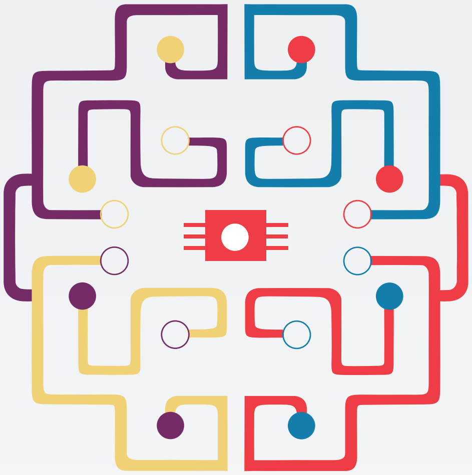
perspective on the opportunity to design security solutions from inception to deployment

Security for the Internet of Things



The Internet of Things is a global technological opportunity of unprecedented proportions. The interconnectedness of devices, networks and people will facilitate the delivery of transformative products and services, as well as greater cost savings, productivity, and safety. This increased connectivity, however, also exposes new security threats.

In this paper, we address the core opportunities and security issues the IoT presents, as well as a process to help organizations and Original Equipment Manufacturers (OEMs) think about how to design and develop secure, effective solutions.

Smart
Systems
Design

Harbor
Research

How should organizations approach security for the Internet of Things?

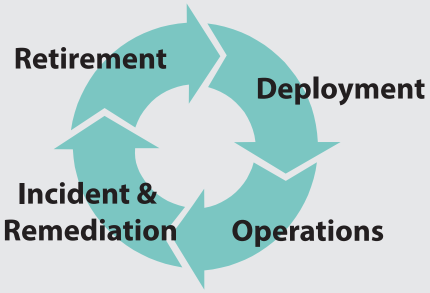
Step 1:
Address Security Impact in the Customer Environment

Where will the solution be?
What will it do?
Who will it report to?
How will it be secured?

Step 2:
Apply a Multi-Faceted Security Approach

- Identity
- Access Management
- Encryption
- Analytics
- Network Security

Step 3:
Define Lifecycle Controls



With a little help from:

Intelligent Gateways

For customers with existing equipment and systems, gateways can help apply encryption, perform analytics, provide hardware-level security, and bring device management closer to the edge and the devices themselves, even in harsh and remote environments

Partners

Partners with security expertise can provide the supplemental products and knowledge that speed up IoT solution development in a competitive and ever-changing marketplace

Harbor Research: Security for the Internet of Things, 2016.

ORGANIZATIONS ARE CONNECTING DIVERSE DEVICES TO THE INTERNET

Table of Contents

Greater Complexity Leads to Greater Security Risk

The Internet of Things (IoT) will drive exponential growth of connected devices and equipment. Modern sensors, decades-old equipment, and a collection of gateways, controllers, routers and databases—all communicating over a jumble of protocols—create a mixed environment of data and interactions that have the potential to provide significant benefits to suppliers and customers. But these useful interactions will also provide potential new attack points for malicious entities. Each organization engaged in architecting and deploying IoT solutions must understand these risks and incorporate privacy and security measures into their solutions to meet customers' security requirements and successfully drive adoption. This paper addresses critical security challenges, opportunities, and dynamics of the current market landscape and provides readers with clear steps to approach security for the IoT.

The IoT can introduce privacy and safety issues, including, but not limited to, the following scenarios.

- » **From digital control to physical threats:** The IoT exposes users to new physical threat vectors. Control systems, vehicles and even the human body can be accessed and manipulated if not properly secured, causing injury or worse through unauthorized access to physical sensing, actuation and control systems, implanted medical devices and other cyber-physical implementations of the IoT. Intruders can also gain physical access to homes or commercial businesses through attacks against electronic, remote-controlled door lock mechanisms. Safety information such as warnings of a broken gas line can go unnoticed through denial-of-service attacks on IoT sensor information, or critical infrastructure damage can occur through override of safety features, power supply or temperature regulation functions.

- » **Use of location data to track and disrupt:** Unauthorized tracking of behaviors and activities can occur through examination of location-based sensing data. The exploitation of information about high occupancy levels or the location of valuable or volatile products can lead to anything from supply chain disruption to a terrorist attack. These risk factors, plus a growing body of compliance regulations worldwide, make organizations more sensitive to the potential damage of personal and large-scale data breaches that may put buildings, energy production sites, or other critical infrastructure at risk.

- » **Loss of privacy:** A hacker's ability to gain unauthorized access to the enterprise network by compromising IoT edge devices and taking advantage of trust relationships can lead to data leakage and the loss of sensitive information. Securing all layers of IoT implementations is a fundamental step to safeguard private information belonging to the enterprise, to its customers, or both.

Such threats typically seek to capture important information on a system, disrupt its performance or data flow, or manipulate the integrity of the data or controls (Exhibit 1). Furthermore, attackers may employ a host of methods to achieve each objective.

NETWORKED PRODUCTS SIMULTANEOUSLY GENERATE UNPRECENTED VALUE AND RISK

The very nature of data, however, provides networked products with the inherent potential both for risk and for unprecedented visibility and value creation.

Joining the Physical and Virtual Worlds

The IoT is evolving towards a fundamentally different architecture than traditional information technology (IT), characterized by a more distributed and interconnected structure that includes many devices with low-power or processing capabilities. The new architecture leads many organizations today to mistakenly view the new device and operations-oriented world of the IoT as a "parallel universe" relative to IT. As a result, IoT security is often managed with one approach, while IT and enterprise systems are managed using an entirely different (and disparate) approach.

The resulting "separate realities" threaten the potential value and required security for IoT implementations and fail to recognize the common security needs across IT and the IoT. Under silo'ed approaches, not only do disparately monitored systems fail to properly communicate and enable the full picture of data and insight, but they also drastically increase security risks and vulnerabilities. Without secure, seamless integration of IT and IoT, businesses risk exposing themselves to a greater number of blind spots and attack points.

Moreover, secure and seamless integration is not easy to achieve. A lack of established security standards in the IoT space continues to plague technology providers and users. In addition, securing data, devices, and apps across a spectrum of cloud and local deployments requires complete, end-to-end visibility into a system that ranges from device to cloud to the people managing both.

Exhibit 1. Hacking the Internet of Things: Objectives & Threats

Attacks on networks, devices and applications have three main goals: to capture, to disrupt, or to manipulate.

Capture
Attempt to obtain information or to gain control over a system or device

Disrupt
Attempt to disrupt, degrade, deny or destroy data flows or stored data

Manipulate
Attempt to change or alter data, commands or activities

Types of Threats

- Malware - infection by viruses, worms, trojans, adware or spyware
- Denial-of-Service (DoS) - overwhelm or overload system to degrade performance or availability
- Outside intrusion – unauthorized access from the outside
- Privilege escalation – altering access controls to gain more authority or data access
- Impersonation or spoofing – misrepresenting oneself a trusted device orother identity
- Unauthorized insider access or misuse
- Physical security – overcoming physical barriers or other safeguards
- Social engineering – manipulation of employees or persons (phishing emails, stealing passwords, etc.)
- Other traffic interception or stored data access and modification

Harbor Research: Security for the Internet of Things, 2016.

Many poor policies and practices are commonplace in today's IT systems:

» **No segmentation:** Poorly designed control networks that fail to compartmentalize communications, to employ sufficient "defense" mechanisms or to restrict "trusted access" to the control system network

» **Risk when not in use:** Hastily configured operating systems and embedded devices that allow unused features and functions to be exploited

» **Insufficient patching procedures:** Untimely implementation of software and firmware patches and inadequate testing of patches prior to implementation

» **Social engineering failures:** Insufficient oversight of personnel practices, including poor password standards and limited use of VPN configurations

» **Lack of management and control:** Incomplete or non-existent change management or change control for system software and patches

EXISTING IT SECURITY PRACTICES ARE IMPORTANT BUT INSUFFICIENT

Device and Network Challenges in the IoT

Devices at the edge, constrained in memory and compute resources, may not support complex and evolving security algorithms on their own due to the following factors:

» Limited compute and processing capabilities

» Insufficient processing power available to support today's standard encryption algorithms

» No backup connectivity if primary connection is lost while operating autonomously in the field

At the network level, the IoT further complicates security needs in several ways. Networks often:

» Operate across multiple network types, from a wired or WPAN at the device level to WLAN at the gateway, and up to the cloud or to a server, across multiple parties leveraging multiple protocols and standards

» Require physical protection, particularly for remote assets and in harsh environments, including tamper detection techniques and design

» Include devices with long lifecycles, such as smart meters or industrial equipment

» Must scale to and manage billions of entities in the IoT ecosystem

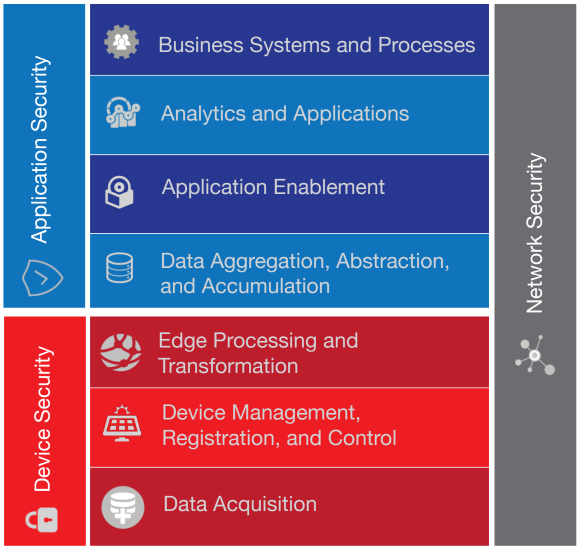
The complexity of this environment and the compute and power limitations of many IoT devices complicate security at the device, application and network levels. For instance, traditional device types, including equipment found in manufacturing facilities, were not designed with an eye toward the future of Internet networking. Security implications were fewer when data were only intended to travel on a closed operations network.

As a result, organizations must consider a holistic security approach that address all three layers of an IoT solution (Exhibit 2).

Security can no longer be ignored in the context of product design; it can no longer be left to IT or to a network operator down the line. Solution providers prioritize security at the earliest phases of design to protect their customers, as well as themselves, from the potential damage of equipment hacking or data loss.

This responsibility extends beyond just the IT and product design teams, requiring the involvement and input of C-level executives and management in order to develop and optimize a secure, long-term IoT strategy. Relevant third parties such as distributors, resellers, systems integrators, field technicians, and others must also be held accountable for their security practices. A true IoT solution involves many devices and organizations, and the entire ecosystem must prioritize security for the solution to succeed.

Exhibit 2. Internet of Things Security Stack


Application Security
Business Systems and Processes
Analytics and Applications
Application Enablement
Data Aggregation, Abstraction, and Accumulation
Device Security
Edge Processing and Transformation
Device Management, Registration, and Control
Data Acquisition
Network Security

Application Security
Security applications and development tools to guarantee only trusted instances of applications and development tools are running and communicating with each other, ensure data privacy and integrity, and ensure only trusted users have control

Network Security
Mechanisms to ensure availability of communication networks, security across heterogeneous network connections, and prevent unauthorized users access to data and controls

Device Security
Processes to ensure devices securely join the network, ensuring proper authentication and authorization as securing data within the devices

Harbor Research: Security for the Internet of Things, 2016.

IIoT SECURITY REQUIRES NEW THINKING & APPROACHES ACROSS ALL ORGANIZATIONS

Securing New IoT Solutions

Resource constraints and complex deployments that include both existing and new systems are the factors that will distinguish the IoT from traditional IT. Fortunately, even in the radical new world of the IoT, many of the same practices, technologies, and skills that have been developed in the past few decades remain relevant to the IoT with most of the new risks dispersed at the edge. In fact, as risks grow with the complexity of IoT solutions, IT security must also evolve, as well.

To support this shift, Harbor Research has outlined a three-step process to help organizations think about how to implement security technology in IoT solutions, including conducting an impact assessment, considering five primary security functions, and defining lifecycle controls (Exhibit 3). Leadership and integration teams should be careful not to limit themselves to any narrow line of questioning or way of thinking as they move through these phases, but be open to a new mindset that will help them creatively apply security measures in innovative ways.

Step 1: Address Security Impact in Diverse Environments

Understanding the impact of security in various potential IoT environments is an obvious first step in the solution design process. Given the diversity of both devices and the environments in which they will be deployed, each deployment is unique. Security solutions must be tailored to different usage environments and applications—whether they vary by size, industry, risk profile, or available product and service portfolio.

It is important to note that proper IT security is the implied baseline of any IoT solution deployment. Before bringing on new connected solutions, organizations should audit their environment to ensure they have implemented and are compliant with strong IT governance and best practices.

Organizations should consider the following practices:

Plan for environmental context. By establishing an understanding of the potential customer's environment, whether physical, regulatory, or end-user related, solution providers can make design and development decisions based on the specific needs of that industry or customer. For example, in developing connected HVAC systems for industrial buildings, a business may need to consider what types of data will need to be delivered to regulators, if any, or how easy it should be to adjust the building temperature and what access management controls may be required.

To assess the environment, know the questions to ask. Organizations should ask questions about what kinds of data will be created and transported, how private or sensitive the data are, to whom they will be delivered, the duration of storage, what outside linkages or integrations will occur, and what existing protocols or compliance requirements already exist in the respective verticals and industries (Exhibit 4). The entire risk landscape should be considered, including the physical environment, third-party suppliers and vendors, the legal and regulatory environment, and existing applications and infrastructure.

Front Page Hack: The Target Breach

» **What Happened:** The Target data breach in 2013 exposed the names, addresses, phone numbers and credit and debit card information of 70 million customers. Hackers used a vendor's credentials to access Target's network, then installed several malware programs and collected credit card information.

» **How It Happened:** A lack of proper employee training, access control and network segmentation controls are likely to blame. A third party vendor's access to the network was not properly restricted and cordoned off from POS and customer data, allowing hackers to use the vendor's credentials as an entry point into Target's entire network. The data breach was a classic example of the emerging threat vectors that can allow attackers to steal sensitive data through non-traditional access points.

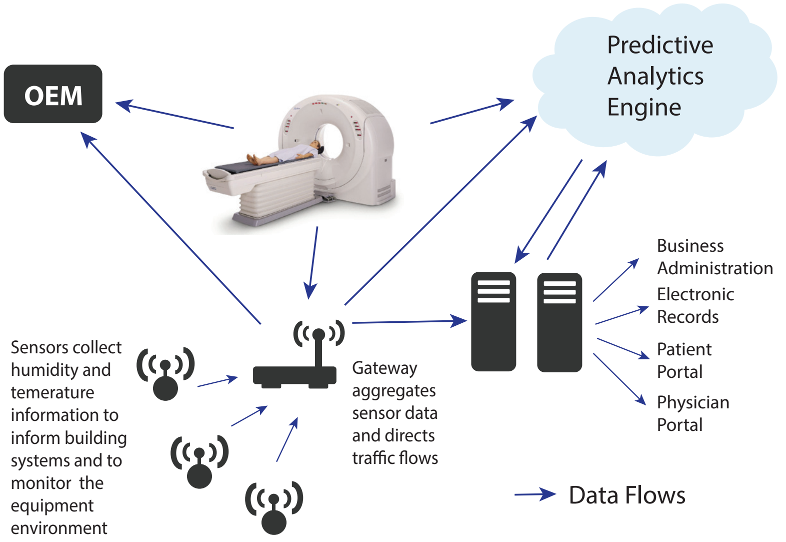
Exhibit 3. Three Steps To Address Security for the IoT

1. Assess Security Impact

Evalute the customer environment and ask questions about the network, devices and applications already in place.

- What types of data will the customer send?
- Where will they send that data?
- Will any of the data be private, sensitive, or at greater risk?
- Where will the customer store the data?

An MRI machine exemplifies the transfer of critical sensor data, image data, and highly sensitive patient scans. In this scenario, OEMs, hospitals, and other service providers may store such data.



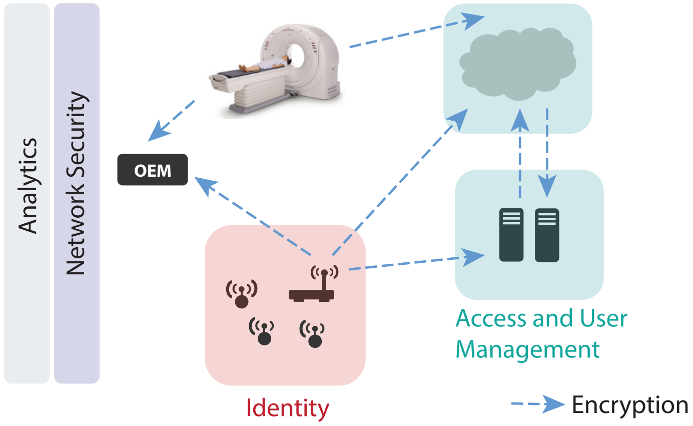
Sensors collect humidity and temerature information to inform building systems and to monitor the equipment environment

Gateway aggregates sensor data and directs traffic flows

2. Apply a Multi-Faceted Security Approach

Address all five security functions to fully protect the network, devices and data and applications as they move throughout the deployed system.

- Identity
- Access and User Management
- Encryption
- Analytics
- Network Security



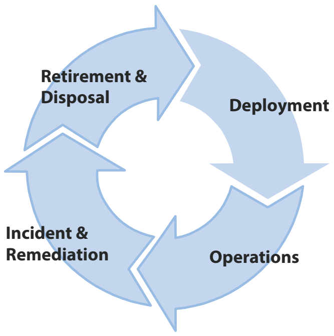
3. Define Lifecycle Controls

Consider the entire lifecycle of devices in the system and the security implications within each phase.

1. Deployment
2. Operations
3. Incident & Remediation
4. Retirement & Disposal

Exit the system: clear data and replace device as needed

Establish trust: verify identity and device integrity



Prepare for the worst: fail safely and establish a pre-determined response

Maintain device and data security: conduct device monitoring and provide updates and patches

Harbor Research: Security for the Internet of Things, 2016.

ENSURING THAT NEW IoT SOLUTIONS ARE SECURE IS A MULTI-FACETED PROCESS

Provide clear communications about privacy and security risks. In addition to educating customers on the benefits of device connectivity in a given environment, organizations must also provide clear 'opt-in/opt-out' capabilities so that customers are fully aware and supportive of data flow and understand the security and privacy implications. Customers will need to understand the value they receive in terms of higher quality service and lower cost of ownership. Finally, providers should clearly communicate the importance of internal communication within the customer's entire organization: employees at all levels should receive ongoing education and governance training in security best practices in order to appreciate the importance of security structures.

Step 2: Apply a Multi-Faceted Security Approach

IoT data will move across all communication layers, from endpoint to application to data center to cloud. Solutions must address key security functions across the architecture, based in five primary areas: **identification, access and user management, encryption, analytics, and network security**.

A) Identification: As IoT products find their way into greater business contexts, an increasing number of devices will have their own identity, separate from any controlling individual. More intelligent devices with sufficient processing power will be capable of announcing themselves to the network, but others may need additional support using embedded modules or gateway aggregation.

Exhibit 4. Understand the Customer Environment: Use Cases & Sample Questions

Understanding the Customer Environment: Use Cases & Sample Questions

Temperature Control System in a Food and Beverage Processing Plant	Delivery Truck Tracking System for a Distributor	Fire Safety System in a Large Commercial Building
• Who or what other parts of the network should have access to this data? • Are any of the data subject to government regulation or other industry standards? • What if data or signals are intercepted, disrupted or altered? How might this affect the functionality and operations of the plant? • If sensors lose connecitivity to the control center, is there a system to enable real-time or low-latency actions? • Are there any risks of physical tampering or other damage?	• What data are being collected, and how are they transmitted? • Could a malicious attacker gain access to the vehicle control system through the network or other entry point? • Are any of the data confidential? If competitors or malicious parties gained access, how might this affect the business? • Is there potential for device manipulation? How can the enclosure be secured or tamper-evident? • How might data relayed back to the truck impact the business?	• What type of data are being collected, processed and transported? • Who has access to these devices, and what degree of control do they have? • What other building or business systems and networks have been integrated? Are there any risks to the enterprise network? • What would happen if communications were disrupted? How might this affect occupants and the business? Are any backup systems in place should the device lose its connection?

Harbor Research: Security for the Internet of Things, 2016.

TAKE A COMPREHENSIVE APPROACH TO SECURING DEVICES, APPLICATIONS, AND NETWORKS

Front Page Hack: Remote Jeep Control

- **What Happened:** In July 2015, two hacking researchers successfully took control of a Jeep Cherokee while it was on the road and were able to remotely turn on the windshield wipers, control the radio, shut off the transmission and disable the brakes. The hack exploited vulnerabilities in car entertainment and wireless systems.
- **How It Happened:** The Jeep attack exploited a connected vehicle from several angles. First, similar to the Target data breach, makers failed to recognize the scope of the security perimeter, resulting in insufficient border controls from the cellular and Wi-Fi networks to the internal control system for the vehicle. The hackers used an individual vehicle's IP address to access thousands of vehicles across Sprint's nationwide network, using the cellular connection that links the vehicles' computers to the Internet. Connected cars are an excellent example of a challenging IIoT product, with complex, multi-million endpoint deployments, multiple network levels, long lifecycles and direct ties to the safety of their users.

Establish identity verification. Device identities must be authenticated in order for each node or device to participate on the network. Since many IoT devices do not have the necessary computing or logic to support current authentication protocols, intelligent gateways can securely bridge less capable devices to the network while performing critical attestation, authentication and encryption functions, as well as applying a root of trust. Ideally, all devices in an IoT solution will feature security hardware or cryptoprocessors to create a mutual root of trust with the rest of the network nodes. This root of trust enables a secure boot, which loads and verifies local firmware and software so the system is assured that each device participating on the network is what it says it is. More modern and capable devices will have native root of trust, and the network will be able to directly confirm their identity.

B) Access and User Management: Access and user management is the next critical security function that must be addressed in IoT solutions. This includes the management of the device identities outlined above within the larger system architecture, as well as endpoint activation management, provisioning and commissioning, asset management, security updates, and other functions. In addition to cyber security, hardware should also be secured against physical access and ruggedized to withstand industrial environments as needed. Equipment should not only be resistant to physical abuse but also able to send an intrusion alert in the event of tampering.

Balance security and usability. From a cyber perspective, organizations should strike the right balance between usability and security for the applications at hand. Usable security is all about finding a balance between minimizing the attack surface while also ensuring the solution is not so difficult to use that it is less prone to be adopted. Providers that strike this balance are far more likely to find success with their customers.

Workflows should be designed to implement security measures during installation, including simple, intuitive interfaces that also restrict the ability to introduce holes such as accepting default passwords. Designs should also provide means to "right-size" security measures for a given use case and associated risk profile. In highly sensitive environments, for instance, the default configuration should be at the most secure settings possible.

Include device-based safeties and boundaries. Simple hardware steps, like implementing lockouts based on idle time or maximum attempts to authenticate, are some of the most straightforward ways to ensure that unauthorized users cannot gain control of the device. The device should also be enabled to support remote monitoring, control, and updates within a secure environment from the manufacturer or the customer, or both, depending on the end use. This is especially important for devices that will be deployed in dispersed or harsh environments, like sensors installed at remote oil wells or along power lines, where no one will be on hand locally to shut the device down or start upgrades as needed.

C) Access controls should only allow the device to access resources that support its specific role. That way, if a component or application on the device is compromised, its access to other parts of the system is minimal, limiting systemic damage. An intelligent gateway can not only ensure that all data coming from less capable

UTILIZE BOTH EXISTING AND NEW BEST PRACTICES TO SECURE SOLUTIONS

devices is secure before passing it on to the network, it can also provide a more robust barrier for controlling access back through to these devices. Several scenarios should be considered to ensure that all authentication possibilities have been covered, including device-to-device, device-to-gateway, gateway-to-cloud, user-to-device, administrator-to-device, and possible device-to-cloud interactions.

Enable context awareness at the device and policy level. For all of these interactions, the key enabler for improved visibility will be implementing context-aware security strategies. Security policies and systems must be flexible to incorporate new sensors, devices and other equipment as the network grows. Rigid security policies that grant simple yes/no access only to pre-authenticated identities and passwords will quickly fall behind, leading to frustration among users.

All of these factors can then be assessed against security policies used to determine access. Policies may include what operating systems and applications are allowed during standard working hours, but as many IoT devices will operate round-the-clock in disparate locations, these policies should be determined carefully, incorporating feedback from key stakeholders

D) Encryption: Encrypting large volumes of real-time data is a challenging aspect of IoT security, but it is at the heart of its value. To encrypt these data, organizations must determine which of the various protocols available for the IoT most closely match the needs of the customer to provide sufficient protection, or that are best suited to integrate with other protocols in use. Just as in classic IT scenarios, data will need to be protected at all stages, including while at rest, in transit, and in use.

Deploy encryption at multiple points. Organizations should ensure that all ingress and egress data and control connections are protected using a secure standard, such as SSL/TLS, and add random data to hashed data to make them more difficult to hack. The encryption of data during transport must take into consideration the constrained resources available on the devices, so most encryption algorithms must have a small processing footprint. It is generally optimal for endpoints to take on this function but, for less capable devices, intelligent gateways can be leveraged to perform more robust encryption.

The system also needs a firewall or deep packet inspection to control traffic flows. Although it does not need to filter Internet traffic or higher-level network activity, since network appliances will cover those data, it will need to filter the data that will terminate on the device, making the best use of limited computing resources. Strong, ubiquitous encryption reduces the easy entry and privacy risks to which many IoT solutions on the market today have exposed themselves.

D) Analytics: As devices become smarter, so must the security systems in place to monitor them. Security analytics that actively assess network traffic, whether based in a firewall or other hardware, to search for malware or other anomalies that may indicate a threat to the system in real time will support a more advanced network of devices.

Device analytics should provide a line of defense. Identifying cyber attacks and breaches and then organizing an appropriate response can be automated using

Use Case: Immunization Storage Equipment

» **Customert:** Medical refrigeration equipment supplier

» **Problem:** Refrigerate various vaccinations at appropriate temperatures

» A medical equipment provider was developing a refrigeration system for vaccinations that could be used in doctors' offices and hospitals. The unit included three separate refrigeration units with an internal elevator and a turntable to control the movement of the vials. To comply with strict FDA regulations, vials had to be monitored based on lock codes, expiration dates and specific temperature needs for each type of vaccine.

» The system required data flows to four different channels, ranging from manufacturers' codes to inventory controls to medical billing to distributor supply chain tracking. The system was also integrated with hospitals' enterprise backbone.

» Dell leveraged its SecureWorks solution to secure the different data channels with different sets of protocols, while maintaining HIPAA compliance.

Use Case: Commercial Irrigation System

- **Customer:** Irrigation system provider for commercial buildings and golf courses
- **Problem:** Conserve water and increase system visibility
- A commercial irrigation system provider was looking to increase visibility into its water usage patterns and improve water conservation efforts. Previous tracking and control was based on programming PLCs and on-site observation, which required a significant use of employee time.
- The company partnered with Dell to develop a remote system that controlled individual sprinkler heads using satellite communications. Satellite communications were relatively straightforward, but the key challenge was interfacing and securing control devices for the sprinkler heads.
- **Solution:** Dell's SecureWorks was used to monitor data flows from sprinkler to tablet to satellite, as well as water runoff and weather data, providing constant monitoring for the entire system.

sophisticated analytics and incident response tools. Other functions include automatic extraction of suspicious files and integration with other network security products. At a broader level, advanced threat intelligence analytics correlate anomalies in the network against known threats from global threat databases and a wide range of third-party sources. Customers' networks can classify attacks based on newly identified threats and tactics from a worldwide information base. Designing IoT solutions that can be incorporated into broader threat intelligence solutions will be important in a constantly changing threat environment.

Many of these technologies are still developing in the marketplace, presenting an imperative for organizations developing IoT solutions to be actively aware of the latest advances and prepared to update their solutions as new technologies become available.

E) Network Security: Embedding antivirus, whitelisting, memory protection, and other essential security functions directly into IoT devices and gateways will support greater security throughout the network, but the network itself will also require attention in order to offer seamless protection.

Segment traffic to reduce risk and improve performance. Customers may choose to segment IoT data from IT system traffic, as this is where valuable corporate data, sensitive information, and financial transactions can be found. Segmenting network traffic can also limit hackers' ability to take direct control of actuators and device or equipment controls, with chaotic and potentially dangerous consequences for operations. The border between these two systems should be designed as seamlessly as possible.

More connected devices mean more traffic on the network, which can contribute to latency and lower overall performance of an IoT solution. Intelligent gateways can perform some of the analytics and data processing at the edge and send actions directly back to connected endpoints without having to move the data over the network to a datacenter or cloud environment. Gateways can also determine which data need to be sent on to other applications or centralized computing. This edge functionality will be increasingly important as more and more devices find their way onto the network.

Add network-level management and awareness. Network-wide security will also require device and endpoint management. This includes many of the broad elements mentioned previously, such as identity management and provisioning and commissioning for new devices, as well as security policy management and overall network traffic monitoring. Context awareness is important at the network level, as well, and advanced firewalls that can apply context-aware policies across all network traffic can be an excellent tool to ensure IoT security.

EXTEND IIoT SECURITY ACROSS THE SYSTEM ARCHITECTURE AND THROUGH THE DEVICE LIFECYCLE

Step 3: Define Lifecycle Controls

IoT security extends across the entire system architecture and through product lifecycles, from deployment to retirement. The life span of devices within the IoT will vary significantly, combining smaller devices and components with short life spans as well as equipment, such as industrial machinery, that can last for decades. This is a radical departure from the world of IT, where equipment lifecycles are fairly regular and predictable. Therefore, it is essential that businesses monitor and enhance the security of IoT products from when they are manufactured to when they are discarded.

A) Deployment: IoT security is as much about deployment best practices that minimize the attack surface as it is about securing product features and functionality. When a device is first powered on, the authenticity and integrity of the device software must be verified using cryptographically-generated digital signatures or other identifiers (like RFID, X.509 certifications, a MAC address, or another hardware-based root of trust). Identification and authentication protocols may change as advancements toward smaller footprint credential types are developed for the IoT, but establishing trust with the network and system will always be the first step in securing device operations.

Consider configuration attributes unique to IoT deployments. While it may be more simple to set initial configuring and provisioning based on existing network policies, the security-minded best practice is to re-assess the settings based on the new workloads and workflows. The solution should include basic install guidelines, including functions or instructions to change default access and pairing passwords. In addition, if the device ever loses its connection from the network due to being moved or losing power for any reason, provisions should exist to require the device to re-authenticate itself prior to receiving or transmitting data.

B) Operations: Once a connection is made—wired or wireless— operations begin. The network is responsible for managing the device and its software and firmware, and the device itself should support continuous monitoring, automated vulnerability assessment and penetration testing, and integration with existing security frameworks. Reliable status monitoring offers peace of mind to the customer, manufacturer, and greater ecosystem and can indicate if the device has been tampered with.

Plan for security dynamics across operational contexts. Managing the security of device operations should include (but is not limited to) the following:

- Proactive security assessments and monitoring
- Real-time security response in the event of an attack
- Ongoing identity management
- Provisioning and commissioning
- Integration with additional devices, networks, or data streams
- Security policy and credential management
- Evaluating and re-evaluating situational awareness

FUTURE-PROOF PRODUCT SECURITY TO ADAPT TO EMERGING TECHNOLOGIES

Support secure operations through ongoing updates. Perhaps the most critical security priority during a product lifecycle is to support updates and patches without disrupting operations. Although customers will ultimately be responsible for implementing updates, device manufacturers have an obligation to make the process as simple and painless as possible. Tracking these devices will be key to understanding their operations and when an upgrade or patch is required. Security patches from third-parties and open source libraries may be supported, depending on the product and customer environment.

Device manufacturers should make updates available on a regular basis to help end users stay up-to-date with both security and overall technological and connectivity advances. Each update should provide context for the files being sent, as well as information about how they were transported in order to show that the file is indeed reputable. Updates should be rolled out and authenticated by the device in a way that does not disrupt its activities, consumer bandwidth, or impair its functional safety. Firmware updates should have the option to occur automatically while in service but be deferential to customer preference.

More conservative users in traditional industries may hesitate to roll out changes they don’t see as necessary, so manufacturers should distinguish between a critical security upgrade that patches a known vulnerability and a non-critical functional update. Updates should come with clear release notes to describe criticality and allow administrators first test them in a quarantined pilot if desired. Systems should also have interlocks to ensure that all IT, operations, and other key stakeholders are aware of an impending update before it is deployed to ensure there are no surprises in mission-critical operations.

Exhibit 5. The OEM’s Role in IoT Security

The OEM’s Role in Architecting Security

The IoT offers OEMs the potential for new revenue streams and deeper customer interactions. By leveraging connected equipment and devices in the field, OEMs can better understand how the equipment they manufacture performs during use and over time. This will allow OEMs to tailor their products to better meet customer needs and increase revenues by providing additional value-added services such as proactive maintenance and automated delivery of replacement parts. Customers will be hesitant to adopt these solutions, however, if they feel their security may be compromised. Basic security functions remain important when considering IoT devices, including:

- Ensuring the data are properly encrypted as it travels across the network
- Ensuring only authenticated devices and users can access private data
- Ensuring complete visibility into the system is possible in order to detect unusual or malicious activity
- Ensuring regulatory compliance and the protection of sensitive data and IP

In addition, as OEMs move to retrofit and upgrade existing systems, they must avoid a “rip and replace” mentality that would disregard the significant capital investments inherent in existing equipment and systems. Providing sufficient security for IoT solutions is a critical but complex and constantly evolving challenge. It is in OEMs’ best interest to support the end customers’ overall security to capitalize on emerging opportunities and revenues.

Harbor Research: Security for the Internet of Things, 2016.

IIoT SECURITY STRATEGY AND SOLUTION DEVELOPMENT WILL REQUIRE NEW PARTNERSHIPS

C) Incident & Remediation: If a security incident does occur, the device should be prepared to fail safely, if needed. For less advanced devices, an intelligent gateway can provide this function by identifying a malfunctioning or corrupted device and responding appropriately. Many IoT devices, however, cannot risk going offline without causing significant disruption to operations. Instead, the device should be prepared to alert the wider network, especially any peer devices, and avert traffic until remediation can take place.

The device should also be incorporated into system-wide incident response policies. In some instances, these policies can require operations engineers to preemptively shutdown, quarantine, or halt certain activities or devices in a given deployment to reduce the risk across the entire operation. An intelligent gateway can step in and provide near-real-time analytics and response when networks are slow or down to help pinpoint and lock down problem areas.

D) Retirement & Disposal: IoT devices will eventually need to exit the system securely. Due to the sheer number of devices being connected, this is likely to be a common occurrence across systems and should be fairly straightforward. Devices that have held sensitive or critical information should be securely wiped, including removal of certificates and data. In addition, providers may advise customers to consider how and when the data themselves may be disposed of, particularly as they have proliferated across the device, network, server, and cloud.

The true value of the IoT is data: therefore, data generated by the device require security procedures, governance, and planning just as much as the device itself. Thus, stakeholders must ensure that their overarching IoT security strategy incorporates both device lifecycle and data lifecycle security dynamics.

Partnering For Success

The guidelines described in the previous section provide useful tools for considering the many aspects of IoT solution security. Although the concepts are simple, the implementation of security in today’s solution environment can be extremely complex—so complex that organizations should not expect to go it alone. Organizations should seek out partners that understand the converging IT/ IoT picture and associated heterogeneous stacks, offer industry-specific technology and data policies, and can work to architect and deploy a solution together effectively and securely. Often, this will require customization in order to leverage and integrate with existing systems and design an effective product for end customers.

One such potential partner is Dell. The global hardware, software, and services company offers a broad security portfolio and large global footprint. Alongside its traditional IT capabilities, Dell has experience serving operations technology customers and OEMs, working with customers to design, develop, and deploy secure IoT solutions. As a part of its commitment to IoT solution enablement, Dell’s recently released intelligent Edge Gateway is intended to help provide the secure bridge between existing traditional systems, sensors, and other devices across all manner of connected environments.

In Conclusion

Security is the biggest challenge facing the IoT today. In developing new solutions for the IoT, organizations must consider the larger context and implications of security and privacy from the very beginning and select the partner best suited to serve both existing and new technologies in their customers' unique environments. The basic IT building blocks of identity, access and user management, encryption, analytics and network security are the critical baseline to any IoT deployment, but the amount of data and the number of devices involved will require meticulous security development. Choosing the right partner to support this process and fill any gaps plays a significant role in determining how quickly and successfully an organization is able to bring its solution to market. Strong partners that use best-in-class technologies and are flexible enough to work with multiple vendors and systems, particularly traditional equipment, should be targeted for IoT solution development.

ABOUT HARBOR RESEARCH

Founded in 1984, Harbor Research Inc. has more than twenty five years of experience in providing strategic consulting and research services that enable our clients to understand and capitalize on emergent and disruptive opportunities driven by information and communications technology. The firm has established a unique competence in developing business models and strategy for Smart Systems and the Internet of Things

ABOUT DELL

Dell has over a decade of experience working with OEMs to develop and deploy connected solutions for the Industrial Internet of Things. Dell's extensive security portfolio includes the Edge Gateway 5000 Series, which delivers powerful analytics capabilities, industrial-scale form factors, and multiple input/output options and is equipped to withstand extreme environments. Dell works with customers in a collaborative partnership to bring new solutions to market quickly and securely. Dell works with customers in a collaborative partnership to bring new solutions to market quickly and securely, helping bridge traditional systems and the IIoT across a wide array of industry applications.

ABOUT THE AUTHORS

Glen Allmendinger - Founder and President, Harbor Research

Glen has managed Harbor's consulting and research activities since its inception. Glen has worked with a range of leading technology innovators, product OEMs and service providers, assisting them with strategy and market development for new smart product, systems and services opportunities. He has participated in pioneering work in the Smart Buildings, Healthcare, Retail, Transportation, Energy and Industrial arenas, helping clients determine the scale and structure of emerging opportunities, competitive positioning and design of new business models. Glen co-authored the pioneering article "Four Strategies For The Age Of Smart Services," Harvard Business Review, October 2005 and has also authored articles for a wide range of publications, including The Economist and The Wall Street Journal, as well as being a frequent speaker at industry forums.

Haley Newkirk - Research Analyst and Consultant

Haley is a research analyst and consultant at Harbor specializing in security and industrial smart systems development opportunities, including strategy development, go-to-market design and creation of new revenue and business models. Haley is also part of the core consulting team for client engagements focused on applications for infrastructure systems in the building, transportation and security sectors, as well as projects focused on new residential and consumer–focused services. Haley earned her bachelors degree from the University of Colorado. She is fluent in French and English.

Jessica Groopman – Research Director and Principal Analyst

Jessica is research director and principal analyst with Harbor Research where she heads research and content strategy and helps lead Harbor's Smart Systems Lab program. Jessica specializes in consumer-side Internet of Things. Her current focus is the application of sensors and smart systems in consumer-facing businesses, with an emphasis on user experience, the ethical use of data, privacy, contextual marketing, automated service, and wearables. She helps clients in retail, hospitality, insurance, and technology understand, position, and act on smart systems opportunities. Jessica is a regular speaker, moderator, and panelist at IoT industry events. She is also a regular contributor to numerous 3rd party blogs and news/media outlets, and is featured on Onalytica's top 100 influencers in the Internet of Things. Find more on her blog at www.jessgroopman.com.