WHITE PAPER

Ayla Networks

How To Select the Right IoT Platform

Considerations Beyond Connectivity — Security, Flexibility, and Data Intelligence

Contents

Opening

Although it has been with us in some form and under different names for many years, the Internet of Things (IoT) is suddenly the thing. The ability to connect, communicate with, and remotely manage an incalculable number of networked, automated devices via the Internet is becoming pervasive, from the commercial kitchen to the residential basement room to the arm of the fitness buff.

If you're reading this white paper, you probably have an interest in adding Internet connectivity, mobile application control, and likely also some "smarts" to your product or device, and so it all can be controlled and monitored by a smartphone or tablet. Let's make an assumption that you already believe that working with an IoT Platform provider will accelerate your time to market and increase your ability to deliver a world-class connected product, versus trying to do it all in-house. But what's most important to consider when evaluating and selecting an IoT Platform?

The ease and simplicity of getting basic networking to work on your prototype, getting it to talk to a cloud and your mobile app are essential and a critical first step. But what else must you think about and consider, so that this new era of IoT doesn't come biting you back later, like an angry junkyard dog.

This white paper focuses on three critical considerations when choosing an IoT platform, specifically what to evaluate in a platform architecture so that your needs are met today, and more importantly, are going to be met in the future as you expand your family and functionality of smart-connected products. The key platform architectural attributes are: (I) Security, (II) Flexibility and (III) Data Intelligence.

This white paper will elaborate on each of these considerations, and close with an introduction to the IoT platform from Ayla Networks, the end-to-end solution that leading manufacturers are choosing to deliver world-class IoT products. Finally, an appendix is included at the end with a table of specific features to look for as you evaluate the best IoT platform for your needs.

White papers can often be dry, and we tried to write this paper a bit differently. The prose is somewhat informal, written more like the way we'd write a blog post. In this way, we hope you find it more interesting to read. Tell us what you think – email us at wewantyourcomments@aylanetworks.com – we'd love to hear from you.

Part I:
7 Steps to Security for the Internet of Things

The Internet of Things (IoT) is starting to appear everywhere in many shapes and forms. But security is one of the hurdles that could trip up the growth of the IoT. Following security principles used in enterprise computing can help clear that hurdle.

Think of the IoT's breadth for a moment. Already there are more connected devices than people on the planet, according to Norio Nakajima, an executive vice president at Murata. By 2020, there will be 50 billion connected devices, outnumbering people by more than 6 to 1.

Many of these devices will be controllable over the Internet, and they will increasingly be responsible for collecting and transmitting sensitive information. Today consumers might own a FitBit that collects information on their exercise routine. In a few years, those same people might have an Internet-enabled insulin pump that continually delivers data to their doctor. In the wrong hands, data from home management systems could be used to assess your whereabouts. Likewise, businesses could be vulnerable when they connect things like HVAC, irrigation, and commercial appliances.

Hackers often scan for poor or misconfigured security on networks, and IoT environments will likely be no different. This was the case in the early days of Wi-Fi Internet connectivity, when weak security on access points and wardriving prevailed until education and configurations improved. The IoT could be vulnerable. By design, it's always connected to the Internet. Therefore, it must have strong security built in.

But that's only half the problem. Security also has to be really simple to implement. Otherwise, people won't use it. They will blame the manufacturers and service providers instead. If we don't iron out how to make strong security goof-proof, a very public breach could result.

It's nearly impossible to make any Internet application platform 100% impenetrable from attack, but implementing the best-practices of enterprise-class security can thwart all but the most persevering hacker with malicious intent.

What does enterprise-class security really mean in the case of an IoT cloud-based platform? Here are seven key principles.

1. End-to-end security mechanisms

Mobile apps and connected devices must be authenticated separately. Both the mobile app and the end user's credentials must pass authorization. The identity of the connected device is best maintained in hardware. That is, the device's credentials can be burned into its connectivity module at the factory, so it's not exposed to anyone. This dramatically raises the bar for spoofing. Someone would have to steal your device, your mobile app, and your password.

2. End-to-end data encryption

Standard-based encryption from device to mobile app is arguably one of the best deterrents of data theft. Many services encrypt data once it gets to their datacenter, but in many ways data is more vulnerable when it's in transit. The challenge with doing this from end to end is making all the authentication and key management happen without user configuration, so the data encrypts automatically.

3. Access and authorization control

This means giving different user types different levels of data access. Consumers might let their utility link to their thermostat to turn down the AC on peak power days. But the utility would be able to using the data for power consumption analysis only. Or maybe consumers would give retailers limited access to monitor their AC for proactive maintenance and repair.

4. Activity auditing

IoT device manufacturers and service providers need to keep log records so that any breaches can be traced back to the source. Auditing data is also an important way to identify patterns that can pinpoint problems before they happen. Additionally, it's a way to rate vendors. If businesses could compare the security practices of vendors in an open and honest way, cloud providers and IoT service providers would have a huge incentive to invest in security.

5. Hardened cloud infrastructure

Hosting data in the cloud can be far more secure than keeping it at home or in a company-run datacenter. Cloud providers can invest more money and personnel in strengthening their operations against attack. But you still see hackers gaining entry into well-known organizations. How do you know security

best-practices are followed? ISO 27001 is a security certification standard that specifies security management best-practices and comprehensive security controls for datacenters and other environments. For example, Amazon Web Services (AWS) is compliant with ISO 27001.

6. Equal protection across multiple protocols

Devices will communicate over WiFi, cellular, ZigBee, Bluetooth, and other wireless (and wired) protocols. Security has to be equally strong across all of them, regardless of whether the mobile app is talking to a connected device over the Internet or locally (e.g. at home, on the same WiFi network as the connected device).

7. Education

Vendors have to be ready to teach consumers and buyers -- through easy-to-read web pages or through their customer service desk -- why security is important and why they need to think about it. Sadly, human error is still one of the biggest cybersecurity vulnerabilities.

Together these measures will significantly increase the security for the Internet of Things. But the IoT will be at risk if end users believe the added steps required for strong security outweigh the value. Automated, push-button functionality absolutely can be done, but it is very difficult to develop well, and it requires an engineering team with deep experience. Most manufacturers won't be able to hire world-class security teams. The cost and complexity will far outweigh the benefits for appliance makers or light equipment manufacturers. Instead, they should look for partners that can provide it for them.

Make no mistake. The IoT is coming. But so are the hackers.

Part II:
The Internet of Things & the Great Unknown

What will the next killer app be for the Internet of Things? We have no idea.

In fact, we don't think anyone has a clear idea yet. This is an entirely new market, and if the history of technology is any guide, consumers and even business buyers will behave in unpredictable ways. Digital Equipment CEO Ken Olsen didn't think anyone would ever want a computer in their home. Bob "Father of Ethernet" Metcalfe predicted the Internet would suffer a mind-boggling collapse in 1997.

For product engineers and marketers, unpredictability is an occupational hazard. Tablets might be a rip-roaring success today, but they flopped in 2002 when Microsoft lined up nearly every major manufacturer to release them. You also have the unanticipated success stories like Twitter and Facebook. Wi-Fi analysts questioned whether consumers would use public hotspots. FitBit and Nest helped create and popularize two (connected) product categories -- wearable health monitors and smart thermostats -- by incorporating design aesthetics and intuitive experience that hit the right pitch with customers.

The Internet of Things market is amplifying but still in the early stages of adoption. We are just starting to visualize what connected products can do to improve industrial productivity, create world-class customer experiences, and drive new understandings between manufacturers and their customer behaviors. What's behind the next corner is really anyone's guess.

Engineers developing the next generation of connected products need to design for flexibility, so they can quickly adapt to how the uses for their products will evolve and grow. Marketing doesn't have a crystal ball, and it cannot really know what features are wanted in the future.

Designing in flexibility is easier said than done. It's often expensive, and many manufacturers arent willing to add the insurance costs of accommodating TBD new features. This often results in products with rigid designs that can't evolve to meet the customer's unanticipated needs, or those that require forklift upgrades to do so.

What does this all mean for a development team tasked with designing and supporting world-class connected products? Here's a partial list of flexibility-increasing architectural considerations that will increase the adaptability of connected products.

1. **Design for networking agnosticism:** What's in a thing? If it's going to be part of the Internet of Things, it probably has some sort of system architecture featuring a microcontroller unit (MCU). Most things don't have any operating system -- just a simple MCU and a few sensors. Manufacturers should be able to connect almost any MCU-based system to the Internet without being redesigned just to add networking and security. This is accomplished by removing the burden of networking stacks from the host

MCU and providing a very thin bit of code that can easily be ported to the host MCU. If networking stacks are completely removed from the host MCU (e.g., if they pre-exist on the comms chips/modules), then a simple driver is all that's required to connect to the Internet. This also provides great future proofing; next year's product may use a different MCU. With this approach, that's no problem. Marketing can choose any new features it wants, and engineering can deliver it using the most appropriate components.

2. **Design for data agnosticism:** OK, so I'm recycling terminology, but my point is similar. Just as there could be nearly any type of MCU-based architecture in a thing, there could also be just about any type of data. And you can be sure that, even across some product line, the data is going to change each year with enhancements and new iterations. Any solution that somehow requires a crystal ball for what sort of data will be leveraged (including what you name that data) will result in significant downstream redevelopment. A better solution includes integrated databases in the backend with no preset data schema. Marketing and engineering teams should be free to decide what they want devices to do and what sort of data they should collect. When they need to change the product, there should be no major engineering burden and no major customization. The manufacturers that do this best will easily out-innovate competition and get new products to market faster.

3. **Built-in feedback loops:** This is really the home run of IoT design. Imagine easily getting products to market with any architecture or data set, as well as being able to learn on the fly as those products are used in the field. The world's premier companies -- Amazon, Apple, Google -- already do this by selling Internet services and connected products. They leverage their platforms to know which features customers like and which ones they don't. They use built-in feedback loops to design products their customers love. This will also be critical for manufacturers seeking to build IoT products. Those that can gather data, learn from their products, and adapt quickly to change them to suit their customers will be the winners. Doing this involves a complex integration of devices, databases, and business intelligence and analytics tools, but it will be crucial for responsiveness and success.

4. **Configurable cloud-based rules engines:** The Internet of Things is truly enabled when devices can interact with other devices. Moreover, marketing is always looking for a way to make different products work better together. This is a great goal, but it's very difficult when marketing doesn't know what products are coming next, so it doesn't know how products might interact. A configurable cloud-based rules engine solves this challenge, providing the ability to modify a product's characteristics and behavior after it has been in the field, making it work with new products that are being launched. By putting the rules engine in the cloud and making it highly configurable, manufacturers can much more rapidly enable a network effect among their products.

5. **Open APIs:** Integrations of other enterprise application or cloud platforms may not be a requirement today, but they will surely be in the future. Integrations may be unidirectional (e.g., inbound from weather.com or outbound to saleforce.com) or bidirectional (e.g., to/from a specialized analytical engine or separate IoT cloud platforms). Either way, cloud-centric platforms provide the foundation for an open interface approach.

Adapting quickly in the Internet of Things will be greatly facilitated by outsourcing the thorny problems like security, data management, and networking. Trusted providers of IoT application-enablement platforms, meanwhile, will spend a lot of their time and energy crafting highly flexible and scalable solutions that can be dropped into myriad designs without a hitch. That's very cost effective, too.

Plan to be adaptable in a new market in an unpredictable world. Look to partners who can help get you there faster. Trial and error will be the norm.

And that is something we can predict with complete confidence.

Part III:
Putting the Smarts in the IoT

We watched The Wizard of Oz in 3-D at a company outing last week, and we can't get the tune out of our head from when Dorothy first meets the Scarecrow, and he sings, "If I only had a brain." We think much of the Internet of Things now under development may end up lamenting the same tune.

The IoT has become a catchall phrase. Smart cars, smart home gadgets, smart wearables, and more -- all end up with the "smart" moniker. But the brains in the Internet of Things are more than being tied to the Internet and connecting to an

ecosystem of other devices. It's more than a remote monitor for your smartphone or tablet. It's really all about data intelligence.

For the Internet at large, the real value has been the capability to provide significant new value in the way to collect, manage, and make sense of all the data we create. For the IoT, of course, the data will come from the things, and perhaps also from users in the form of metadata. Think of the user cases, such as gathering data from blood pressure cuffs and weight scales for the chronically ill and aging and then identifying patterns to predict deteriorating health. We will save billions alone in healthcare from the ability to collect, analyze, and respond to health data from connected devices.

In another use case, imagine consumer products that help manufacturers learn which features are most popular and how their products are faring in the field. By leveraging the data, manufacturers will be get higher-quality products to market quicker with the set of capabilities that their customers really love.

Finally, consider the broad set of commercial products sold. They typically have complex channels to get to market, and the various channel participants can have different access data privileges. There are several categories of data intelligence functions to consider, and they are best managed through a secure portal for the manufacturer's operations team to administer.

1. **Flexible data definition tools:** The platform needs to include intuitive tools for the manufacturer to customize the definition for what data to collect for a given device and how it is to be collected (e.g., how often, how much). It also needs to be easy to set up and define new types of devices. There should be no limit on what types of devices can be defined. Manufacturers should have to work with only one platform for all the connected devices they will launch.

2. **Data virtualization and non-SQL database:** The system for organizing the device data for retention also has to be very flexible. While accommodating most any data definition of a device, the platform needs to adapt quickly to the fact that device data definitions will change (expand) often, and that each device will have many different data definitions out in the field. As a result, the inherent rigidity of an SQL database -- and the development lag to change SQL database schemas -- is overcome.

3. **Data processing and analytics services:** An IoT platform really starts to multiply value when it includes services to process the collected data and turn it to usable information. At the foundation are the capabilities to create and control event triggers in a highly customizable fashion. Finally, there are data analytics modules for business intelligence -- e.g., reports and dashboards that the marketing, product strategy, and service support teams each will want to consume.

4. **Role-based data access control:** Manufacturers need to be able to define various user profiles, each with fully customizable control of what data for which the user has read and/or write access and then to classify each user ID to a defined profile.

5. **Data scalability:** This may be the least sexy part of the data intelligence potential of the IoT, but it's a critical prerequisite to making it all work. Again, the manufacturer will need good tools to manage the warehouse of data as the data set grows, e.g., culling and archiving data over the long term. Much of this should be customizable and automated.

A manufacturer can try to assemble a breadth of development expertise and build a platform with all these data intelligence functions in-house. But building all this will require hiring and retaining significant expertise and paying an ongoing cost: lots of money and lots of risk. The alternatives are to be like Google and buy a company that can do it for you (got $3.2 billion burning a hole in your pocket?) or to go about it the smartest way and select an off-the-shelf IoT platform from a company that does only that.

Any other way to compete would be, well, not so smart.

About Ayla Networks

Ayla Networks provides the leading application-enablement platform as a service (PaaS) for the Internet of Things. It is a comprehensive software solution that transforms everyday products into intelligent, interactive products quickly, easily, and economically. The Ayla IoT Platform combines innovative software and networking technologies with cloud-based platforms and digital information services, and supports best-in-class hardware from leading component vendors. Our streamlined approach allows manufacturers to integrate Ayla connectivity into products without substantial design modifications or changes to existing business models, and in a way that consumers will understand and appreciate.

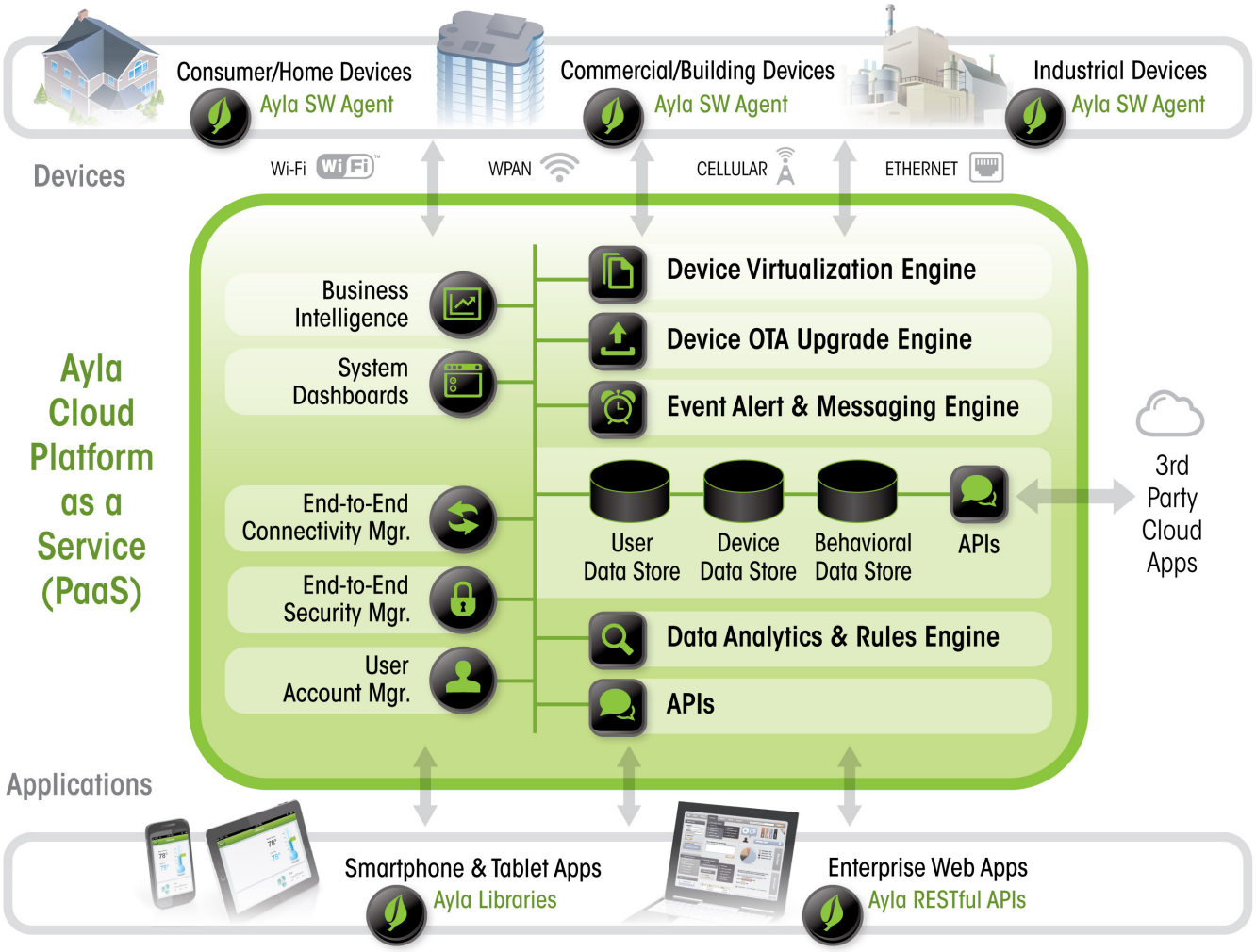

Figure 1: End-to-End Architecture of the Ayla IoT Platform

Figure 1 shows the end-to-end architecture of the Ayla IoT Platform. The end-to-end solution encompasses software agents on the connected device, a suite of software services in the cloud, and extensive software libraries for the leading mobile operating systems – enabling manufacturers to easily, securely, and cost effectively build Internet-connected devices with amazing customer experiences that can scale. This single platform can be easily leveraged across a family of different IoT products.

The Ayla IoT Platform is Composed of:

- **Ayla Embedded Agents**
  Agents incorporate a fully-optimized networking and security stack to connect devices to the Ayla Cloud Services easily. Agents are pre-burned into leading communications modules and chips, making it practically plug-n-play.

- **Ayla Cloud Services**
  The heart of the Ayla IoT Platform, the cloud services provide secure connectivity between devices and apps, virtually manages an unlimited number of device templates in the field, processes all data pushed and pulled to devices, and provide an extensive toolset portal for manufacturers to securely manage their customers' products anywhere.

- **Ayla Applications Libraries**
  Libraries contain all the necessary APIs for creating mobile apps to control Ayla-enabled devices with a smartphone or tablet in a secure manner. Supports both iOS and Android devices.

The Ayla IoT Platform robustly supports all of the architectural capabilities and key requirements outlined in this white paper. Please refer to the Appendix A below for a tabular description of these capability requirements and a summary of Ayla's support.

Appendix A

Summary of Key IoT Platform Requirements

Key Functional Considerations When Evaluating IoT Platforms	**The Ayla IoT Platform**
SECURITY	
1. End-to-end security mechanisms	**Yes, multi-level authentication**
2. End-to-end data encryption	**Yes, TLS/SSL on all links**
3. Flexible & configurable access and authorization control	**Yes, role/time based**
4. Activity logging for audits	**Yes , within OEMportal toolset**
5. Hardened cloud infrastructure	**Yes, compliant to ISO27001**
6. Equal protection across multiple communication protocols	**Yes**
FLEXIBILITY	
1. Designed for networking agnosticism	**Yes**
2. Designed for data agnosticism	**Yes**
3. Built-in feedback loops	**Yes, data analytics within cloud**
4. Configurable cloud-based rules engines	**Yes, within cloud**
5. Open APIs	**Yes, to apps, to other clouds**
DATA REQUIREMENTS	
1. Flexible data definition tools	**Yes, within OEMportal toolset**
2. Data virtualization and non-SQL database	**Yes, abstraction layer in cloud**
3. Data processing and analytics services	**Yes**
4. Flexible & configurable role-based data access control	**Yes, role/time based**
5. Data scalability	**Yes, very high**