Security for the future of AI

Matt Hatton, founding partner at Transforma Insights, interviewed Vincent Korstanje, the chief executive of Kigen, about why security is the most critical consideration at the intersection of generative AI, IoT cybersecurity and blockchain, the implications of global supply chain fragmentation, and why one Eddie Murphy movie is very relevant to the new IoT world

Matt Hatton: The interview is for the CES edition of IoT Now. Kigen will be heading over there. What are you expecting to talk about?

Vincent Korstanje: In **Kigen**, we're thinking a lot about artificial intelligence now and its implications for our customers and society at large. It'll hardly come as a surprise as practically every industry sees a new paradigm of innovation with AI. The consumer tech domain is set to see the strongest increase with US$10.8bn of revenue growth by 2028 from Gen AI. As customers begin to implement it rapidly, it's encouraging that we are guiding the direction on security for AI. There are a couple of angles to this.

AI is mostly used to assist in performing tasks passively, but it's much more interesting when it makes decisions for you. Autonomous driving is one particular example where AI is starting to act, and those decisions have the potential to be life-critical and mission-critical. To act, AI needs to compute critical vehicle, passenger and surrounding data and to get it into engines. If the AI is acting, and there's no human filter, you had better make sure that the whole process, from sensing to acting, is highly secure. In an AI-powered world, security isn't a feature; it is a necessity.

So, where do you start? The answer is: Device security. A secure OS is the best way to secure a device. And our way to market is to help connectivity providers secure their credentials on the device. For device makers directly, we enable them to get their chosen connectivity with carrier-grade security. That element on the device is an expensive and secure asset, which allows you to use it for other value-added use cases and services that need data to be signed. Both parties can use the Open IoT SAFE app, providing the highest level of security for getting data off the device. And, more than that, sign the data coming off the device so there is proof of where you got that data from. This becomes essential if you're trying to secure the whole system to then use it with AI innovation.

Of course, Gen AI models are not perfect yet, and won't be until and unless we act with urgency on security built into AI-everywhere.

MH: Can you give me an example of secure data proof driving revenue for OEMs?

VK: Sure, we have a great implementation with a customer, **Energy Web**, which is a leader in decentralised energy trading – via data monitoring units to smart meters, solar panels, EV charging stations, wind turbines and so on across the world's largest zero-carbon ecosystem. The data from those devices is put in a blockchain, and the information is sold to energy providers to derive additional benefits, for instance, on where energy stores are available and when they can be used. Blockchain is great, but if the data is tampered with, then it makes it all invalid. You need to sign, tag and track the data all through the supply chain.

Our collaboration with Energy Web and **KORE** focuses on doing just that, allowing data trading to increase energy efficiency. What's really unique here is having end-to-end security that empowers unique capabilities of services built on exchanges, be it trading or transacting. For OEMs today, ▶

SPONSORED INTERVIEW

In an AI-powered world, security isn't a feature, it is a necessity

thinking of what experience and service model they want customers to engage with is essential, and a simple investment in IoT SAFE with readily available software and stack components unlocks new revenue streams.

Security of IoT data, networks and devices remains a challenge for OEMs. The issue of lack of ownership of security is a hindrance and here's a standards-based, future-proof solution that addresses this. This is where Kigen comes in.

What we enable in IoT with the benefit of eSIM also allows for doing more with data being delivered into AI. Data, in general, is important. You need to protect it and understand it: Who has collected it? What has been done with it? Making sure that the data can't be changed. All of that is going to be very important to talk about at **CES**.

MH: What are your perspectives on the impact of IoT on some of the geopolitical challenges happening now?

VK: Our customers have been faced with overcoming the pandemic and component shortages, followed by some disruptions through global political conflict and a high inflationary economic climate. As a result, we see a heightened focus from countries to bring more manufacturing, IP and supply chains locally. This can present challenges, but it also has spurred business model innovation.

Kigen has a horizontal play, making security simple and accessible. We horizontally disaggregate the supply chain: we just provide the SIM software and enable other companies to provide the hardware (to the names OEMs would be familiar with as module and chipset vendors), and work with all across the supply chain. We focus on what we're good at and let others build on that for differentiation. This has a strong benefit for end customers, especially where there is a need for local ecosystem collaboration. ▶

Vincent Korstanje
Kigen

The main consideration in the creation of data silos is interoperability

For instance, take Kigen's recent collaboration with **Protahub** and **floLIVE** in Turkey, which is targeted at opening markets with strict requirements about manufacturing in-country. Turkey has some of the strictest data sovereignty and localisation regulations, and permanent roaming is prohibited. So the connections must be managed locally. We work with Protahub, the entity authorised in Turkey to comply with all types of connectivity regulations, from maintaining IP traffic inside the country to remote, full localisation, with a single stock-keeping unit (SKU) SIM and connectivity. 71% of countries have data privacy laws and another 9% have legislation pending, which can pose issues for cross-border connectivity and data requests, so the same approach applies beyond one country.

Similarly, in India, we work with SIM makers to support operators that have standardised on Kigen. We're opening a world-leading data centre in India, which will be the leading facility with **GSMA** SAS-UP certification by the time of CES. We're enabling local production in the country as India intensifies local efforts as a manufacturing hub and the world's fastest-growing digital economy. We've also just empowered manufacturers for eSIMs to be produced locally in Brazil with our software, of course, with our own quality control to ensure compatibility.

Further, there is the dynamic of the two largest powerhouses: China and the US, and the need for there to be two different supply chains independent of each other. We're agile and committed to flexibility. This allows us to enable supply chains for different players to be more localised but with the same functionality and compatibility across all vendors. It's an ethos we have retained from being founded within **Arm**, which allows different companies to make chips in their own markets.

Thinking about China and the US, We, and everyone else, have to work with the FCC, enabling the compliant solutions to coexist. We need to work with those other economies but be mindful of security implications. The new EU Data Act is also symptomatic of the wider phenomenon.

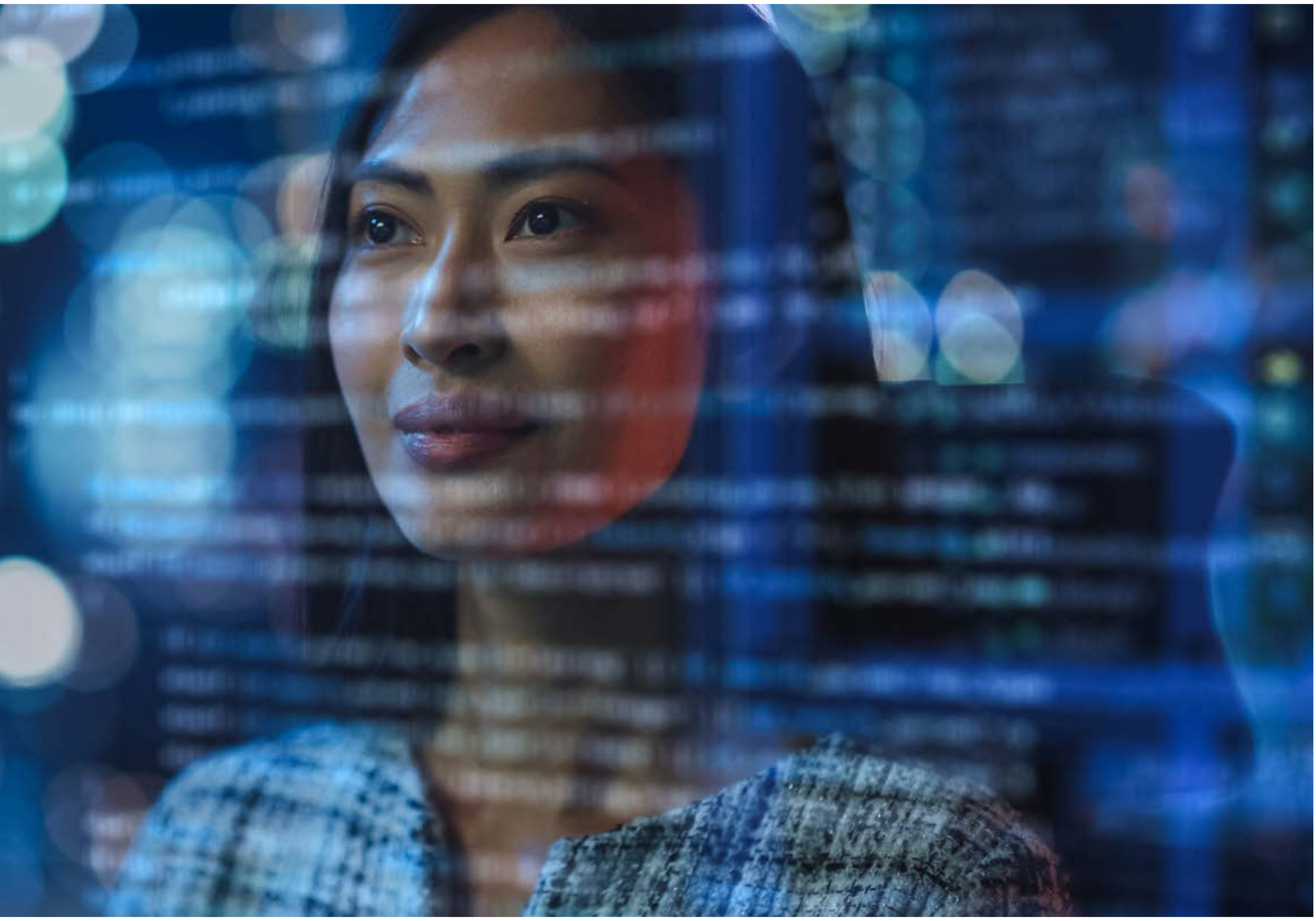
MH: Interesting you should mention the EU Data Act, as we're seeing an increasing amount of regulation around IoT. How do you see that, and other regulations, having an impact?

VK: From a business view it's quite interesting. For years, data has been identified as the new oil, which shows the importance of data and by extension, data trading. Data trading is the data which can be aggregated and bundled up for weather predictions; many organisations could benefit from access to that data. Much of the new EU rules are aimed at helping make data interoperable.

The main consideration in the creation of data silos is interoperability. With this, what you can do is create environments where you can trade data, for instance data from all the all the leading brands of thermostats. What we need to do is find more ways of data trading to solve problems.

Kigen's fundamental approach to this issue is that you can't trade data if you don't know its heritage. Consider smartphone photos: each has a geolocation and time stamp, but you can change those, so it can't be used as proof of anything. If you cryptographically sign a file, you can't change it again, meaning it could be used as proof and it becomes valuable. Moving to IoT, consider the moisture sensor again. It will become a hygiene factor to make sure no one has messed with the data. The more you make automated decisions, the more it's critical that it can't be tampered with. Every IoT device will need to provide information on when its data was produced, where, who has access to it, and so on.

MH: At Transforma Insights, we've looked closely at the topic of security risks and there aren't many IoT applications where there's no risk of intervention from a bad actor. Is that how you see it? ▶



VK: Yes, indeed. Think about commercial espionage and providing bad data about commodities. If you've seen the movie Trading Places, a lot of that revolved around providing false weather data which was very relevant to the prices of a commodity market, frozen orange juice.

MH: Great to get a reference to an Eddie Murphy movie into an interview, but sadly we can't dwell on it too long. I want to delve into how some of the technologies you're involved with are transforming the experience of consumer products?

VK: "How to transform experiences for customers?" I listen keenly from our customers, OEMs and device makers around this and feel we are at a great intersection of the tools available to them: Generative AI, cybersecurity, future of digital payments and more! Our job at Kigen is to make them successful in rolling these devices out of the market with the best chance of doing this now and lasting for the longest time for consumers to benefit. So three things:

Firstly, security that just works. End-to-end security, designed with a secure element that's resilient to hacks and built on standards such as GSMA and **Global Platform** so that consumers trust their IoT applications. Biometers, payments and deeper integration into the services that people rely on – are all enabled through these. We're bringing that into IoT devices as default.

Secondly, it's about using connectivity to deliver a product with a service. A product that is always connected is always able to deliver that benefit. And this extends to lots of use cases. Wi-Fi has been an easy route to connectivity, but it has its limitations in both resilient and consistent experience. Consumers expect unhindered always-on connectivity with a unique device experience, on the move: a connected watch or wearable on the run used to need a smartphone, now we see customers moving to narrowband-IoT (NB-IoT) enabled cellular products that can offer personal trainer and coach service, social encouragement, all independently.

Third, we have launched our eSIM consumer OS that is garnering interest particularly driving enriched mobility and travelling experiences, smart streaming wearables, voice and music streaming speakers and even laptops. Last year, our eSIM-enabled **Motorola** Satellite Link was unveiled with **Skylo**'s profile at CES, and went on to high praise as the 'Product of MWC22' for the simple experience delivering peace of mind in even the most remote situations. Similarly, we are looking ahead to supporting the next tranche of eSIM experiences that contain the ultimate blend of Gen AI applied with strong security and out-of-the-box connectivity. ■

www.kigen.com

We are looking ahead to supporting the next tranche of eSIM experiences that contain the ultimate blend of Gen AI