CYBERSECURITY

USE CASE

FIRST MOVER CHALLENGES IN THE EMERGING FIELD OF IoT CYBERSECURITY

Daniel Tjornelund Sep. 2020

Prelude

"Data is the new oil" – a statement reiterated by many these days, and a widely recognized truth. The increased digitalization of our society, and the new commodity it spawned, data, presents a great opportunity for many. A new enabler in this new data-era is appearing - the Internet of Things (IoT).

IoT is essentially a term, given to the connection of devices (e.g. connected devices) to the internet. Using IoT, organization, businesses, and even cities and governments plan to improve their outcomes, increase productivity and reduce cost across their operations and services.

For example, smart traffics lights will prioritize the most congested lanes, making it easier to travel in and out of modern cities. Smart buildings will help the residents of high raised buildings - some of which host thousands of people - to efficiently get into the building in the morning hours, out-and-in again at lunch time, and out again at the end of the day, using smart elevators and quick access-control.

Instead of the flow of vehicles and people, other technologies focus on the optimization of energy. One example for these, is smart lighting inside buildings, parking-lots and roads, which can be managed according to demand and visibility conditions, instead of simply an on/off switch, or timer, and save valuable resources, while reducing operational costs considerably.

Smart meters, for water, electricity and gas are already being installed by the millions, to replace the need for manual readings, with a continuous and automatic reading.

Physical security is another aspect addressed by modern, connected cities. Many cities today cover their streets, buses, trains, and public areas with cameras, to protect the residents and visitors of the city. The images produced by tens of thousands of cameras can be analyzed by strong technologies to identify criminal activity, and even finding bags left unattended, reducing the risk of a terror-act, or just making it easy to return a lost item to their rightful owners.

The list is long, ranging from refrigerators, through wearable items and industrial equipment – connected devices are already shaping our society, crowning IoT as one of the biggest revolutions of the digital age.

The challenge

A key aspect of IoT, is the ability to gather and share data (over the web). But this connectivity creates worries and doubts in the hearts of the same people IoT devices were meant to serve: who can access the data gathered by the many cameras in my city? Can someone hack into the smart elevator in my office building and hold its passengers as hostages? Who will make sure that the smart traffic lights in our city do not get hacked and create a terrible accident?

It seems that the issues of security and privacy have become a central concern for anyone dealing with IoT devices, from its manufacturers to the users, and consequently, the legislators.

Product-Market fit

Cybersecurity is nothing new, plenty tools are already in use by the industry, governmental institutions, and consumers alike. The proliferation of IoT devices simply opens a new market: cybersecurity for IoT devices.

And the opportunity is enormous; IoT adoption is growing, and with it, also the security and privacy concerns. Projections show that by 2050, billions of connected devices will influence every aspect of our society, while the deployment of modern cellular communication infrastructure (e.g. 5G) is expected to serve as a strong catalyst for this trend.

The emergence of IoT devices has created an interesting sub-category within the cybersecurity industry, comprised of two competing approaches, utilizing different methods: one approach makes use of familiar cybersecurity methods related to network-security. According to this approach, the communication to and from the IoT devices is monitored and controlled, to make sure that nothing malicious is occurring. The competing approach focuses on the devices themselves, monitoring the devices operation, ensuring they are intact.

The first approach is often referred to as “Outside-In” (as it protects the devices from the outside) and it is the most common of the two, since it builds on known cybersecurity concepts, and is widely accepted - and understood - by the market. The second approach is a less common, and more experimental one. It is inspired by methods coming from the computers and servers’ worlds, where installed software (e.g. anti-virus) protects the devices themselves from the inside – hence, it is often called “Inside-Out”.

The question left for the first movers in the IoT cybersecurity industry, is:

Which of the approaches should they utilize: Outside-In, or Inside-Out?

The pros and cons are clear: the more mature Outside-In approach is relatively easy to implement, as it built on well know principles, and - even more importantly - it has the trust of the market, which understands it better and knows how to evaluate different offering, based on the features and specs provided. This approach will have a much easier time penetrating the new IoT market.

All of that being true, the Outside-In approach suffers some major limitations, primarily associated with the fact that devices may be infected with malicious software via other means than its

communication, one such being via its software's bill of materials (BOM), for example via the device's supply chain (crowned supply chain attacks), another possibility being by someone gaining physical access to the device when installed. Furthermore, the raise of 5G cellular network will make it feasible to connect the devices one-by-one to the web (and not in a network configuration), deeming the Outside-In approach irrelevant, simply because it is not financially viable to monitor the communication to each device separately.

In contrast, the Inside-Out approach makes it possible to discover supply chain attacks, as well as those performed via physical access. It will even remain relevant after the 5G network is fully rolled out, as the protecting element is placed in the devices themselves. On the other hand, the technological challenge is much greater, as the approach has to be adapted to work on IoT devices that typically have far fewer resources (memory, compute power) than the servers and computers it has been utilized for until now.

Nevertheless, it is seemingly a simple decision, as the Inside-out approach is more "future proof". And indeed, most recent IoT cybersecurity startups have chosen this approach, in contradiction to the trend just a few years back.

Reducing TTM vs. VOC

The decision has been made, and now the challenge is to develop the Inside-Out solution, which will protect the world's IoT devices from being compromised and taken advantage of by malicious forces.

The handful competing IoT cybersecurity startups have much to gain from being first movers in the market, primarily in regards to setting the new standards for IoT cybersecurity, both in the eyes of the market, and – maybe even more importantly – in shaping the upcoming cybersecurity regulations on the IoT devices' design.

Yet, to enjoy the first mover's advantages, these startups need to move quickly through the development of their MVP and its commercialization. And there is much to do.

On the technological side, the solution needs to be adapted to work on IoT devices, for example by making it possible to accommodate an agent, or sentinel, on devices with very small memory capacity, and making sure it does not require too much power (many IoT devices are battery operated).

On the business side, an overwhelming market education task awaits: manufacturers of IoT devices need to be made aware of the upcoming (possible) IoT device regulations and the inability of Outside-In cybersecurity tools to protect their customers devices, while the end users must be informed of the security and privacy risks associated with IoT devices and, finally, the regulators must be convinced to adopt the Inside-Out approach to IoT cybersecurity, with hopes that they'll create rules and regulations accordingly.

But, in rushing their development and pushing hard to educate the market, these cybersecurity startups risk missing out on the voice of the customers. It is a catch-22.

This catch has led many of the startups into a problematic situation: the MVP they

thought they had created, in fact does not cover most of their customers' needs. For example, if the customer's operating system (e.g. Linux, RTOS, Windows etc.) is not supported by the solution, or, a vital capability - for example the ability to work in hybrid cloud mode, or in "air-gapped" environments - is lacking.

This is the result of lack of attention to the Voice of Customers during the design phases of the solution, driven by the rush to minimize the TTM. The only remedy for such situations is quick adaptations of the product and its features when facing a "deal breaker" with a potential customer.

Such "last minute" adaptations are costly, resulting in a market where the startups with the strongest financial resources (basically, larger investments) have favorable odds of success.

Direct, or Indirect Sales?

Another decision the first movers of this newly created IoT cybersecurity market must take regards the GTM. Best practice states that direct sales is the preferred option in the early stages of a startup: direct sales will result in strong vendor/customer relationships, which in turn may lay ground up-sell, and increase the chance of customers being willing to serve as references, both for other potential customers, and for investors. Also, the direct sales approach facilitates more precise understanding of the Voice of Customers and, in turn, improved product development, a crucial aspect for emerging technologies.

Yet, it is understandable that the task of educating the market seems too big of a mouthful for some of the players in the new field, pushing them to base their GTM primarily on channel partners, leaving them to deal with the daunting task.

While the decision to use channel partners distances the vendors from their customers, it helps build credibility, providing the channel partners are branded as leaders in the space – enough to avoid creating antagonism when presenting cybersecurity approach which contradicts common beliefs.

Moreover, the tendency to ignore/downplay the VOC while developing the solution - in favor of better TTM - zeros a key advantage of the direct sales approach, namely, the feedback from the customers.

What is to come?

Many aspects of this new market are still to be discovered, here are a few:

First and foremost, will the Inside-Out cybersecurity approach turn victorious in the battle for the trust of the IoT devices' makers? And will it result in regulation which reflects and understanding the approach is superior to the Outside-In approach?

Secondly, will the Indirect sales strategy – adopted by some of the vendors - prevail, or will the indirect relationships with the market's customers prove too damaging to the startups ability to satisfy their customer requirements?

The answers to the questions above will unfold before us during the next few years.