

CIO

www.cioprime.com

PRIME

Be Informed. Be Inspired. Be Ahead

**WHY IOT
SECURITY
MATTERS:
PROTECTING
YOUR SMART
DEVICES
AND DATA**

**TOP 7 IOT
SECURITY
BEST PRACTICES
EVERY BUSINESS
SHOULD FOLLOW**

**LEADING
THE FUTURE OF
IOT
AND
SECURITY:
CEO of RIoT Secure AB
in
2025**

Aaron Securing the
Future of IoT
Ardiri



COVER STORY

AARON ARDIRI

Securing the
Future of IoT

On a Mission to Make Connected
Devices Safe and Scalable!



Think about the first time you held a device that felt magical. Maybe it was an early mobile phone, a handheld game, or a computer that seemed to do the impossible with very little power. Behind that magic were people like Aaron Ardiri, who learned early on how to make the most out of systems with almost no resources.

Aaron began writing code in the late 1980s, when computers were small in memory but big in possibilities. He worked on resource-constrained systems, where every byte mattered. Those challenges shaped his view of efficiency and security because a single misstep could bring everything crashing down. Over time, he explored almost every platform, building assemblers, emulators, and secure connectivity stacks for microcontrollers. Each step reinforced the lesson that security must be built into technology from the ground up.

Years later, as the Internet of Things started expanding, Aaron saw a familiar problem return. Developers were pushing boundaries but wrestling with the same issues he had faced decades earlier: how to create something new while keeping it safe and scalable. The stakes were higher now, with billions of connected devices entering daily life.

That realization led Aaron to create RIoT Secure. His vision was to clear the path for developers, so they could focus on building value without being weighed down by the complexity of securing and managing devices. RIoT Secure ensures that connected devices stay protected, connected, and manageable throughout their lifecycle.

For Aaron, it is about more than technology. It is about giving creators the freedom to innovate without fear of



compromise. His journey proves that lessons from the early days of coding still guide the future of connected systems. Efficiency, discipline, and security remain the cornerstones of progress.

Envisioning the Future of IoT Security

RIoT Secure AB sees IoT security as an ecosystem rather than a feature. The company's vision is to embed security

by design into every device, making trust, communication, and lifecycle management as seamless as Wi-Fi is today.

As billions of devices come online, the company believes the future depends on a foundation where secure communication, resilient updates, and compliance are automatic. By decoupling security into a dedicated microcontroller and offering a platform-based approach, RIoT Secure

gives IoT builders the ability to scale securely without slowing their innovation.

Addressing Overlooked Vulnerabilities in IoT

A major vulnerability often overlooked in the Internet of Things lies in the full lifecycle of devices. Companies usually direct attention only toward the initial deployment, leaving long-term security gaps exposed. Devices often remain active for many years, sometimes even decades, and attackers use this time to exploit weaknesses such as outdated firmware, fragile identity management, and insufficient update mechanisms.

RIoT Secure takes a different approach by addressing these challenges from the very beginning. Each device is given a secure identity at the start, backed by enforced secure boot, reliable over-the-air updates, and the safeguarding of intellectual property through advanced technologies like Shield. With these measures in place, security does not fade with time. Instead, it grows stronger as new threats emerge, ensuring that devices stay protected throughout their entire lifespan.

Balancing Innovation with Regulatory Demands in IoT Security

He sees compliance as a floor, not a ceiling. Regulations ensure a minimum level of security, but innovation allows him and his team to go far beyond that baseline. Their modular architecture – combining μ TLS, Fusion, Oasis, Brawl, and Shield – lets them adapt to regional standards while maintaining a globally consistent platform.

This flexibility means their customers can comply with EU cybersecurity laws, U.S. FDA requirements for

medical devices, or industrial regulations, without compromising on innovation.

What Differentiates RIoT Secure's Solutions from Others in the Market

Most cybersecurity providers retrofit security on top of devices, effectively like band-aids. RIoT Secure integrates security inside the device lifecycle, from secure boot to decommissioning.

Most providers focus on one piece of the puzzle, but the company's strength lies in the integrated stack: μ TLS for secure communication, Fusion for microcontroller programming, Oasis for trust management, Brawl for WebAssembly runtime flexibility, and Shield for intellectual property protection. Together, these deliver an end-to-end, future-ready solution unmatched in scope and depth.

Role of AI in Predicting and Mitigating IoT Threats

Aaron explained that AI complements

IoT security by allowing the detection of anomalies at scale. He shared that AI is leveraged both on the device side, where lightweight inference models can run within constrained environments, and on the server side, where aggregated intelligence identifies suspicious patterns across fleets of devices. According to him, this dual approach ensures threats are detected early, isolated quickly, and resolved before they escalate.

Integrating Security by Design in IoT Ecosystems

The long-term strategy is to make security invisible but inherent. This means developers do not have to think about certificates, key storage, or firmware protection, as they are built into the RIoT Secure microcontroller from the start.

By offloading these complexities, the approach ensures every IoT solution built on the platform begins with secure-by-design principles, without requiring developers to be



cryptography or compliance experts.

Partnerships as a Driving Force for RIoT Secure's Future

Aaron explained that partnerships are essential because IoT does not exist in isolation. By collaborating with larger enterprises, RIoT Secure integrates into their ecosystems; by working with governments and standards bodies, the company helps shape the frameworks that ensure safe, global adoption.

He added that the goal is never only to comply with standards, but to help set them, so that device makers, regulators, and end-users all benefit from a consistent, trusted security foundation.

Building a Culture of Innovation and Expertise at RIoT Secure

RIoT Secure invests heavily in cultivating a learning-driven culture. Many of the engineers came from embedded backgrounds, and they have been trained to think like security architects.

The company also creates opportunities for interns and researchers to explore advanced areas such as WASM runtimes for microcontrollers, a field where it has become a pioneer. This blend of mentorship, research, and real-world deployment fosters an environment where talent grows, stays, and thrives.

Ethical and Safety Principles in IoT Leadership

For him, the guiding principle is responsibility at scale. When devices control medical equipment, aircraft, or energy systems, failure is more than a data breach; it involves human lives. His leadership decisions always weigh innovation against resilience,

prioritizing transparency, auditability, and trust. He believes IoT security must serve not only businesses, but society as a whole.

Security Models in the Era of Edge, 5G, and Distributed Systems

According to Aaron, these technologies shift intelligence closer to the edge, which increases both the attack surface and the value of each device.

His team's response is to design lightweight runtimes and cryptographic stacks that allow even resource-constrained devices to operate securely in high-performance, low-latency environments. By leveraging 5G and edge processing, they also enable more distributed anomaly detection and policy enforcement, strengthening resilience at scale.

Measuring Success in Delivering Trust and Resilience in IoT Networks

Aaron explained that success is measured in three key ways.

- The first is **security integrity**, which refers to how effectively devices resist tampering and breaches.
- The second is **lifecycle reliability**, which reflects the ability to manage, update, and secure devices over the years in the field.
- The third is **developer efficiency**, which indicates how quickly customers can move from prototype to secure deployment.

According to him, when all three indicators are strong, it shows that trust and resilience are being delivered not only as a promise but also as a measurable outcome.

RIoT Secure's Vision for Global IoT Security

Projecting forward, five years, Aaron envisions RIoT Secure not just as a technology provider, but as a global benchmark for IoT security, making lifecycle protection as universal and unquestioned as HTTPS is for the web.

He believes every connected device, from healthcare and aviation to smart cities and industrial automation, should be born with trust built in: authenticated, updatable, and resilient by design. The company is already taking steps to influence international standards, embed its architecture into communication modules and chipsets, and prove through large-scale deployments that security can be seamless without slowing innovation.

The impact Aaron aims for is clear and measurable: devices that remain secure for a decade or more, developers who can bring solutions to market in half the time, and ecosystems that can update and evolve without fear of compromise. For him, success will be defined not by the number of devices secured, but by the fact that the global connected world is safer, more reliable, and more future-proof because RIoT Secure set the standard.

