Ayla Networks

4 Things

to Consider When Selecting an IoT Platform Provider

It would be difficult to overstate the value of the Internet of Things to consumers, manufacturers, and virtually every other vertical market in the world. The breathtaking pace of the release of new and useful smart devices is taking the world by storm and improving the quality of life and the workplace in ways once unimagined.

The market for IoT products is immense, and competition is fierce.

The seemingly insatiable appetite of the public and of businesses for IoT products provides many opportunities for OEMs to design, create, and market smart devices to fulfill virtually any requirements.

However, taken on their own, IoT devices are complex and challenging to maintain and support. Fortunately, OEMs have the choice of many IoT platforms that will take care of much of that complexity, simplifying implementation and day-to-day operations. A well-designed platform enables OEMs to focus their efforts on their specialized IoT devices without concern for the backend management, security, privacy, communications, and more.

When evaluating IoT platforms, you should look for the following characteristics:

- Platform as a Service (PaaS)
- Maturity & experience
- Scalability
- Business agility
- Updatable
- No development of backend (configuration vs. custom coding)
- Security & privacy by design
- Simplicity

Look for a mature platform to simplify onboarding and security. Tech trends constantly change; agility and the ability to adapt and innovate are crucial to remaining relevant. IoT is viewed as technically complex. The platform provider must handle this complexity for you. Simplicity is vital, and the platform should be easy to use.

In this article, we will cover the four things that you, the OEM, need to consider when you are launching an IoT product.

Time to Market

Fierce competition demands that new IoT products get to market quickly, as many times the difference between success and failure has nothing to do with quality or marketing. Instead, the primary problem is simply a matter of the time it takes to get into the hands of consumers.

Fast time-to-market matters because it allows the OEM to iterate more quickly, test more often for market demand, accept less project risk, and gain a competitive advantage.

This problem is addressed using pre-built or pre-integrated services to support IoT devices, which means less cycle time to rollout.

Getting to market quickly can seem like an insurmountable problem because the IoT is technically complex. Devices must communicate securely with backend servers and databases for control, data storage, security updates, and other reasons. You can imagine the complexity of sending out a new firmware update to millions, or even hundreds of millions, of devices.

The entire process is more straightforward when OEMs can leverage a mature, fully featured backend. The best solution is a Platform-as-a-Service (PaaS) offering where the complexities of control and data storage are centralized in a remotely managed environment. This effectively moves the responsibility and overhead of managing a network of independent IoT devices to a third-party solution provider. They become responsible for managing the backend, freeing up your business and personnel to focus on what your company does best.

Your upfront cost is low since the PaaS system is already tested and working.

It's run as a managed service, so you won't have to hire additional support personnel. Your job as an OEM is to build in logic for your basic devices. Security, data privacy, and communications are taken care of on the mobile app and by the PaaS platform.

The result of a well-designed backend, ideally using a PaaS, is that your IoT products can get to market fast. The faster you can get a new product to market, the less likely it is that the competition will get there ahead of you.

Security and Privacy

A well-publicized, major breach can destroy the years of building a brand and reputation of a business. Additionally, a breach can put customers at risk, invading their privacy and even leading to real-world dangers such as identity theft and ransomware. As an example, consider the chilling implications of a security breach in a smart camera system; the personal lives of anyone owning those cameras could be at risk.

When you're evaluating a platform, ask if it prioritizes security so that you don't have to think about it.

> The platform should not give OEMs options for security; that might sound counterintuitive, but good security is implemented straight out-of-the-box without any need to turn it on, tune how it works, or disable critical features.

Unfortunately, many platforms get to market quickly without sufficient concern for security, which is a recipe for disaster. Security must be built into the platform with a policy of "security by design." Platform providers validate security, compliance credentials, and claims with third-party auditing firms who perform penetration testing regularly. They understand that security regulations and attack methods are ever evolving, requiring constant vigilance. Platform providers generally request audits of their own infrastructure to ensure their customers have peace of mind. You can think of platform providers as silent partners, working behind the scenes to keep the IoT platform secure and private.

Security must be built into every part of the deployment – the mobile application, cloud, and device (hardware/module plus firmware). Good security consists of hardening the device itself, ensuring that the device to cloud communication is encrypted and that the mobile app uses best security practices.

Privacy means to protect the data so that it cannot be seen by unauthorized eyes.

Consumer data should never be sold or abused, and the OEM should control their data. Standards such as GDPR, the California Consumer Privacy Act (CCPA), the Consumer Privacy Protection Act (CPPA) in Canada, and ISO 27001 must be supported, including the requirement of access logs. The platform should also give consumers control of their data, and the data should not be monetized.

Security is built-in, not bolted on or implemented as an afterthought. It must be designed as an end-to-end solution that just works behind the scenes with no burden on the user. Privacy should also include role-based access control in the apps so the user can only see what they're authorized to access.

Working the Larger Ecosystems

Typically, a home user integrates multiple products into their environment, including Amazon Alexa, Google Home, Nest, Apple Homekit, Samsung Smart Things, Wink, TP-Link, LIFX, Philips, Ring, and so forth. After all, consumers look for solutions that work for them at the right price. It's best to ensure an IoT platform has options to remove barriers to stitching devices from different ecosystems together and supports the interoperation of multiple platforms.

The best ecosystem for consumers consists of devices that work together, united by a single application for management and control purposes.

Imagine the convenience of a single device or application such as Alexa to enable users to use voice skills to control Visio televisions, Alexa plugs, and a different manufacturer's smart light bulbs. Owners of Alexa devices then create custom utterances or "scenes" (group activations) like "Good Morning" to simultaneously turn on the television, a smart coffee maker, and the lights in the kitchen.

Interoperability is not just a word; it's a design philosophy in which multiple devices can talk to one another and operate in tandem. The OEM is responsible for the basic logic in their device, and the PaaS platform needs to facilitate that interoperability.

The IoT platform must support standards and protocols, and they must be accessible via standard APIs. This allows developers to build in the functionality they need without concern for the underlying technology, communication methods, and controls. Additionally, the platform must promote interoperability by publishing the architecture of its data schema. This allows manufacturers to add new properties to support additional functionality, services, and devices.

A well-designed platform makes it easy for smart devices to work together without the concern of the manufacturer and the need for technical skills.

Consumers should not have to deal with multiple applications for their devices. Thus, the interface should support a unified access and control dashboard.

Public cloud companies are built around the idea of getting customers to use as many resources such as data as possible. In contrast, the incentive of a good platform provider is to optimize cost by reducing resource usage and optimizing data.

Business Outcomes and Ownership Costs

A platform must support leveraging the data that comes back from devices for business outcomes. This is needed for product developers to understand how consumers are using the features of the products. This allows you to leverage actionable data to make informed decisions and enhance product iterations. You'll know what features and functionalities to abandon or to improve upon based upon actual usage and performance in the field.

In terms of operation, if the device is not performing well, the platform provider needs to help the customer fix it.

Understanding usage leads directly to improved product quality, which improves the overall customer experience.

OEMs can then be preemptive in their troubleshooting and in the design of future products, and it enables them to sell more units of existing products.

Another significant advantage of implementing devices to use a well-designed PaaS platform is scalability. As your devices become increasingly more successful, you can expand nationwide or globally without building new or expanding existing teams. You don't have to worry about adding new support staff regardless of how many devices are installed since maintenance and ongoing technical support is handled by the platform provider.

Scaling, however, must not be done just for the sake of scaling. The platform must be able to scale and support devices around the globe at a reasonable price point. Scalability is further enhanced since you no longer need to devote staff to managing the backend; instead, your team can focus on what they do best: designing and manufacturing high-quality products. This reduces the initial cost of development since the IoT PaaS partner handles the implementation, management, and ongoing updates and maintenance of the backend. You simply design your products to interface with the PaaS platform, and you're all set.

Since the PaaS service is based in the cloud, the major expense of on-premises hardware is eliminated or highly reduced.

You don't need to install new hardware to expand when you add new products and services. By running as PaaS, you are free to focus entirely on your products without concern for anything except for the product's hardware and application.

Heightened product quality and enhanced support yield great customer experiences, resulting in more 5-star ratings. Low star ratings (whether retail or application) can be the kiss of death in IoT, as many consumers will ignore products or services with less than t hree or four stars. Better products and happy customers lead directly to additional sales, referrals, and good ratings on social media.

Understanding business outcomes allows you to control efficiency and cost by building in a feedback loop where you always understand what's going on in the field with your devices. This encourages an environment of continuous improvement and growth, with the result being higher unit sales.

The key is harnessing the data coming off the device in meaningful ways. Understand how to use this data to control costs, grow, improve your products, and improve the customer experience. Good data analytics is an essential component of a well-designed IoT platform because it will give you a real-time and historical picture of how your devices perform in the field.

Useful data analytics leads to:

- Increased product quality, resulting in 5-star reviews and happy customers.
- Differentiated product lines, which result in more units sold and additional revenue streams.
- Better remote diagnostics and remediation, which leads to lower return rates and higher customer experience.

The same business model could apply to any product that requires replenishment, such as salt pellets for water softeners, filters for water dispensers or air purifiers, and coffee grounds for coffeemakers. The possibilities are virtually endless. Consumers enjoy the freedom these options allow, and because of that, they tend to become steady revenue streams.

Conclusion

As an OEM, your focus must be on designing, implementing, and selling unique and useful products to a hungry consumer market. By choosing the right IoT platform solution provider, you can free your business from the need to support the complexities of supporting your devices. The platform provider will manage security, privacy, communications, updates, data, and support of your entire network of IoT Devices. As a result, you won't need to worry about the day-to-day maintenance of those devices. Instead, you can sit back, review the real-time and historical dashboards about your devices, and implement and sell the best IoT products possible.

Focus on what you do best: building the highest quality products for your customers.

Leave the management and servicing of the IoT platform to a responsive managed service solution provider.