Demystifying IoT Cybersecurity

The Internet of Things introduces new vulnerabilities across the entire ecosystem. Here's what you need to know—and prepare for.

IOT **CYBERSECURITY** ALLIANCE

The Internet of Things (IoT) is becoming ubiquitous as new—and old—devices plug into a variety of networks. From smart coffeemakers in the kitchen to sensors embedded in 20-year-old motors on the factory floor, the IoT is expanding rapidly and relentlessly, as organizations attempt to capture new efficiencies or gain new insights from newly connected devices.

Across smart cities, homes, and vehicles, in industries ranging from healthcare to manufacturing, billions of IoT devices are in the field today and billions more are expected to come online in the next few years. Gartner predicts that more than 20 billion connected devices will be in operation by 2020, rising from 8.4 billion in 2017[1]. Technology research firm IDC predicts global IoT spending will total nearly $1.4 trillion by 2021[2].

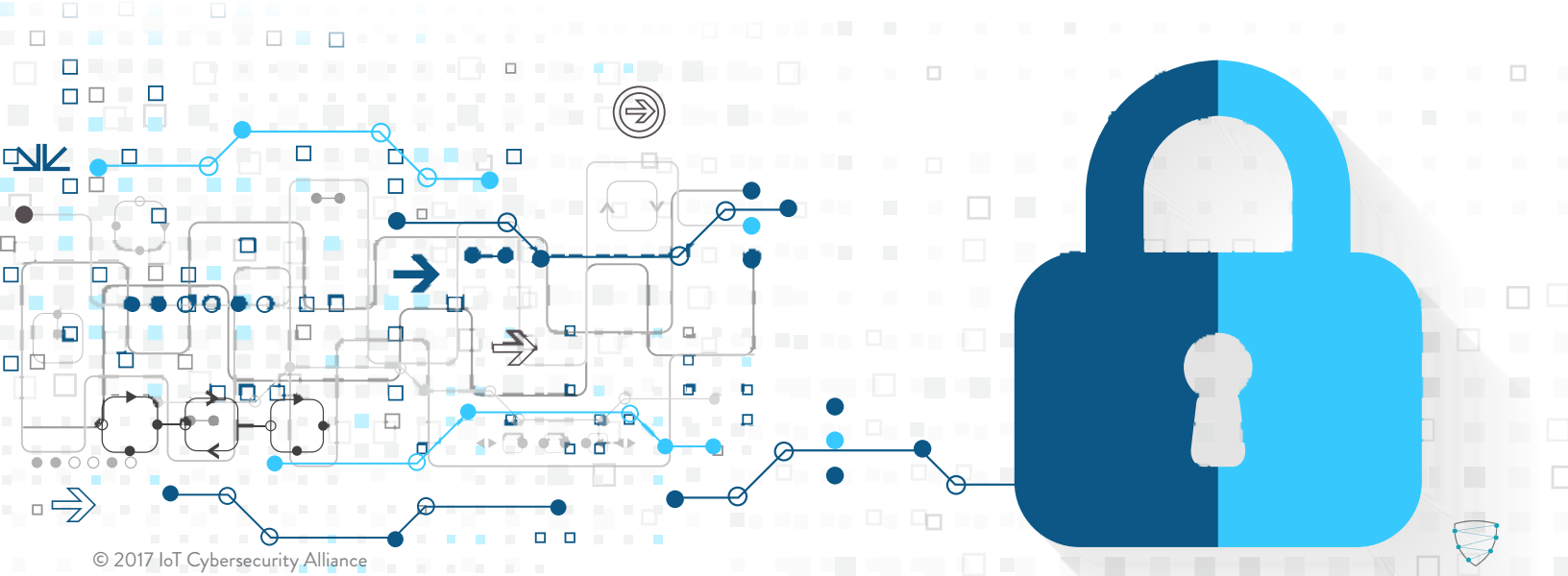
But as the IoT opens new windows of opportunity for businesses, it also introduces new types of risk. Many IoT devices may not have been designed with security in mind. Some lack the onboard processing power or memory to provide robust security controls. As more IoT devices are produced, the attack surface and potential vulnerabilities will evolve and expand, quickly outpacing current methods to defend against them.

There is no magic bullet, no single solution that will secure the IoT at every level and every touchpoint. It's natural to focus on the "things" when formulating an IoT security approach, but the scope needs to be much broader. The only sustainable approach involves a multi-layer, end-to-end framework that takes into account all connected devices, along with the applications they run and the networks they use to transmit information. The framework should be built on emerging best practices but is unique to each business, just as every IoT deployment is unique.

In this white paper, we will examine the growing complexity of IoT cybersecurity and the challenges that IoT architects and implementers must consider when deploying and managing IoT devices and services. The stakes are high: As with other aspects of IT transformation, IoT initiatives are likely to extend well beyond IT functions to touch many aspects of the business, from the supply chain to the point of sale. Even an organization that is not developing or deploying its own IoT products or services can be vulnerable, as recent IoT-based botnet attacks have demonstrated[3]. It's imperative, therefore, for IoT security to be top of mind for every organization.

Defining the Threat

Most people think of the IoT threat along traditional lines: Attackers compromise a vulnerable device to gain unauthorized access to systems and steal data. But in reality, the risk is much broader:



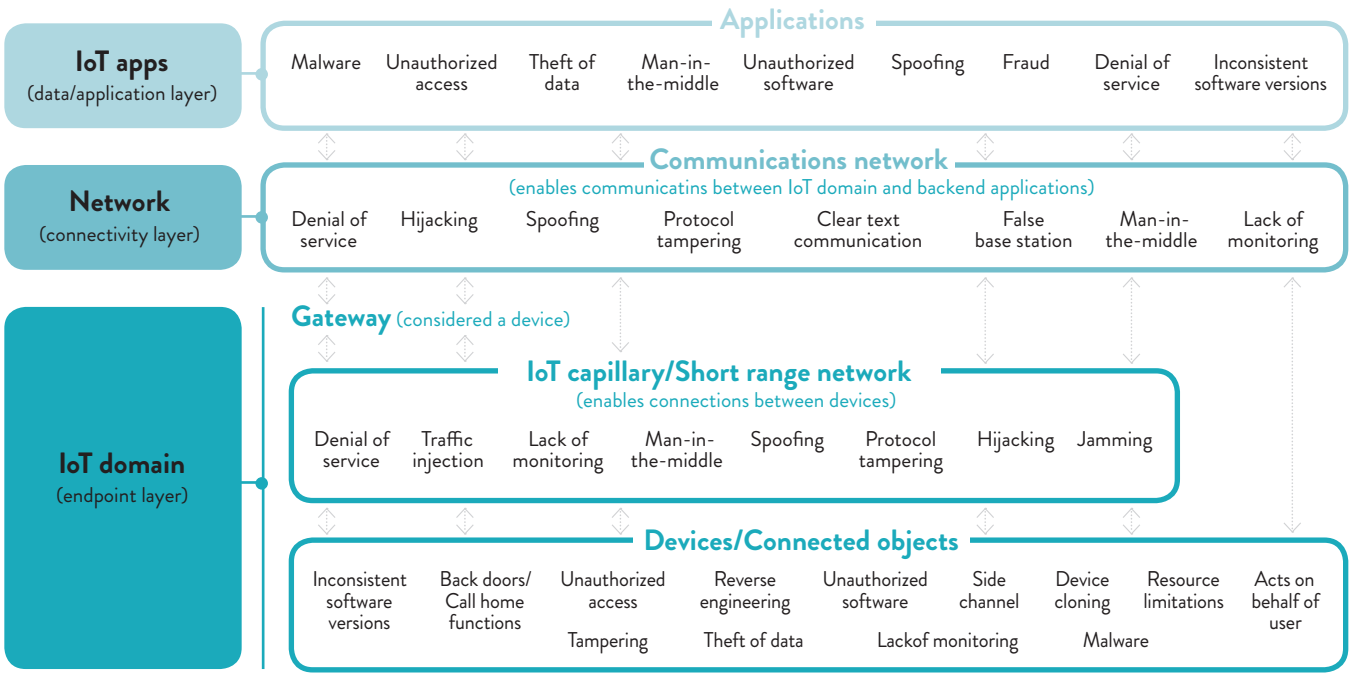


Figure 1: IoT Ecosystem Security Considerations

The IoT expands the attack surface for many common cyberthreats, ranging from malware to man-in-the-middle attacks, across a much broader ecosystem of connected devices.

- Devices can be subverted into performing incorrect actions or sending inaccurate data. When the device in question is a vehicle or a power plant, such activity can potentially threaten human safety.
- Connected devices may be a threat to a network if vulnerabilities along the IoT ecosystem are not adequately addressed. Attackers can turn thousands of compromised devices into a botnet used for massive Distributed Denial of Service (DDoS) attacks that can take down websites and interrupt business operations. The 2016 Mirai botnet is a prime example of the disruptive nature of these attacks[4].
- Mirai and similar malware also demonstrate how IoT risk extends beyond your own organization. If your connected devices are used as part of a greater attack on other entities, you could be subject to reputational or financial damage[5]. Or, in turn, your organization could be victimized by a compromised IoT device from a business partner.

Beyond the devices themselves, IoT deployments can introduce risk across the entire ecosystem, via multiple threat vectors [Figure 1].

Where the IoT truly differs from typical cybersecurity threats, however, is in the physical world. As criminals and nation-states look to compromise power grids, for example, the human safety factor adds a chilling new dimension to the threat.

The Complexity of IoT Cybersecurity

The nature and diversity of threats underscores the complexity of attempting to secure the IoT. Challenges extend across three main components of the IoT ecosystem: endpoint/gateway devices, the network/connectivity layer, and data and applications. [Figure 2]

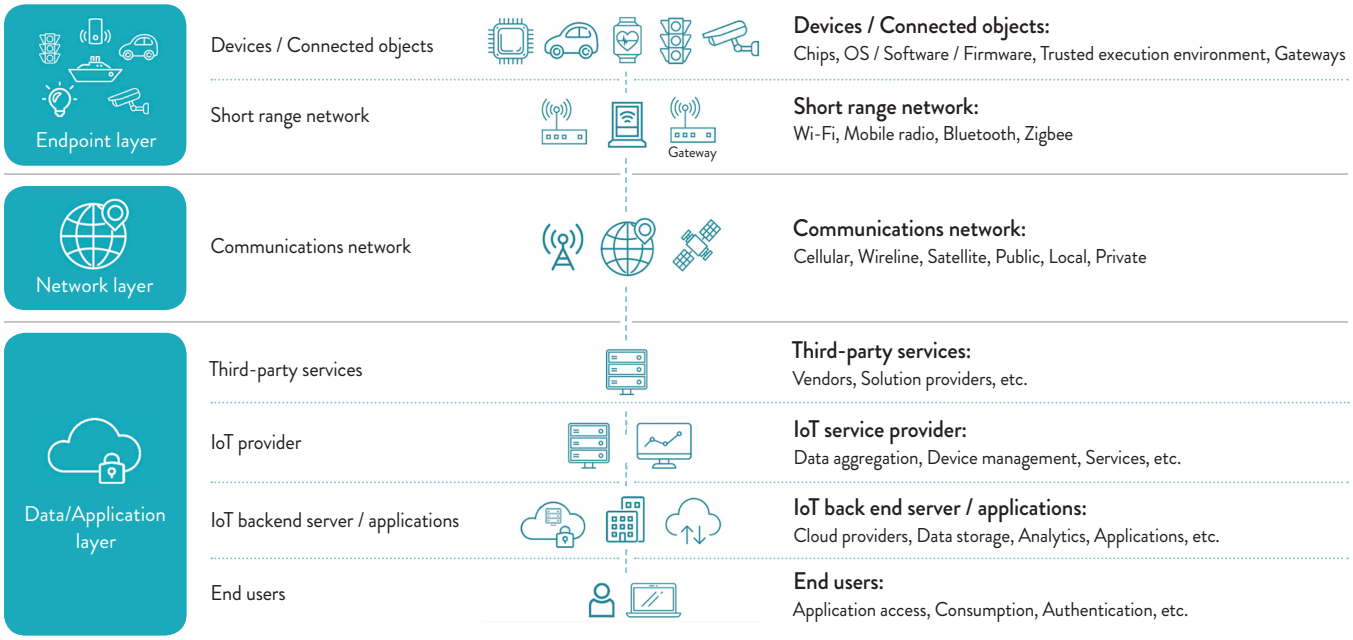


Figure 2: Risk Assessment Across the IoT Value Chain

Organizations will need to assess risk across the entire IoT ecosystem, from end-user applications to physical endpoints that extend well beyond the traditional network perimeter.

Defining an IoT 'Device'

We define an IoT device as any networked "thing" that can generate, store, and send data, or act on remote commands. We exclude general-purpose devices such as smartphones and PCs. Common examples include:

- ***industrial controls such as temperature and RPM sensors***
- ***security cameras***
- ***traffic lights***
- ***point-of-sale terminals***
- ***medical devices (insulin pumps, MRI machines)***
- ***connected vehicles (including infotainment systems, telematics, and navigation systems)***
- ***smart appliances/home automation systems***
- ***ATM machines***
- ***personal fitness bands***

This list is representative of existing IoT devices. With the IoT still in its relative infancy, many types of devices and use cases are yet unknown.

Endpoint/Gateway Devices

Some IoT devices on the market today may be inherently insecure if they have been designed and manufactured with application and cost in mind, not security. Some devices may lack the power or memory capacity to support anti-virus software or encryption. Some may lack basic security features such as secure boot and cryptographic functions. A single organization may have hundreds of these devices operating at any time, with some purpose-built devices—which are dedicated to a single task, such as measuring temperature or moisture—connecting to the network sporadically. In addition, many endpoint devices connect to the network via a gateway serving as an intermediary. The variety and volume of these devices add more complexity to an organization's security posture.

Consider a smart TV installed in a conference room. Once compromised, that TV could be used to listen in on and view any meetings taking place—a scenario fraught with potential business implications.

Devices exist in all manner of IoT deployments that are interwoven with sensors, from smart buildings and bridge decks to farmers' fields and the lights hanging over factory floors. These sensors can be infected with malware and their data streams corrupted. Because these devices often have limited resources, they may not support mechanisms such as authentication, integrity, or encryption to securely communicate to remote systems.

Other devices, such as closed-circuit television cameras, were designed to be networked, but not necessarily connected to the internet or controlled with rich interfaces like a webpage or a smartphone. Some of these cameras were built with permanently open ports to "listen" for updates and have hard-coded and easily guessed passwords built in at multiple layers, rendering the entire device insecure.

This is how the Mirai botnet took hold. It continuously scanned the Internet, looking for devices with known and often hard-coded user name/password combinations. Once identified, it then took over each device by signing in as an administrator and putting it to work on the biggest DDoS attack in history.[6]

Managed vs. unmanaged devices

Managed devices include software agents that allow them to be monitored, so network administrators can do updates, resets, reboots, or even turn off the device. Managed devices are inherently more secure than unmanaged devices, which may not have the capability to be managed—or even easily identified—on the network. Unmanaged devices may run a variety of real-time or open source operating systems, oftentimes with inconsistent security services and capabilities, which present different threat thresholds. They may use a mix of wireless transports, ranging from Wi-Fi to low-power WAN protocols such as LoRa.

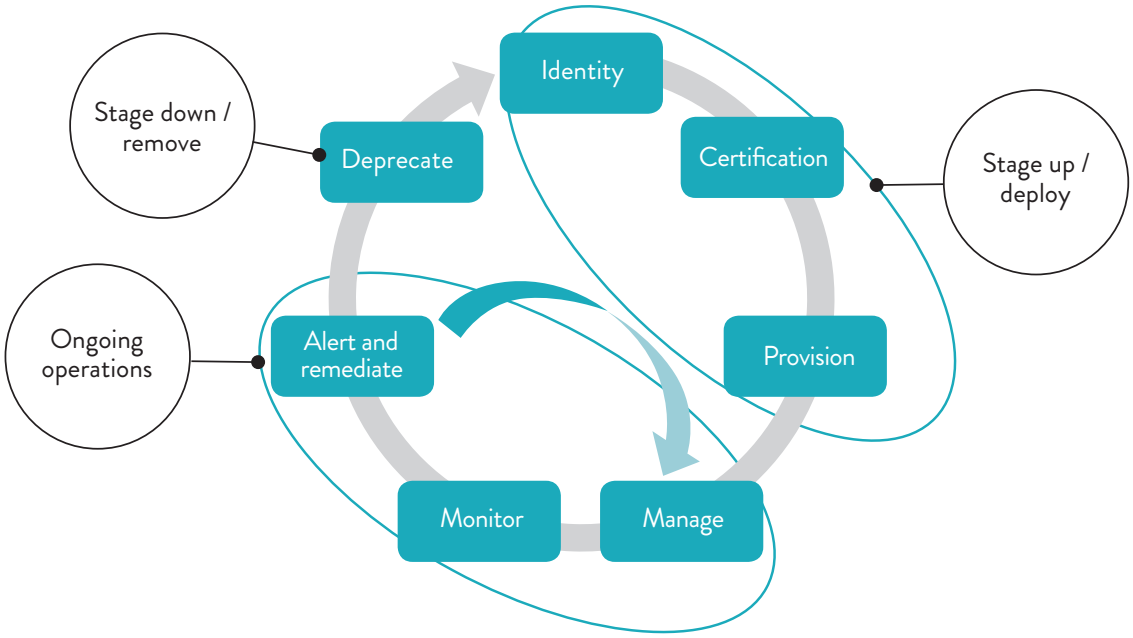


Figure 3: Managed Devices: End-To-End Lifecycle Management

The ability to identify, monitor, manage, and remediate devices is critical to help reduce risk as IoT deployments scale.

Identifying and securing this influx of newly connected yet unmanaged devices will become increasingly difficult. Consider a smart TV installed in a conference room. Once compromised, that TV could be used to listen in on and view any meetings taking place—a scenario fraught with potential business implications.

Complex lifecycle management

IoT devices often have long lifespans. Unlike PCs, smartphones, and laptops, which organizations generally upgrade every few years, IoT devices—especially in industrial environments—can last up to 20 years on a single battery.

The embedded nature of many IoT devices can make them inherently difficult to upgrade. The security posture of many of these devices can degrade over time as new exploits are uncovered and manufacturers discontinue support or go out of business. Because these devices are literally out of sight, owner/operators may develop a "set and forget" mindset and not actively manage, update, or upgrade them. For hackers, these outdated or forgotten devices are tempting targets.

IoT deployments in an organization, therefore, require end-to-end lifecycle management, including frequent inventorying, for any and all connected devices. [Figure 3].

As IoT devices evolve, their processing power and functionality will increase, so security capabilities must keep pace. As security teams take steps to secure devices today, they must also consider future platforms and computing paradigms to efficiently plan security for the future.

Emerging standards

Given the breadth of IoT use cases, many potential standards are likely to emerge. This is not a new problem in technology, but when applied to thousands of IoT product manufacturers, coupled with the long lifecycle and varying security capabilities of these devices, and the relative immaturity of the market, the challenge of potentially divergent or conflicting standards becomes exponentially more complex.

Also, the IoT marketplace itself is fragmented, with smaller device makers building on open standards, proprietary or industry-specific application stacks, or not using standards

at all. This creates multiple threat levels, from the firmware to the operating system. For example, many proprietary, open source, or real-time operating systems are in use, and many watered-down versions of Linux and Unix don't support security or firmware updates. Open source software and protocol stacks, such as OpenSSL, can become vulnerable over time if they are not regularly patched.

Operators may develop a "set and forget" mindset with some IoT devices and not actively manage, update, or upgrade them.

Network/Connectivity Layer

The connectivity layer within the IoT ecosystem cuts across global wireless, wireline, and satellite networks, as well as public, local, and private networks. The variety and volume of devices increases the complexity of security at this layer, as IoT "things" change the concept of the network perimeter. Whereas once communications beyond the network were secured via VPN, the IoT forces security teams to account for corporate assets in both friendly (private) and hostile (public) environments.

The many competing converging IoT communications protocols further complicate the issue. Some are new. Some have been in place for 20 years. Not all IoT communication is IP-based, and not all communication protocols have inherent security. The challenge is understanding where the holes are in these different protocols and how to plug them. Just as early versions of Bluetooth were not highly secure, security teams must vet an even broader set of short- and long-range IoT communication/networking protocols, including ZigBee, Thread, LoRa, and 6LoWPAN. Understanding the security limitations of each becomes an even bigger challenge as non-IP IoT devices connect to a bridge device or edge gateway in order to connect to the TCP/IP backbone. Controlling local access to the IoT, therefore, must be accounted for as part of an IoT security strategy.

One approach is to segment IoT devices from sensitive portions of your network, whenever possible. There's no need for the smart coffeemaker in the breakroom to access the corporate network that houses customer data. Consider a traditional "security through obscurity" approach by using appropriate IP addressing schema to segment as many IoT devices as you can.

Encryption in transit

Authenticating and encrypting data as it traverses the network is another key step in protecting against unauthorized access. For devices that cannot encrypt their own data, a network that uses advanced encryption can safely transport traffic from a compromised device. One option is to decouple encrypted transport from device encryption, using the TLS (Transport Layer Security) protocol that is commonly used for file transfers, VPN connections, and web applications.

Just as you need to think about endpoint security as you're building, purchasing, or deploying IoT devices, you need to think about highly secure connectivity as you're shopping for a network service provider. Some older networks still being utilized, such as 2G, use less robust encryption algorithms or authentication schemes, and low-priced network services may not offer advanced encryption or segmentation. Consider these factors as part of your due diligence.

Applications and Data

Securing workloads and applications is a critical component of any IoT deployment. Web, cloud, and mobile applications are frequent targets for hackers looking to infiltrate corporate networks. The IoT could amplify these attack surfaces if organizations field devices with outdated operating systems, unsupported proprietary software, or poorly configured or non-existent authentication protocols. Purpose-built devices and the applications they run may not be manageable using traditional IT tools and processes.

The implications of a broader attack surface on data security, privacy, and compliance are significant. Data no longer lives in a traditional data center. IoT devices beyond the network perimeter are generating mountains of data that IT teams must manage, secure, and maintain, both in transit and at rest. Securing data that IoT devices generate, store, share locally, or transmit across public or private networks becomes exponentially complicated in a world of connected cars, medical devices, and factory equipment.

Data privacy, perhaps more than any other issue, may define the direction and growth of IoT as device proliferation expands the spectrum of privacy concerns. Security and legal teams will need to revisit privacy and compliance policies to account for increasingly sensitive personal or behavioral data that can be used to identify or monitor individuals. Insulin pump data alone may not be sensitive, but if coupled with a patient's personally identifiable information (PII), the story changes. IoT lifecycle management will require clear guidelines on what information is collected, where it's stored, how it's used, and how long it's kept.

6 Hard Truths About IoT Security

- ***IoT operates at a scale far beyond traditional operational and information technology***
- ***IoT devices can operate in easily accessible environments***
- ***Some IoT devices are embedded in products or systems, making them inaccessible and difficult to maintain***
- ***Data accumulates over time, amplifying exposure and risks***
- ***Weak configurations will persist***
- ***The IoT threat landscape is constantly shifting and diversifying***

Organizations will also need to revisit policies for notifying customers about how their personal data is collected and used. Many IoT devices lack traditional interfaces for communicating privacy information to end users. For example, the manufacturer of a connected thermostat may not have direct contact information for the device's owner. With multiple participants in an IoT ecosystem, liability also becomes an issue, should a breach occur. Who owns the data generated by a vehicle's infotainment systems? And who's responsible if that data is breached?

About the IoT Cybersecurity Alliance

Our mission in creating the IoT Cybersecurity Alliance is to forge a community where industry-leading cybersecurity and IoT experts come together with the intent of demystifying IoT security, collaborating to address real-world IoT security challenges, fostering a security-first IoT posture, and providing educational tools to share best practices and thought leadership.

Creating a Multi-Layered Defense

As we stated in the introduction to this paper, there is no one-size-fits-all solution to address these challenges. Successful IoT deployments require multi-layered, end-to-end security that ranges from baked-in security requirements up front to the ongoing management and protection of sensitive machine-generated data.

The following best practices are critical to any end-to-end strategy:

- Build and/or choose IoT devices with HW based security that provides a strong set of security features including secure boot, secure update mechanisms, tamper proof device identifiers, and cryptogrographic support to protect data at rest and in motion.
- Segment data according to need in a highly secure manner; not every IoT device operating in an organization must be connected to the corporate network.
- Employ authentication, such as certificates, to see to it that only approved devices are allowed onto the network.
- Enable and protect device identity, access, and authorization to increase visibility of IoT endpoints as well as your ability to track, monitor, and manage IoT devices.
- Choose devices that utilize Trusted Execution Environments (TEEs) to enable hardware security, harden data protection, protect Roots of Trust (RoT) and device identity, and isolate sensitive code.
- Deploy comprehensive device management and provide prompt device and application updates.
- Align your IoT ecosystem with internal security policy, best practices, and industry regulations.
- Select network providers (mobile/fixed) that can provide an enhanced security posture including traffic and automated threat analysis to help protect connected IoT devices and help prevent targeted IoT attacks.
- Use specific security solutions to help protect data and applications in the cloud, on premises, or in the network, including:
  - ~ Firewalls with application-layer visibility and controls
  - ~ IoT application whitelisting
  - ~ Intrusion detection/prevention
  - ~ Data loss prevention
  - ~ Vulnerability scanning
  - ~ Web security
  - ~ Malware scanning/automated malware defense
  - ~ Endpoint security solutions
- Build a unified threat platform to monitor assets, centralize and analyze IoT data, and detect and respond to threats.
- Work with a trusted advisor to procure devices and solutions to harden IoT deployments.

By focusing on these cornerstones of IoT security, the challenges won't become any less complex—but they will be more manageable.

Future papers will focus on these best practices, risk management, and the specific steps organizations can take to more securely build and manage IoT deployments.

For more on this topic, visit www.iotca.org.

1. Gartner press release, February 2017, http://www.gartner.com/newsroom/id/3598917
2. IDC press release, June 2017, http://www.idc.com/getdoc.jsp?containerId=prUS42799917
3. Wired, October 2016, https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn
4. PC World, October 2016, http://www.pcworld.com/article/3135273/security/fridays-ddos-attack-came-from-100000-infected-devices.html
5. Money Morning, August 2015, https://www.moneymorning.com.au/20150808/how-three-hackers-managed-to-shift-the-stock-price-of-three-multi-billion-dollar-companies.html
6. Wired, December 2016, https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

IOT **CYBERSECURITY** ALLIANCE