FUJITSU

White paper

Why managed services and security underpin IoT in a hyperconnected world

The Internet of Things (IoT) is here, now. And every organization is grappling with both the opportunities and challenges it presents. How your organization responds could spell the difference between success and failure.

Introduction

The Internet of Things (IoT) is here, now. And every organization is grappling with both the opportunities and challenges it presents. How your organization responds could spell the difference between success and failure.

The IoT opportunity is driving enormous levels of innovation. However, it's not easy to build a realistic, pragmatic business plan for delivering secure and managed IoT solutions. Thanks to its breadth of digital experiences, technical innovation and work in key technology and business markets, Fujitsu understands these issues and knows how to securely manage and resolve IoT challenges in partnership with customers.

Imagine the ideal business world. Your organization knows exactly what's going on with every piece of equipment in real time, so you can fix any problem immediately – or before it becomes a problem. Any customer can at any moment let you know if they are unhappy with something, allowing you to address concerns on the spot. And no matter where or what time employees are working, you can provide them with the help they need right away.

These are the sorts of fast, responsive, hyperconnected customer-first benefits that are possible with the Internet of Things. But no two enterprises are alike. That means there's no one single way of deploying an IoT program that works for all enterprises.

Whatever type of system your organization ultimately ends up deploying, management and security will always be vitally important considerations. After all, a complex, highly connected IoT infrastructure can only be as effective as its weakest link. All the many different elements must be managed well for optimal performance. And, because an IoT system by definition connects devices and things to the network, every one of those elements must also be adequately protected against today's all-too-common threats and free of the vulnerabilities they target.

It is still early days for enterprise-focused IoT programs but Fujitsu is already helping many large customers to deploy pilots or full-scale projects for a variety of applications. What follows is an overview of what we have learned about effective management and security for enterprise IoT.

Evolution of IoT services and security

The term 'Internet of Things' can cover a wide range of territory, from long-established applications to speculative, yet-to-be-tested technologies.

If we consider an IoT system to consist of networked devices and machines that can be remotely controlled, and that can in turn provide performance information and other data back to the controller, it's clear that such systems are nothing new. Manufacturers, utilities, telecommunication companies and other organizations have been using such systems for decades now. These systems have advanced to ever-more sophisticated, digital methods and today we are just a few years away from seeing billions of devices of all kinds connected to the network for all sorts of purposes[1]. These include not just enterprise servers and PCs but tablets, smartphones, industrial machines, electricity meters, water meters, closed-circuit security cameras, streetlights, traffic lights, motion sensors and even meeting rooms, parking spaces and streets.

Ever-smaller, more powerful and more energy-efficient processors make it possible today to attach a chip to almost any kind of device for a nominal cost. The plus side of this is that almost anything that can be equipped with a processor can become connected and even, to some extent, 'intelligent'. The downside is that such low-cost chips come with equally low-cost built-in security – or no security at all. This is likely to result in one or both of the following scenarios:

- Ultra-low-cost devices that cannot be updated and present security risks
- A highly heterogeneous and distributed pool of devices that bring added complexity for service management, with varied update/patching regimes and impact, particularly on incident, change and release management.

While we are likely to see development in 'embedded' security that is built into a device, many layers will exist beneath the IoT device layer. As a result, the service management regime will need to shift to greater levels of integration and automation to stay in contact with the threat landscape and provide a more proactive managed service in real time.

Organizations need to recognize the risks and challenges associated with IoT deployments, and work out what is acceptable and what is not. They will also need to decide how they will manage sensors, devices and gateways over the lifetime of solutions, not just during the deployment phase. This means giving serious consideration to the management of incident, change and release processes, with a specific emphasis on managed security.

Fujitsu's expertise in IoT deployments enables it to work with customers to build in security from the start, while also planning for ongoing updates and management over the lifetime of a system. Fujitsu has helped numerous customers deploy IoT systems effectively and securely by following several key principles.

The process begins by clearly defining the desired business outcomes, then identifying the main challenges and creating a blueprint for implementation. Next, after defining an IoT innovation roadmap for a customer, Fujitsu can work to deliver an effective program that includes security services, assurance and well-orchestrated service management. Backed by Fujitsu's deep experience in IT security, infrastructure and enterprise services, this step-by-step process maximizes an organization's prospects of success in any IoT project.

IoT in real life

IoT technologies today continue to evolve dramatically, and there is no 'one-size-fits-all' solution. So any enterprise looking to deploy a system of connected, automated and intelligent devices must be careful to stay focused on several key considerations.

First, always start with your primary business challenge. While many different IoT applications are possible, not all of them will be right for your organization. The projects with the greatest potential for success will be created to achieve specific outcomes.

[1]Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 per cent from 2016, and will reach 20.4 billion by 2020. From Feb. 7, 2017, http://www.gartner.com/newsroom/id/3598917

One good way to approach this challenge is by not thinking about IoT at all. Instead, focus on your organization's needs and goals, then ask what data, devices and applications can help meet those needs in a way that best serves your customers, employees and other stakeholders.

For example, one transport and logistics company Fujitsu works with had a key objective to improve safety of both drivers and the general population, as well as to ensure optimal delivery times. To achieve this, it is testing a system designed to detect when drivers become drowsy on the road. The pilot project uses wearable sensors to measure driver attention levels and issue alerts and reports when readings fall below safe, acceptable levels.

Another Fujitsu customer in healthcare was keen to improve how patients transition from intensive care into general care and, eventually, to be released to home. To achieve this, it is rolling out systems that measure physical data – everything from body temperatures to sleep patterns – for critical-care and stroke patients to deliver more personalized care based on real-time information and to reduce hospital stays.

Much like the Open Systems Interconnection (OSI) model, a seven-layer model that has underpinned much thinking in the network age, the IoT presents a layered challenge. Right now, much of the focus is upon the upper layers. However, in architecting an organization's IoT strategy, the layers below are also vital to success. Perhaps the most important layer is service management. This is the layer that will ultimately control and manage IoT capability, and it underpins the layers above. Fujitsu has ample experience in addressing this aspect, and it continues to invest in both service management and automation.

In both the earlier transport and healthcare examples, Fujitsu is helping organizations address the unique security issues those applications pose, to ensure that sensitive driver and patient information is protected. It is also ensuring that services are monitored, incidents are anticipated and addressed, upgrades are deployed and application releases are managed with minimal impacts. The solution in each case, however, differs considerably because of the special requirements of those particular industries. Other organizations in other sectors would also have different ways to address security and service management concerns.

Whatever industry you operate in, the key to a successful, secure and well-managed IoT deployment is to understand as best as possible your ecosystem, your organization and your infrastructure profile, as well as your customers' needs. Your unique security and service management considerations will depend upon the specifics of each.

For instance, the challenges for a system focused just on heating, ventilation and air-conditioning in an office complex will be considerably different from those for a smart city. A smart city will have many more public-facing infrastructure elements – security cameras, traffic lights, etc. – that increase the threat surface and critical protection requirements. There will be differing availability requirements and service levels, and complexity of change and release cycles will need to be managed as impacts can be critical.

Summary

Whatever system you end up deploying, it's important to make sure that, as much as possible, security and service considerations are built in from the start. After that, be sure you can keep an eye on things to know immediately – and respond immediately – when a security failure is detected. The right managed security service provider should also have a wealth of experience on which to draw, and should be able to support threat-hunting services that can detect both internal and external threats.

A well-run orchestration and managed service can help ensure that business operations are maintained without interruption. For example, Fujitsu offers end-to-end managed lifecycle services – from development and deployment of applications in agile ways, through deployment, upgrade and management of IoT devices (sensors, devices, gateways) and digital service desk support and engineering services – to ensure that customers can address concerns quickly and proactively.

While today we're seeing the greatest interest in IoT systems among utilities, manufacturers and transport companies, many more services will eventually apply to a wider range of industries. Looking ahead, we can envision new, hyperconnected business services that could enable great improvements in everything from disaster responses and waste management to medical care in underserved areas.

Whatever the application, it's important that organizations putting IoT technologies to use to become hyperconnected businesses of the 21st century do so securely, and in a well-managed way that helps them to achieve their goals and better serve their stakeholders. Fujitsu has the IT, automation, security, orchestration and managed services experience to help your business do just this.

Our goal is to help your organization plan, deploy and manage a secure and effective digital infrastructure so you can understand your world from a new perspective: a more data-driven, real-time, intelligent and networked perspective. That's the definition of a Fujitsu hyperconnected business.

To learn more visit www.fujitsu.com/global.

Contact
ASK FUJITSU
Tel: +44 (0) 1235 79 7711
E-mail: AskFujitsuHQ@ts.fujitsu.com
Ref: 3759

www.fujitsu.com/global