the game when dealing with the hardware and software that undergird the platform. Differentiation—as seen in remote services, smart monitors, data siloes, and M2M interactions—are the heart of the IoT solution. By focusing on them, businesses can build their Industrial IoT capabilities much faster and efficiently, and outlay fewer research and investment resources.

But to arrive at that point of specialization, the platform must deliver on many fronts. The metrics of an industrial IoT platform essentially determine how flexible, multi-functional, sustainable,

and safe it is. The cumulative effect of these attributes must also be considered: the crux of IoT lies in the interplay between systems and technologies. The effect, ideally, is always greater than the sum of parts.

The essential components of an IoT platform are as follows:

Device management
: Devices do not exist in stasis. They are in continual need of management, reconfiguring, updates, and setting control. Edge devices, which act as translation and data hubs between networks, may well create more problems than they solve if they must be serviced manually; remote access via the IoT platform is essential to their economic viability.

  Device management architecture must be bi-directional and flexible to allow for all network components to be connected, observed, and able to communicate. In the event of obsolescence, damage, or a security breach, the platform management system can remove or brick the device.

  Because there are so many devices to monitor or patch into the platform, there is great value in streamlining the process of managing them. A manual build-out to incorporate each device is impractical. IoT management will depend on coding that can port with the microcontroller units (MCU) in the system architecture of devices. This is a far more efficient and scalable method of IoT expansion.

The "build-deploy-evolve" approach to app development
: Situated on top of a robust platform, the life cycle of an app should be open-ended: create it, market it, and improve it over time. This "build-deploy-evolve" platform strategy should be enabled from the onset to support feedback loops and future iterations of the app function.

  As an example, consider a farming conglomerate that deploys a smart agriculture app that raises crop yields while reducing water usage by 10%. This will be a value buy for the next few years, until the app is upgraded to include a thermal imaging component, which highlights irrigation inefficiencies and saves even more water. A rewrite of code for the app may not be worth the cost; the smart app, supported by the IoT platform,

will weave in the new data seamlessly, with minimal downtime. It is adaptable and future-proofed.

Bi-directional, flexible connectivity
: Even now, when IoT has become a reality for many industries, it is often viewed as a unidirectional capability for collecting data. But this "one-way street" mindset undersells the platform and leaves businesses in the 20th century. Bi-directional connectivity enables greater control of products, seamless update delivery, and quicker responses to problems.

  In the realm of consumer-grade IoT, this two-way connectivity is a given. Smartphones would not be so highly valued if they could not receive system updates without inconveniencing their users. When this principle is applied to the industrial grade, solutions with enormous cost-savings implications are evident.

  Imagine an automotive brake recall that affects hundreds of thousands of vehicles. If the problem resided in software, a company that employed a robust, bi-directional platform could resolve the problem via software updates, with potential savings of billions of dollars and public relations headaches. When performance and operational data can be pushed from the product out to service technicians, many similar possibilities fall into place.

Back up beyond the cloud
: Cloud computing is exciting because of the opportunity it presents to scale and centrally control an entire industry ecosystem. But we can never lose sight of the worst-case scenario: what happens when the network goes down or the cloud provider is one of many that may go out of business as competition becomes fiercer? Catastrophe is likely if mission-critical products and data can't be pulled out of the cloud in time.

  All industries must have a back-up plan in their platform. As the IoT ecosystem becomes more complex and responsive, machines will need to be able to perform computational tasks independent of cloud-based oversight. IoT platforms will have to contain features that store critical apps and data either on site or with reliable third-party storage.

Meanwhile, businesses should be aware that cloud computing can be too much of a good thing: many are buying more computational power than they actually need.

The cost of data is also a bi-directional proposition. Data generated by field assets may be important, but shipping all of it to the cloud via cellular networks would be cost-prohibitive, and almost certainly unnecessary. With localized data analytic capacities, only essential data outputs need to be sent up the chain via cellular connection. This is also a prescription for controlling the torrent of data that will arrive once the full component of devices is locked into the IoT universe.

Data analytics

Data is the lifeblood of the IoT and a great source of its value. An industrial IoT platform should provide a full complement of data analytics facilities, both to extract that value and keep businesses from drowning in a torrent of new information that is poorly coordinated. Basic descriptive analytics, visualization, diagnostics, and predictive and perspective analytics should be supported by platform capabilities. The goal is to expand the predictive capacities of the network, refining function and troubleshooting, while enabling real-time responsiveness to emergencies.

Collaboration and breaking down silos

The IoT is designed to break down silos that have limited interaction between departments and different levels of supply chains. By linking a system of land area networks (LAN) and establishing new protocols for sending data up and down value chains, an industry player can become more agile and reactive by seeing everything from everywhere, and having one conduit to control when agency-wide action is required. This is one of the most transformative aspects of IoT technology. Warranty management, remote service, automated consumables, and product designs are just a few of the functions that can benefit from interactive access to IoT data. Collaboration will depend on customized apps and dashboards that present information in intuitive, interactive ways.

That said, the platform should be outfitted with proprietary standards for collaboration. Protocols that direct data to the right analysts and consumers will need to be in place, along

with filters that conform to security standards and user preferences. There is no need for all the data generated to go everywhere.

Availability, scalability, and reliability
: There is always the possibility of importing problems into a technological solution through lack of foresight and insufficient consideration of worst (and best) case scenarios. When businesses attempt homegrown solutions or work with small market, pure-play vendors, scalability can be compromised or disabled. A solution that works on one edge of the platform may not work unilaterally. The innate benefits of IoT will not translate, and problems may be baked into the new platform.

  An IoT platform must be tested for reliability under the most traffic-intensive work environments, with fault tolerance and network disaster recovery protocols mapped out. Reliability cannot be an open question when the most critical functions of a business are on the line.

Maintainability
: In today's fluid work environment, it is important that system protocols can be picked up and understood by a new team of workers. An IoT platform must be evaluated for its qualities of transference. Platforms must be well-organized, intuitive, and interactive to ensure a seamless transition as new administrators and developers are passed the torch.

Flexibility and network agnosticism
: Your business may need an IoT platform to remain competitive over the next few quarters. But that does not mean that all settings will begin in the ideal position, and that all processes will be streamlined from the start. IoT technology is a solar system that is still being organized, and many adjustments are in store for every industry that employs it. New requirements and opportunities may be months, or years, away.

  Platform and device agnosticism are requisite in this intermediary phase. This means the IoT solution must be able to lock in with all prominent tech systems without excessive configuration. Since there is no guarantee that an IoT platform will be maintained by the same vendors who installed it, or that legacy assets will not prove valuable enough to keep, the platform itself must prove adaptable. But it also must prove to be *extensible*:

permitting the continued flow of data and operations while preferred functions are extended.

The successful IoT platform will be purpose-built to address the specific requirements of the business operations, including the right tool kits and device-management features. It will be sufficiently flexible that no one single feature, or set of features, resists replacement. This flexibility will enable apps, data analytics systems, security, workflows, and protocols to be updated, replaced, added, or removed as needed.

Security and data privacy

There is likely no aspect of the Internet of Things that raises more questions and concerns than the safe transfer of data and the integrity of operating systems. For every expansion of network, down to the IP-enabled sensor or device, there comes a new possible security breach. Data privacy standards, or the lack of them, can be the source of logistical headaches with revenue-loss implications, as the European Court of Justice's 2015 ruling against the "Safe Harbor" pact indicated.

An IoT platform must support security at multiple points across the hardware and software components. Gateways and edge devices must be sophisticated and flexible enough to adapt to new security methodology. Depending on the deployment of assets, fog computing methods–which keep more operations within localized networks–may provide an extra layer of safety. This is an area where trust in the vendor's approach will be critical; since vendors often lose customers when a security breach occurs, there is incentive for both parties to find the right solution.

The implications of data privacy breaches may not seem as ominous, but they should not be underestimated. Although the IoT in theory allows all members of an organization to access information simultaneously, this is far from ideal in present circumstances (and may never be so). There will always need to be safeguards in place that keep data streaming to those who need it and away from those who do not.

A medical device, for instance, may produce a data stream that is relevant to its operator, supporting technicians, product engineers, and billing systems. However, regulation and usability will need to dictate that each group will access only the cut of

data relevant to it. There are serious implications for international companies, which must abide by different privacy requirements in different countries, and may need to implement strict safeguards that conform to the laws of different markets if data makes its home in a nation with looser privacy requirements.

Security and data privacy is yet another aspect of the IoT platform configuration that cannot be viewed solely in the present moment. Careful analysis of revenue potential, industry growth, and international opportunities will be needed to make future preparations today.

6. How to Evaluate IoT Platform Vendors

Just like the technology itself, the creators of IoT architecture and components are evolving, and their solutions will be subject to the judgments of the market for many years to come. The trick for businesses will be to evaluate what these vendors are offering, their track records, what their architecture looks like, and how viable they seem to be to the future of IoT.

Determining which vendor can deliver the particular solution a business needs is an analytical process. Ultimately, though, decision makers will also have to trust their abilities to identify capable partners with staying power.

First, let's talk about the differences between two categories of vendors: pure-play vendors and large enterprise vendors. It's convenient to assign big versus small, slow versus fast generalizations to enterprise and pure-play vendors, respectively. There is some truth to these distinctions, but it may not apply to the conditions of your industry. To find the best IoT solution, it's worthwhile to consider what both pure-play and enterprise vendors offer.

There are many well-established pure-play and enterprise vendors, but as the IoT expands, there will likely be many more that vie for market share. Some vendors, like cloud providers, will fail.

The pure-play vendor will likely be newer and more aggressive and responsive to potential clients. They may serve a particular segment of IoT development (software, gateways, etc.) that is of particular importance to the specifics of the platform your company needs. Many are new arrivals and eager to build new client relationships.

If pure players are serving other companies in your industry, investigate whether they are fulfilling requirements similar to your own. If your business is international and has many offices abroad, it may not be practical for a smaller vendor to deliver support everywhere it's needed.

Enterprise vendors are more likely to offer global reach. The largest are good bets to still be viable in five years, when your platform requires upgrades. Most have the means to execute for great variety of industries. They are more likely than pure plays to provide a comprehensive platform solution, either through their own capabilities or through a deep partner network.

Some customers may harbor concern that an enterprise vendor will deliver a truly unique solution and excellent service. Also, some enterprises deliver required functionality through service engagements, which may lock customers into contracts or restrict access to new—and superior—products or services. Depending on your platform specifics and the current business climate, this may not be in your interest.

Evaluating the "Ideal" Vendor

Because the needs of every market vary, the right IoT vendor may well have a track record of success with other companies in your industry, possibly even your competitors. You should evaluate the full set of their customers and what platforms they have built so far. The most recent projects are important, but if they have been in the field for some time, consider where they started and how they have evolved: do they grasp the potential of IoT? Do they have standards in accord with your own business practices?

To determine which type of vendor will deliver the best technology solutions, it is helpful to employ the same metrics discussed in relation to the needs of your IoT platform capabilities. There should be a clear consideration of device management, communication technology, and safety-privacy issues.

- **Tools for in-house developers.** The best IoT platform vendors will be good for the heavy lifting required to build out the technology stack. But they also need to provide a strong set of tools for customers that expect to make their own needed refinements to their devices and apps. Vendors should have out-of-

the-box tools for building digital models that correspond to physical things.

The models should produce a template-driven model that allows unique iterations of the model to be provisioned and assigned to a physical product. Additional tools should be available from the IoT developer for full customization.

- **Data collection and retrieval.** Consider the vendor's specialization when it comes to data. Depending on how data is used, a developer may need to engage a vendor that specializes in predictive data, descriptive or diagnostic analytics, or data storage. Many vendors are beginning to offer solutions that service more than one of these distinctions, but developers should still consider the best uses for the IoT data flow and seek vendors with track records for collecting and analyzing data.

  Vendors should be evaluated for their ability to assess the data needs of customers. For large companies that can expect their data to increase by orders of magnitude, a robust plan for maintenance will be needed beyond advanced collection capacities. In most cases, access controls will need to be intuitive for the average user: unless a company has a wealth of data science at its disposal, it should be working with a vendor that can streamline data collection and retrieval.

- **Building apps and device management.** The vendor's partner ecosystem may be of particular importance. As apps become more specialized and essential to differentiation, companies must be certain that the vendor is part of an ecosystem that will generate creative solutions that make devices and apps stand out. The vendor must be able to supply ample out-of-box tools to expand the app suite and adapt to changes in the marketplace. Companies may understand their problems and customer bases better than technical vendors, but at the right moment, they should be able to depend on deep support that can keep their apps and devices at the elite level.

- **Connectivity and flexibility.** Cloud services will often be an essential part of the IoT platform, but there are many protocols to choose from. Some vendors have proprietary technologies that could be hard to maintain or reproduce if a company switches to a new vendor. The IoT is a function of connectivity: you need to evaluate how your vendor prefers to establish its connections, and what sorts of back-up technologies it will

install. The protocols will need to sync with what currently exists and the networks that conceivably could expand as the IoT solution takes root. If local connectivity is part of the solution, the vendor must have both the means to enable connection at the outer edges of the platform and sufficient back-up technologies.

- **Effective UI and scalability and extensibility.** The fundamental purpose of an IoT platform is to expand reach by making more processes automatic or simple to perform. Even in industries with an abundance of technological knowledge, there will always be a need to free up human resources to tackle new, complex challenges and reach more of the market.

  The platform vendor should have a proven track record of getting more done for less. Also, their capabilities should be discernible from many angles. CIOs, CFOs, and product managers should all be able to see the benefits of a cross-cutting platform. There should be effective test beds for developing new products and systems that demonstrate relevance to the bottom line and day-to-day operability. APIs should be robust and compatible with the existing or projected technology platform.

- **Security throughout the chain.** Security is perhaps the point of greatest concern and discussion around IoT, since there is a basic tension between the need for greater functionality and the risk that comes from exposing more portals of the Internet to more users—and potential hackers. Much like choosing a financial advisor, selecting a platform vendor will depend greatly on the risk tolerance of an organization. In an ideal world, every vendor has a response to security challenges at all phases of deployment, but inevitably there will be trade-offs between risk and function.

  Larger vendors have often had more time and resources to consider and meet security threats on both the software and operational ends. The methods for mitigating risk and responding to breaches must be suitable for the needs of an industry. If, for instance, a company has a global reach, is there an independent security office run by the vendor that can respond immediately to a breach? Will their protocols apply in a variety of markets?

  Vendors can also be evaluated for their internal protocols, the operational security features that must be adhered to by users. Vendors that are focused overly on app or device functionality

may rely on rudimentary processes, such as basic passwords, that can leave networks susceptible to human error or override even by unsophisticated hackers. It is critical that priority is given to securing the data that is most valuable to an organization.

- **Picking a winner.** It is always tricky to determine an industry's winners and losers in advance. But in the case of a brand new technology, quality and success often become linked. Poor solutions and practices will not last when there is such fierce competition for market share and a rush to perfect powerful tools.

  There will always be room at the top for new players that can change market dynamics; niche providers may well produce solutions for industries with specific, hard to fulfill needs. But a track record of success, or even a current run of success should not be dismissed lightly. The IoT will crown winners and losers in many industries, but this is especially true for the technology vendors themselves.

7. Summary

The IoT will be the subject of endless analysis—and hype—as its influence expands. Keeping up with the research will be almost as challenging as maintaining your company's current technological apparatus. But few industry players can stand pat: hype aside, the IoT's influence is already established, and it can only expand.

Companies can cut through the noise by continuing to focus on the essential tasks and functions of their IoT platforms. A methodical approach that breaks down what is necessary, desirable, and superfluous can streamline the approach and make the structure of the ideal platform easier to see.

The future of your IoT platform can take shape by following through with the analysis recommended in this report. In tandem with robust research about vendors and what they offer, this advanced preparation can lock in the enormous benefits of the Internet of Things, even as the technology is still changing.

About the Author

Matthew J. Perry is a writer and editor with a particular interest in how the Internet of Things can make cities smarter. He has written for Cisco Systems and collaborated on 10 published books. He lives in New York City.