

THE INTERNET OF THINGS 2018

HOW THE IoT IS EVOLVING TO REACH THE
MAINSTREAM WITH BUSINESSES AND CONSUMERS

January 2018

Peter Newman | Research Analyst

BI INTELLIGENCE

KEY POINTS

- **The Internet of Things (IoT) continues to develop as a transformative technological force that is changing how companies operate and consumers live.** But, as these connected devices continue to proliferate, the IoT is increasingly moving away from the fringe and entering the mainstream, with a plethora of use cases now proven.
- **The IoT relies on an ecosystem that's built around any particular deployment or installation, whether that's in a home, a factory, or on a city's streets.** There are five components in an IoT ecosystem:
 - **Hardware**, or the IoT devices within the IoT solution.
 - **Networks** that connect the IoT solution to the user.
 - **Remotes**, which provide the user with an interface to connect to and manage the IoT solution.
 - **Platforms** that provide messaging, analytics, and data storage components.
 - **Security protocols** that ensure the IoT solution remains protected.
- **BI Intelligence forecasts that companies, consumers, and governments will install more than 55 billion IoT devices worldwide through 2025, while companies and consumers will spend nearly \$15 trillion on IoT devices, services, and maintenance.** Connected to the internet and equipped with sensors, these devices power much of the developing data-based economy and bridge the divide between the physical and digital worlds.

- **Smaller device installations continue to be the norm in the enterprise space, but larger deployments are starting to proliferate, according to exclusive BI Intelligence data.** Smaller IoT projects were most common in 2017, with 52% of respondents saying their company used 50 or fewer IoT devices. However, while just 19% said their company used more than 1,000 devices in 2017, that's a more substantial proportion of respondents than last year.
- **The majority of companies surveyed by BI Intelligence will invest less than \$1 million in IoT implementations,** with 31% planning to spend less than \$100,000 through 2022 on IoT solutions, and a further 37% planning to spend between \$100,000 and \$1 million. However, plans for spending seem to be rising from last year. In our 2016 survey, 54% of respondents said their companies planned to spend less than \$100,000.
- **The IoT tools that companies are putting into place are already having tangible impacts on businesses.** For example, heavy equipment and machinery manufacturer Caterpillar was able to save a mining client over \$600,000 in lost production costs by using predictive maintenance tools to predict, and ultimately cut down on, one of its machine's downtime.
- **And executives at companies around the US are expecting to see the investments they've made in IoT solutions start paying dividends soon.** Although just a small spattering of companies currently earn more than 10% of their revenue from IoT projects, over 41% predict their IoT projects will provide at least one-tenth of overall revenue five years from now, according to a survey from PwC and MAPI.

- **In the consumer IoT market, the continuing rise of the smart speaker, as well as an increased focus on home security products, are beginning to spur growth after years of sluggish connected device uptake.** And the market is likely to accelerate further as companies continue to gravitate toward these newer products. In fact, BI Intelligence expects the total number of installed smart home devices to eclipse 800 million in the US alone in 2022.
- **However, the amalgamation of smart home devices into our daily lives will be driven in large part by whether companies can successfully push adoption beyond tech-savvy consumers and early adopters.** Early data is promising, though, and suggests other portions of the population are at least somewhat open to these devices. As such, positive feedback from early adopters could lead to evangelism, resulting in greater adoption among additional segments.

[Download the charts and associated data in Excel »](#)

INTRODUCTION

The Internet of Things (IoT), or the network of connected devices that collect and share data globally, is typically seen as an industry at the cutting edge of technology. But it's becoming increasingly clear that many companies providing IoT solutions, as well as those using them, are starting to view the IoT as less of an industry itself, and more as a set of mainstream tools that can be used to address problems that come about. That shift in mindset is making the IoT more accessible, and driving companies and consumers to install billions of connected devices that allow them to obtain huge quantities of data, and put it to use to make tasks more efficient.

BI Intelligence forecasts that companies, consumers, and governments will install more than 55 billion IoT devices worldwide through 2025, while companies and consumers will spend nearly \$15 trillion on IoT devices, services, and maintenance. Connected to the internet and equipped with sensors, these devices power much of the developing data-based economy and bridge the divide between the physical and digital worlds. They are part of a broader ecosystem that also includes the networks that connect them, the remotes that allow users to manage them, the platforms that facilitate analysis and storage of the data they generate, and the security protocols that protect them from malicious interference.

In this report, BI Intelligence provides an overview of the IoT as it stands at the start of 2018. We offer a detailed overview of the IoT ecosystem, including developments in hardware, networks, remotes, platforms, and security, as well as trends in device installations, company projects, and investment. Additionally, we profile the enterprise and consumer IoT segments individually, drilling down into the drivers and characteristics that are shaping each market.

This report leverages Business Insider's 2017 Global IoT Executive Survey, which builds on our 2016 study to create exclusive time-series data and provide new insights on developments in the IoT marketplace. It also incorporates data from other exclusive BI Intelligence surveys conducted throughout 2017.

THE IoT ECOSYSTEM

The IoT relies on an ecosystem that is built around any particular deployment or installation, whether that's in a home, a factory, or on a city's streets. The IoT device itself is just one part of a larger deployment, and each piece of the ecosystem is critical to leveraging the data a device acquires to increase efficiency.

There are five components in an IoT ecosystem:

- **Hardware**, or the IoT devices within the IoT solution.
- **Networks** that connect the IoT solution to the user.
- **Remotes**, which provide the user with an interface to connect to and manage the IoT solution.
- **Platforms** that provide messaging, analytics, and data storage components.
- **Security protocols** that ensure the IoT solution remains protected.

Hardware

The primary goal of the IoT is to add internet connectivity to nonconnected devices in order to help users gather actionable data on the location where the devices are installed. Adding connectivity to such objects, though, requires specialized hardware, namely chipsets and sensors. Microchips pair with sensors to enable the computing that lets "smart" devices communicate with each other and with centralized platforms. Some common types of IoT sensors gauge temperature, measure vibrations, record moisture levels, or document chemical levels like pH.

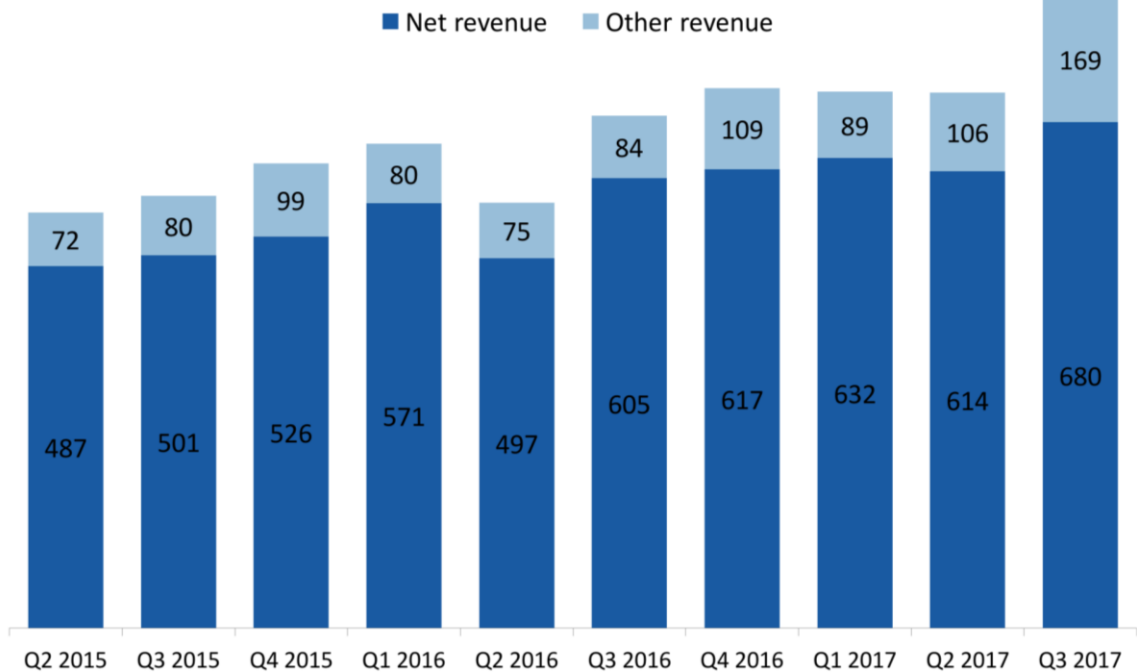
These types of IoT devices can also often be controlled, allowing remote changes to status. For instance, manufacturing equipment that measures how close to specification each product output is can relay that back to a user, and either shut off in response to a command or automatically based on recognition of certain conditions. In a consumer setting, users can install connected light bulbs that monitor time and energy use, while switching on and off in response to remote control through an app or voice command.

Growing demand for IoT devices has continued to transform the semiconductor industry, with leading companies in the microchip space adapting to capitalize on the growth of the IoT and its increasing share of the silicon market. IoT devices generally need specialized processors; they don't need the versatility of powerful, electricity-hungry processors like PCs, but instead require low-powered processors that fulfill a few specified functions.

- What's coming in 2018:** Companies developing sensors and chipsets, including Intel, ARM, and Qualcomm, are looking to expand beyond the silicon space to provide more elements of an IoT solution. And they're starting to see success: While Intel's IoT Group grew steadily overall through 2017, its major gains came from the Group's "other services" business. In 2018, we'll likely see such firms accelerate their efforts to diversify their revenue from the IoT, making service provision an even greater focal point.

Intel IoT Group Net Revenue

Global, millions (\$)



Source: Intel earnings

BI INTELLIGENCE

Networks

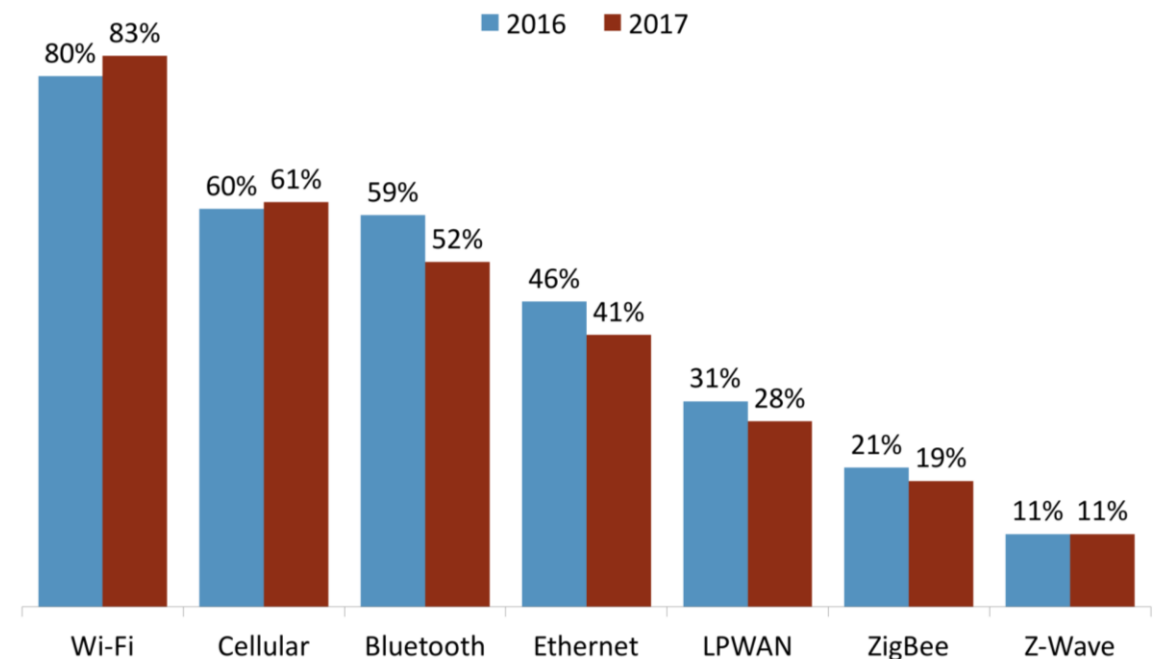
IoT devices use a variety of networks that enable the transmission of data to analysis platforms. Without these networks, there is no Internet of Things, only things. IoT solutions can employ a variety of networking protocols to enable communication. Some of the most popular and widely used are:

- **Wi-Fi/Ethernet:** The ubiquitous IP-based networking standard, it can be wired or wireless, with very high data rates over relatively short ranges. It's known and used by consumers as well as in enterprise and industrial use cases.
- **Mesh networks:** Multiple devices are connected to one another on a mesh network. Each device acts like a router, spreading data around for transmission to create multiple pathways to move data from device to server. This makes the network resilient even if some devices fail. Examples of mesh networks include Z-Wave, ZigBee, and Bluetooth.
- **Cellular:** Another widely used communication standard, cellular service can transmit at a variety of rates. The faster the cellular network (4G is the fastest and newest, followed by 3G and 2G), the more power that device will use, forcing users to weigh transmission speed against power draw and battery life.
- **Low-power, wide-area networks (LPWANs):** Specifically designed for IoT solutions, LPWANs are much like cellular networks, but they offer very low power usage for devices at the price of low rates of data transmission. Companies in the LPWAN space raised [huge sums of capital](#) and expanded their operations globally throughout 2017. Sigfox, which operates a proprietary LPWAN, has now raised over \$300 million, while LoRa network operator Actility completed a Series D round of \$75 million in April.

Wi-Fi, cellular, and Bluetooth remain the most commonly used network standards among IoT solution providers and device makers. And, despite greater investment, LPWANs haven't seen an increase in use from last year, according to our exclusive data. This suggests that solution providers are looking to integrate into existing infrastructures, instead of adding additional complexity by utilizing newer networks, in order to ensure client success and satisfaction.

Networks And Communication Technologies Providers Use In Their IoT Services

Global



Source: Business Insider Global IoT Executive Surveys, n=116 IoT providers, 2016; n=96 IoT providers, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

- **What's coming in 2018:** LPWANs will start to move into wider use this year. IoT devices are often able to provide great insights with small amounts of data; they can transmit a location or a few temperature readings from the course of a few hours, for example, which can then be boiled down to just a few bytes of data — exactly what LPWANs are designed for. Sigfox, Semtech, Actility, and others will offer different variants of LPWANs as they compete for market share. At the same time, telcos and other mobile companies will continue to develop 5G, which will fill in for IoT solutions where LPWANs don't fit the bill.

Remotes

Remotes enable users to interact with an IoT solution. Examples of remotes are smartphones, tablets, computers, connected TVs, smartwatches, and — in growing prominence this past year — smart speakers. These devices can offer an IoT component as a secondary capability, but their main use is something else. A smartphone can provide its location to a platform just like a GPS tag, for example, but users don't buy a smartphone for that express purpose. Understanding the use case of each remote helps a company better optimize its IoT solution. For example, providing a laptop instead of a smartphone to an agriculture supervisor who's monitoring moisture levels in a crop field is inefficient and will detract from the value the IoT solution could provide.

In the enterprise space, computers and tablets are the primary remotes because they allow users to visualize data in a variety of ways and consume large quantities of information at once. They also enable users to manipulate data and control IoT devices through the remote's interface, a key capability. The shift toward mobile devices highlights the increasing number of workers unattached to a specific workspace. This trend is illustrated by Apple's [partnership](#) with GE, which is aimed at allowing companies to create iOS applications that let workers monitor and manage industrial equipment using the Apple Watch, iPhone, and iPad.

In the consumer market, smartphones are still the most common remotes — but smart speakers are close behind. Smartphones are lightweight, highly portable, have high computing power, and enable users to easily connect to and manage their IoT solutions. Ericsson [estimates](#) that there will be more than 6.8 billion smartphone subscriptions by 2022, up from 3.9 billion in 2016, meaning that there will be nearly as many smartphone subscriptions as there will be people in the world. Because of this prevalence, smartphones will remain the top remote for the next five years in the connected home market. However, smart speakers like the Amazon Echo and Google Home are becoming increasingly central to the consumer IoT. Device sales have continued to grow as companies, including Amazon, have introduced smart speakers in new form factors and with various capabilities. Such voice-controlled systems employ artificial intelligence (AI) to make communication more interactive. Amazon's Alexa, Google Assistant, and Apple's Siri enable consumers to interact with smart home devices through voice commands, and are able to respond as well. As these assistants develop additional capabilities, they will likely move beyond conversation and into automation. The assistants will be able to observe users' actions and commands, use them to deduce preferences, and then change settings autonomously.

- **What's coming in 2018:** Voice will continue to grow in prominence as a remote, especially in the consumer space, with smart speakers driving much of this growth. But the biggest development will be the rise of AI and the diminished role that actual commands will play in controlling IoT devices and the smart home. Instead of responding to a directive from a mobile device, smart home systems will start to learn when inhabitants go to bed, and then turn off the lights and lock the doors on their own, for example.

Platforms

The term "IoT platform" refers to the middleware that transmits messages between devices and data storage — in other words, the glue that holds the IoT together. This definition also generally includes multiple components of the IoT such as data storage, analytics, and, in some cases, data communication and visualization. For example, an IoT platform provider may provide a middleware service that connects its data storage and analytics components, but choose to bundle the components together under the term "platform" because it makes it easier to package multiple services. As a result, many platforms are modular, meaning different components of a company's IoT platform can be used with those of other companies to ensure that a customer is getting the best service. Many IoT platform companies have seen excellent growth over the last few years: Software company PTC [generated](#) \$94 million in IoT software revenue, including from its ThingWorx IoT platform, in its fiscal 2017 (ended September 30), up 29% from the prior year.

The leading cloud providers are among the top players in the IoT platform space, and they continue to release new and more capable software development kits (SDKs) to enable IoT devices to be easily integrated into their cloud platforms. The cloud providers charge per device, or per number of messages sent through their platforms. Amazon charges \$5 to \$8 per million messages sent, depending on the region, for example. The more devices connected, and the more active they are, the higher the rates will be.

Some companies, however, are looking to bypass the use of cloud platforms by managing their devices locally. That's why companies like Amazon and Microsoft, which offer leading IoT public cloud platforms, have also started offering more robust edge computing solutions, which allow companies to collect, store, and process data close to where it's produced, so they don't need to rely on network connectivity to keep IoT devices functioning. Amazon introduced [AWS Greengrass](#) to this end, while Microsoft [rolled out](#) Azure IoT Edge, and Cisco [acquired](#) Springpath to bolster its own edge computing offerings.

- **What's coming in 2018:** To encourage greater and more widespread IoT use, platform companies will introduce tools to allow nontechnical employees, like sales and marketing staff, to build and operate IoT projects. Cloud provider [Salesforce](#) has already begun to do this, and other platforms will likely follow this trend and introduce more advanced data visualization, along with simpler application development protocols, so that nearly anyone in a company who has access to data from IoT devices can use a simple, graphical interface to set up their own data feed and control devices.

Security

Although no hacks have recently reached the scale and impact of the [headline-making](#) Mirai Botnet attack on Dyn in 2016, a similar botnet, [Reaper](#), has apparently spread to devices globally using known vulnerabilities, so as not to provide any clues about the attempted intrusion. Compromised devices include products from major manufacturers like D-Link and Netgear. And other devices, like [LG appliances](#), [pacemakers](#), and numerous [Android-based products](#), were found to be open to intrusion due to various potential exploits.

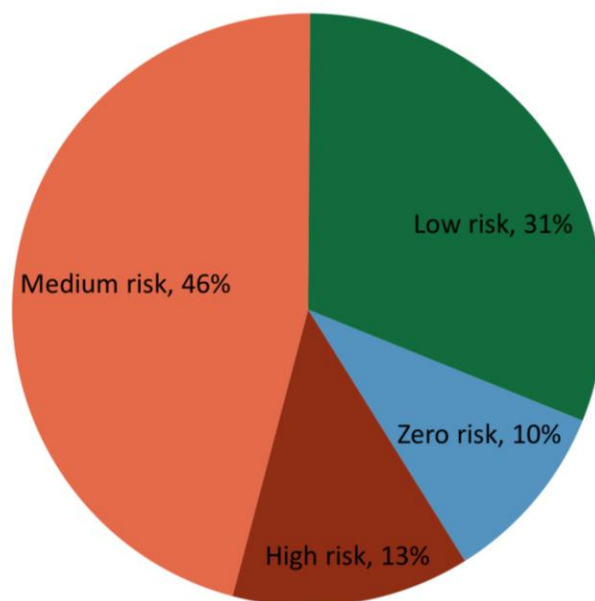
Consumer IoT products are uniquely vulnerable to these sorts of attacks.

That's because they're often produced by companies that haven't developed connected products in the past, and therefore boast little experience to draw on. In addition, consumers generally don't want to deal with security issues on their own — particularly if it means putting up with a cumbersome setup or diminished user experience. Device makers must strike a balance between developing secure devices that can resist hacks and presenting consumers with an easy setup process and seamless integration. A device that's extremely secure may be too complex to gain significant market share because it requires frequent password changes or too much user interaction, while a device that's not secure enough is vulnerable to hacks and could force the device maker to initiate a costly [recall](#) and possibly lose consumer trust.

Industrial and enterprise IoT solutions are better equipped to deal with security concerns. They're built from the bottom up with security in mind because corporate buyers generally demand robust protection for their systems. But, at the same time, there's a somewhat worrying acceptance of risk: [59%](#) of network and security professionals are willing to tolerate what they characterize as medium-to-high risk when it comes to securing IoT devices, according to a survey from ForeScout and Forrester. This means some companies are willing to allow devices that they see as liable to be compromised onto their networks, potentially opening the door for hackers to make their way in, intercept data from devices, or even embroil them in botnets.

IoT Device Risk Tolerance Among Network And Security Professionals

Q: How much security risk is your company willing to tolerate in relation to compliance requirements for IoT security?



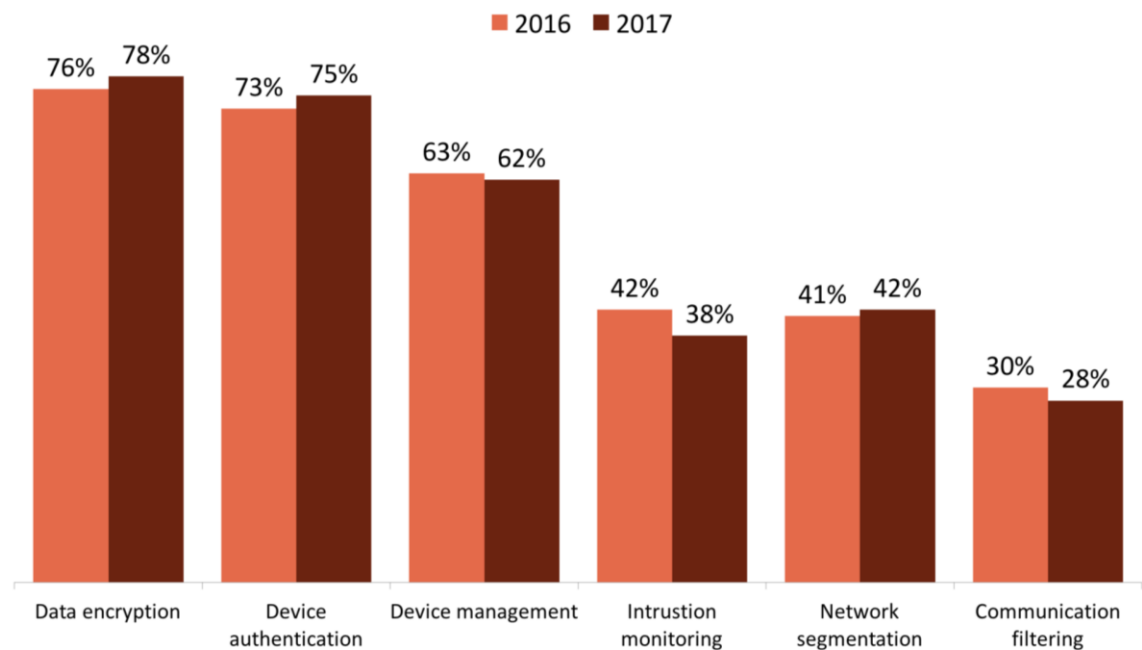
BI INTELLIGENCE

Source: ForeScout and Forrester, n=603 global IT and business decision-makers, 2017

Our survey data indicates that IoT solution providers and device makers offer a robust range of security measures. Of those surveyed, 78% indicated that their products or services offer data encryption, 75% data authentication, and 62% device management. These figures are all in line with last year, which shows that companies coming into the space, and those with more experience, continue to maintain a similar level of security services to keep their solutions relevant.

Security Measures Providers Use In IoT Services

Global



Source: Business Insider Global IoT Executive Surveys, n=116 IoT providers, 2016; n=96 IoT providers, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

- **What's coming in 2018:** Companies in the consumer space will pay more attention to security, but low-cost, low-margin device manufacturers on the fringes of the market, combined with inexperience on the part of companies entering the connected device space, will leave gaps that hackers will occasionally exploit. In the enterprise and industrial spaces, look for more solutions to implement security at the hardware level, along the lines of what both [Intel](#) and [ARM](#) have aimed for with recent initiatives, as well as for those protocols to integrate more closely with cloud-based storage platforms.

IoT MARKET OVERVIEW

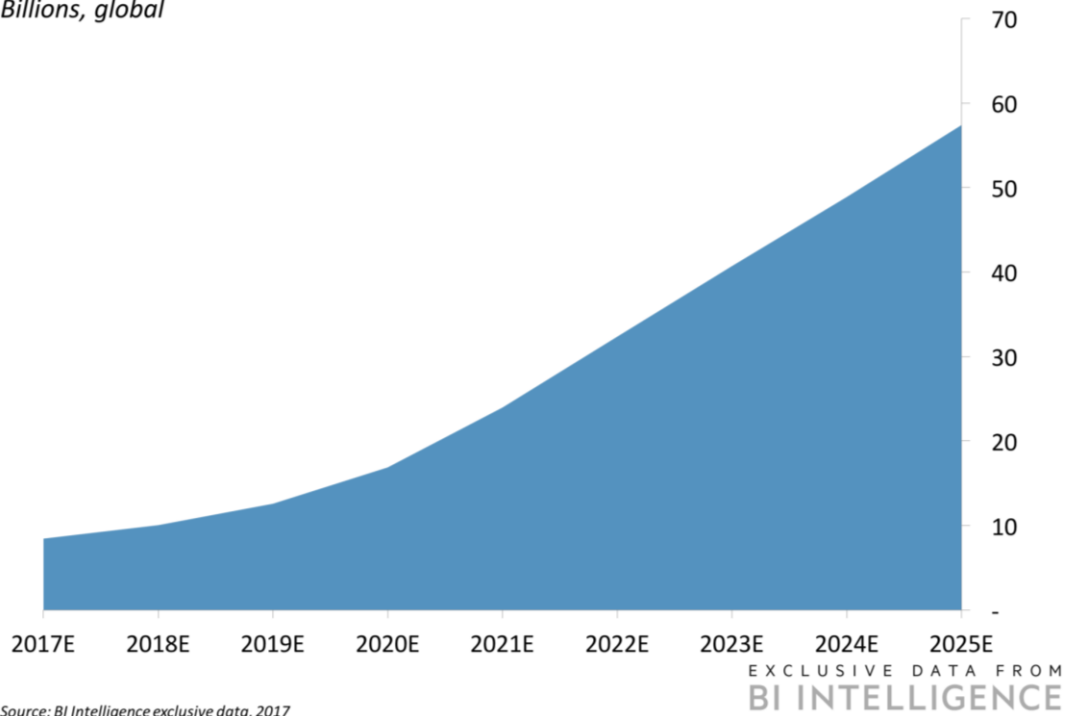
Companies and consumers around the world will continue to buy, install, and use connected IoT devices with growing frequency. This growth will be fueled primarily by commercial and industrial implementations, enabled by the burgeoning ecosystem, robust platforms, expanding networks, and tumbling hardware costs.

BI Intelligence forecasts that, by 2025, there will be more than 55 billion IoT devices installed around the world. This estimate is based on analysis of various environments that have or could support IoT devices, trends in device installation, and the development of platforms and IoT-specific networks that will support more IoT devices.

In particular, our forecast includes an expectation that the initiatives companies are working toward now, like Intel's [secure device onboarding \(SDO\)](#) or the rolling out of LPWANs, will start to have major impacts on device installation numbers around the world. The total number of IoT devices will grow steadily over the next few years before entering a period of rapid growth in the early part of the 2020s. This rapid growth won't last very long, however, as mature markets will eventually start to approach saturation, with far fewer devices globally not yet connected. After that, device numbers will continue to rise, but at more moderate levels.

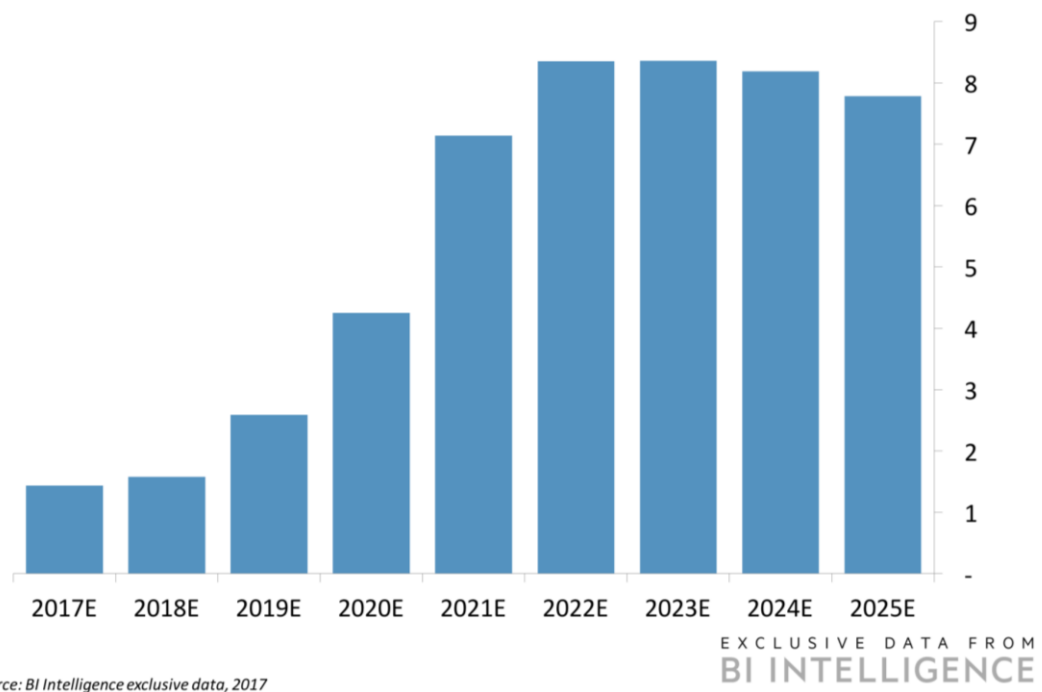
FORECAST: Total IoT Device Installation Base

Billions, global



FORECAST: Total IoT Device Annual Installations

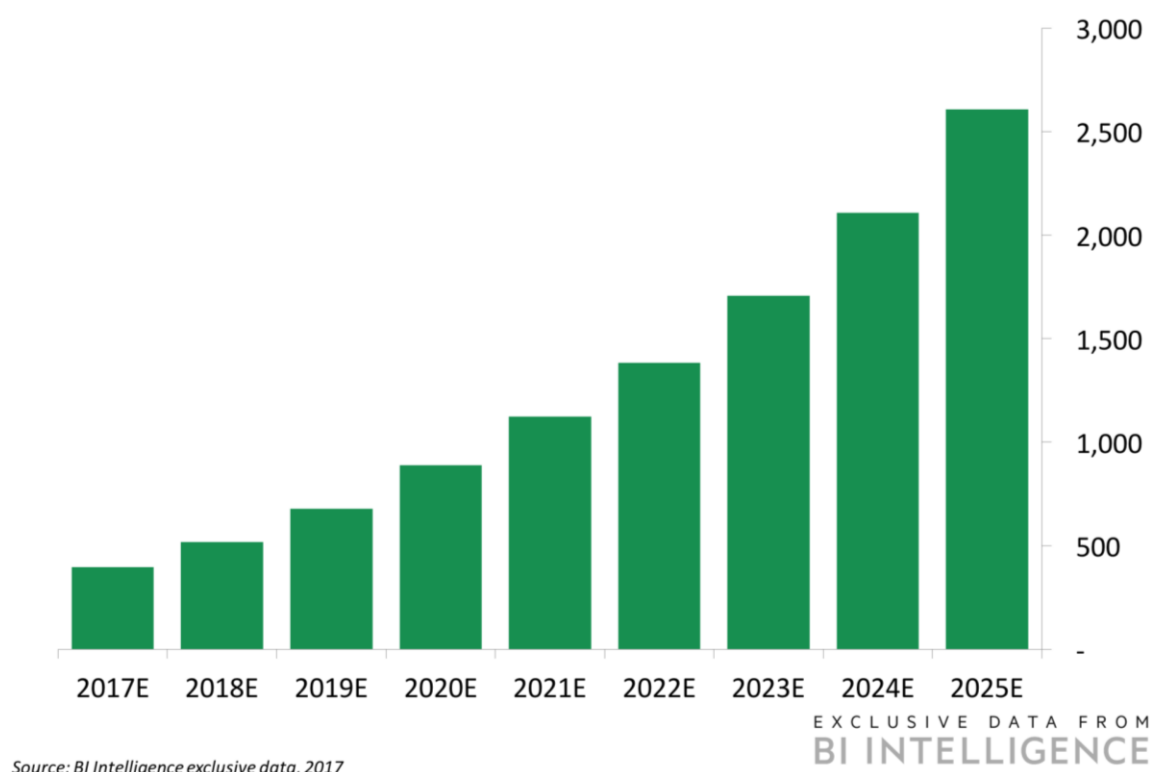
Billions, global



Meanwhile, IoT investment will rise steadily, rather than exponentially, through 2025. That's because growth in the number of devices will be fueled by falling device costs on both an upfront and continuing basis. Platforms are set to drive much of this shift by providing tools to drive down the expense of setting up and managing IoT devices. Overall, we forecast that companies and consumers will spend \$14.6 trillion on IoT devices, solutions, and supporting systems through 2025, with annual investment surpassing \$1 trillion in 2021.

FORECAST: Global IoT Investment

Billions (\$), global



Key Trends In The IoT

As 2018 gets underway, there are a couple of big trends we've identified among companies offering IoT solutions that are likely to inform the market's ongoing evolution. These developments don't necessarily impact all IoT providers or all companies using the IoT, but they're driving key changes in the way IoT solutions are delivered to businesses. Companies offering IoT solutions are generally gravitating in one of two ways: either they're expanding their suites to offer as close to a full-stack solution — an all-encompassing solution that can meet a company's entire IoT needs — as possible, or they're specializing and providing one very specific service for a client's IoT demands.

The Move Toward The Full Stack

Much of this trend is being driven by IoT platform companies, which are looking to establish themselves as the only IoT vendor that a company needs to work with. By developing full-stack offerings that include services like edge computing and remote network installation, these firms can ensure they're never forced to turn away a potential client. That means they're capable of supporting all different kinds of environments, from urban manufacturing facilities to offshore oil rigs.

Companies often need to add network connectivity to their IoT offerings to complete the stack and turn their solutions into one-stop-shops. This is leading to wide-ranging partnerships between companies in different sectors, in particular, telecommunications companies and wireless network operators. Companies like AT&T and Verizon in the US, Orange and Deutsche Telekom in Europe, and China Mobile and China Telecom in China are emerging as key players in enabling and supporting IoT solutions in their own right, as well as in partnership with IoT platform companies and solution providers.

The ____-As-A-Service Explosion

Companies are also developing IoT products to market and sell to potential customers as an ongoing service, rather than as discrete products purchased at one time or another. This ____-as-a-Service model doesn't necessarily apply to all industries or classes of IoT solutions, but there are a number of spaces where it's taking off. Here are a few examples:

- Companies have launched Drones-as-a-Service businesses for both industrial [inspection](#) use cases and [anti-poaching](#) efforts. Drones can be difficult to operate and require a skilled pilot, and they're also often employed in ways that call for intermittent use. In these sorts of cases, it can make more sense for a company to contract with a firm specializing in drones, as the firm can bring the equipment and expertise needed, as well as perform a particular task, such as inspecting oil pipelines, on a regular basis.
- [Kraken Robotics](#) moved away from just manufacturing and selling discrete robotic systems, and has started to offer its autonomous submarines to companies as a service, similarly utilizing its experience and expertise to provide robotic inspections of underwater oil and gas facilities and pipelines as a service to clients. This Robotics-as-a-Service model allows clients to leverage underwater robots for inspection without needing to invest in learning how to operate and maintain them.

A ____-as-a-Service model can afford companies with specialized knowledge and equipment a potentially lucrative place in the IoT by leveraging their core competencies to carve out a niche in the ecosystem. As such, for those companies that can't scale to compete with the big platforms, moving to this kind of setup may be a worthwhile option.

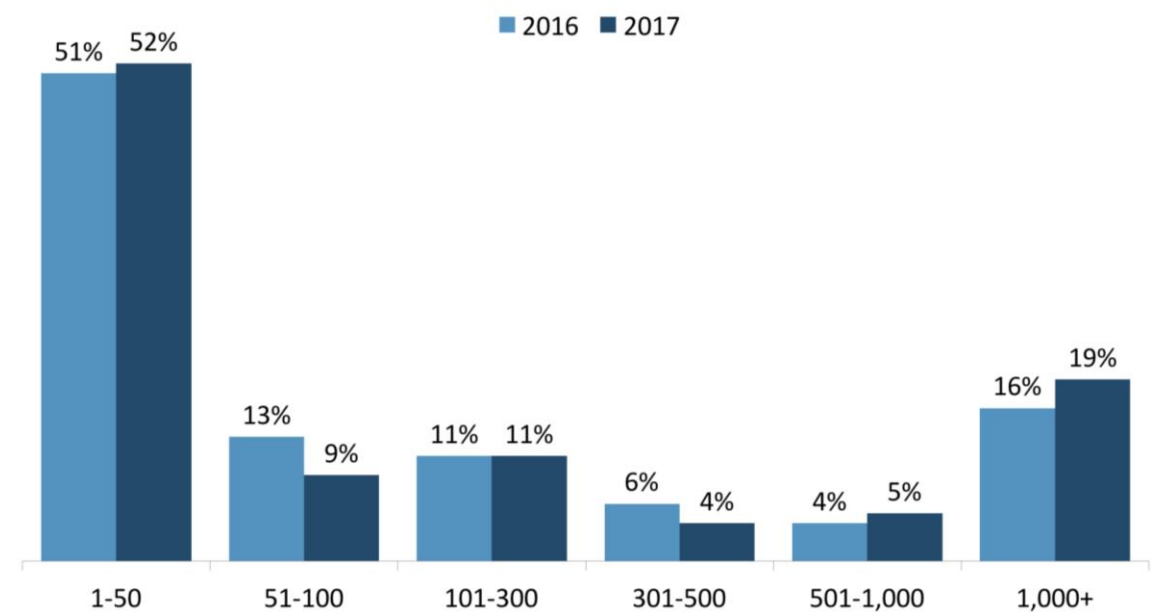
IoT Implementations

BI Intelligence's survey highlighted several trends regarding IoT solution implementations, which we define as device installations at a particular organization as part of a concerted and directed plan. A single implementation can involve installing multiple IoT devices, with the number depending on the needs of that company or group.

Smaller device installations continue to be the norm in the enterprise space, but larger deployments are starting to proliferate. Smaller IoT projects were most common in 2017, with 52% of respondents saying their company used 50 or fewer IoT devices. However, while just 19% said their company used more than 1,000 devices in 2017, that's a more substantial proportion of respondents than last year. Deploying IoT devices in large numbers requires major capital investments, which companies are likely reluctant to pursue until they fully understand the technologies involved.

The Number Of Devices Companies Use In Their IoT Solutions

Global



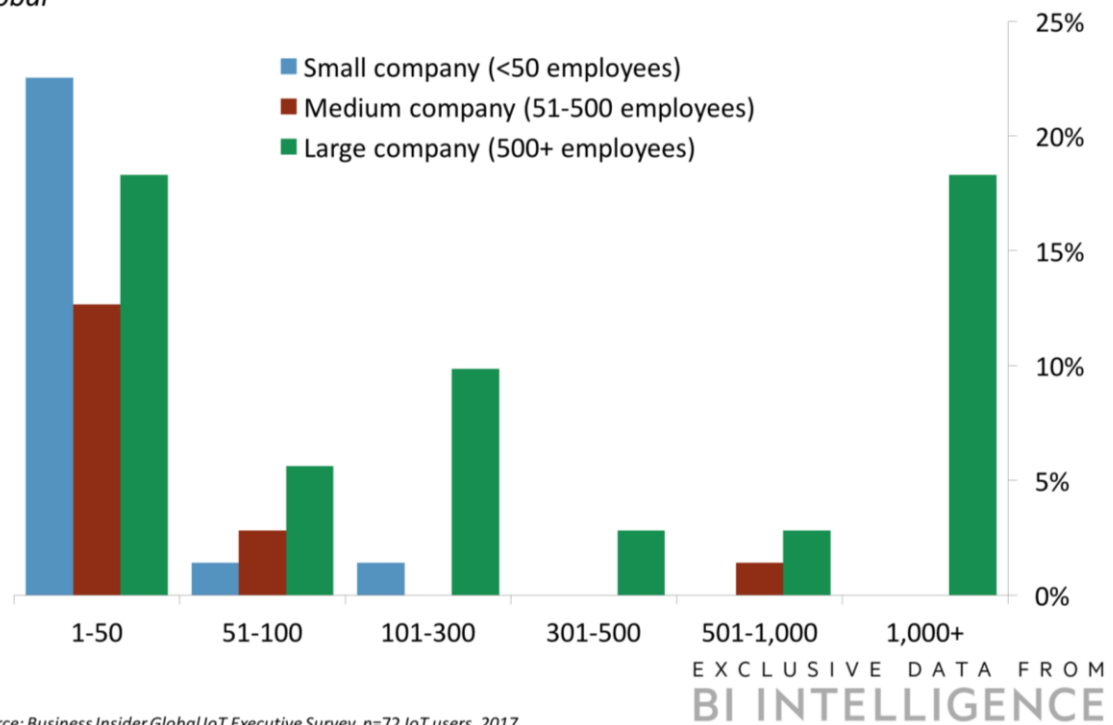
Source: Business Insider Global IoT Executive Surveys, n=235 IoT users, 2016; n=75 IoT users, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

The likelihood that a company will take on a larger IoT project remains correlated with the organization's size. In fact, we found that larger deployments, with more than 1,000 devices, are now even more concentrated among larger companies, those with more than 500 employees, than they were in 2016. Although some smaller organizations with specific operational needs may also venture into larger projects, they're likely to move forward only after smaller experimental pilot programs. In addition, we expect that many companies will look to minimize the number of devices they require for an implementation, relying more extensively on multipurpose sensors, such as cameras, that, when linked to cloud-based software, can take the place of multiple single-use devices.

Company Size And The Number Of Devices Used In IoT Solutions

Global



Source: Business Insider Global IoT Executive Survey, n=72 IoT users, 2017

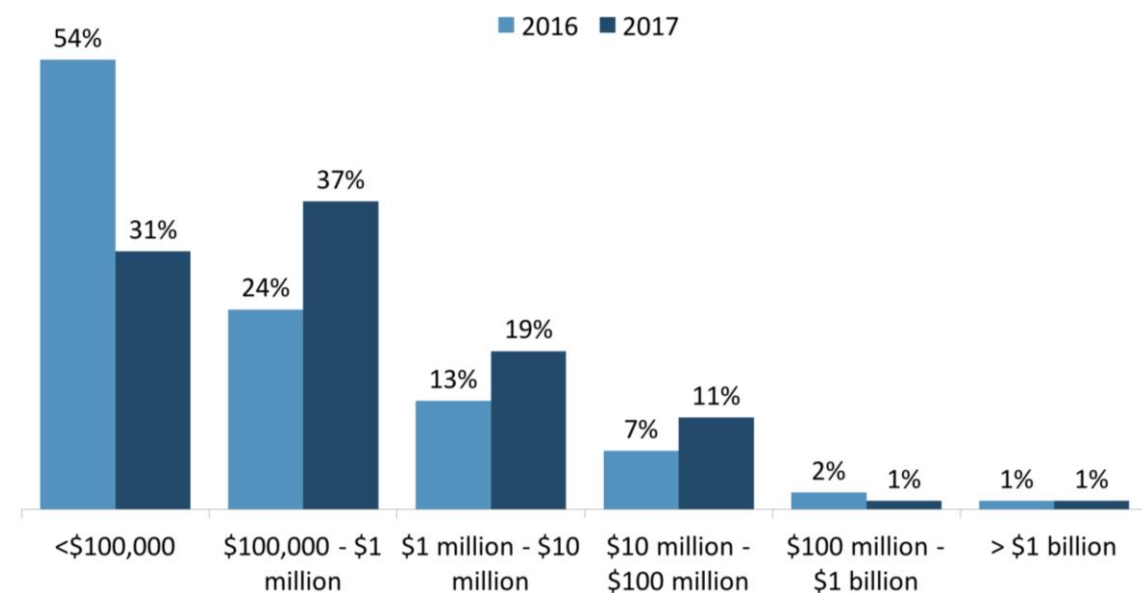
IoT Investment

For a more detailed picture of investment in the market, we asked companies implementing IoT solutions how much they plan to invest in their IoT solutions through the next five years.

- **Most executives surveyed said their companies plan to make limited investments in the IoT.** Thirty-one percent expect to spend less than \$100,000 through 2022 on IoT solutions, while a further 37% plan to spend between \$100,000 and \$1 million.
- **However, plans for spending seem to be rising from last year.** In our 2016 survey, 54% of respondents said their companies planned to spend less than \$100,000. This shift is likely due to some companies moving past the pilot stage, and pursuing wider IoT device rollouts that require more investment.
- **There are fewer responses as the investment numbers grow larger, though the paucity of companies able to make multimillion dollar investments in the IoT provides some explanation for this trend.** It's also important to bear in mind that a single investment of \$100 million represents the same overall investment in the IoT ecosystem as 10 investments of around \$10 million.

Companies' Planned 5-Year Investment In IoT Solutions

Global



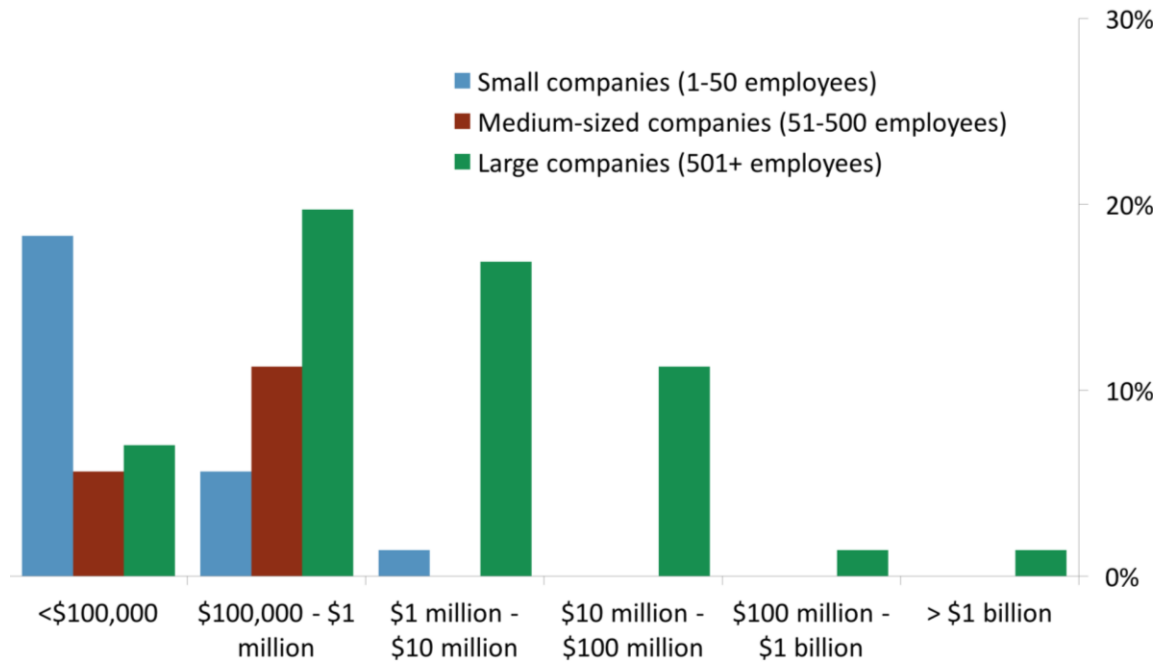
Source: Business Insider Global IoT Executive Surveys, n=235 IoT users, 2016; n=75 IoT users, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

As with IoT device installations, spending is heavily dependent on the size of the company and its number of employees. Companies with more than 500 employees are much more likely to plan to spend more on their IoT projects than companies with fewer employees, for instance. That's likely because companies with the resources to employ a substantial number of workers also often have the ability to allocate funding for large, potentially transformative IoT projects.

5-Year Planned IoT Investment, By Company Size

Global



Source: Business Insider Global IoT Executive Survey, n=72 IoT users, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

THE ENTERPRISE IoT MARKET

The major savings, both in capital and time, that implementing IoT solutions can bring is forcing companies to reckon with the IoT in order to stay competitive. This has made the enterprise sector the most mature part of the IoT, with many companies incorporating IoT technologies into everyday practice. In this section, we examine the process companies go through when contemplating an IoT solution, as well as the benefits such implementations can provide.

The Path To The IoT

The path from exploring the possibilities of the IoT to choosing to implement a solution is a long one that generally includes several stakeholders. To get a better understanding of the decision-making process, we asked companies that had and had not implemented IoT solutions about what factors ultimately contributed to their decisions.

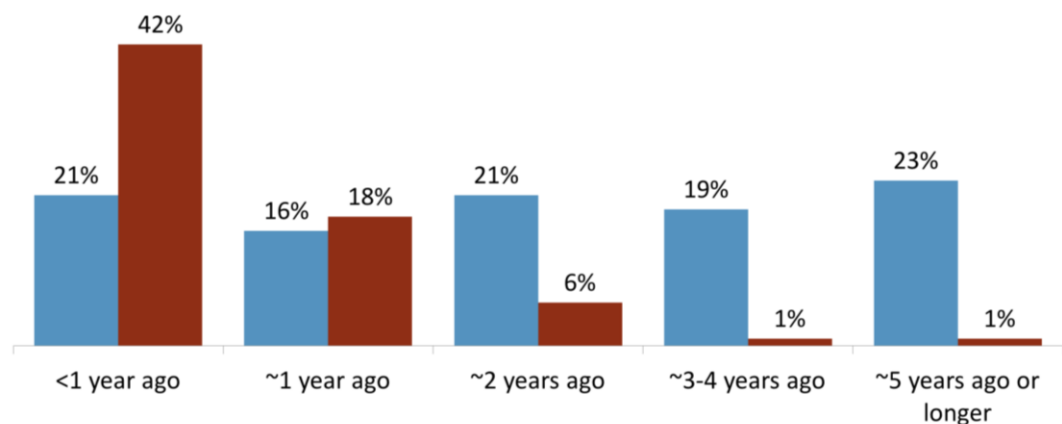
The Timeline Of IoT Investigation

Global

Q: When did your company first start looking into IoT solutions? (IoT users)

Q: When was an IoT solution seriously considered at your company? (IoT nonusers)

■ IoT users ■ IoT nonusers



Source: Business Insider Global IoT Executive Survey, n=75 IoT users; n=175 IoT nonusers, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

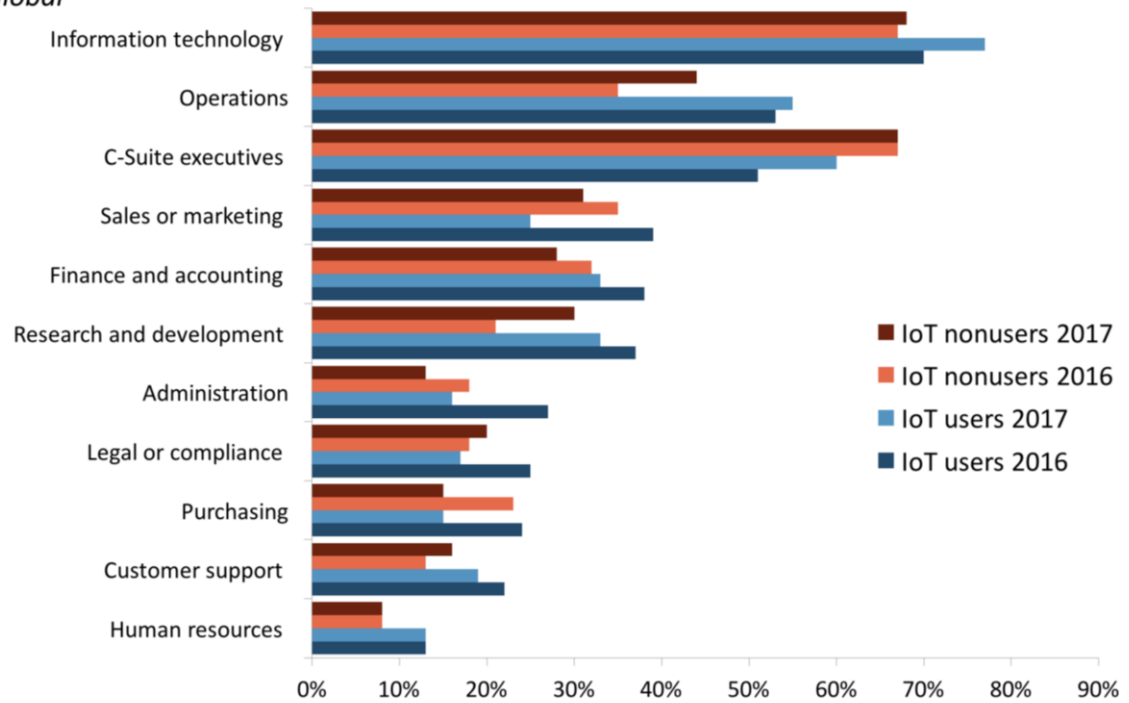
Decision-Makers

Choosing to move forward with an IoT project is a major decision for a company, and who is brought into the decision-making process can have a meaningful impact on the end result. BI Intelligence asked our survey respondents which groups were involved in the conversation.

- **Information technology (IT) was the most-cited department involved in the decision-making process.** At companies that had implemented an IoT solution, a slightly higher (78%) percentage of respondents indicated that the IT department was involved, compared with those that decided against implementing an IoT solution (68%). This makes sense given that companies rolling out an IoT solution will need IT staff to oversee its deployment and troubleshooting.
- **Like last year, we found that operations was far more involved in the decision-making process at companies that moved ahead with implementing an IoT solution (55%) than at those that didn't (44%).** This signals that companies that implemented an IoT solution were aiming to improve their day-to-day activities by involving operations teams in the decision-making process. Improving these functions offers an immediate return, which is a powerful enticement for implementation.
- **And C-Suite executives were largely involved in the process at both companies that have (60%) and have not (67%) implemented IoT solutions.** Interestingly, though, they were more often involved at companies that chose not to implement an IoT solution. This could indicate that teams wanting to implement IoT solutions were unable to articulate the value to upper management.

Departments Involved In IoT Decision-Making

Global



Source: Business Insider Global IoT Executive Surveys, n=84 IoT nonusers, n=232 IoT users, 2016; n=173 IoT nonusers, n=75 IoT users, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Implementation Drivers

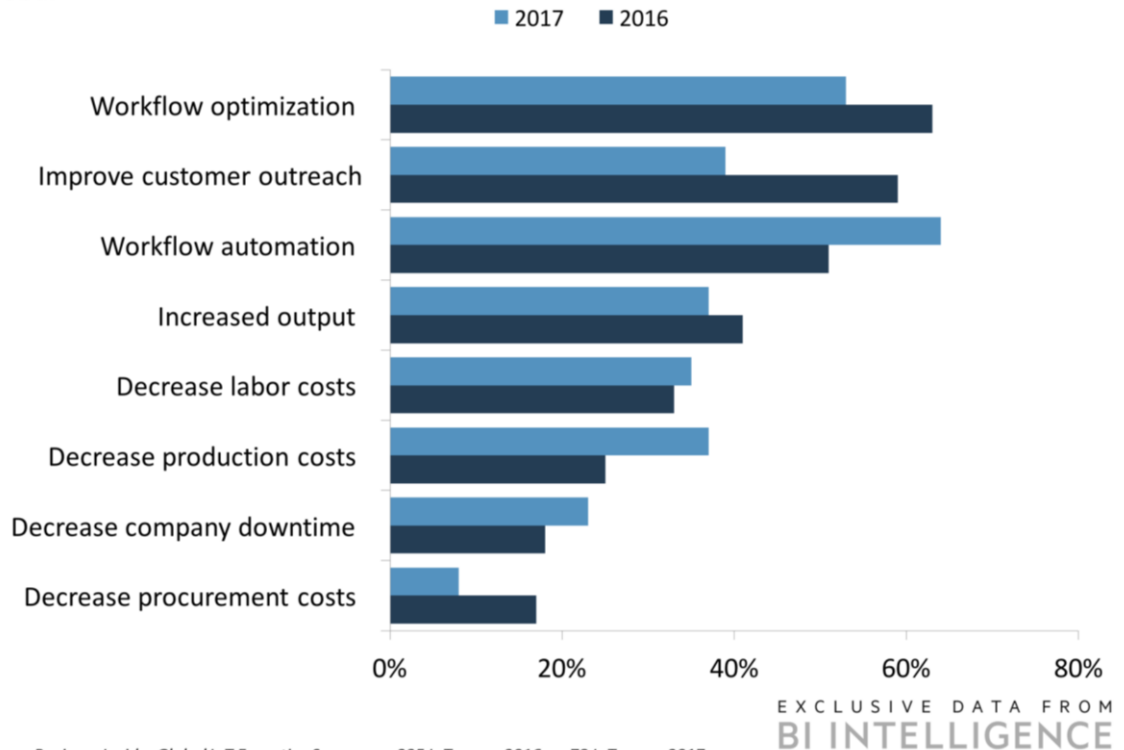
Companies considering implementing IoT solutions are above all looking to maximize value with minimal risk to their investment. Those that decide to move forward likely believe they can successfully secure several benefits of the IoT, like workforce optimization, workflow automation, and even increased output.

- **Workflow automation is the top driver prompting companies to adopt an IoT solution.** In fact, 64% of respondents to our survey reported using IoT solutions to automate portions of their business.
- **Optimizing workflows is another key driver, cited by 53% of respondents.** IoT solutions give workers and managers valuable data on where products and assets are. And managers can use that data to improve how they utilize resources and workers, thereby making processes more efficient.

- **Other drivers pushing businesses to adopt IoT solutions include decreasing production costs (37%) and increasing output (37%).**

Drivers That Led IoT Users To Seek Out Solutions

Global



Source: Business Insider Global IoT Executive Surveys, n=235 IoT users, 2016; n=78 IoT users, 2017

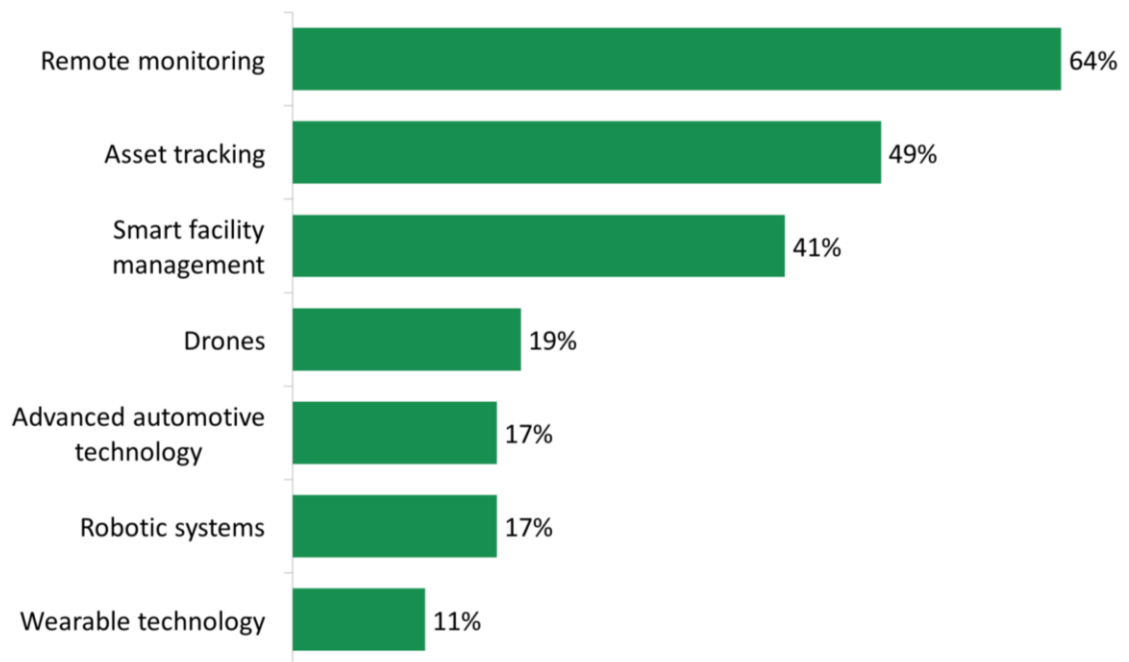
Enterprises are employing IoT solutions in a plethora of ways to achieve these results:

- **The most common use for IoT solutions is remote monitoring, which is utilized by 64% of respondents.** Remote monitoring devices provide a wealth of data on assets and equipment that can be leveraged to follow utilization and trends, ensure proper procedures are being followed, and enable large-scale analysis to increase efficiency and engage in useful practices like predictive maintenance. These types of devices can also set the stage for automation, which can be an even bigger cost-saver.

- **Similarly, 49% of respondents say their companies use IoT devices for asset tracking.** Many firms use IoT devices to gain visibility throughout their supply chains or to enable better tracking of shipped goods. These simple IoT devices can provide critical data to streamline operations and identify potential issues or bottlenecks.
- **A growing use for IoT solutions is smart facility management, employed by 41% of respondents.** These setups, which can include things like connected lighting and smart HVAC, can reduce costs for companies by using automation in infrastructure to limit electricity use, while also reducing the number of personnel needed for oversight.

Types Of IoT Solutions Companies Are Using

Global



Source: Business Insider Global IoT Executive Survey, n=75 IoT users, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

Implementation Challenges

Any new IoT project will face challenges, but the prospect of such issues can sometimes deter companies from taking steps to implement IoT projects in the first place. We asked those that had implemented an IoT solution about the top challenges they faced, and similarly asked those that hadn't implemented a solution what barriers kept them from moving forward.

- **Nearly half of companies that implemented an IoT solution cited security as a challenge, while 32% of those that didn't said it was a barrier.** Security is a concern that enterprises implementing an IoT solution will continue to grapple with. But it's also one that can be overcome, as evidenced by those that managed to move forward with their implementation anyway.
- **IoT users also cited the technology's maturity as a major challenge to implementation.** Moving forward with an IoT project involves putting technology into a new environment, which is bound to produce bugs and anxiety. However, as more companies implement IoT solutions, many of these bugs are starting to iron out on their own. Over time, this challenge should fall away entirely.
- **The main challenge stopping companies from adopting IoT solutions — selected by 51% of nonusers — is convincing management and decision-makers that such a deployment is the best course of action to pursue.**

Barriers To Implementing An IoT Solution

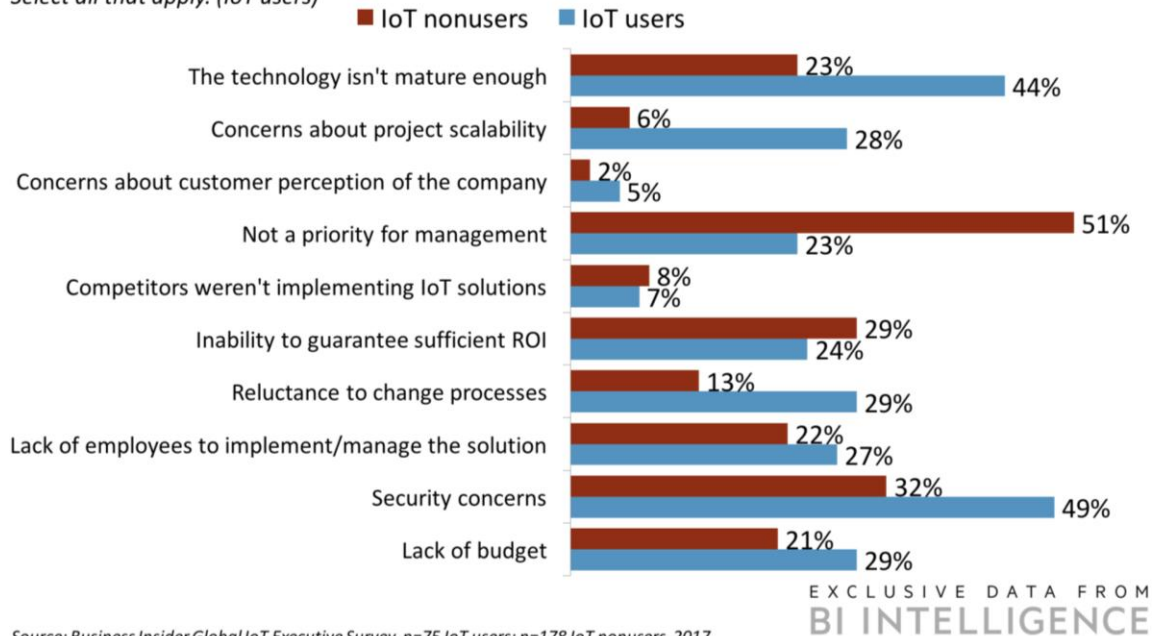
Global

Q: What were the main reasons your company decided not to implement an IoT solution?

Select all that apply. (IoT nonusers)

Q: What were the main challenges your company faced in implementing an IoT solution?

Select all that apply. (IoT users)



Overall, there's not a huge difference in profile between companies that have and have not implemented IoT solutions. For the most part, companies are seemingly approaching the IoT as a tool to address specific problems they might face. That means the decision to implement an IoT solution is more about clearing a certain obstacle, or improving a critical business area, than any kind of burning desire to remain on the cutting edge of technological trends. Based on our survey data, the main factor likely to influence if a company adopts an IoT solution is whether the situation and circumstances that would call for it are present.

The IoT Impact

The IoT tools that companies are putting into place are already having tangible impacts on businesses. This finding is borne out in our exclusive survey data, in other studies, and in our conversations with individuals working in industries where solutions are being put to use. In particular, BI Intelligence [spoke with](#) Tom Bucklar, director of innovations and digital at heavy equipment and machinery manufacturer Caterpillar, about the results the company is seeing from its IoT efforts. Here are some of the biggest takeaways from the discussion:

- **Caterpillar started outfitting the machinery and equipment it makes with sensors and embedded connectivity over a decade ago.** Everything from the company's forklifts to its heavy manufacturing machinery and engines are now built with embedded connectivity solutions and sensors. In total, this amounts to 560,000 connected Caterpillar vehicles around the world. This allows Caterpillar and its partners to gather key data on equipment use and lifecycles.
- **In addition, the company has built a set of software and analytics tools, as well as application programming interfaces (APIs), to help it and its customers process, analyze, and store this data.** Caterpillar itself provides data analytics for its clients, but this transformation has led it to also build out a network of partners to give its customers more options.
- **However, processing, analyzing, and visualizing the sheer volume of data produced by these solutions is often difficult.** IoT devices around the world will produce 18 zettabytes (about 18 trillion gigabytes) of data annually as soon as next year, according to [Cisco](#). This volume of data can be overwhelming for Caterpillar and its clients, so the company is working on finding ways to sift through all of it and provide actionable alerts on urgent information. The company is also investing in analytics and software to help with this, but it remains a troublesome challenge.

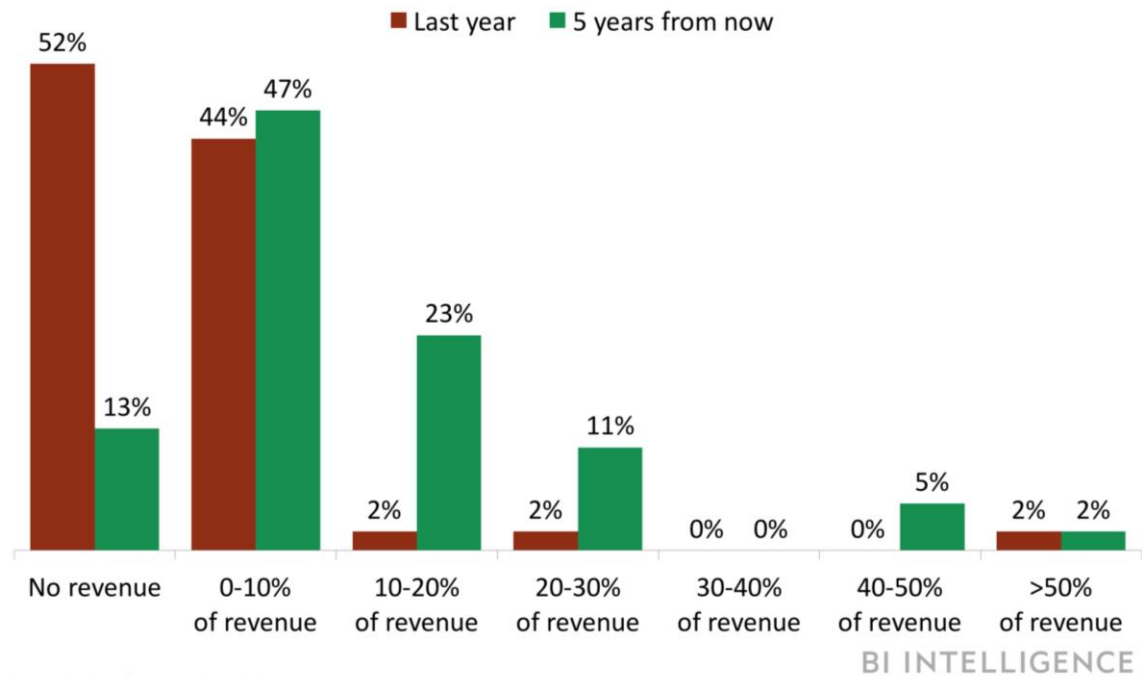
Caterpillar's efforts have helped it provide customers with software and services that increase the value of its offerings by cutting operating costs and increasing productivity. These software and services perform a variety of tasks, including predictive maintenance and making its machines autonomous. Bucklar shared that Caterpillar saved a mining client over \$600,000 in lost production costs by using predictive maintenance tools to predict, and ultimately cut down on, one of its machine's downtime. In addition, another client in the construction industry increased its asset utilization by 15% through streaming data that Caterpillar helped collect and analyze on 10,000 pieces of equipment. And its autonomous vehicles have helped increase productivity at mining sites by 20%, compared with the manually driven alternative.

Executives at companies around the US are also expecting to see the investments they've made in IoT solutions start [paying dividends soon](#).

Although just a small spattering of companies currently earn more than 10% of their revenue from IoT projects, over 41% predict their IoT projects will provide at least one-tenth of overall revenue five years from now, according to a [survey](#) from PwC and MAPI. And just 13% expect they won't bring in any revenue from their IoT projects. Connecting equipment and facilities allows companies to gain critical insights into their day-to-day operations, enabling them to identify processes that need to be improved, or to shut down machinery that needs minor repairs in order to avoid more disruptive failures.

US Companies Predict Revenue From IoT-Driven Products To Climb

How much they say they earned last year vs. their 5-year outlook

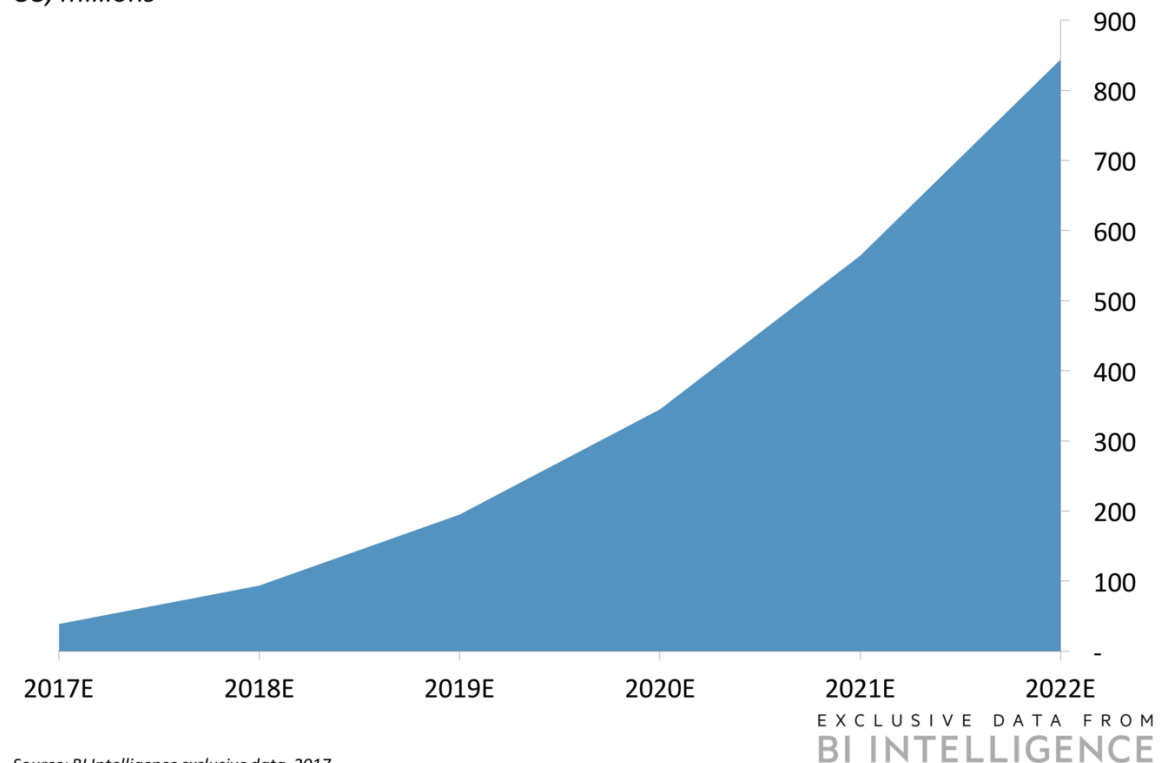


THE CONSUMER IoT MARKET

The consumer IoT market is made up of the portions of the IoT that serve end users in their homes or personal lives. The most common types of consumer IoT devices include smart home devices, such as the Nest Thermostat or the August Doorlock. However, in 2017, this space was largely defined by the continuing [rise of the smart speaker](#), as well as an increased focus on home security products. These trends began to spur growth in the consumer IoT after years spent getting off the starting block, and the market is likely to accelerate further as companies continue to gravitate toward these newer products. In fact, BI Intelligence expects the total number of installed smart home devices to eclipse 800 million in the US alone in 2022.

FORECAST: Total Installed Smart Home Devices

US, millions



Source: BI Intelligence exclusive data, 2017

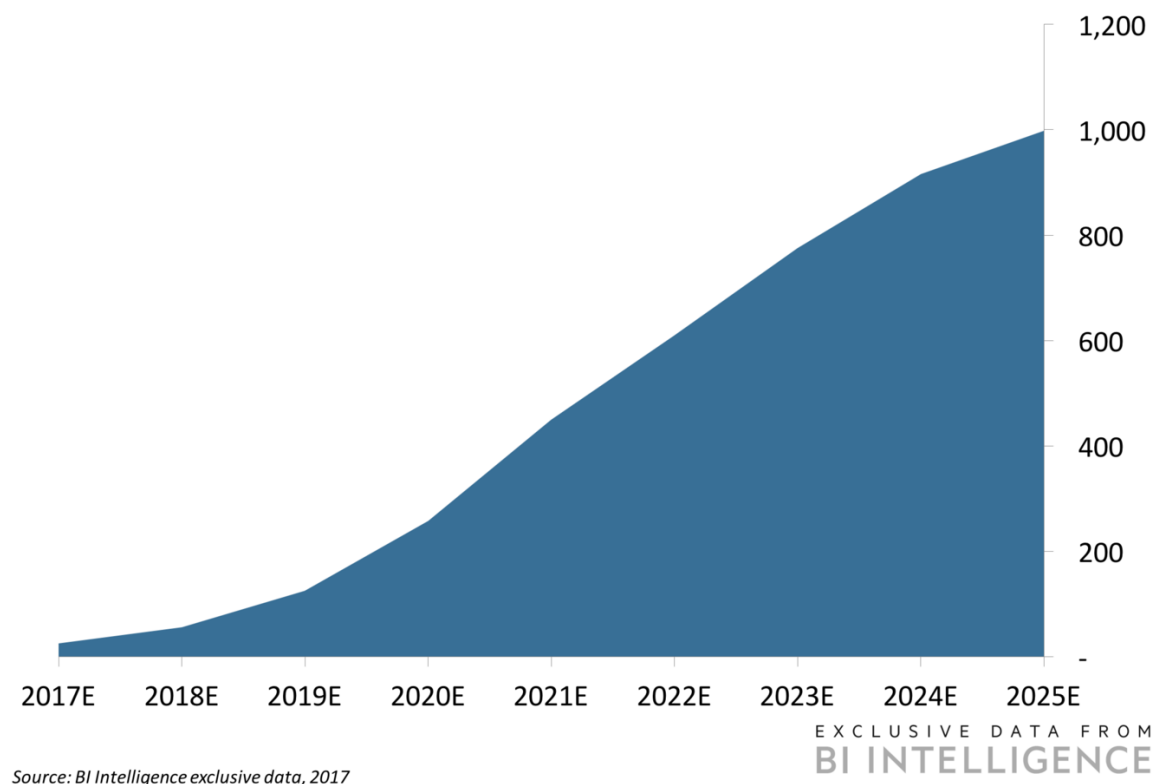
Smart Speakers

Prior to last year, Amazon was just about the only major player in the smart speaker market, and its Echo devices were only available in the US, UK, and Germany. Since then, the Amazon Echo has experienced resounding success, amassing [more than 75%](#) of the US smart speaker market. That success has spurred competitors to develop smart speakers of their own, with new entrants pushing into the market all the time.

BI Intelligence forecasts that nearly 1 billion smart speakers will ship globally through 2025. Shipments will rise steadily over the next few years as low-cost devices continue to flood the market, especially in Asia. At the same time, consumers in Western markets will likely buy into the strategies that Amazon, Google, and others are pushing by purchasing multiple smart speakers and installing them throughout their homes.

FORECAST: Global Smart Speaker Install Base

Millions, global



Here's a rundown of some of the biggest players riding the Echo's coattails, and a look at those potentially gearing up for market entry:

- The first [major competitor](#) was the Google Home, which leveraged Google Assistant to provide users with many of the same features they could find in Alexa, combined with Chromecast integration and Google's search functionality. Google has invested heavily to publicize the Google Home, paying for a [Super Bowl ad](#) and other campaigns.
- Apple announced its HomePod in a bid to grab a share of the market. The HomePod is a high-quality speaker capable of answering questions and controlling smart home devices. Apple has expressed hope that the HomePod will serve as a new pillar product, but the device was [delayed](#) until February 2018, missing out on the 2017 holiday season.
- Microsoft launched [Invoke](#), a smart speaker powered by its Cortana voice assistant, in partnership with Harman-Kardon. [Samsung](#) seems likely to follow suit after the introduction of its Bixby voice assistant and a number of connected home products.
- Baidu is reportedly working to improve its AI and voice recognition [software](#) in order to release a smart speaker in the Chinese market that leverages its search capabilities. Additionally, Alibaba, the Chinese e-commerce giant, released the [Tmall Genie](#) smart speaker, which is focused around its core business in China. Meanwhile, [Xiaomi](#) launched its low-priced voice-activated Mi smart speaker for the Chinese market as well.
- Facebook is purportedly looking into a smart speaker with a screen for viewing pictures and videos.

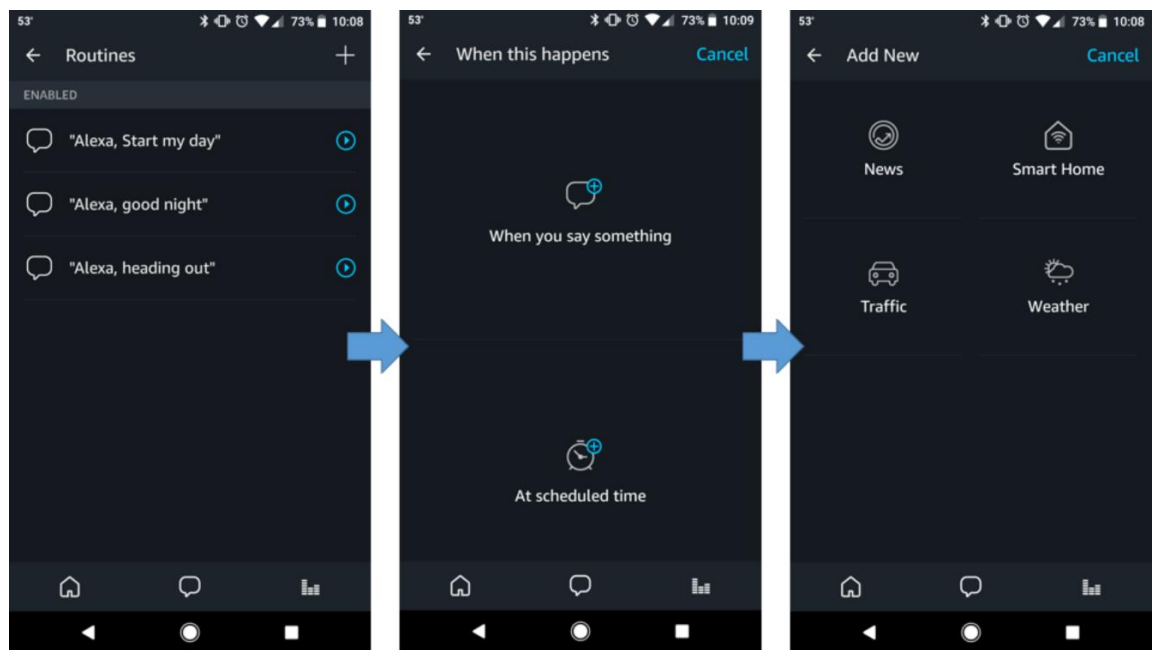
And Amazon itself has continued to introduce new devices to expand the ecosystem that it, for the most part, created on its own, introducing the smart home-oriented Echo Plus and the alarm clock-like Echo Spot in late 2017.

Smart speakers will remain a useful way to control the smart home, but their main job is to provide a platform for AI-powered voice assistants. These voice assistants will eventually outgrow the smart speaker, and there are already indications that the assistant may be more permanent than the device. Smart speakers will continue to play a critical role in the smart home as an access point for the voice assistants that will become more and more central to people's lives, but these assistants will also be available in other places. Alexa is already being integrated into lamps, appliances, and phones, for example. Meanwhile, Siri and Google Assistant started off in the phone before moving to the smart speaker, and are still mostly used and available on mobile devices. So, rather than being the hub of the smart home and the primary way to access Alexa, Siri, or Google Assistant, smart speakers will gradually transform over the next few years into one of many peripheral devices in orbit around the central, omnipresent voice assistant.

Smart Home Devices

The market for smart home devices overall hasn't taken off as many had projected in recent years. There were no killer features that pushed consumers to buy and use IoT devices in their homes or personal lives, and the devices were generally overpriced, difficult to set up, and part of a fragmented ecosystem that made control a hassle.

The smart speaker has started to provide solutions to many of these problems. Using the speaker, consumers have a ready-made hub and a natural interface to let users control smart home devices. Amazon and Google make it simple for users to incorporate things like smart light bulbs, connected door locks, and smart appliances into their homes. They've also introduced ways for consumers to control multiple devices at once. This can be done through "[Routines](#)," which allow users to combine controlling smart home devices with other Alexa capabilities, like reading out news and weather based on a single phrase; preset rooms that incorporate multiple devices; or linking phrases within a single sentence to control numerous devices at once.

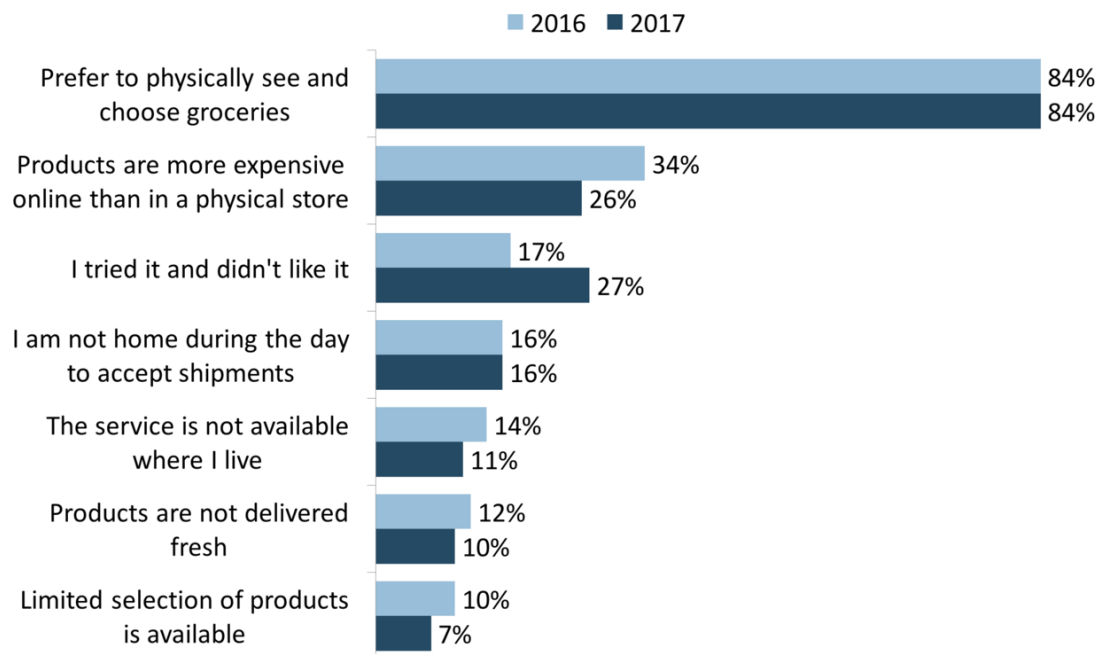


Amazon's Echo Plus also incorporates a number of smart home network standards, meaning that consumers don't need to use a separate hub for devices that operate using a standard like ZigBee, Z-Wave, or Bluetooth Low Energy. Philips' Hue smart bulbs use the ZigBee standard, and thus typically need a separate hub to enable a Wi-Fi connection, for example; the Echo Plus can take the place of that ZigBee-based hub. This gives the Echo Plus a key advantage over a number of potential alternatives, as it means that consumers can control a plethora of devices on different standards through one portal. That said, there are a few routers on the market that also boast this functionality, like internet service-provider Comcast's xFi Advanced Gateway, which sports similar connectivity to the Echo Plus, but without the smart speaker component.

Another key innovation has been the development of services that take advantage of smart locks. Smart lock company [August](#), which was acquired last year by lock giant Assa Abloy, has partnered with crowdsourced-delivery startup Deliv to create an in-home delivery service for retailers using connected locks, for example. The new service, known as August Access, will allow any retail partner to use Deliv couriers to deliver packages into homes equipped with a compatible smart lock from August, Emtek, or Yale using a single-access code. Additionally, Amazon is working on a similar program leveraging its new [Key smart camera](#). Such services could be the first example of a use case for smart home devices and may well galvanize smart lock adoption. That's because they promise to increase convenience, but only for those who actually own smart locks.

Up to this point, smart locks haven't offered much beyond eliminating the need to carry keys. However, a service like August Access could eliminate the need for consumers to restrict delivery times to periods when they'll be home. That could be especially convenient when it comes to grocery deliveries — [16% percent](#) of consumers don't order groceries online because they aren't home to accept shipments.

Reasons For Not Using Online Grocery Delivery



Source: AlphaWise and Morgan Stanley Research

BI INTELLIGENCE

Home Security

Another significant trend in 2017 was consumer IoT companies' shift to smart home security video-monitoring solutions. The many steps taken by companies in this area could turn a self-installed security system into a gateway to wider consumer IoT adoption in 2018. Here are some examples:

- **[Nest](#), the Alphabet-owned smart home company, announced a suite of security-focused products, called Nest Secure.** The suite expands Nest's security lineup and offers a unified control and management system for consumers. The system starts at \$499, though securing an entire home could send that much higher, as door sensors beyond the two included cost \$59 each. Additionally, Nest provides cameras that can slot into this system — the company [purchased](#) connected-camera company Dropcam in 2015 and has introduced a number of cameras paired with AI and face recognition software. This could potentially allow consumers to equip their homes with comprehensive, video-enabled security, providing Nest with a new revenue stream.
- **Smart home company [Wink](#) is introducing a bundle that will combine a number of home security devices paired with its hub.** The bundle will include a pair of door and window sensors, as well as a ground-level motion detector and the company's smart home device hub for \$200. Companies making devices that rely on hubs are facing competition from simpler systems. In response, Wink and others are looking to home security bundles to take advantage of existing products and expertise to offer new services.

- [T-Mobile](#) will offer a smart home security bundle with devices from **Nest**. The company will offer the bundle for an upfront cost and require a 24-month service agreement. Devices from T-Mobile will feature a cellular backup, and offer the same home-monitoring capabilities as ones purchased directly from Nest. T-Mobile is looking for ways to offer new services using its cellular network, and this is a relatively low risk way to do that for the telecom. That's because home security devices are typically connected to a Wi-Fi network, so there won't be very many circumstances when that cellular backup is put to use.

Much like smart home companies have adapted to what's worked by flocking to the smart speaker, home security will also continue to be a catalyst for overall smart home growth. That's because products in this area boast easily digestible use cases that are likely to spur strong customer uptake, providing companies with lucrative paths to diversify revenue.

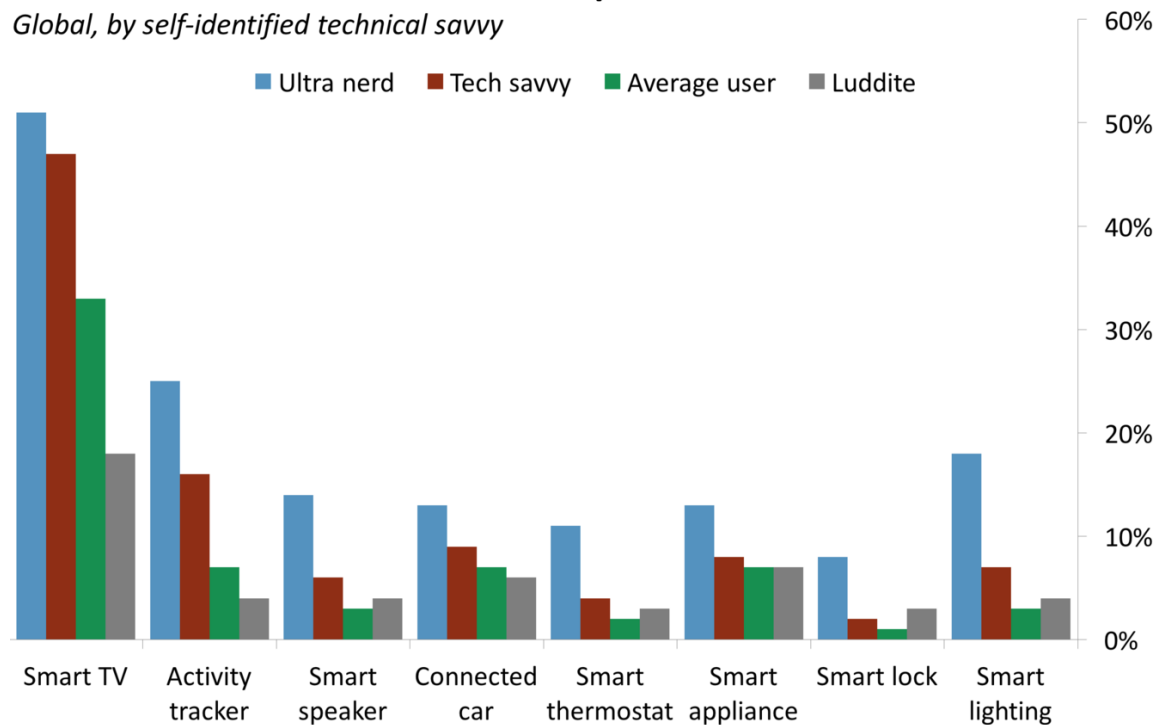
Consumer Sentiment And The Connected Home

The amalgamation of smart home devices into our daily lives will be driven in large part by whether companies can successfully push adoption beyond tech-savvy consumers and early adopters. A survey from Mozilla provided to BI Intelligence gives useful insight into this question. It's a public survey conducted through Mozilla's Firefox web browser, email, and social media, with respondents answering the survey in one of six languages. And while the data is skewed toward early adopters, with 52% of respondents characterizing themselves as technically savvy or more capable, its huge pool of responses provides useful feedback that companies can leverage to prepare their products for a mass-market push.

One of the key takeaways from Mozilla's study is that smart home devices are moving beyond the bleeding edge of consumers. Tech-savvy consumers own connected home devices at higher rates than average or less savvy users, following the pattern one would expect from an emerging technology sector like the smart home. However, the limited but consistent penetration among less technically savvy consumers just a few years after the introduction of the earliest connected home devices shows that these devices aren't confined to early adopters — 15% of early adopters have smart appliances, compared with 8% of “luddites,” for instance.

Connected Home Device Ownership

Global, by self-identified technical savvy



Source: Mozilla, n=176,926, 2017

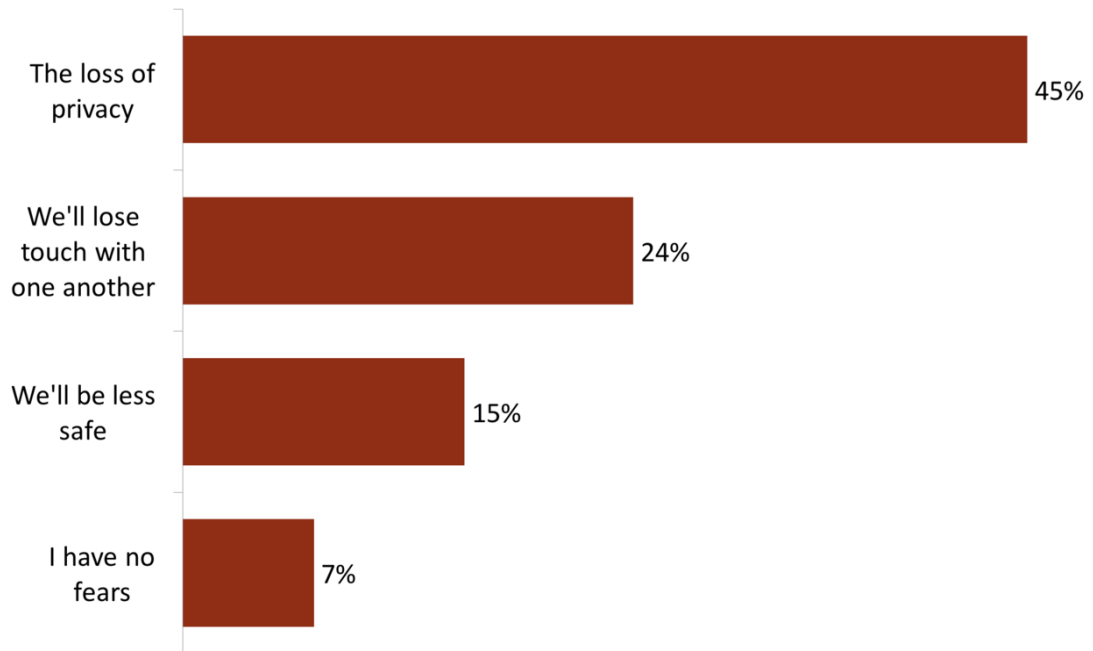
BI INTELLIGENCE

The study also illustrates that the proliferation of smart home devices is instilling new sets of fears and anxieties in the consumers who make up their target market:

- **45% of respondents are most afraid that connected devices will threaten their privacy.** Despite this, people are putting always-listening devices like Amazon Echo and Google Home all around their houses. This is because such companies have strategies aimed at getting their smart speakers — sometimes equipped with cameras — into bedrooms, kitchens, and living rooms. These companies have been successful in providing benefits that make consumers ignore any privacy concerns they might have.
- **Nearly a quarter of respondents fear losing touch with other people.** As voice assistants spread throughout homes and devices start to automate services, there's potential for these devices to take over many of the things people do with one another, like buying products or arranging services. This could lead to consumers increasingly turning to voice assistants instead of other people.
- **Security is the biggest concern among 15% of respondents.** The emergence of ransomware attacks like WannaCry, along with news of IoT devices being compromised by hackers looking to take them over or use them in botnets like Mirai or Reaper, have left consumers wary of connected devices.

Privacy Fears Predominate The Connected Future

Q: What is your biggest fear as we move towards a more connected future?



Source: Mozilla, n=176,314 global consumers, 2017

BI INTELLIGENCE

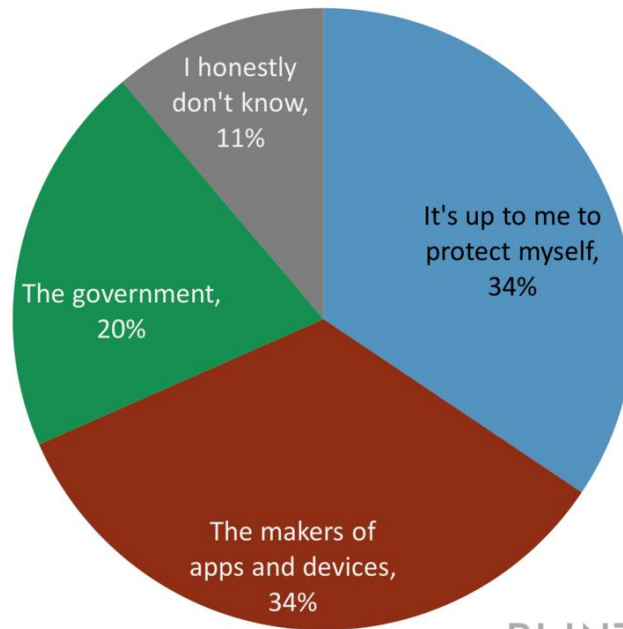
Consumers are turning in several directions for help in addressing these security and privacy concerns:

- **Over one-third are turning to device-makers and app developers.** These companies are the ones that stand to benefit most from the growth of connected devices, and are pushing consumers to adopt them. Therefore, respondents likely see security and privacy protections as a fair trade for adopting their solutions.
- **But another 34% of respondents don't see anyone to turn to for protection.** These consumers believe that since people adopt loosely regulated, connected devices by choice — with or without security measures in place — there's no one to turn to for protection. While this view may be acceptable for tech-savvy respondents, others may be uncomfortable relying on themselves for protection.

This data illustrates that device-makers have to take steps to protect consumers from privacy and security vulnerabilities to allow the market for connected devices to continue to grow.

Global Consumers Torn Over Who To Turn To For Protection

Q: Who is most responsible for protecting the online safety, privacy, and security of the connected apps and devices you own?



BI INTELLIGENCE

Source: Mozilla, n=174,690, 2017

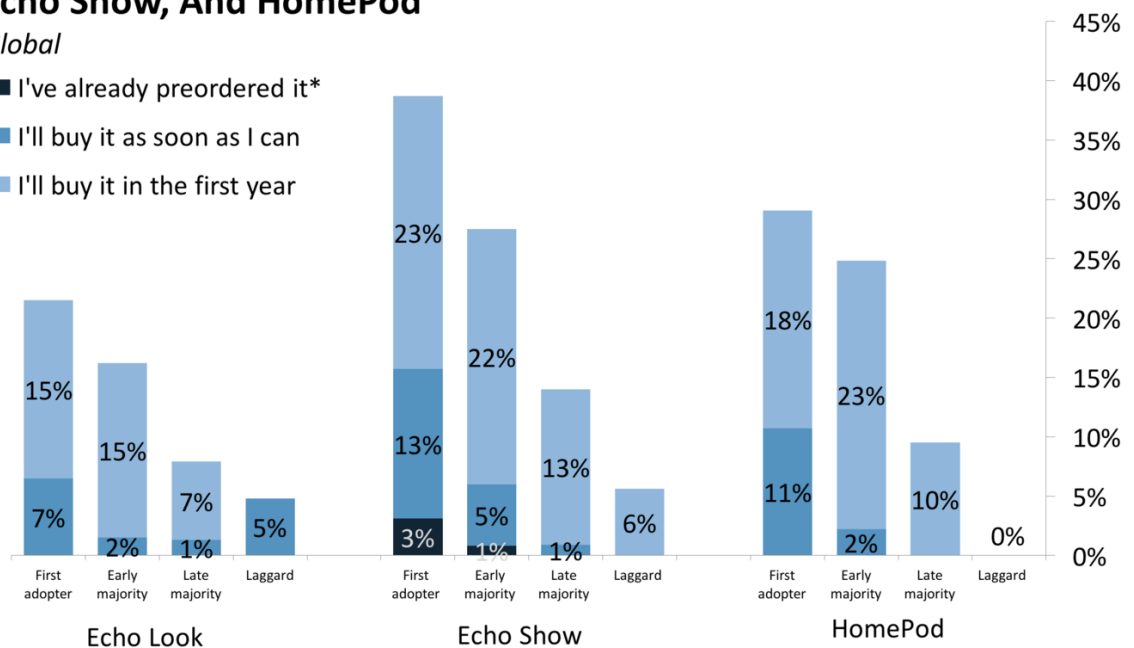
Additionally, the findings from Mozilla's survey parallel a number of results from BI Intelligence's Tech Adoption Surveys, which focused on recently launched smart speakers from Amazon and Apple, and were fielded within two weeks of each announcement to gauge first reaction. In both studies, tech-savvy respondents showed a clear propensity to adopt faster, but laggards also showed interest. This suggests that less tech-savvy consumers are open to being swayed into making a purchase, which could lead to more mainstream adoption.

In our Tech Adoption Surveys, self-described first adopters were most likely to say they'd purchase the newly announced smart speakers, with 39% saying they'd buy the Echo Show, for example. But, at the same time, 28% and 14% of early and late majority respondents, respectively, also planned to buy the device, illustrating interest in the Echo Show beyond just first adopters. Given the openness other portions of the population exhibit to these devices, positive feedback from early adopters could lead to evangelism, resulting in greater adoption among additional segments.

Likely Buyers Among Early Adopters Of Echo Look, Echo Show, And HomePod

Global

- I've already preordered it*
- I'll buy it as soon as I can
- I'll buy it in the first year



EXCLUSIVE DATA FROM
BI INTELLIGENCE

*Note: Only the Echo Show was made available for preorder.

Source: BI Intelligence Tech Adoption Surveys, Echo Look, n=2,052; Echo Show, n=779; HomePod, n=876, May-June 2017

This trend will likely continue to play out throughout the consumer IoT market in 2018 and beyond. Companies are looking to entice early adopters to try and use their devices and services, and they're essentially relying on these users for free marketing. Early adopters show off the devices they own and convince family members and friends to try them out, often giving them as gifts and setting them up for the recipients. Amazon's Echo Dot has been the top-selling product in consecutive holiday seasons, and is a very common present from tech-forward early adopters, for example. By achieving success with early adopters, smart home companies can secure themselves the best chance at winning mindshare with the general population.

SURVEY METHODOLOGY

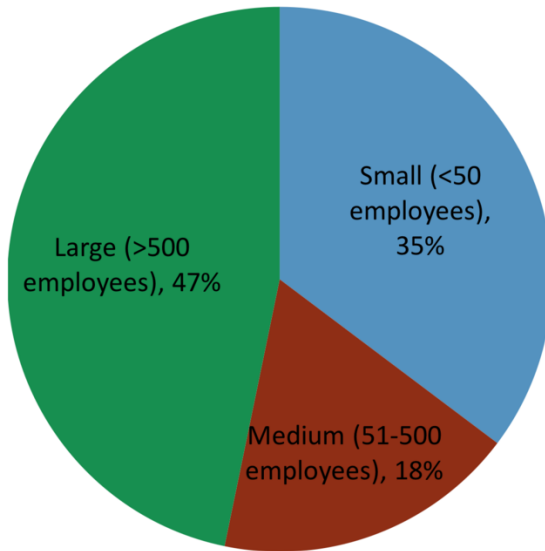
The Internet of Things 2018 Report contains the top findings and analysis from a survey of over 400 executive decision-makers from The BI Insiders Panel (BIIP) on the ways the IoT is impacting their business.

The study was fielded to global respondents from BIIP in November and December 2017. Respondents were executives who act or would act in a decision-making or advisory capacity on implementing IoT solutions at their company. They were routed to specific questions based on their responses to a qualifying question. Respondents fell into three groups:

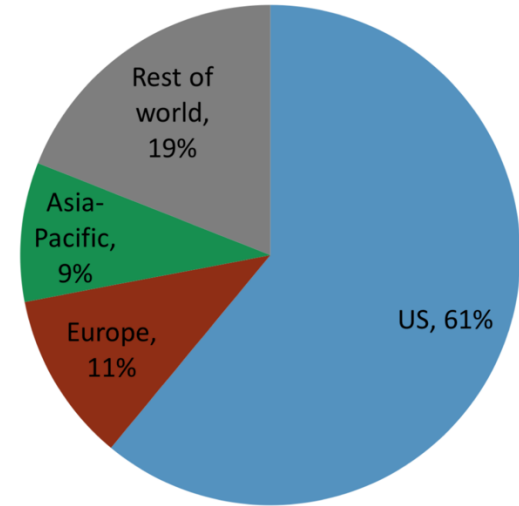
- **IoT Providers:** individuals who work at companies that manufacture IoT devices and/or provide IoT solutions to customers or clients. This block of questions focused on the various aspects of IoT solutions that companies providing them would have the most insight on, as well as the ways they interact with their customer bases.
- **IoT Users:** individuals who work at companies that have implemented some form of IoT solution. These questions focused on the details of implementing and using IoT solutions.
- **IoT Nonusers:** individuals who work at companies that have not yet incorporated any IoT solutions or technologies into their operations. Questions in this block looked into whether IoT solutions had entered into consideration, and if so, what the decision-making process looked like.

Executives taking this survey came from all sorts of companies around the world; almost half, 47%, work for larger companies with more than 500 employees, while just over a fifth identify as C-Suite executives. The distribution of respondents is slightly skewed toward the US, with 61% of respondents based there. It also includes respondents from a spectrum of industries, including but not limited to manufacturing (14%), technology (18%), and healthcare (12%).

Company Size Of Respondents



Respondents' Locations



Source: Business Insider Global IoT Executive Survey, n=424 executive decision-makers, 2017

EXCLUSIVE DATA FROM
BI INTELLIGENCE

The report also leverages insights from [BI Intelligence's 2016 Global IoT Executive Survey](#), which was conducted using a comparable sample from BIIP in September and October 2016, and included over 500 respondents from a similarly wide array of industries. Thirty-five percent of respondents to that survey came from the C-Suite, and all were responsible for, involved in, or privy to the IoT decision-making process.

About BIIP

Leveraging Business Insider's reach, with 100 million unique visitors monthly, BIIP is an exclusive online community of over 18,000 individuals, including over 9,000 executives with decision-making power from all over the world.

Designed to be a leading-edge indicator of what's next in digital, BIIP members tend to be tech-savvy early adopters at forward-thinking companies. This means that the BIIP community is an especially sensitive indicator of what's coming next for businesses around the world and what behaviors, devices, and technologies will be the winners in digital disruption.

In addition, our in-depth understanding of who BIIP members are and their habits give us great flexibility in targeting different demographics (age groups, including millennials, and income levels), employment (decision-makers at Fortune 500 companies, job level including C-suite executives, and company size), and behavior and ownership groups (including iPhone and Android users to owners of products like smart home devices and smartwatches) — allowing us to find the right group of users and potential users for every digital product, platform, or service.

While this report goes over the top findings of this study, the full study's crosstabs and data tables are only available to enterprise-access level clients. For more information or to see if your company qualifies, please reach out to Stephanie Sharabianlou at ssharabianlou@businessinsider.com.

THE BOTTOM LINE

- The IoT continues to develop as a transformative technological force that is changing how companies operate and consumers live. But, as these connected devices continue to proliferate, the IoT is increasingly moving away from the fringe and entering the mainstream.
- The IoT relies on an ecosystem that is built around any particular deployment or installation, whether that's in a home, a factory, or on a city's streets. There are five distinct components in an IoT ecosystem: hardware, a network, a remote, a platform, and security protocols.
- BI Intelligence forecasts that companies, consumers, and governments will install more than 55 billion IoT devices worldwide through 2025, while companies and consumers will spend nearly \$15 trillion on IoT devices, services, and maintenance.
- Smaller device installations continue to be the norm in the enterprise space, but larger deployments are starting to proliferate.
- The majority of companies surveyed by BI Intelligence will invest less than \$1 million in IoT implementations. However, plans for spending seem to be rising from last year.
- The IoT tools that companies are putting into place are already having tangible impacts on businesses.
- And executives at companies around the US are expecting to see the investments they've made in IoT solutions start paying dividends soon.
- In the consumer IoT market, the continuing rise of the smart speaker, as well as an increased focus on home security products, are beginning to spur growth after years of sluggish connected device uptake.
- However, the amalgamation of smart home devices into our daily lives will be driven in large part by whether companies can successfully push adoption beyond tech-savvy consumers and early adopters.

BI INTELLIGENCE

BI Intelligence, Business Insider's premium research service, provides in-depth insight, data, and analysis of everything digital. Our research is fast and nimble, reflecting the speed of change in today's business. We give you actionable insights that enable smarter and better-informed decision-making. We publish in-depth reports, news, and an exhaustive library of charts and data focusing on key areas of tech: mobile, e-commerce, digital media, payments, the Internet of Things, transportation and logistics and more.

If your organization would like to learn more about our research, including a license to republish our charts, please contact: intelligence@businessinsider.com

Copyright © 2018 Insider Inc. All Rights Reserved.

Proprietary and Confidential Property of Business Insider, Inc.

Licensed for Use by BI Intelligence Subscribers Only.

Access to and use of this proprietary and confidential information is limited by the terms and conditions.