Securing the Internet of Things: Seven Steps to Minimize IoT Risk in the Cloud

Companies moving to capture the enormous opportunities presented by smart, connected products and the Internet of Things (IoT) face substantial risk as well, especially when it comes to the security of customer data and intellectual property in the cloud.

Worrying about security in the cloud is nothing new. But the tremendous increase in scale and complexity that accompanies the Internet of Things greatly increases the attack surface of organizations compared to traditional information technology deployment, and thus greatly increases the risk to brand, reputation, and daily operations.

Organizations that wish to profit from the Internet of Things must broaden their security focus from simply protecting IT assets to assuring security, privacy, and availability for products and services that are often entrusted with life and limb through connected homes, transportation systems, healthcare, public infrastructure, and more.

In particular, this requires planning and investment at each level of the IoT value chain, from connected assets in the field, through the cloud itself, to the increasingly broad range of connected users, systems, partners, and supporting infrastructure.

This white paper from PTC Cloud Services provides a framework and seven steps companies should take to minimize risk during the all-important planning stages of an IoT initiative.

CONTENTS

• Understanding IoT Risk
• Hacking the IoT
• Core Components and Users
• Expanded Vulnerability
• Seven Steps to Minimize Risk
• Looking Ahead
UNDERSTANDING IoT RISK

Along with their great potential benefits, the scale and complexity of IoT deployments represent a large increase in risk for organizations that embrace them.

Most important, the IoT changes the traditional information and cloud security paradigms in important ways that must be addressed early in deployment planning if organizations hope to prevent adverse outcomes for customers, business partners, and users.

Among the most important IoT security concerns are:

Public Safety (life and limb)

Because IoT capabilities are deployed in “real world” settings, they can more easily cause real-world damage to life and limb.

Imagine the failure of a telematics system directing your autonomous vehicle, or firmware operating life-sustaining medical devices or the electric grid.

Product Liability

While traditional product liability law is well established, it is less clear on the role that software and cloud-based infrastructure providers may have in failures that result in liability or other legal claims involving connected products.¹

Business Disruption

With the IoT, a balky software update that previously would have been a headache for in-house users can now ground an entire fleet of cars or trucks. A failure at a cloud provider hosting IoT services could cause regional or even global disruptions to IoT deployments and the businesses that rely on them.

HACKING THE IoT

The security risks that come with IoT deployments are often fodder for headlines about spamming refrigerators and hackable cars. What are the real hacking risks?

Here are some to consider:

- Denial of Service: The limited size and processing power of many IoT devices makes them extremely sensitive to so-called denial of service (DoS) attacks, in which a flood of bogus traffic overloads the device’s ability to respond to legitimate requests. Historically, such attacks have targeted public-facing web- and ecommerce servers. But IoT’s heavy reliance on cloud-based assets creates serious vulnerability to the downstream effects of DoS attacks on endpoints, as well.
- “Man in the Middle” Attacks: Improperly configured or deployed IoT networks can allow attackers to use rogue wireless infrastructure and intercept traffic between devices and cloud-based management systems, thus opening the door to compromised data and penetration of upstream assets and applications.
- Device Spoofing: Improper implementation of digital signing technologies like public key infrastructure (PKI) can enable a knowledgeable attacker to “spooﬀ” legitimate devices and disrupt IoT deployments.
- Malware: Cyber criminals are fast adapting their creations to operate on embedded IoT devices, including point-of-sale systems, home broadband routers, and connected health devices.
- Application-based Attacks: Application vulnerabilities pose one of the most significant risks to the Internet of Things. Attacks that target security weaknesses in the firmware and applications running on embedded systems, or on back-end application and database servers, can provide instant, high-level access to IoT deployments.

Compliance/Regulatory Risk

In regulated industries, IoT deployments will complicate the already difficult job of identifying and securing protected data and devices. Whether it is protected health information or credit card data, organizations will need to expand their current audit and compliance regime to encompass IoT devices and their supporting infrastructure and data in the cloud.

CORE COMPONENTS AND USERS

The first step to addressing IoT risk is to understand the key components of typical IoT deployments.

Properly addressing the full scope of security concerns requires careful planning and investment at each level and with each component in the IoT value chain.

While the details of individual programs will certainly vary, most deployments will include the same core elements, as depicted in Figure 1.

Smart, Connected Products

For the last 30 years, the "Internet" has been something of a computing monoculture of powerful, multi-function endpoints such as servers, desktop and laptop computers, and, more recently, smart phones and tablets. Most of these endpoints ran one of several main operating systems and relied upon a relatively limited set of hardware and software.
As the IoT connects hundreds of billions of new devices, that profile is changing. Low-power, single-purpose endpoints running a wide variety of open source and proprietary operating systems are fast becoming the norm and will soon eclipse traditional endpoints.

Unlike their predecessors, IoT devices often lack the processing heft to do advanced encryption or lack a graphical interface through which users can manage the device. They may have constant or intermittent connections to the network from which they are managed. Traditional operating systems such as Windows, Android, and iOS share the stage with customized versions of Linux, existing and new commercial real-time operating systems (RTOS), and purpose-built IoT contenders like PTC ThingWorx®, RiOT, mbed, Contiki.

Cloud-Based Services

Access to cloud-based services and resources is a second foundational element of the IoT.

As companies deploy ever more diverse connected products and devices, the applications, storage, compute power, and intelligence that support them generally shift from powerful endpoints like desktop and laptop computers to systems deployed in the cloud.

Additionally, management and analytics platforms hosted in the cloud are an ideal way to manage globally distributed populations of thousands or millions of connected endpoints. Already, cloud-based services provide platforms to deploy and manage IoT applications and collect, store, and analyze data from smart, connected product endpoints. Cloud-based management servers provide resilience, scalability, and easy access to third-party applications and services provided by business partners.

Smart Product Applications

Much of the true power and value of the IoT comes from the applications that companies, business partners, and end users rely upon to monitor, control, optimize and operate connected products and devices. Already, open source and proprietary IoT development platforms are facilitating the creation of literally millions of new IoT focused applications.

External Information Sources

With the IoT, companies and end users will increasingly gain the ability to integrate data from a fast-growing ecosystem of information service providers tapping into product, service, environmental, business, governmental, and social sources.

Business Systems

While the IoT is changing our definition of what is and can be a “computer,” organizations that wish to reap the benefits of IoT devices still must find a way to integrate IoT data into existing mission-critical applications and processes such as PLM, ERP, CRM, and SLM if they wish to create new, innovative applications and services.

Communications Infrastructure

The IoT is deployed on top of existing communications infrastructure, including wired, wireless, cellular (3G and 4G), and satellite communications which connect intelligent endpoints in the field to applications and management infrastructure in the cloud.
Connectivity

Extended connectivity is another defining characteristic of the Internet of Things, which extends Internet access (broadly defined) to new classes of devices. Commercial IoT deployments will rarely be part of the public Internet. However, most will piggyback on top of or rely on the same general purpose infrastructure and communications protocols (TCP/IP, UDP, MQTT, CoAP, and others) that connect everything else in our digital lives.

IoT Users

Finally, IoT deployments typically involve a wide range of end users of the smart, connected products, as well as business and IT users inside the company and with partners. The end users are typically your own customers or the end users of your customer or partner organizations. They might interact with your products in any number of settings, including home, office, factory floor, car, store, hospital, or sports or entertainment venue.

Business users help define the objectives, scope and purpose of IoT initiatives, and benefit from the services and data they provide. For many business users, this requires new skills and new ways of working.

Network and systems administrators perform many of the same tasks they do for traditional IT but with a much broader and more complex set of assets, applications, data, and users to manage, support, and secure.

EXPANDED VULNERABILITY

While many of the IoT threats are similar to those that sophisticated IT organizations have long addressed, the expanded set of components and users in typical IoT deployments present novel opportunities for malicious actors to inflict damage on unprepared organizations.

Three new and critical key areas of vulnerability include the devices, the expanded cloud-based infrastructure, and the growing reliance on shared components.

Devices

Poor product planning, design, and development are the root causes for many IoT-related security incidents, from leaked data and invasions of privacy to compromises of sensitive IT environments.

Even when IoT products ship with robust security features, they often have default configurations that undermine those features. The net result is often IoT devices that are easy prey for malicious actors operating within or even outside of a protected environment.

Cloud

Robust cloud-based applications and infrastructure provide the backbone of IoT deployments. Securing that infrastructure and communications to and from IoT endpoints, applications, and information sources is one of the most important considerations for any organization looking to launch a new IoT offering or migrate existing products to the IoT.

Companies already familiar with cloud security have a good introduction to the requirements for the cloud side of IoT, but the added scale and complexity of connectivity, communications, and the endpoints themselves add greatly to the challenge.
Shared Components

Off-the-shelf boards with programmable SOC (system on chip) integrated circuits have eliminated many of the costly, early stages of IoT device creation. Powerful development tools and languages make it relatively easy for companies to set up device-to-device and device-to-cloud communications, endpoint management and updating, and new application and service design in support of IoT devices.

But the embrace of open source and shared code to accelerate IoT initiatives also entails risk. As illustrated by the recent disclosure of critical, long-lived vulnerabilities in ubiquitous open source technologies like OpenSSL and Bash, a heavy reliance on shared libraries and code can result in unexpected “common mode” failures.

SEVEN STEPS TO MINIMIZE RISK

The job of securing IoT deployments is in many ways an extension of the kinds of security functions most companies have developed over the last two decades, such as data encryption, application firewalls, identity authentication, and internal monitoring. These investments and approaches can provide important building blocks for an overall security plan.

Beyond those basics, however, companies need to focus on securing the new IoT endpoints, applications, data feeds, and the cloud-based services that sit in the middle of the entire IoT ecosystem.

This section provides seven specific steps that companies should take to create effective risk-mitigation strategies for IoT products, services, and deployments.
1. Secure Cloud Infrastructure

Cloud infrastructure that supports IoT technologies demands security at a variety of layers, with a three-pronged approach focused on confidentiality, integrity, and availability (CIA).

Among other things, communications between deployed endpoints and IoT hubs and cloud management servers must be encrypted to prevent snooping, while input to IoT application servers and back-end databases must be sanitized to weed out malicious traffic and application-based attacks.

At the application layer, layered security protections to prevent application-based attacks on deployed assets are a must. Availability of IoT services must be assured with proper data backup and disaster recovery and resilience planning, in keeping with internationally recognized standards. Further, access to IoT application servers and data must be secured, with rigorous enforcement of “least privilege” policies to limit access to administrative features and sensitive data to those users with a need to access them. Finally, physical access to and maintenance of data centers and the physical assets used for hosting must be strictly controlled in keeping with internationally recognized standards.

2. Leverage Standards-Based Best Practices

The cloud-based systems that host IoT services should be protected in the same way as other IT deployments: by relying on industry standards and best practices for security management, including the use of robust, layered defenses. Security controls and processes should be aligned with government- and industry-recognized guidelines such as ISO/IEC 27001:2013, the newer ISO 27018, the Federal Risk and Authorization Management Program (FedRAMP), and the NIST Cybersecurity framework.

These standards and certifications help ensure that cloud and service providers have a system of controls in place based on proven methods for managing complex information-security processes like security assessment, threat detection, continuous monitoring, user authorization, and data protection in traditional IT as well as cloud environments.

3. Design for Security

Thorough security planning must be a foundation of the design and development process for IoT-related products and services to make sure they can connect and communicate securely and will resist casual and determined attempts to compromise their integrity.

Including secure application design principles early in the design and development process for IoT services can eliminate low-hanging fruit for attackers.

Static and dynamic testing prior to release can identify more subtle but exploitable vulnerabilities, including SQL injection, cross-site scripting, and cross-site request forgery attacks, which can be difficult to identify and prevent in the wild. Finally, to the extent that IoT management servers rely on open source applications and code, organizations need to pay close attention to the security of that shared code.

### SEVEN STEPS TO MINIMIZE RISK

- Secure Cloud Infrastructure
- Leverage Standards-Based Best Practices
- Design for Security
- Secure IoT Devices
- Secure Device Connections
- Secure IoT Services and Apps
- Secure Users and Access
Organizations that leverage open-source components need to keep close tabs on how and where that shared code is used. By maintaining a software manifest, IoT makers can easily assess the impact of any new vulnerability and take steps to update shared and open-source libraries that are subsequently found to be vulnerable to attack prior to the development of an exploit or, failing that, develop steps to help customers remediate exploitable vulnerabilities.

4. Secure IoT Devices

Fundamentally, securing connected devices is similar to securing other elements of your IoT infrastructure. You need to protect data at rest on the device and in transit between endpoints and other IoT infrastructure (such as hubs or other devices), or between back-end management systems. Similarly, you have to secure devices against authentication-based attacks like brute-force password guessing.

IoT endpoints deployed in the field don’t benefit from the physical protections afforded to most IT assets. They can easily be scanned and probed, or collected, disassembled, and studied by an adversary to discover weaknesses. Organizations that are planning or designing new connected products need to take steps to ensure that their IoT devices and deployments are secure even from attackers who have perfect knowledge of the operation of their IoT endpoints.

Fortunately, this often boils down to following security best practices: enforcement of strong authentication for local users and administrators, strong encryption for data at rest, device authentication using unique, dynamically generated keys, and avoiding a reliance on hidden and ‘back door’ administrative accounts. Additionally, employing systems that allow for close monitoring of deployed devices, including logging of inbound communications (probing), device configuration changes, and local authentication attempts can ensure that efforts to compromise IoT devices in the field don’t escape notice.

5. Secure Device Connections

Communication between IoT devices, applications and back-end services should be secured using Secure Socket Layer/Transport Layer Security Protocol (SSL/TLS) encryption, as with other sensitive online transactions. Beyond that, IoT management interfaces and applications need to be designed to throw off brute-force authentication attacks and set a high bar for user and administrator provisioning to make trivial account compromises such as default administrator credentials (or password-guessing attacks) impossible.

Finally, logging changes and activities on endpoints and management servers are a must for customers and business partners to understand the scope and impact of adverse events in the field.

6. Secure IoT Services and Apps

As noted earlier, the hosted cloud services that form the back end for IoT deployments represent a potential rich target for attackers.

Improperly designed and configured cloud-based services are susceptible to attacks both from internal and external sources.

Application-based hacks such as SQL injection or cross-site scripting can be used to gain privileged access to management interfaces as well as carry out denial-of-service attacks. Insecure web interfaces can also be used to compromise accounts directly via attacks on user authentication interfaces that guess user credentials (so called “brute force” attacks) or serial requests to identify valid credentials (account enumeration.)
The same is true of applications that are used to access IoT management interfaces via mobile apps or web browsers. Like the services they connect to, mobile apps and web-based GUIs are susceptible to brute-force password guessing attacks and theft of credentials through “man in the middle” and other snooping attacks. Both mobile and traditional “PC” platforms are also susceptible to malicious software infections, making local data theft and interception — or manipulation of session traffic — a possibility.

To minimize these risks, robust procedures are required during initial design and subsequent maintenance of IoT products and services to identify security vulnerabilities in core and third-party software and libraries. In addition, application program interfaces (APIs) used by IoT applications need to be vetted to ensure that no unauthorized “backdoor” accounts can provide unauthorized, administrative access to IoT deployments.

Finally, encryption of data at rest on IoT applications and cloud services is required to protect inadvertent data leaks or to limit the downstream impact of a compromise of the IoT cloud application.

The proliferation of third party services and data with IoT deployments greatly adds to the security challenge in this area. Consider in advance how you will support potential partner connections and feeds and how you will manage access and entitlements for business partners, contractors, and outside providers.

7. Secure Users and Access

It should go without saying that the diversity of end points and services that define the Internet of Things creates new and challenging use cases that must be supported. For example: A “smart city” deployment focused on garbage collection may need to accommodate everyone from smartphone-carrying citizens, to sanitation workers charged with emptying the containers, to data analysts employed by or working on behalf of the city.

As with traditional IT products and environments, careful thought needs to be given to user roles and entitlements during the design, development, and testing phases of a new IoT deployment.

Organizations that are developing a new IoT product or creating a “connected” version of an existing product need to consider the different use cases for the technology and the user roles that support those use cases. Simply making every user an administrator may make feature development simple and smooth deployment, but it could be a costly design decision once your product is deployed.

Good IoT product design ensures that user provisioning and de-provisioning are seamless and that products are infused with security best practices such as strong password creation and updating or multi-factor authentication (where possible). IoT devices, supporting infrastructure, and control systems should also support multiple user roles with granular permissions that can be adjusted to suit a variety of predetermined use cases. Consider which user-interface features and what data should be accessible to different users, and enforce access policies consistently throughout your product ecosystem.
LOOKING AHEAD

As companies embrace the Internet of Things, the need to secure the newly connected billions of devices and the entire IoT ecosystem creates a set of questions and potential obstacles to broad IoT adoption. Companies anxious to accelerate their IoT initiatives must focus on, and invest in, a comprehensive and thoughtful approach to security in order to minimize business risk and maximize return on investment.

This guide provides a starting point for discussions as well as seven specific steps that companies should take as part of the design, development, and implementation of an IoT strategy or solution. Organizations should use the guidelines presented in this document to begin building a solid foundation of security at the cloud, device, application, and service levels that supports the reliable expansion of IoT products and services.

Fortunately, IT leaders and providers of cloud services have a tremendous base of experience with many of the security approaches and measures outlined in this paper. The challenges over the next few years will surely be more expansive and complex than those focused on traditional IT, but companies that apply the best practices of the past to the broader IoT ecosystem of the future should be well served indeed as they explore the vast new opportunities that will emerge in the years to come.

ABOUT PTC CLOUD SERVICES

PTC Cloud Services has more than 15 years of experience helping clients realize the full value of their solution investment by placing hosting and application management in the hands of the experts. With hundreds of IoT deployments already under management, PTC Cloud Services professionals have the know-how and experience to help design, manage, and continually optimize your IoT operations, security, and environment. They ensure consistent application availability with proactive monitoring, performance tuning, and speedy issue resolution with immediate access to PTC R&D and technical support.

Talk to an expert or learn more at PTC.com/go/cloud.