# IS YOUR ENTERPRISE READY FOR IoT?

A practical guide for understanding the Internet of Things

INTREPID

01

What is Internet of Things? **(3-5)**

02

Why is Internet of Things Important? **(6-7)**

03

The Key to IoT: Connectivity Through Networks **(8-11)**

04

Network Protocols **(12-20)**

05

Establishing Network Protocol Standards **(21-23)**

06

How will IoT affect Our World? **(24-27)**

07

Why IoT is Important for the Enterprise? **(28-30)**

# 01

# WHAT IS
INTERNET OF THINGS?

### What is Internet of Things?

The "Internet of Things" (IoT) is the network of physical objects and devices which are embedded with software, sensors, and network connectivity to enable the collection and exchange of data.

### To Put it Simply IoT is

# MADE OF 2 MAJOR ELEMENTS:

01

**DEVICES**

Devices offer control and contain sensors which gather data

02

**NETWORKS**

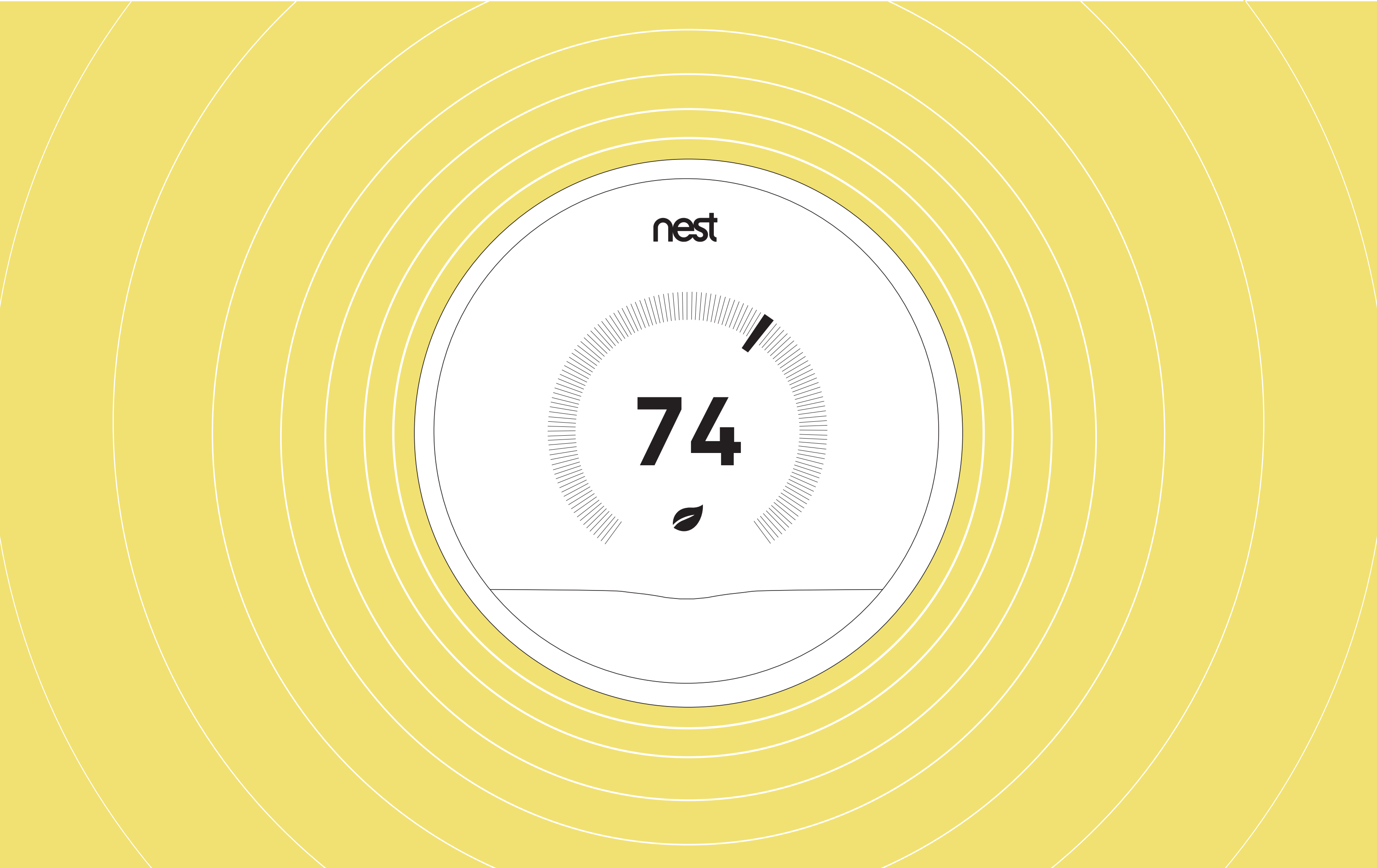
Networks facilitate communication

IoT devices can range from the familiar–smartphones and personal computers–to newer and emerging technologies, like wearables, manufacturing equipment, home automation products, smart cars, and other units of hardware that can send or receive data. In an enterprise context, IoT refers to the connected devices equipped with **embedded software** that allows for communication with a custom built application on a smartphone or computer.

Devices can read and analyze information collected by **sensors**, which can be placed within devices, objects, and machinery. Sensors detect, measure, and record information about the physical environment, such as light, heat, pressure, and motion.

Though IoT cannot exist without devices, it's **the network** that allows them to communicate and form the Internet of Things. Networks are wireless connectivity options, the most familiar and prevalent of which is **Wi-Fi**. In IoT, network connectivity can come in many forms, with major considerations being the number of devices involved, and how these devices are using information–be it simply receiving and sending data, or taking on a more active role by monitoring, analyzing, and reacting to it.

An example of a widely adopted and well-known IoT enterprise device is the **Nest thermostat**. What makes Nest an IoT device is not just the software and sensors that monitor humidity, activity and light, nor is it the built-in intelligence Nest uses to learn the user's temperature preferences and optimize the house for energy efficiency. The third and final piece is **connectivity**; Nest communicates with smartphones over Wi-Fi networks so users can control and monitor the temperature of their home from the palm of their hand.



# 02

# WHY IS THE INTERNET OF THINGS IMPORTANT?

## Why is the Internet of Things Important?

Before delving into the workings of the Internet of Things, it's important to understand the impact IoT has made.

## Billions of Connected things

IoT has already become integral in thousands of homes; prior to being bought by Google, Nest was selling 100,000 of their smart thermostat units each month. **Gartner** forecasts that by 2020, there will be **20.6 billion connected things** in the world, and we are set to hit 6.4 billion by 2016.

However, consumers may not be the ones to lead IoT adoption. A 2015 report by **Business Insider** predicts that businesses and governments will be quickest to utilize IoT, using smart, connected devices to obtain and analyze data to **improve productivity** and lower costs.

## Growing Investments

The Business Insider report also estimates about **$6 trillion** will be spent on IoT solutions over the next five years. It's a number that's not hard to believe, given that funding has already doubled since 2010, with nearly $7.5 billion already invested into IoT over the past six years according to **CB Insights**, a research and analysis company that reports on venture capital, angel investment, and emerging high-growth industries.

| Year | Amount Invested | Connected Things |
|---|---|---|
| 2016 | $7.5 billion | 6.4 billion |
| 2020 | $6 trillion | 20.6 billion |

# 03

# THE KEY TO IoT: CONNECTIVITY THROUGH NETWORKS

## What are Networks?

Networks facilitate communication and transfer information between devices, but understanding how they do so can make the workings of IoT seem complicated, partly because of the intangible nature of networks. Networks are wireless connectivity options, the most familiar and prevalent of which is **Wi-Fi**.

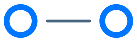
## Types of Networks

In IoT, connectivity can come in many forms, with the major considerations being the number of devices involved, and how these devices are using information–be it simply receiving and sending data, or taking on a more active role by monitoring, analyzing, and reacting to it.

there are 3 major

# NETWORK TOPOLOGIES IN IoT:

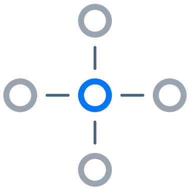
### POINT-TO-POINT



USED BY

Bluetooth SMART

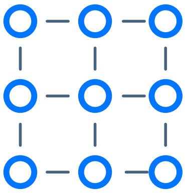
### HUB-AND-SPOKE



USED BY

Wi Fi™

### MESH NETWORK



USED BY

ZigBee

ZWAVE THREAD

## 01 Point to Point Networks

Point-to-point networks, also known as device-to-device (D2D), involve communication between two devices. These one-to-one relationships are already prevalent. A simple example would be wireless speakers that connect to a laptop; the network formed is like a **private conversation** between two people.

Unlike mesh networks, connecting one device to other devices does not extend the range of the network. A wireless mouse and a set of wireless speakers that are both connected to the same computer form independent networks–the mouse and computer have one, the speakers and computer have another.

## 02 Hub and Spoke Networks

In a hub and spoke network–also known as a "one-to-many" or "star" arrangement–a set of devices connect to a dedicated central device, or hub. **Wi-Fi** uses a hub-and-spoke setup: multiple devices can connect to a single wireless router.

Today, most **smart home automation** systems rely on a hub-and-spoke setup. Unfortunately, this means there's also a single point of failure–if the hub goes down, so too, does the entire network.

## 03 Mesh Networks

A mesh network acts like a **wireless "fog"** that connects devices within its range. There is no designated central device; instead, one device becomes the "leader." All of the devices in the network directly connect with one another, creating a web of devices that makes it easier to extend both the range and the size of the network.

Unlike point-to-point or hub-and-spoke, multiple devices in the network have the ability to relay information. By **signal hopping**, devices that would be too far apart to communicate over a point-to-point network can do so in a mesh network by using intermediate devices; the signal hops from one device to the next to reach the final destination device.

A strength of the mesh network is that the devices in a mesh network can **automatically reconfigure themselves**. If the leader device leaves the network, another can be designated as the leader. Devices can drop out of or join a mesh network without affecting the network's overall strength. So, if one device goes down, the other devices will keep the network up.

### popular examples of

## MESH NETWORK PROTCOLS IN IoT:

THREAD GROUP

ZigBee

INSTEON

ZWAVE

# 04

# NETWORK PROTOCOLS

## Network Protocols

Think of network protocols as **languages**. Some IoT products can be **multilingual**: Smartphones, for example, "speak" both Wi-Fi and Bluetooth LE.

# THERE ARE 4 MAJOR ELEMENTS

**to consider when comparing network protocols:**

### 01 Power

**Power** refers to the amount of energy that is needed for the network to perform at full functionality. A network that requires too much power can quickly drain the device batteries and render them useless.

### 02 Data Rate

The **data rate** determines the speed and amount of data that can be moved. A low data rate may not necessarily be bad; a wearable or fitness device only needs to feed a small volume of data to its smartphone companion. Data rate is intrinsically tied to power, the more data being sent, the greater the power requirements.

### 03 Range

The reach, or **range**, of a network is the extent to which devices can continue to communicate with the other parts of the network. A long range is necessary for smart home automation, as multiple rooms will need to connect to the same network to allow for communication throughout the entire home.

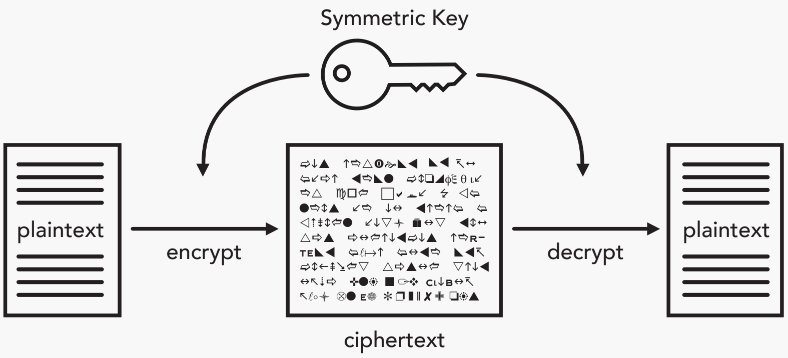
## 04 Security

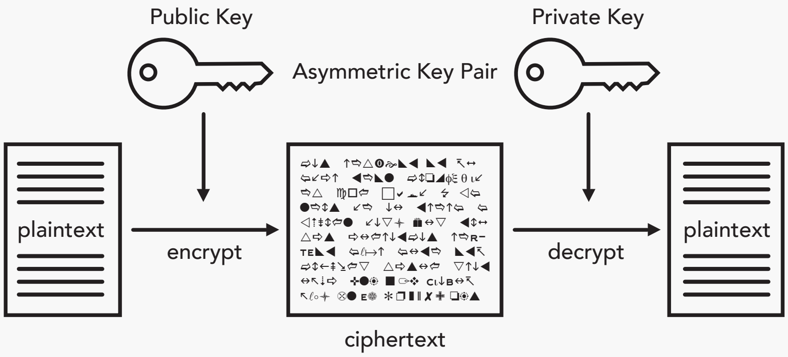
**Security** refers to the type of encryption in the protocol as well as where encryption is being implemented in the technology stack. For more reading on this, we recommend **Wireless Connectivity for the Internet of Things**.

Some protocols are encrypted at the application layer, others are encrypted at the transport layer. The important takeaway from this is that encryption at the transport layer is inherently more secure.

There is also a difference between asymmetric versus symmetric key encryption. The diagram below shows the difference between the two. Imagine a lockbox with a message inside, versus a lockbox with an encoded message inside–if intercepted, the latter will be more secure, as it has an additional layer of protection. The major takeaway is that asymmetric encryption is more secure.

Wi-Fi is an example of a symmetric key, while Thread is an example of asymmetric encryption. This report will explore more about specific network protocols below.





# Wi-Fi

While Wi-Fi is the most **ubiquitous** of the network protocols, it is **power-intensive** and can quickly drain device batteries. The wireless router acts as the hub for a hub-and-spoke network setup, meaning Wi-Fi can boast a high bandwidth, supporting **fast data rates** and a direct connection to the Internet.

Although a wireless router means there is no need to buy an additional hub, the current Wi-Fi network has yet to find its place in home automation. Without a dedicated power source or long-lasting battery, and because signals can drop when faced with physical obstacles like walls and floors, Wi-Fi is not well suited for the smart products and sensors spread throughout a home.

However, in the coming years Wi-Fi will release an updated network, **Wi-Fi HaLow**, which will double in speed and, as a lower-power network, will be able to work both within and beyond the home.

| Power: | Data Rate: | Range: | Security: |
|---|---|---|---|
| High | 11 to 300 Mbits/s | 10 to 100 meters | Medium |

# Bluetooth LE

**Bluetooth LE** (also known as **Bluetooth Smart** or BLE) is a secure, reliable technology for short-range communication. BLE uses **frequency hopping** and encryption to ensure a safe, secure connection for users.

Its strengths are in its **pervasiveness** (most mobile devices have Bluetooth LE capabilities) and its single **device-to-device** connectivity. In other words, BLE's limited range means it's better suited for smart products like wearables and fitness devices, which can be used and kept in close proximity to a smartphone.

In the world of home automation, BLE is essentially a **one-room network**–separate BLE-connected devices by a wall and the connection is lost. However, this will soon change, as **recent announcements** detail plans to update BLE by extending its range by implementing mesh networking.

| Power: | Data Rate: | Range: | Security: |
|---|---|---|---|
| Low | 1 Mbits/s | 50 meters | Low |

# Thread

Thread is a new wireless network standard designed for the home and connected products. It's a secure, and scalable means of connecting IoT products.

Thread is similar to Blutooth LE, in that it sends small amounts of data and is **low-power**. But, while BLE thrives at device-to-device connections, Thread is a **mesh** network, so not only can the range of the network be easily extended to accommodate devices across a large zone, but it can also support over 250 devices per network. Other advantages of the mesh network include the concept of a self-healing network, where if one device is dropped from the network, it can be reinstated without user interaction.

Although Thread doesn't have as large of an installed base as BLE, its **interoperability** means it works with other existing network protocols, like ZigBee. Its ability to support multiple popular application layer protocols and platforms makes integration simple.

Thread is also considered a highly secure protocol. Users must authorize any Thread-enabled devices before they are allowed on their home networks. To communicate with each other, the devices must recognize each other's MAC addresses, making it difficult for unauthorized devices to access the network. Device-to-device Communications are encrypted with DTLS (Datagram Transport Layer Security), an encryption protocol designed to prevent tampering and message forgery.

| Power: | Data Rate: | Range: | Security: |
|---|---|---|---|
| Low | 90 kbit/s (app layer) to 250 kbit/s (physical layer) | Up to 300 meters | High(er) |

# Zigbee

Because it is a low-powered, wireless mesh network that has been around for a many years, ZigBee has been a popular choice for smart home automation. Perhaps the most well-known IoT product that uses the ZigBee network is the **Philips' Hue** lighting system.

ZigBee products communicate on the same frequency band as Wi-Fi and Bluetooth, which has caused issues with **interference**.

| **Power:** | **Data Rate:** | **Range:** | **Security:** |
|---|---|---|---|
| Very Low | 90 kbit/s (app layer) to 250 kbit/s (physical layer) | 10 to 300 meters | Low |

# Z-Wave

Similar to ZigBee, Z-Wave is a recognized name when it comes to home automation, with big-name brands like **Honeywell** using the Z-Wave network protocol for their home security systems, thermostats, and lighting.

Because it is a mesh network, Z-Wave's range is comparable to Thread's and Zigbee's, but its weakness is in its low data rates, which are much slower than Thread, ZigBee, and Wi-Fi. Z-Wave operates on a radio frequency, meaning it is less likely to suffer from interference from Wi-Fi and Bluetooth systems that share ZigBee's frequency band. Unfortunately, it also means that Z-Wave hardware is country-specific, as countries use different radio frequencies.

| Power: | Data Rate: | Range: | Security: |
|---|---|---|---|
| Low | 40 kbit/s | 30 meters | Medium |

## Networks Differences Disappearing with Time

Today's network protocols present varying strengths and weaknesses. So which network protocol provides the best package and will become the leading industry standard? Unfortunately, those answers are still not clear.

**Q** **So which network protocol provides the best package and will become the leading industry standard?**

**A** **Unfortunately, those answers are still not clear.**

Companies like **GE** have adopted multiple network protocols, putting out separate sets of smart, connected lighting systems–one compatible with Zigbee, another with Z-Wave, and yet another with Bluetooth. In fact, for home automation technology research company **Forrester** has gone as far as to predict that **no one company will dominate** a unified smart home market.

While no single network protocol stands out as the best option, it's important to keep in mind that the differences between the protocols are quickly dissolving. As each protocol works to improve its technology to match the specifications of its fellow networks, it will become more difficult to distinguish them. Two major players, Bluetooth LE and Wi-Fi, have already announced plans on improvements of their weaknesses, in range and power respectively, in the coming years.

# 05

# ESTABLISHING NETWORK PROTOCOL STANDARDS

There are currently no agreed-upon industry standards or official network protocol governing bodies. Instead, groups have formed to create standards around their corresponding network protocol technology.

These groups have similar missions: promote their corresponding network protocol, provide certification for approved products, and push for innovation and improvements.

# GROUPS & ALLIANCES:

### Wi-Fi Alliance

The Wi-Fi Alliance is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability. There are currently about 600 Wi-Fi Alliance member companies.

### Bluetooth Special Interest Group

The Bluetooth Special Interest Group (SIG) does not make or sell Bluetooth-enabled products, but companies who use Bluetooth technology in their products must become a member of SIG. It's a non-profit responsible for developing Bluetooth standards, protecting Bluetooth trademarks and evangelizing the technology.

### The Thread Group

The Thread Group is a consortium of companies with over 220 members, including Nest, Samsung, and Silicon Labs, who use the Thread technology to fundamentally simplify the connected home.

### ZigBee Alliance

The non-profit behind ZigBee standards, ZigBee Alliance works to provide open, low-power networking standards, with a focus on monitoring, control, and sensor applications.

### Z-Wave Alliance

The Z-Wave Alliance is made up of over 375 companies. Its focus is on the smart home automation space, working to solidify Z-Wave as the standard for wireless home products.

### Collaboration and Interoperability

Although the IoT industry is fragmented, there have been efforts to improve interoperability to ensure communication between products that use different network protocols.

Most recently, Zigbee and Thread announced a collaboration that will allow ZigBee-based products to use the Thread protocol, as well as a certification program that will ensure interoperability between the two.

# 06

# HOW WILL IoT AFFECT OUR WORLD?

With IoT, consumers will no longer simply be sold physical goods, but instead, a combination package of product and service. Using data, businesses will be able to anticipate and react to product failures and improve efficiency.

the Internet of Things affords us

# 5 MAJOR CAPABILITIES:

## 01 Monitoring

The Internet of Things will promote the monitoring of products, and provide the ability to report failures and malfunctions more rapidly–be it a smart carbon monoxide detector, or a sensor for tracking storage conditions for produce to ensure food safety at grocery stores.

Perhaps the industry most affected by IoT will be the medical sector, where resources can be freed up by using a series of sensors instead of human personnel to monitor patients. More importantly, patients' health status can be monitored beyond the walls of medical institutions, encouraging preventive care.

## 02 Control

Smartphones will become remotes for controlling conditions and environments. The role of control is most evident in home automation, where IoT gives consumers control over everything from lights to locks to coffee machines. Homeowners can administer routines and schedules for IoT devices to follow to provide them with greater comfort.

Beyond the home, the control aspect of IoT has considerable potential for the sciences, where stable lab conditions can be essential for securing accurate readings and test settings for experiments.

## 03 Optimization & Speed

Some IoT devices are equipped with the software to act as self-learning machines and are able to adapt to the information they gather. These built-in analytics, algorithms, and triggers will work to provide automatic adjustments and improve efficiency.

Private companies have already begun to take advantage of IoT-equipped factories and production lines, but the potential for governments is equally promising. With frequent updates on the state of buildings, bridges, and roadways, governments can improve and repair infrastructure as needed, and identify problems as they arise.

Increasing network speeds may also create greater optimization. The release of 5G cellular technologies promise greater connection speeds and lower latency for connecting to IoT devices.

## 04 Autonomy

The iRobot Roomba is an example of how a connected device can operate on its own: using sensors it’s able to know when to clean floors and can react to different layouts. IoT products like Roomba, self-driving cars, and self-run factories will also provide us with new freedoms.

## 05 Security and Privacy

As devices in the home and elsewhere become more ubiquitous, security and privacy issues become more prevalent and pressing. Concerns about unknown third parties accessing IoT devices and eavesdropping are common, and IoT solutions need to be able to prevent this type of scenario.

Further issues arise around the user's privacy. As data is collected from the multiplicity of devices, questions about who owns that data and what can be done with it are a hot topic both amongst businesses and governments, as regulations surrounding these issues do not yet exist.

Lastly, the concept of ownership does not extend only to data, but also the hardware and infrastructure. In a smart home, if the owner decides to sell, they must be able to hand over credentials to a new owner. Questions about what to do if one user is on Apple products but another is on Android or Windows products creates a barrier that will need to be addressed. Many companies are racing to have their devices serve as the "hub" for all home automation, supporting every available protocol and product.

# 07

# WHY IS IoT IMPORTANT FOR THE ENTERPRISE?

# IN SUMMARY,

there are several identifiable trends in the IoT space:

## 01 Fast Growth Potential

An important predictor of any sector is previous growth, as well as forecasted growth based on investment. Between Gartner's 20.6 billion things prediction, as well as the significant investments made by enterprises, venture capitalists, and startups alike, the IoT space is certain to see exponential growth in the coming years.

## 02 Emerging Technologies, Merging Protocols

In the coming years, new IoT devices and sensors will be developed, but by the same token, protocols will begin to unify and standards will emerge naturally. Knowing and understanding these technologies in both their current state as well as their potential is important for creating future-proof products.

## 03 Consumer Adoption in the Home Automation Space

The lack of a standard for home automation means consumers more often purchase specific solutions–a Nest thermostat, Sonos speakers, Philips Hue light bulbs–building their smart homes product by product rather than using one cohesive system. At the same time, products that unify these disparate systems (such as the Amazon Echo) are becoming a hot trend among leading technology companies.

## 04 Adoption in B2B and Government

Predictions by Business Insider show that governments and businesses are leading the charge in IoT adoption, which will improve the infrastructure available for consumer adopters later on.

**The result of these trends is that now is a critical time for enterprises to make investments in IoT technologies, and to begin to develop their capabilities around connected devices from a technological and design perspective—not doing so means risking being left behind in terms of both market share and mindshare.**

By dedicating time to research and learn about emerging technologies within and beyond their industry, as well as actively exploring the potential of IoT products enterprises can strategically position themselves for success.

Most importantly, an enterprise will employ tactics beyond knowledge and understanding of appropriate technologies for their industry—it will invest in connected devices and building IoT-compatible applications.

617.949.0533 // inquiries@intrepid.io // intrepid.io