Flux7

Succeeding with the IoT-Ready Infrastructure

In this paper, enterprises that have embraced IoT share their lessons learned for building an IoT-ready cloud infrastructure that's future-proof.

It wasn't that long ago when the majority of Internet of Things (IoT) discussions were comprised of little more than pointing to a few edge IoT use cases, predictions, and outright hope regarding the promises of the technology. Today, IoT is moving from marketing to Main Street. And those companies that get it right will operate more effectively, break into new markets, and find new services their customers want.

At Flux7, we've helped numerous organizations build IoT architectures that do just this, helping deliver market advantage to the business all with an agile, secure, future-proof cloud based infrastructure. In this paper we will walk through important considerations and common challenges -- all based on our extensive hands-on experience. We'll discuss how to successfully design and deploy a winning IoT initiative, and then we'll bring it home with several Flux7 IoT case studies that illustrate when in action how these designs benefit the business.

Important Considerations and Common Challenges

When it comes to building successful IoT implementations, security, development, app design and operation processes must be considered from the beginning. Ongoing security and privacy concerns must be forever managed. And the right infrastructure must be not only secure, but elastic and agile enough to deliver innovation for many years to come. Tactical mistakes in designing and deploying this architecture can create massive headaches that are costly to fix; indeed, they can be more costly than building the infrastructure properly the first time.

Given these important considerations, let's take a look at several challenges to address early on to successfully design and deploy a winning IoT initiative as based on our years of experience building cloud-based IoT architectures across industries and for companies of all sizes:

- **Infrastructure:** Many enterprises try to build their IoT back-end systems on-premises, typically in a virtualized private cloud. They'll manage their virtual workloads, and manage the IoT platform and most of their network capacity in-house. There are significant challenges to this. The first is having to build enough capacity to handle the maximum potential bursts in usage that could arise. The networking and connectivity planning also have to be managed carefully.

  Configuration and version management is another potential challenge in that they are needed to help ensure code meets and maintains security and operational requirements. If something were to break without the operational processes and supporting technology to manage and maintain version and configuration control, the question "what changed" would go unanswered, greatly impacting problem resolution and project success.

Additionally, failing to design the right IoT infrastructure from the beginning often underpins organizations having to make future, rushed decisions to compensate for inadequate design. For instance, not having adequate elasticity can spur additional, and harried, capacity plans to quickly overcome that constraint. Such rushed decisions typically lead to overspending and a fragmented architecture.

Other types of mistakes that can be easily made once the infrastructure is off-course include developers realizing there is so much extra capacity in the data center that they are less rigorous in their work, and design oversized systems and deploy bloated code. Unnecessarily long, slow, and wasteful of resources, bloated code can create ongoing maintenance headaches that often result in missed deadlines and a loss of agility.

- **Vendor confusion.** The field of IoT vendors has expanded rapidly, and is continuing to grow daily. There are cloud infrastructure and platform providers that are making IoT solutions available. Networking equipment and appliance makers are doing the same, and there are a slew of dedicated point-product IoT vendors offering their tools as well. Gartner expects the IoT market to provide new market revenue of $300 billion by 2020. You should expect turbulence ahead as many of these smaller vendors are acquired and big standards battles are fought over time.

- **Connectivity.** Network connectivity is also crucial. The local area wired and wireless networks must be correctly designed, and they must be able to scale their capacity for the amount of traffic from IoT devices that they'll be carrying. When thousands of endpoints are transmitting, utilization can become quite high. And as is most often the case today, connectivity must extend far from the local network and into fields, factory floors, offices, and even roadways. Enterprises need to design their network and applications so that latency never becomes a problem, and so that bandwidth is adequate and expandable.

- **Keeping good processes in place.** When it comes to IoT, maintaining quality development processes is crucial. Here, agile testing methods and approaches to IT management such as DevOps are essential. Not only do such approaches keep new apps and features moving forward at a brisk pace; they also ensure software quality stays high. Updating and fixing IoT software is often costlier and more cumbersome than fixing or, to avoid duplication, updating software on servers and traditional endpoints.

- **Security.** All of the same challenges that apply to traditional software apps, servers, and endpoints apply to IoT devices and the data they generate. These devices can be breached, succumb to denial-of-service attacks, and the traffic can be snooped upon, copied, and even spoofed. None of those risks go away — in fact, the enterprise attack surface expands.

A successful IoT architecture can scale, and will offer a development pipeline that can provide for innovation, data analysis, and take whatever the future can throw at it.

Building a successful IoT implementation

When it comes to supporting their IoT infrastructure, many of our customers have embraced the cloud. Amazon Web Services (AWS) IoT is Amazon's managed cloud platform. AWS IoT enables enterprises to connect IoT devices that interact with other devices and their cloud applications. And it scales to trillions of messages originating from billions of devices. AWS IoT enables devices to communicate with applications and devices persistently, even when devices aren't connected.

AWS IoT also works well with AWS's established cloud ecosystem: AWS Lambda, Amazon Kinesis, Amazon S3, Amazon Machine Learning, Amazon DynamoDB, Amazon CloudWatch, AWS CloudTrail, and Amazon Elasticsearch Service. With Amazon Elasticsearch and built-in Kibana integration, enterprises can build IoT applications that gather, process, analyze, and act on data generated by connected devices.

AWS provides the following native capabilities:

Read and set device state at any time.
AWS IoT stores the latest state of a device so that it can be read or set at any time. This way, a device appears to applications as though it were persistently online.

Secure device connections and data.
AWS IoT provides authentication and end-to-end encryption throughout the connection. This way if a device isn't authentic, it won't be able to send or receive data with AWS IoT. AWS provides the ability to create very detailed permissions, as well.

Process and act upon device data.
With AWS IoT, enterprises can, based on self-defined rulesets, filter, transform, and act upon device data. And new devices, and rules and features can be implemented at will.

Flux7 Infrastructure for IoT Solutions

Flux7's experience with IoT solutions draws on our combined hardware and software knowledge, and from our focus on emerging technologies such as AWS IoT and containers like Docker. From our successes, we've created best practices to address the unique infrastructure challenges IoT applications create.

Scalability: Flux7-built infrastructure addresses the variable scaling needs IoT solutions often present. Whether there is seasonal variability or data must simply be sent at unusual hours or in unpredictable volumes, we use our knowledge of AWS's pricing and structure to:

1. Select the most efficient compute power

2. Automate failover and autoscaling

3. Smartly shut down unused instances

Security: We create systems using AWS' Security by Design security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing. Using these principles we build in features such as AMI hardening and encryption, incorporating third party solutions like Hashicorp Vault to ease the management of keys and other secrets.

Microservices infrastructure: IoT application developers must manage the leading edge of emerging security standards, aggressive feature wars and pressure to break new ground in delivering customer and business value. This dynamic mix makes IoT application development an ideal fit for a microservices approach. By breaking development into components, teams are able to work more autonomously, speeding time to market and enabling innovation by reducing the cost of experimentation. Our container-based microservices frameworks on AWS help enterprises enable this efficient development strategy.

Service Catalog: By creating push button solutions that meet application requirements, Flux7 service catalogs enable self-provisioning of AWS infrastructure and support an agile development model while reducing developer bottlenecks and ensuring secure, compliant builds every time.

To identify requirements and keep projects focused on clear deliverables, we work with our clients in three phases: Assess, Attune, and Engage. A lot of our "lessons learned" enable our engagements to move quickly, and then we apply a very extensive tool chain that Flux7 has built in-house. Here are our three phases:

- **The Assess Phase**

In this phase, Flux7 assesses the state of the environment, workflow, and business requirements, and then designs future technology, workflow, and the game plan to get there. Once we have the game plan, we optimize it into a course of action that makes the most sense for your specific organization's situation. In addition, as experts who work on the front edge of the IoT technology ecosystem, our experts help clear vendor confusion, recommending the best-fit solutions for your IoT implementation.

- **The Attune Phase**

Here, we execute on the plans developed during the Assess phase, and create the IoT architecture. It is a way for organizations to rapidly move forward on IoT initiatives. During this phase, Flux7 embeds Security by Design and DevOps principles to ensure quality from the outset and through the life of the solution.

- **The Engage Phase**

This phase comes after the enterprise has reaped some value from its IoT efforts, and is ready to internalize its own expertise to create the same architectures. To provide this knowledge transfer we follow a model familiar to anyone who has worked in the culinary industry. There, if one wants to learn from a culinary course they don't just sit in a class. They observe in the chef's kitchen for a few weeks, and then the students will cook and the chef will watch and guide them. We take the same approach and the goal is to get the customer involved as much as possible.

Cloud IoT in Action

A successful IoT infrastructure is secure, elastic, and agile, and is one that provides transparency into events. The communications network needs to be designed and built to provide optimal bandwidth for the job. While those attributes are the ideal end state, there's no one-sized IoT infrastructure template that will work for all enterprises. As a result, following are the stories of several enterprise organizations that have embraced IoT and how Flux7 helped them build a tailored IoT-ready cloud infrastructure that's future-proof.

Real World IoT Success Stories

The Flux7 Pristine IoT Case Study

Pioneering Google Glass in healthcare.

Pristine solves clinical workflow challenges for major health systems and academic medical centers so they can provide services at lower cost, with higher quality healthcare outcomes . By using Google Glass for hands-free video communication, Pristine's customer clinicians call for the expert help they need, exactly when they need it.

Flux7

Pristine's IoT Challenge

Pristine's rapid growth and resource constraints meant it didn't want to hire additional staff, or commit to managed services, to complete its IoT initiative. Pristine sought best-practices advice from experienced cloud infrastructure experts and the expertise that could provide a self-healing, controlled IoT architecture. As user demand reached an inflection point, the company also needed to be agile and rapidly accelerate short-term product development while managing toward its longer-term strategy.

For its infrastructure, Pristine turned to AWS to support all of its applications. Reflecting the company's strong focus on maintaining an outstanding customer experience, this infrastructure supports client apps for the web, Android, iOS, and Google Glass. This meant the company needed to prioritize hiring for skills specific to the devices customer clinicians would be running its apps on. "We had in-depth knowledge about iOS and Android, but scalable infrastructure on AWS was a different beast," said Mark Troutfetter, vice president of engineering at Pristine.

This created a dilemma for Pristine. The company needed to move quickly to get its cloud architecture up and running, but it didn't fully understand the nuances of AWS. And Pristine was concerned that a less than optimally configured infrastructure on AWS could lead to security issues, downtime, or create the potential risk of privacy breaches. That's why Pristine selected Flux7 to provide a DevOps assessment that would produce a strategic plan and provide the technical expertise necessary to move its infrastructure forward.

The Results:

• Flux7 designed Pristine's AWS infrastructure

• Built a real-time communication system with high availability

• Flux7 solved a significant technical challenge for Pristine when it provided servers that could auto-scale in real time, without any communication degradation

• Increased Pristine's ability to meet HIPAA-compliant software requirements

• Created a scalable mobile app infrastructure

• Provided for rapid medical device product development

• Through the infrastructure, Pristine can provide a high degree of guaranteed system uptime to its clients

The Flux7 Horan & Bird Case Study

IoT shines a light on this solar panel company.

Horan & Bird's IoT Challenge

Improve customer engagement and create new marketing channels while enhancing business accounting processes.

Through improved monitoring, Horan & Bird hoped to improve the efficiency of its business. First, by making certain that customers fully understood the savings they earn from solar panel use, Horan & Bird hoped to increase customer engagement. It also sought to develop a white-label product for resale by other solar panel providers throughout Australia. And, it wanted to more accurately identify customers late on their lease payments for more timely disconnect notices.

Through an extensive evaluation, Flux7 engineers helped Horan & Bird select an inexpensive internet-enabled power monitoring gateway. Flux7 experts wrote the entire software stack—from interfacing with the monitor to saving the data in the cloud to displaying the data and sending emails to customers. During development, they kept in mind the goals of improving customer engagement, being able to disconnect non-payers in a timelier fashion, and creating a step-by-step implementation program Horan & Bird could sell to other Australian solar companies.

Flux7 designed a way for Horan & Bird to monitor the power output of each solar panel as well as monitor each customer's electricity consumption, and then log and store that data in the cloud.

To achieve this, Flux7 combined AWS, SailWider's Power Gateway hardware with Python, Cassandra, Twitter Bootstrap, Celery and Amazon SES software. The overall combination with the client's product and service portfolio created a powerful one-click dashboard that maximizes customer value.

The Results

The monitoring provided Horan & Bird the ability to analyze customer data as needed, and to derive important customer-level and global business-level metrics. Horan & Bird is now also able to identify potential new leads and upselling opportunities, then develop new marketing channels, thereby increasing business. It's also been able to decrease accounts receivable actions and increase collection rates by being able to rapidly recognize solar power customers who are not making lease payments.

Fugro Launches IoT Based Service with Flux7 Cloud Expertise

Supports Customer Demand with High Availability, Security and Portability

The IoT Challenge

Fugro recently launched OARS (Office Assisted Remote Services), an innovation which uses advanced technology to reduce, and potentially eliminate, the need for surveyors onboard sea-going vessels, optimizing project crewing, safety and efficiency. With the launch of OARS, Fugro anticipated healthy customer growth requiring the company to proactively address scalability and downtime recovery. Given its customers' remote locations which could literally be anywhere in the world, deploying consistent, sophisticated services with consistent uptime and continuous delivery of upgrades was the incredible challenge the team of software engineers at Fugro faced.

The Results

Fugro reached out to Flux7 who immediately got to work with its award-winning Assess, Attune and Engage consultative approach. The first step in the process was to assess Fugro's current design plan, from which Flux7 built an architectural IoT blueprint. This long-term, independent plan for infrastructure development and deployment featured Docker and Amazon Web Services (AWS) at the hub to provide a high degree of uptime, ensure data security, and enable portability across global regions. Following assessment and planning, Fugro and Flux7 began the work to implement the IoT infrastructure with resiliency, scalability, and continuous delivery built in.

Using Flux7's deep AWS and Docker expertise, the team was able to "Docker-ize" Fugro's IoT backend. With Docker containers, Fugro is able to build once and run in many places, while creating immutable infrastructure which increases reliability and uptime. Adding Jenkins to the mix allows Fugro to have a continuous deployment flow in which Jenkins triggers the build of new Docker images for target machines.

Flexing the capabilities of Flux7 and automation, the team launched the service in one fifth the time of typical Fugro launches.

Flux7 and Fugro applied networking designed to provide an encrypted channel on top of low bandwidth satellite-backed Internet connections to the vessel. The team designed the system with high availability and infrastructure flexibility to help ensure data would not be lost due to a disaster recovery issue. With a layered security approach, redundancy and elasticity built in, the OARS project implementation features a high degree of security for all data involved.

Several vessels in multiple geographic regions have already begun using OARS as a result of this project's speedy implementation time. Compared to the previous environment, the new IoT environments now launch in a matter of hours.

Flux7 Global Manufacturer IoT Case Study, Internet of Things

Creating a scalable IoT infrastructure while achieving EU data privacy law compliance.

The IoT Challenge

Using Hadoop, internal data centers, Rackspace and CenturyLink, this manufacturer wanted to facilitate new services that connected its customers with data insights from the equipment they purchased. But the efforts weren't working as well as it would have liked. To improve its ability to facilitate continuous, data-driven, IoT-powered improvement for its customers' operations, it needed to overcome significant Hadoop scaling issues. The manufacturer also needed a way to provide IoT data-driven insights that complied with EU data privacy laws.

The Results

Understanding the organization's scaling challenges and need for EU data privacy compliance, Flux7 recommended that the manufacturer approach the project with DevOps and a public cloud architecture, executed through AWS. The experienced Flux7 consultants were able to provide education, guidance, and extensive cloud, DevOps, and IoT expertise.

Under the guidance of Flux7's AWS architecture experts and certified consultants, the manufacturer's internal teams were able to quickly understand what could be done to rapidly move forward. Together with Flux7, internal staff developed a DevOps workflow that proved to be highly agile and leverages AWS and Ansible, a platform for configuring and managing computers, while maintaining tight security controls that meet EU data privacy laws.

This global manufacturer now has a solution that makes it possible for it to stream, analyze, store, and share data collected by thousands of customer machines in a secure, EU data-compliant cloud architecture. As a result, the manufacturer's competitive advantage revolves around this successful IoT strategy and the ability to seamlessly connect its customers with data insights that enable them to improve quality and productivity in real time.

Flux7

Conclusion

As we've seen, there are many challenges when it comes to building successful IoT implementations — from the infrastructure through instilling good app design processes. And as the customer IoT success stories above have shown, an infrastructure that is not only secure but elastic and agile enough to deliver innovation must be in place. For more information on how to successfully design and deploy a successful IoT infrastructure, call 844-Flux700 today. And for additional insights on leading edge infrastructures, AWS news, and technology trends, **sign up** to receive our blog in your inbox.

Contact us today for a needs assessment: http://bit.ly/1GHDZvf

www.flux7.com | **Info@flux7.com** | **844.358.9700**

Flux7

www.flux7.com/cloud-infrastructure-assessment/