Microsoft

Securing your Internet of Things from the ground up

Comprehensive built-in security features
of the Microsoft Azure IoT Suite

Executive Summary

The Internet of Things (IoT) poses unique security, privacy, and compliance challenges to businesses worldwide. Unlike traditional cyber technology where these issues revolve around software and how it is implemented, IoT concerns what happens when the cyber and the physical worlds converge. Protecting IoT solutions requires ensuring secure provisioning of devices, secure connectivity between these devices and the cloud, and secure data protection in the cloud during processing and storage. Working against such functionality, however, are resource-constrained devices, geographic distribution of deployments, and the large number of devices within each solution.

This paper explores how the Microsoft Azure IoT Suite provides a secure and private Internet of Things cloud solution. The Azure IoT Suite delivers a complete end-to-end solution, with security built into every stage from the ground up. At Microsoft, developing secure software is part of the software engineering practice, rooted in our decades long experience of developing secure software. To ensure this, Software Development Lifecycle (SDL) is the foundational development methodology, coupled with a host of infrastructure-level security services such as Operational Security Assurance (OSA) and the Microsoft Digital Crimes Unit, Microsoft Security Response Centre, and Microsoft Malware Protection Centre.

The Azure IoT Suite offers unique features which make provisioning, connecting to, and storing data from IoT devices easy and transparent and, most of all, secure. In this paper we examine the Azure IoT Suite security features and deployment strategies to ensure security, privacy and compliance challenges are addressed.

We've organised the paper to touch on the following subjects:

- **Introduction**. An understanding of the major security issues inherent to any IoT solution and recommendations for what to consider when looking for an IoT solution provider.
- **The value of the Microsoft Trusted Cloud**. A discussion detailing Microsoft's established history as a trusted cloud provider and the cloud features that support security in the design of all of Microsoft's software and cloud services.
- **The comprehensive components that make the Azure IoT Suite unique within the marketplace**. We explore Azure as a trusted platform with built-in security, compliance, privacy, transparency and control features. We then look at how individual components within this platform together form the foundation for the Azure IoT Suite. We then take a deeper dive into how these pieces deliver secure device provisioning, connectivity, processing and storage.
- **Securing your infrastructure**. Using the Azure IoT Suite and Microsoft technology, we offer prescriptive advice and best practices to follow to ensure IoT deployments keep businesses safe and sound.

Introduction

The Internet of Things (IoT) is the wave of the future, offering businesses immediate and real-world opportunities to reduce costs, increase revenue, and transform their business. Many businesses, however, are hesitant to deploy IoT in their organisations due to concerns about security, privacy and compliance. A major point of concern comes from the uniqueness of the IoT infrastructure, which merges the cyber and physical worlds together, compounding individual risks inherent in these two worlds. Security of IoT pertains to ensuring the integrity of code running on devices, providing device and user authentication, defining clear ownership of devices (as well as data generated by those devices), and being resilient to cyber and physical attacks.

Then, there's the issue of privacy. Companies want transparency concerning data collection, as in what's being collected and why, who can see it, who controls access, and so on. Finally, there are general safety issues of the equipment along with the people operating them, and issues of maintaining industry standards of compliance.

Given the security, privacy, transparency and compliance concerns, choosing the right IoT solution provider remains a challenge. Stitching together individual pieces of IoT software and services provided by a variety of vendors introduces gaps in security, privacy, transparency, and compliance which may be hard to detect, let alone fix. The choice of the right IoT software and service provider is based on finding providers which have extensive experience running services which span across verticals and geographies, but are also able to scale in a secure and transparent fashion. Similarly, it helps for the selected provider to have decades of experience with developing secure software running on billions of machines worldwide, and have the ability to appreciate the threat landscape posed by this new world of the Internet of Things.

Microsoft – a secure infrastructure from the ground up

The Microsoft Cloud infrastructure supports more than one billion customers in 127 countries. Drawing on our decades-long experience building enterprise software and running some of the largest online services in the world, we provide higher levels of enhanced security, privacy, compliance and threat mitigation practices than most customers could achieve on their own.

Our Security Development Lifecycle (SDL) provides a mandatory company-wide development process that embeds security requirements into the entire software lifecycle. To help ensure that operational activities follow the same level of security practices, we use rigorous security guidelines laid out in our Operational Security Assurance (OSA) process. We also work with third-party audit firms for ongoing verification that we meet our compliance obligations and we engage in broad security efforts through the creation of centres of excellence, including the Microsoft Digital Crimes Unit, Microsoft Security Response Centre and Microsoft Malware Protection Centre.

Microsoft Azure – a secure IoT infrastructure for your business

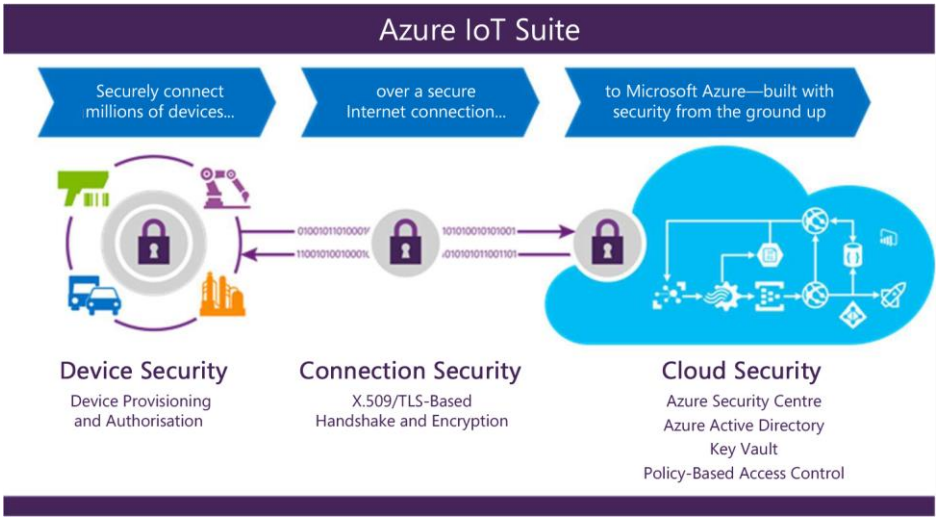
Microsoft Azure offers a complete cloud solution, one that combines a constantly growing collection of integrated cloud services—analytics, machine learning, storage, security, networking and web—with an industry-leading commitment to the protection and privacy of your data. Our assumed breach strategy uses a dedicated "red team" of software security experts who simulate attacks, testing the ability of Azure to detect, protect against emerging threats, and recover from breaches. Our global incident response team works around the clock to mitigate the effects of attacks and malicious activity. The team follows established procedures for incident management, communication, and recovery and uses discoverable and predictable interfaces with internal and external partners.

Our systems provide continuous intrusion detection and prevention, service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. Multi-factor authentication provides an extra layer of security for end users to access the network. And for the application and the host provider, we offer access control, monitoring, anti-malware, vulnerability scanning, patches and configuration management.

The Microsoft Azure IoT Suite takes advantage of the security and privacy built into the Azure platform along with our SDL and OSA processes for secure development and operation of all Microsoft software. These procedures provide infrastructure protection, network protection, and identity and management features fundamental to the security of any solution.

The Azure IoT Hub within the IoT Suite offers a fully-managed service that enables reliable and secure bi-directional communication between IoT devices and Azure services such as Azure Machine Learning and Azure Stream Analytics by using per-device security credentials and access control.

To best communicate security and privacy features built into the Azure IoT Suite, we've broken down the suite into the three primary security areas.



Secure device provisioning and authentication

The Azure IoT Suite secures devices while they are out in the field by providing a unique identity key for each device, which can be used by the IoT infrastructure to communicate with the device while it is in operation. The process is quick and easy to set up. The generated key with a user-selected device ID forms the basis of a token used in all communication between the device and the Azure IoT Hub.

Device IDs can be associated with a device during manufacturing (i.e. flashed in a hardware trust module) or can use an existing fixed identity as a proxy (e.g. CPU serial numbers). Since changing this identifying information in the device is not simple, it is important to introduce logical device IDs in case the underlying device hardware changes, but the logical device remains the same. In some cases, the association of a device identity can happen at device deployment time (i.e. an authenticated field engineer physically configures a new device while communicating with the IoT solution backend). The Azure IoT Hub identity registry provides secure storage of device identities and security keys for a solution. Individual or groups of device identities can be added to an allow list, or a block list, enabling complete control over device access.

Azure IoT Hub access control policies in the cloud enable the activation and disabling of any device identity, providing a way to disassociate a device from an IoT deployment when required. This association and disassociation of devices is based on each device identity.

Additional device security features include the following:

- Devices do not accept unsolicited network connections. They establish all connections and routes in an outbound-only fashion. For a device to receive a command from the backend, the device must initiate a connection to check for any pending commands to process. Once a connection between the device and IoT Hub is securely established, messaging from the cloud to the device and device to the cloud can be sent transparently.
- Devices only connect to or establish routes to well-known services with which they are peered, such as an Azure IoT Hub.
- System-level authorisation and authentication use per-device identities, making access credentials and permissions near-instantly revocable.

Secure connectivity

Durability of messaging is an important feature of any IoT solution. The need to durably deliver commands and/or receive data from devices is underlined by the fact that IoT devices are connected over the Internet, or other similar networks which can be unreliable. Azure IoT Hub offers durability of messaging between cloud and devices through a system of acknowledgments in response to messages. Additional durability for messaging is achieved by caching messages in the IoT Hub for up to seven days for telemetry and two days for commands.

Efficiency is important to ensure conservation of resources and operation in a resource-constrained environment. HTTPS (HTTP Secure), the industry-standard secure version of the popular http protocol, is supported by Azure IoT Hub, enabling efficient communication. *Advanced Message Queuing Protocol* (AMQP) and *Message Queuing Telemetry Transport* (MQTT), supported by Azure IoT Hub, are designed not only for efficiency in terms of resource use, but also reliable message delivery.

Scalability requires the ability to securely interoperate with a wide range of devices. Azure IoT hub enables secure connection to both IP-enabled and non-IP-enabled devices. IP-enabled devices are able to directly connect and communicate with the IoT Hub over a secure connection. Non-IP-enabled devices are resource-constrained and connect only over short distance communication protocols, such as Zwave, ZigBee and Bluetooth. A field gateway is used to aggregate these devices and performs protocol translation to enable secure bi-directional communication with the cloud.

Additional connection security features include the following:

- The communication path between devices and Azure IoT Hub, or between gateways and Azure IoT Hub, is secured using industry-standard Transport Layer Security (TLS) with Azure IoT Hub authenticated using X.509 protocol.
- In order to protect devices from unsolicited inbound connections, Azure IoT Hub does not open any connections to the device. The device initiates all connections.
- Azure IoT Hub durably stores messages for devices and waits for the device to connect. These commands are stored for two days, enabling devices connecting sporadically, due to power or connectivity concerns, to receive these commands. Azure IoT Hub maintains a per-device queue for each device.

Secure processing and storage in the cloud

From encrypted communications to processing data in the cloud, the Azure IoT Suite helps keep data secure. It provides flexibility to implement additional encryption and management of security keys.

Using Azure Active Directory (AAD) for user authentication and authorisation, Azure IoT Suite can provide a policy-based authorisation model for data in the cloud, enabling easy access management that can be audited and reviewed. This model also enables near-instant revocation of access to data in the cloud and of devices connected to the Azure IoT Suite.

Once data is in the cloud, it can be processed and stored in any user-defined workflow. Access to each part of the data is controlled with Azure Active Directory, depending on the storage service used.

All keys used by the IoT infrastructure are stored in the cloud in secure storage, with the ability to roll over in case keys need to be re-provisioned. Data can be stored in DocumentDB or in SQL databases, enabling definition of the level of security desired. Additionally, Azure provides a way to monitor and audit all access to your data to alert you of any intrusion or unauthorised access.

Securing an IoT Infrastructure

Securing an IoT infrastructure requires a rigorous security-in-depth strategy. Starting from securing data in the cloud, to protecting data integrity while in transit over the public internet, and providing the ability to securely provision devices, each layer builds greater security assurance in the overall infrastructure. This security-in-depth strategy can be developed and executed with active participation of various players involved with the manufacturing, development and deployment of IoT devices and infrastructure. The following is a high level description of these players.

- **IoT hardware manufacturer/integrator** – Typically these are the manufacturers of IoT hardware being deployed, hardware integrators assembling hardware from various manufacturers, or hardware suppliers providing hardware for an IoT deployment manufactured or integrated by other suppliers.
- **IoT solution developer** – The development of an IoT solution is typically done by a solution developer, which may part of an in-house team, or a System Integrator (SI) specialising in this activity. The IoT solution developer can develop various components of the IoT solution from scratch, integrate various off the shelf or open source components, or adopt pre-configured solutions with minor adaptation.
- **IoT solution deployer** – Once an IoT solution is developed, it needs to be deployed in the field. This involves deployment of hardware, interconnection of devices, and deployment of solutions in hardware devices, or in the cloud.
- **IoT solution operator** – Once the IoT solution is deployed, it requires long term operations, monitoring, upgrades and maintenance. This may be done by an in-house team comprising information technology specialists, hardware operations and maintenance teams, and domain specialists who monitor the correct behaviour of overall IoT infrastructure.

The following provides best practices for each of these players so as to develop, deploy and operate a secure IoT infrastructure.

IoT hardware manufacturer/integrator

- **Scope hardware to minimum requirements** – The hardware design should include minimum features required for operation of the hardware, and nothing more. An example is to include USB ports only if required for the operation of the device. These additional features open the device to unwanted attack vectors, which should be avoided.
- **Make hardware tamper proof** – Build in mechanisms to detect physical tampering of hardware, such as opening of device cover, removing a part of the device, etc. These tamper signals may be part of the data stream uploaded to the cloud enabling alerting of these events to the operators.
- **Build around secure hardware** – If COGS permit, build security features such as secure and encrypted storage and Trusted Platform Module (TPM) based boot functionality. These features make devices more secure protecting the overall IoT infrastructure.
- **Make upgrades secure** – Upgrading firmware during the lifetime of the device is inevitable. Building devices with secure paths for upgrades and cryptographic assurance of firmware version will allow the device to be secure during and after upgrades.

IoT solution developer

- **Follow secure software development methodology** – Developing secure software requires ground-up thinking about security from the inception of the project all the way to its implementation, testing and deployment. The choice of platforms, languages, and tools are all influenced with this methodology. The Microsoft Security Development Lifecycle provides a step-by-step approach to building secure software.
- **Choose open source software with care** – Open source software provides an opportunity to quickly develop solutions. When choosing open source software, consider the activity level of the community for each open source component. An active community ensures software will be supported; issues will be discovered and addressed. Alternatively, an obscure and inactive open source software will not be supported and issues will most probably not be discovered.
- **Integrate with care** – Many of the software security flaws exist at the boundary of libraries and APIs. Functionality which may not be required for the current deployment may still be available via an API layer. Making sure that all interfaces of components being integrated are secure ensures overall security.

IoT solution deployer

- **Deploy hardware securely** – IoT deployments may require hardware to be deployed in unsecure locations, such as in public spaces or unsupervised locales. In such situations, ensure that hardware deployment is tamper proof to the maximum extent. If USB or other ports are available on the hardware, ensure that these are covered securely. Many attack vectors can use these as an entry point for attacks.
- **Keep authentication keys safe** – During deployment, each device requires device IDs and associated authentication keys generated by the cloud service. Keep these keys physically safe even after the deployment. Any compromised key can be used by a malicious device to masquerade as an existing device.

IoT solution operator

- **Keep systems up to date.** Ensure device operating systems and all device drivers are updated to the latest versions. Windows 10 (IoT or other SKUs), with automatic updates turned on, is kept up to date by Microsoft, providing a secure operating system for IoT devices. For other operating systems, such as Linux, keeping them up to date ensures they are also protected against malicious attacks.
- **Protect against malicious activity.** If the operating system permits, place the latest anti-virus and anti-malware capabilities on each device operating system. This can help mitigate most external threats. Most modern operating systems, such as Windows 10 IoT and Linux, can be protected against this threat by taking appropriate steps.
- **Audit frequently.** Auditing IoT infrastructure for security related issues is key when responding to security incidents. Most operating systems, such as Windows 10 (IoT and other SKUs), provide built-in event logging that should be reviewed frequently to make sure no security breach has occurred. Audit information can be sent as a separate telemetry stream to the cloud service and analysed.
- **Physically protect the IoT infrastructure.** The worst security attacks against IoT infrastructure are launched using physical access to devices. Protecting against malicious use of USB ports and other physical access is an important safety and security practice. Logging of physical access, such as USB port usage, is key to uncovering any breach that may have occurred. Again, Windows 10 (IoT and other SKUs) enables detailed logging of these events.
- **Protect cloud credentials** – Cloud authentication credentials used for configuring and operating an IoT deployment are possibly the easiest way to gain access and compromise an IoT system. Protect the credentials by changing the password frequently and by not using these credentials on public machines.

Note that capabilities of different IoT devices vary. On the one hand, some devices may be full blown computers running common desktop operating systems, while on the other, some devices may be running very light-weight operating systems. The security best practices described above will be applicable to these devices in varying degrees. If provided, additional security and deployment best practices provided by the manufacturer of these devices should be followed.

Some legacy and constrained devices may not have been designed specifically for IoT deployment. These devices may lack the capability to encrypt data, connect with the Internet, provide advanced auditing, etc. In these cases, using a modern and secure field gateway to aggregate data from legacy devices may provide the security required for connecting these devices over the Internet. Field gateways in this case provides secure authentication, negotiation of encrypted sessions, receipt of commands from the cloud, and many other security features.

Conclusion

The Internet of Things starts with your things—the things that matter most to businesses. IoT can deliver amazing value to a business by reducing costs, increasing revenue and transforming business. Success of this transformation largely depends on choosing the right IoT software and service provider. That means finding a provider that not only catalyses this transformation by understanding business needs and requirements, but also provides services and software built with security, privacy, transparency and compliance as major design considerations. Microsoft has extensive experience with developing and deploying secure software and services and continues to be a leader in this new age of the Internet of Things.

The Microsoft Azure IoT Suite builds in security measures by design, enabling secure monitoring of assets to improve efficiencies, drive operational performance to enable innovation, and employ advanced data analytics to transform businesses. With its layered approach towards security, multiple security features and design patterns, Azure IoT Suite helps deploy an infrastructure which can be trusted to transform any business.

Appendix

Each Azure IoT Suite pre-configured solution creates instances of Azure services, such as the following:

- **Azure IoT Hub:** Your gateway that connects the cloud to "things". You can scale to millions of connections per hub and process massive volumes of data with per-device authentication support helping you secure your solution.
- **Azure DocumentDB:** A scalable, fully-indexed database service for semi-structured data that manages metadata for the devices you provision, such as attributes, configuration and security properties. DocumentDB offers high-performance and high-throughput processing, schema-agnostic indexing of data and a rich SQL query interface.
- **Azure Stream Analytics:** Real-time stream processing in the cloud that enables you to rapidly develop and deploy a low-cost analytics solution to uncover real-time insights from devices, sensors, infrastructure and applications. The data from this fully-managed service can scale to any volume while still achieving high throughput, low latency and resiliency.
- **Azure App Services:** A cloud platform to build powerful web and mobile apps that connect to data anywhere; in the cloud or on-premises. Build engaging mobile apps for iOS, Android and Windows. Integrate with your Software as a Service (SaaS) and enterprise applications with out-of-the-box connectivity to dozens of cloud-based services and enterprise applications. Code in your favourite language and IDE—.NET, NodeJS, PHP, Python or Java—to build web apps and APIs faster than ever.
- **Logic Apps:** The Logic Apps feature of Azure App Service helps integrate your IoT solution to your existing line of business systems and automate workflow processes. Logic Apps enables developers to design workflows that start from a trigger and then execute a series of steps—rules and actions that use powerful connectors to integrate with your business processes. Logic Apps offers out-of-the-box connectivity to a vast ecosystem of SaaS, cloud-based and on-premises applications.
- **Blob storage:** Reliable, economical cloud storage for the data that your devices send to the cloud.