

What is the Future of Resilient IoT Connectivity?

An Interview with Thales

THALES
Building a future we can all trust

 **JUNIPER**[®]
RESEARCH





Mover & Shaker Interview with Thales, Platinum Winner of Enterprise IoT Solution, at the Future Digital Awards

Juniper Research interviewed Cyril Proye, IoT Marketing Segment at Thales, in January 2026



Cyril Proye is a marketing specialist working in the IoT Marketing Segment at Thales Digital Identity and Security since May 2024.

Proye previously served as IoT Marketing Director at Linxens; bringing expertise in smart cards, programme management, and new product development.

He is also an active industry speaker; recently highlighting Thales' use of GSMA's SGP.32 eSIM standard to enable secure, flexible global IoT connectivity.

Could you explain what the Thales IoT Suite is, and highlight which industries benefit most from its capabilities?

At its core, the Thales IoT Suite is an engine for operational resilience. We are delivering two critical capabilities in unison: agile connectivity management and uncompromising, end-to-end security. We achieve this by leveraging the eSIM as a hardware 'Root of Trust', paired with our remote provisioning platforms. The result? Absolute control over your devices, anywhere on the globe.

This capability is transformative for industries where downtime is not an option. For utilities, it means smart meters can be maintained remotely; eliminating costly field interventions. In retail, it guarantees the uptime of payment terminals; directly protecting revenue. We also see Smart Cities securing surveillance infrastructure, and Fixed Wireless Access providers delivering a seamless 'plug-and-play' experience worldwide. It turns connectivity from a challenge into a competitive advantage.

What recommendations would Thales share to help organisations efficiently manage large and varied IoT device fleets?

To scale from thousands to millions, the industry must pivot to the GSMA eSIM SGP.32 standard. This is not merely an update; it is the strategic unlock for massive IoT deployment. It bridges the gap between flexibility available in the consumer market and IoT constraints; allowing OEMs to consolidate production into a single SKU - a massive optimisation for global logistics.

For service providers, the value lies in agility. With the eSIM Orchestrator of our Thales Adaptive Connect solution, providers can automate fleet management using sophisticated business rules - like dynamic network selection based on location.

Ultimately, we are driving toward a 'Single Pane of Glass'. Rather than fragmenting control, we offer a unified interface for device, network, and data management. It allows leadership to adjust global connectivity strategies in real time, with precision and speed.

With the rapid changes in regulations and cyber threats, how does Thales ensure end-to-end security for IoT devices throughout their lifecycle?

We adhere to a simple philosophy; trust should be anchored in the combination of secure hardware and software. It begins with the eSIM itself; a tamper-resistant secure element. We do not simply claim security; we validate it. Our entire supply chain - from silicon production to our cloud platforms - is rigorously certified under GSMA eSIM Security Assurance (eSA) standards.

By deploying standards like GSMA IoT SAFE, we protect data integrity from the assembly line to the end of the device's life. Whether security systems or cameras, the credentials inside remain encrypted and compliant.



What role do you see Artificial Intelligence (AI) playing in the evolution of IoT connectivity?

AI is the catalyst shifting connectivity from a reactive utility to a proactive asset. The potential is immense. Predictive analytics enable anticipation of network requirements before latency occurs, while autonomous decision-making enables real-time network switching.

However, at Thales, we believe innovation must be principled. Capabilities are only viable when underpinned by trusted AI. Intelligence must be secure, transparent, and privacy-preserving. When AI influences mission-critical infrastructure, its decisions must be explainable and validated. That is the only way to build an ecosystem that is not just smart, but truly resilient.

More information on Thales' IoT Solutions

THALES

Thales (Euronext Paris: HO) is a global leader in advanced technologies for the Defence, Aerospace and Cyber & Digital sectors. Its portfolio of innovative products and services addresses several major challenges: sovereignty, security, sustainability and inclusion. The Group invests more than €4 billion per year in research and development in key areas; particularly for critical environments such as artificial intelligence, cybersecurity, and quantum and cloud technologies.

Thales' IoT solutions provide secure, scalable, and efficient connectivity for IoT deployments across various industries. The solutions provide a comprehensive suite of technologies that cover the full device lifecycle, including design, manufacturing and deployment. The offering is built on three core pillars:

1. **Build:** Thales works with original equipment manufacturer (OEMs) and IoT solutions providers to create robust designs using eSIM and iSIM standards. This ensures strong authentication and encryption.
2. **Run:** In this phase, Thales provides seamless global connectivity through remote eSIM provisioning and network activation. This allows IoT users to scale operations across various industries and geographies.
3. **Protect:** Thales applies deep cybersecurity expertise to secure devices against current and future threats. This is done through embedded Secure Elements (eSEs), Hardware Security Modules (HSMs), and solutions such as IoT SAFE and Trusted Key Manager to safeguard identities, data, and communications.

Thales partners with over 450 connectivity service providers; ensuring worldwide coverage and resilient operations. Its IoT technologies are designed to support compliance, adaptability, and reliability across multiple regions and networks. The solutions offered create an end-to-end ecosystem that integrates connectivity management, strong security, remote provisioning, and lifecycle optimisation to accelerate digital transformation.