Ubiquitous AI

PRESS RELEASE

June 17, 2026
Ubiquitous AI Corporation

Ubiquitous AI Proposes "Edge Security 3.0" Framework, Advancing Next-Generation Security Design to Drive Value Creation in Embedded Devices

— Transforming Security from "Obligation" to "Value Creation" —

Ubiquitous AI Corporation (Headquarters: Shinjuku, Tokyo; President & CEO: Yuta Oyoshi; hereinafter "Ubiquitous AI") is proposing "Edge Security 3.0" as a new framework to redefine the role of security in the IoT and embedded device sector, and will advance next-generation security design to enable new value creation in embedded devices.

In recent years, with the tightening of international regulations such as the EU Cyber Resilience Act (CRA) and the increasing sophistication of cyberattacks, security has become an essential requirement even for edge devices including IoT and embedded systems. However, many companies still view security as "a cost for regulatory compliance" or "an obligation required for commercialization," leaving them in a reactive posture. As a result, the risk of intrusion, theft, and tampering of critical information via edge devices continues to grow.

Drawing on the technical expertise and implementation know-how it has cultivated over many years in embedded software and security, Ubiquitous AI believes that going forward, security in edge devices should be positioned not merely as a defensive measure, but as a source of competitive advantage that enhances product value and business value.

Why "Edge Security 3.0" Is Needed Now

In the cloud and network domains, security has come to be recognized as an indispensable management issue for business operations. But for edge devices such as IoT equipment and industrial machinery, the approach often remains focused on defense — minimal regulatory compliance and vulnerability remediation.

However, the era of always-connected devices and OTA (Over-The-Air) feature updates is becoming the norm, and product value is increasingly formed not at the time of shipment, but across the entire operational lifetime of the device.

In this environment, Ubiquitous AI believes that embedding security from the design stage — and leveraging it as a foundation for improving product reliability and enabling new service offerings — will be a critical factor determining corporate competitiveness.

Ubiquitous AI proposes the following three stages for the future of edge device security, and will provide and progressively expand its product lineup to realize this vision.

The "Edge Security 3.0" Framework Proposed by Ubiquitous AI

Edge Security 1.0 — "Security as Obligation"
The minimum level of security required for commercialization, including regulatory compliance and vulnerability remediation.

Edge Security 2.0 — "Security that Protects the Brand"
Security that prevents unauthorized use and tampering through encryption, anti-tamper measures, and secure memory, protecting intellectual property and brand value.

Edge Security 3.0 — "Security that Creates Value"
Security that leverages security technologies to enable the following features and services, generating new revenue opportunities and business models:

- On-demand feature activation
- Subscription-based services
- License management
- Feature provisioning based on usage period

Products Supporting "Edge Security 3.0"
Ubiquitous AI is advancing the provision of security technologies implementable even in small edge device environments with significant resource constraints.

Post-Quantum Cryptography Domain
- "PQC (Post-Quantum Cryptography) Library" for the quantum computing era (in development)
- PQC-compatible TLS encrypted communications library (in development)

Device Protection Domain
- "Ubiquitous Securus" — an encryption and confidential data management solution with over 7.3 million cumulative shipments
- Lightweight security technology for small devices (in development)

Device Operations Domain
- "Edge Trust" — a device lifecycle management platform

Future Outlook

Ubiquitous AI has positioned the security domain as one of its key growth areas in its medium-term strategy.

Going forward, the company will continue to strengthen its work on next-generation security technologies including PQC and TPM, while expanding its product and service lineup — implementable even in resource-constrained embedded environments — through the "Edge Security 3.0" concept. The company aims to contribute to solving lifecycle-wide challenges and to enhancing the value of products, services, and their market standing.

Under the policy of "creating value from technology," Ubiquitous AI will position security not merely as a countermeasure, but as a foundation for enhancing product and business value — contributing as a trusted partner to customers' product competitiveness and sustainable business growth.

About Ubiquitous AI Corporation (Tokyo Stock Exchange: 3858)

Ubiquitous AI Corporation delivers advanced technologies and services that support customers in the manufacturing industry, building on decades of experience in embedded software development. With a strong foundation of leading-edge technologies and a global customer base, the company provides proprietary software products alongside related professional services. Ubiquitous AI is committed to the growth of its customers, business partners and society.

Head Office: Shinjuku First West Bldg. 17F, 1-23-7 Nishi-Shinjuku, Shinjuku-ku, Tokyo 160-0023, JAPAN
URL: https://www.ubiquitous-ai.com/en/

Note to investors

This press release is intended to provide information about the qualitative progress of Ubiquitous AI Corporation's business activities and is not a solicitation for investment. For details regarding financial results, key performance indicators, or forecasts, please refer to our most recent earnings summaries and other disclosures published through the Tokyo Stock Exchange.

Media Contacts

Yu Aso
Marketing and Communication Department
+81 3 5908 3451/ https://www.ubiquitous-ai.com/en/contact/others/