



Internet of Things Platform

Petr Leština

Petr_lestina@cz.ibm.com



Watson IoT Platform is a foundation for our industry solutions and IoT business use cases

IoT Industry Solutions

Enterprise Asset Management

Production Quality Insights

Worker Insights

Facilities Optimization

Building Insights

Facilities Management

Asset Performance Management

Production Optimization

Inventory Optimization

Watson Assistant Solutions

Continuous Engineering

Watson IoT Platform

Integrated managed service with SLAs and unified per device pricing

Connection Service

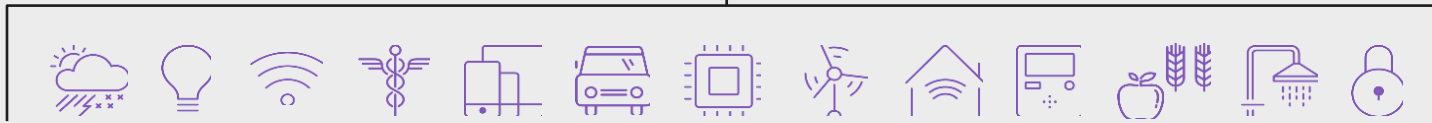
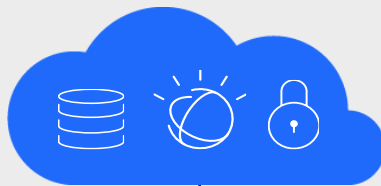
Securely connect and store

Analytics Service

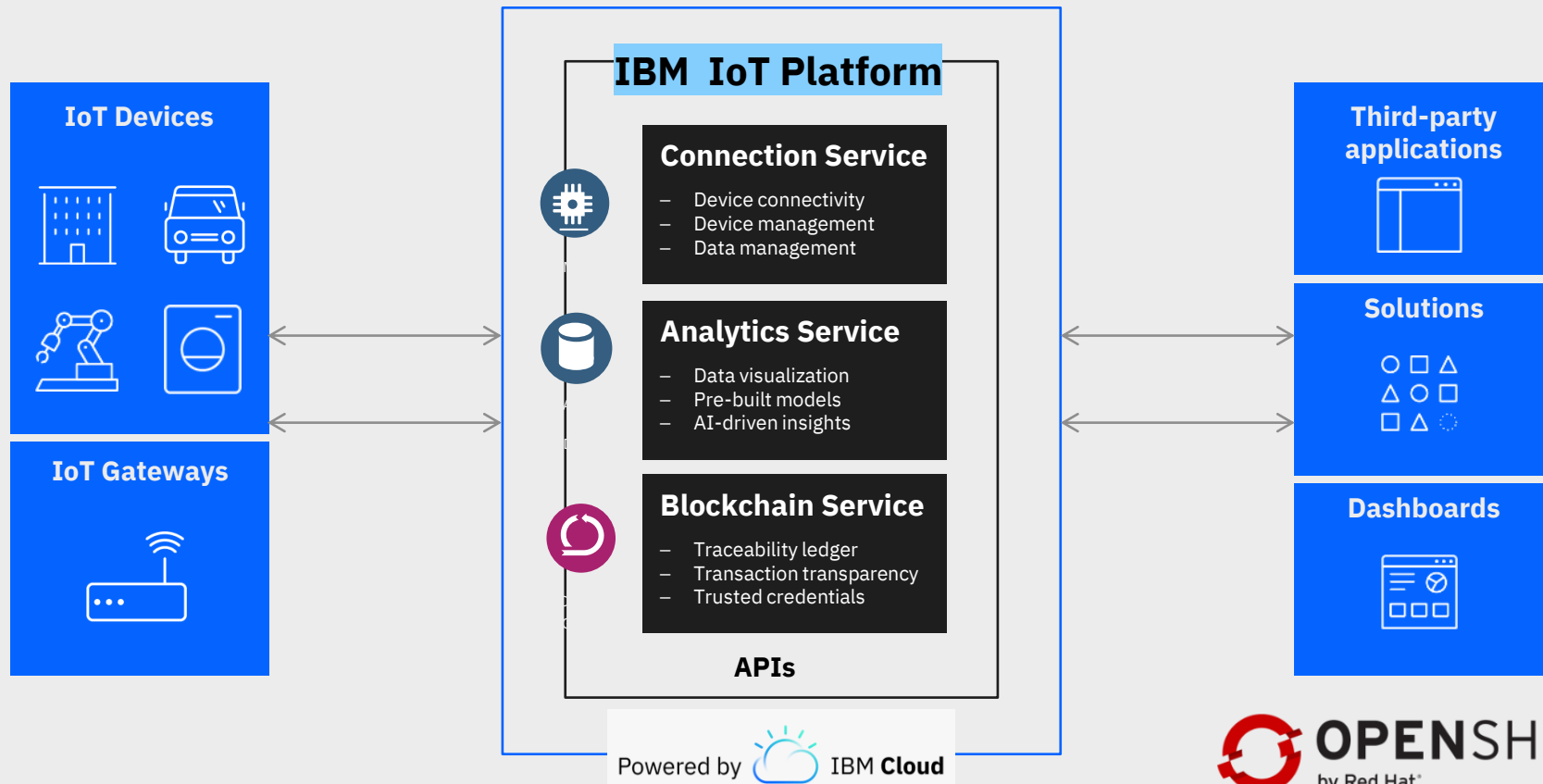
Explore AI-driven insights

Blockchain Service

Govern and deliver



IBM IoT & IBM Cloud



Watson IoT Platform is improving outcomes in key industries



Manufacturing

L'ORÉAL

increased 10% equipment effectiveness (OEE) and 20% operational efficiency



increased production by 10% by predicting issues and avoiding downtimes

Whirlpool

improved quality by 50% and achieve 90% on time delivery



Transportation



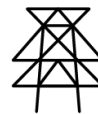
Saving up to \$80,000 a day in shipping costs



Reduce maintenance cost of tracks and trains by 10X



5% improvement in unloading times and vessel utilization



Utilities



Prevent contamination in 40% of tanks with early detection



Saving up to 20% in energy costs to customers



Increase rig utilization by 5% by increasing efficiencies across their fleet

Watson IoT Platform:

Flexible deployment for Industrial Use Cases



Public Cloud

Publicly hosted SaaS
IoT Platform that is
fully managed with
SLA for production use



Private Cloud

A contained and functional data center

Speed of public, control
of private using
containerized
applications for flexibility



Hybrid Approach

Provides both on and offline responses

Combine public and
private and optimize the
IoT data sent,
processed and analyzed

Watson IoT Platform:

Privacy and Security by design

IBM: A global leader in enterprise security

- 8000+ employees, 133 countries, 3,500+ security patents and 20 acquisitions since 2002

IBM Cloud Security and Privacy focus

- Proactive protection: Multi-layer Security Strategy
- IBM Data Policy – Customers owns all Data
- Secure Device to Cloud communication via TLS and device certificate support
- Resource level access control for administration and device control
- Support integration with QRadar for displaying IoT device status

IBM provides Chip to Cloud IoT Security through Partners, Solutions and IoT Platform

- Collaboration with silicon producers and chip designers (ARM, NXP, WISeKey)
- Expertise in Security in IoT, for example **IBM X-Force Red penetration testing**
- Secure by design Watson IoT Platform with Advanced Security policies and dashboard

IBM is the Leader in IoT Security

- Leadership Presence in IoT Security Foundation, IoT Cybersecurity Alliance, and other IoT industry bodies
- IBM Developed & Published IoT Security Best Practices for device and solution creators
- IBM Surveyed 700 Industry Executives: identified 9 practices that differentiate top IoT security performers

Five indisputable facts about IoT security

Some concepts have long been accepted as universal truths. Among the most familiar of those: Sir Isaac Newton's laws of motion, which date back to the 17th century. Today, however, there are new principles defining how technologies will behave in specific situations. For example, the proliferation of Internet of Things (IoT) devices has generated serious concerns for IT security. And that's led us to identify five indisputable facts you need to know about IoT security.

1 Devices will operate in hostile environments

Unlike the mobile phones, tablets and laptops we use and carry with us virtually every day, IoT devices often operate without human supervision. So it's important that IoT devices, such as remote office temperature controls, must be both rugged and resistant to physical tampering. At the same time, they need to be able to recover from an attack and fall safely by degrading to an acceptable processing level—all without requiring human intervention. While cognitive security solutions can handle many threats and attacks, administrators of IoT deployments also need the visibility and control to deal with exceptional situations.



2 Software security will degrade over time

All software in use must be kept updated. And when it comes to IoT sensors and devices, the patching process typically takes place in very distributed, highly uncontrolled environments—at an enormous scale. But even if all known vulnerabilities are addressed with the first release, new exposures and vectors for attack will almost certainly be discovered. The risk of attack increases with the length of time the equipment remains in service. That means system designers will need to be updated repeatedly—for the life of these devices—impacting the supply chain for both software and equipment.



3 Shared secrets do not remain secret

A sizable number of IoT devices come preloaded with identical credentials across multiple devices. Although these default credentials should be changed by users before the devices are made operational, they've often left as is. Default secrets aren't secret. Attackers can use them to take over such devices for unintended purposes, making them vulnerable to sabotage or denigration. By delivering devices that prompt for a mandated password change upon first use, however, manufacturers can help ensure that default credentials can't persist—and that secrets will remain secret.



4 Weak configurations will persist

The default configuration of an IoT device will usually remain in place because it takes thought and effort by users to change it. If the default settings for a given device have access control turned off, for example, it's left up to the owner to take measures to improve that security. Instead, security options should be enabled either by default or as part of an initial setup process, so that users are required to make a conscious decision to remove the default protections.



5 As data accumulates, exposure issues will increase

One of the key business drivers for IoT is the data that's generated from devices and solutions. That puts the spotlight on data security—along with how it's created, used and deleted. Over time, connections between different, seemingly disparate datasets may emerge. IoT devices are accumulating massive amounts of personal and sensitive data, including everything from audio recordings and transcripts to GPS locations and heart rate readings. If the data isn't managed, secured and destroyed when it's determined to be worth less than the risk of holding on to it, the results may lead to loss of privacy and to issues of data ownership—all of which increase the importance of partnering with IoT vendors and solution providers who can be trusted with your data.



Get the facts about what you can do

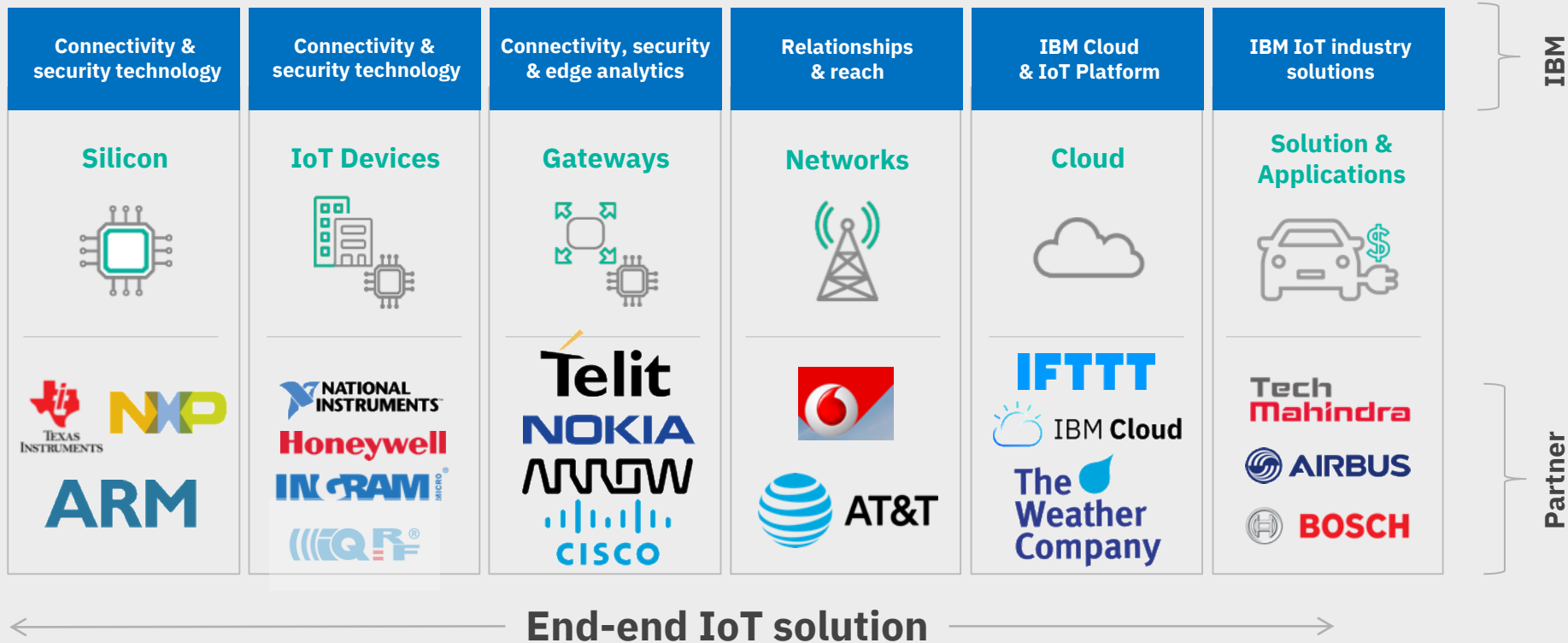
To learn more about how IBM can help your organization create a more secure environment for taking advantage of IoT technology, visit: ibm.com/iot/security



Watson IoT is defining open source and standards



Watson IoT provides end to end solutions with strong industry partnerships across the IoT landscape



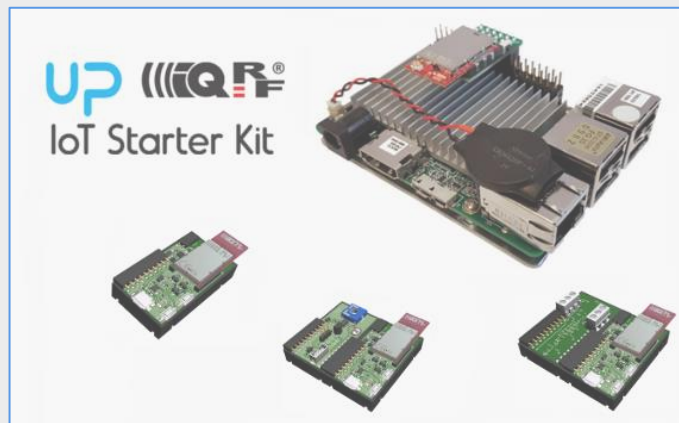
IBM & IQRF Offering

Internet of Things Platform on IBM Cloud and [UP-IQRF IoT Starter Kit](#)



- Includes up to **500** registered devices, and a maximum of **200** MB of each data metric
- Maximum of 500 application connections
- Maximum of 200 MB of each of data exchanged, data analyzed and edge data analyzed

Sign up here <http://ibm.biz/cloud-4-dev>



<https://www.iqrfalliance.org/marketplace/ibm-cloud>

