MEETING AT THE EDGE WITH VMWARE INTERNET OF THINGS (IoT)

A big benefit of IoT is its ability to connect people to the right systems and processes, and to measure the effectiveness of the same.

Introduction

The Internet of Things (IoT) is here and companies are starting to invest heavily in it to be the first in their industry to drive digital transformation. IoT-enabled solutions cover a wide array of business applications and use cases, powered by the ability to connect millions of devices to the Internet and take autonomous actions based on the information they generate. With this enormous potential, it's no wonder organizations are embracing IoT to bridge their physical and digital worlds.

279 Million Connected Vehicles by 2021

Manufacturing 1PB/factory per day

Global Wearable Medical Devices Market projected to double in growth by 2022

The Tidal Wave of IoT Opportunity

$255B
spend globally by 2019
~ Business Insider

27%
average revenue increase by 2018
~ Forbes

50 Billion things
will be connected to the internet by 2020

vmware Pulse™

Employees can connect the dots faster and unlock previously unnoticed opportunities.

Business Insider divides the IoT market into three main categories: consumer, enterprise and government. It also predicts that enterprise will be the largest sector (40%) because businesses have the scale and capital to not only purchase and deploy IoT but also to maintain it. It's not just Healthcare, Automotive, or Manufacturing who have traditionally led the charge with IoT that are investing, but all industries are noticing the benefits IoT brings to their processes, products, or experiences and are wholeheartedly embracing it.

There are many business benefits to implementing IoT.

Improve Business Agility

Due to the real-time nature of IoT and the fact that you now get so much more information from so many more data points, businesses now have access to perspectives and insights which were once hidden. This information boosts an organization's ability to adapt to changing internal and external environments quickly to gain an edge. Good examples of improved business agility are a faster time-to-market for an upcoming product, or a faster response time to customer behaviors and needs.

Power Business Processes

A big benefit of IoT is its ability to connect people to the right systems and processes, and to measure the effectiveness of the same. Because of this continuous monitoring and measurement, it's now easy to pinpoint inefficiencies and waste, and correct them to reduce costs or save time. This can be accomplished through improved asset utilization, improved worker productivity, or increased supply chain efficiency.

Boost Innovation and Growth

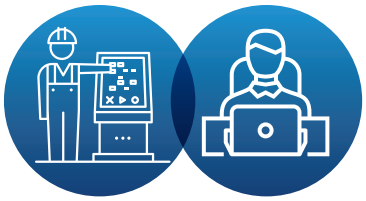
IoT's pervasiveness and inherent connectivity allows you to make sure that the right information reaches the right person or thing at the right time. This means employees can connect the dots faster and unlock previously unnoticed opportunities, whether it's a product idea based on a newly identified consumer need or the identification of a new customer segment for an existing product.

Enable Customer Experiences

With all these connected devices, there now exist many other touch points to gauge customer satisfaction, customer trends, and buying behavior. The insights generated by this information can help Marketing with more targeted initiatives, Sales with understanding customer consumption for cross-selling, and Customer Service with insights that bolster the customer experience in-store and post-sale. In addition, companies can offer new software or services to customers, such as a tractor company offering predictive maintenance services or a utility company offering new software to manage usage.

KEY TAKEAWAY

- OT & IT Must Meet at the Edge to Control It All



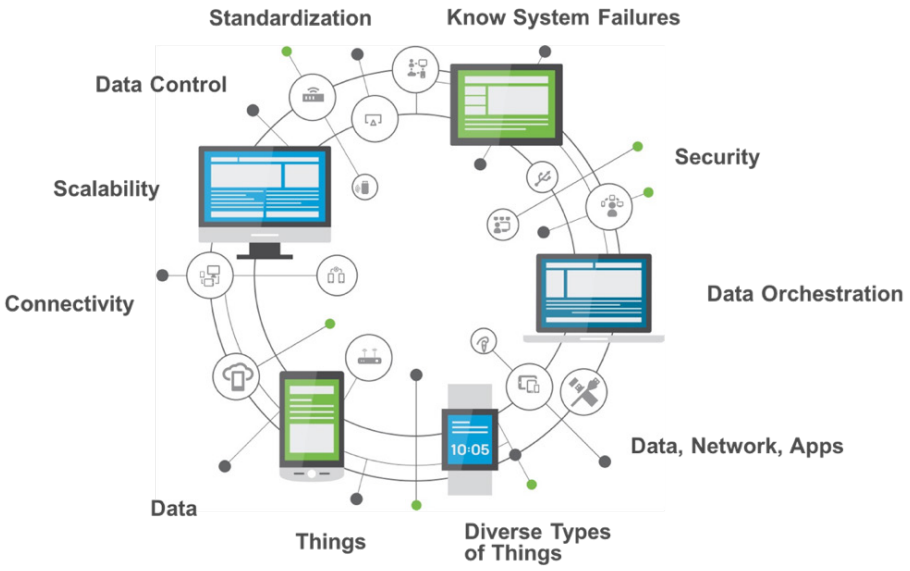
Challenges with the convergence of IT & OT

While the potential of IoT can only be realized by connecting the physical and digital worlds, it also mandates the convergence of information technology (IT) and operational technology (OT). From the beginning, the IT and OT organizations maintained separate goals and objectives requiring completely different skill set. The primary focus of the OT organization was to facilitate and support the operational aspects of a business through automation and management of mission-critical high-performing physical assets and equipment. IT, on the other hand, dealt mainly with the virtual world of the business by managing and securing systems responsible for finance and accounting.

Despite their historical differences, IoT is only possible if these industrial-grade OT equipment could smoothly transition to the internet and communicate to other devices on the same connection. These mission-critical OT equipment operate in harsh environments, remote locations, and were never designed to connect to the internet. Moreover, a strong resistance to change in both organizations and a serious lack of trust for each other, only exacerbates the problem. The impact of these two organizations operating separately not only poses a serious security risk but also slows down innovation, risking an enterprise to lose its competitive edge.

Challenges with Implementing IoT at an Enterprise Scale

Although most companies agree with and want the obvious benefits of implementing IoT, they struggle to put it to work because IoT is hard to implement on an enterprise scale. Companies run into issues including, but not limited to, the following:



"By 2020 more than 25% of identified attacks in enterprises will involve IoT, although IoT will account for less than 10% of IT security budgets." * ~Gartner

*GARTNER, ELIZABETH KIM, DEBORAH KISH, CHRISTIAN CANALES, RUGGERO CONTU, SID DESHPANDE, LAWRENCE PINGREE. FORECAST OVERVIEW: INFORMATION SECURITY, WORLDWIDE, 2016 UPDATE, AUGUST 31, 2016

Lack of Standardization

A "thing" in IoT is defined as any object with Internet connectivity. This could be a crane, a smart light, or even a living thing like a plant/animal/human. Given the diversity in the kinds of things, there's also a big difference in how they communicate. Hence, lack of standardization across IoT chips, components, data communication, and data formats is one of the biggest obstacles to IoT implementation. These new connected devices emit information in new formats that need to be managed alongside existing assets (which were never before connected to the Internet but now are) that transmit data in different formats. For intelligence to really work, all these smart devices need to speak a common language. Thus, having such a fragmented ecosystem makes it hard to choose and implement the right "thing."

Security is a Major Concern

According to Gartner, by 2020, more than 25% of identified attacks in enterprises will involve IoT, although IoT will account for less than 10% of IT security budgets. This makes sense, considering IoT has increased the attack surface area considerably. An unsecure connection could give a miscreant access to not just the confidential information transmitted by a particular device, but an enterprise's entire network. Apart from simple theft of corporate data, in some industries like healthcare or home automation these incidents could cause loss of life and human safety. When it comes to IoT, the concept of Multiple Points of Vulnerability applies, as you need to secure the device, the data within it, and its access protocol with your network.

Adaptability & Scalability

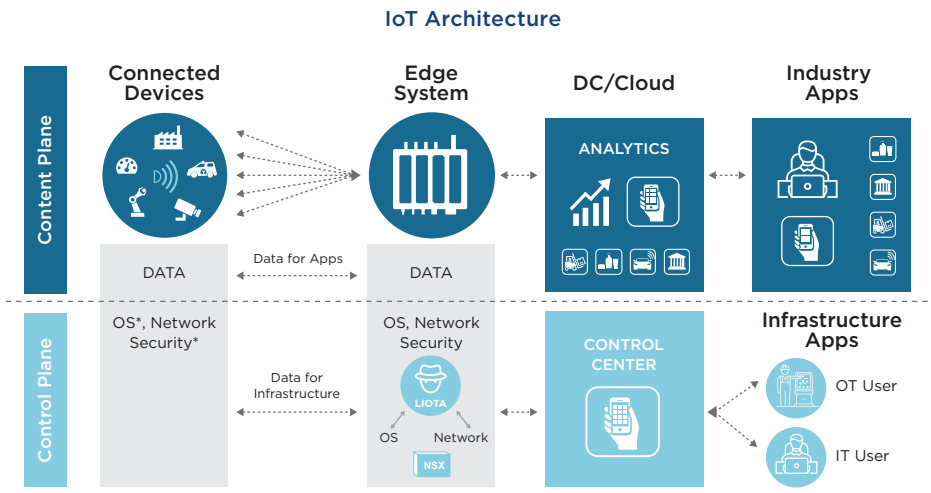
Adopting the Internet of Things will require a change in the way organizations design and architect their systems. Your architecture should be able to scale your expanding IoT use cases in thousands and even millions of units very quickly. At the same time, you have to continue supporting your legacy systems. Your infrastructure design should also be scalable enough to quickly add more devices/things to your systems amicably, in real time, as business needs expand.

Control Plane vs. Content Plane for IoT

As these millions of things start transmitting billions of bits of data, data management becomes a herculean task. Data storage costs go up exponentially and data mining capabilities struggle to keep up with data diversity. Where data will reside and be analyzed are other important considerations.

It's helpful to think of an IoT-ready architecture in terms of a content plane and a control plane. Control plane refers to the infrastructure, security, and management required to deploy an IoT use case from the things and from the edge to the cloud/datacenter. It's important to partner with your IT organization to ensure you have an architecture that will scale from a management and security perspective as more things are connected and more data is collected. The Content plane deals with the flow of data from the edge to the IoT platform/data center, where data is typically sorted, analyzed, and stored for business analytics and applications.

More and more companies are realizing for security, latency, bandwidth, and cost reasons that it doesn't make sense to push all data from devices into the cloud–especially when that data needs to be analyzed for an immediate need or decision. By processing data right at the edge to drive business outcomes, you gain faster results, minimize downtime, and save on bandwidth and storage costs. The right architecture for IoT balances the data analyzed or stored at or near the edge with the data analyzed and stored in the cloud. It's imperative to pick a solution that not only determines the right analytics/applications to meet the needs of your IoT use cases (Content plane) but also helps you manage the operational piece of IoT by securely onboarding, provisioning, configuring, maintaining, and monitoring things on an ongoing basis (Control plane). This is where VMware solutions for IoT come in.



"Through 2020, 90% of Internet of Things (IoT) projects will use some form of IoT gateway." * ~Gartner

*GARTNER, SANIYE BURCU ALAYBEYI, NICK JONES, EXPLORING THE ROLES OF IOT GATEWAYS IN FIVE EDGE USE CASES, AUGUST 8, 2016

Introducing VMware's IoT Solution

VMware Pulse is a family of IoT solutions fully equipped to address the above challenges and manage the Control plane in a cost-effective, secure way. We have two offerings that cover all your IoT operational, management, and infrastructure needs from the device to the edge.

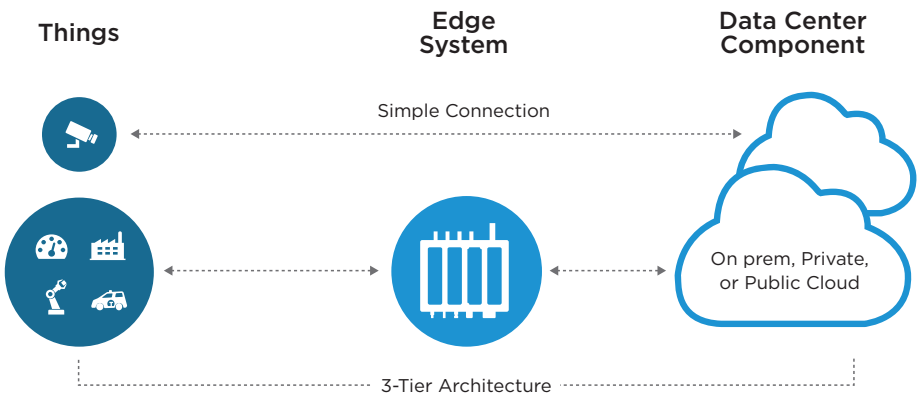
Project Pulse IoT

Pulse IoT is an end-to-end, single-console, Operational Management solution that helps OT (Operational Technology) and IT (Information Technology) onboard, manage, monitor, and secure all things throughout their lifecycle. Our solution helps you on-board edge systems (i.e., gateways) and their connected devices (i.e., sensors), collect telemetry from them, analyze the data stream to determine the operational health and status of the system or device, and maintain these with timely software updates. It also detects operational anomalies, takes action on them in real time, enables pushing content, applications, and configuration to the devices and systems, and controls their lifecycle.

> Introducing Liota - The Little IoT Agent

Little IoT Agent (Liota) is an open source SDK for IoT solution developers that resides primarily on IoT gateways/edge systems and collects preconfigured data from things. Liota is a critical part of Pulse IoT because it enables complete device lifecycle management on a diverse set of things and edge systems. Liota makes all your things heterogeneous and takes the guesswork out of managing their diverse protocols. It also performs data orchestration, which allows you to optimize data flow from the things to the edge and to the cloud, wherever it needs to go (i.e., Hadoop, SAP Hana, SalesForce, etc.). With Liota, Pulse IoT can be optimized to detect all edge systems and automatically on board them and get them configured to manage and monitor them in the future.

LIOTA™



vmware Pulse™

> Onboard

With Pulse IoT, you can enroll, register, and provision all your things/devices/end points (any OS, protocal, type of thing) from a single console, know their location, functioning status and software upgrade requirements, and share this view with your counterpart in IT so you're both clear on the status of the overall IoT use case. This way, if there are any issues with any of the things, they can be resolved in the most efficient, cost-effective way.

> Manage

After your things/devices/end points are onboarded and provisioned, they will need to be managed, over the air, on going until they are retired. This means the software will need to change and upgraded, bugs will need to be fixed, applications will need to be delivered to things and/or end users, and when anomalies occur action will need to be taken automatically or immediately. In addition OT and IT will want complete visibility of their things/devices and know their status at any given time.

Doing this without Pulse IoT would be a very costly and manual process. No thing or end point should ever be connected to the internet without proper management and security.

> Monitor

As an administrator, you can preconfigure rules to accurately detect anomalies and get a complete picture of the "health" of your things for anyone who needs it. You can also specify automated actions to be taken on these operational anomalies, over the air, in real time. This is especially critical to minimize costs and downtime because if something fails you can quickly identify the issue and fix the software over the air vs. physically going to where the thing resides to fix it.

> Secure

We offer best-in-class, enterprise-grade security with authentication, authorization and encryption of the device. We also provide mechanisms to keep your infrastructure's security level updated over time by helping push out on-demand security patches, upgrades, and updated configurations. Project Ice provides security not just at the thing level, but also at the network, app and user levels. For example, with Pulse IoT you can create a tunnel or micro-segmentation of data streams from the device to the gateways and from the gateways to datacenter/cloud in order to secure one data stream from another and one device from another.

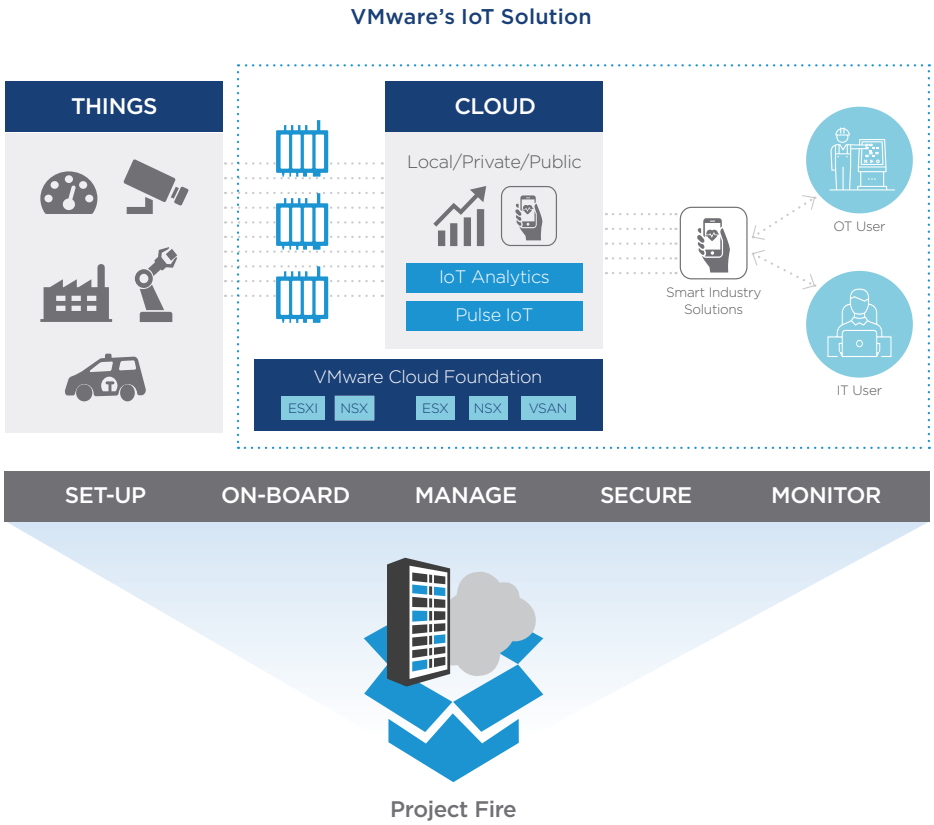
KEY TAKEAWAYS

- Reduce time and cost to deploy IoT by +6m
- Scale from PoC to production easily
- Optimize local analytics/data on-prem and in the cloud
- Speed up time to value with Pre-configured with Project Ice and Analytics
- Minimize risk of data leakage or security breaches

Project Fire

Implementing an IoT use case in your organization can be a daunting task. Most companies trying to embrace IoT struggle with how to get started quickly and efficiently, and how to deploy IoT with speed, efficiency and scale. It requires several steps to get started, including figuring out the right use case, choosing the correct data and things required, and determining the right infrastructure and architecture for the solution. Most companies want a solution that can be right at the edge, near their things, to minimize cost, latency, and security issues. In addition, companies need a way to build a PoC and deliver the necessary ROI before implementing it in their production environment so as to not disrupt the normal course of business.

Project Fire brings together Pulse IoT, VMware Cloud Foundation, and a partner IoT Analytics/Platform solution (like ThingWorx) into a complete, pre-integrated, preconfigured IoT "pop-up data center" that allows you to get started with your IoT use case in hours/days vs. months and scale it at the speed of your business. To be clear, Project Fire is not a bundling exercise but a truly integrated infrastructure platform built using best practices and pre-tested to ensure complete operability with your existing VMware infrastructure and set up to autmaticaly onboard your existing edge systems/gateways. The solution gets your IoT use cases up and running quickly, and helps balance your on-prem and cloud needs with your cloud provider of choice. It also helps you deploy IoT in an isolated environment that can scale as needed, away from your system of record, and minimizes risk of data leakage or security breaches.



vmware Pulse™

KEY TAKEAWAY

- VMware Will Meet You at the Edge to Help You Manage, Monitor, Secure and Optimize Your IoT Solution

Why VMware is the Right Choice for You

VMware is a recognized world leader in helping you run your business successfully from the desktop, to the data center, to the cloud. As enterprises prepare for the onslaught of upcoming IoT use cases, VMware IoT solutions ensure your business is ready to support them. With its core expertise in Device Management, Operational Analytics, Security, and Cloud Management, VMware is working with strategic IoT partners like Deloitte, ThingWorx, IBM, SAP, Dell, HP, and many niche IoT providers to help meet the needs of IoT across things, edge, and platforms. This provides customers with a one-stop, single-point solution. With VMware IoT solutions, you can:

Manage Broader

By managing millions of things as easily as one. VMware reduces your operational cost with a single control console to be used across OT and IT organizations, to on-board, manage, update, monitor, and secure your diverse IoT things and applications.

Operate Smarter

To minimize “thing” downtime and cost of failure. VMware IoT provides an accurate picture of “thing” health, as well as the ability to apply rules and act on anomalies as they arise, promoting efficiency and reducing operating costs.

Protect Better

To prevent and minimize security threats across things, data, networks, applications, and users. VMware solutions minimize data and network exposure and allow you to take timely action in case of breaches.

Innovate Faster

By speeding up IoT implementation in your enterprise and ensuring the right information is delivered to the right thing or person at the right time. This gives an edge to your enterprise to deliver innovations to market faster and to gain a competitive edge.

LEARN MORE

Visit us at http://www.vmware.com/solutions/iot

To become an early adopter customer and enjoy special benefits, please reach out to your VMware sales representative for more information.

Conclusion

Enterprise IoT is extremely hard to scale. Customers have to cobble together different heterogeneous offerings to make their IoT use cases work. Most solutions in the market focus on managing the "Content plane" but few focus on end-to-end management of the "Control plane" for IoT. With the diverse types of things, lack of standards, and remote locations of IoT in the "field," the amount of data that needs to be orchestrated to edge systems/clouds and the difficulty detecting anomalies in real time to understand the "health" of things is a major hindrance to successful IoT implementations in the enterprise. VMware IoT solutions address all of these challenges in flexible modules, in a way that meets the needs of your IT and OT organizations.

When looking at ways to improve your business with IoT scenarios, some of the most important decisions you'll make are the vendor and partners to work with. While there are many IoT vendors with conflicting messages, VMware has a clear strategy, a long history of success and trust in your current environment, and a global ecosystem of partners who are experts at managing the "Content plane." Working together, we can help your business unlock the potential of the IoT so you get a full, end-to-end IoT solution that works for you.

vmware®

Pulse™

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com