WALLIX anticipates cybersecurity shifts and unveils its 2026 technological vision

Paris, January 8, 2026 - WALLIX (Euronext ALLIX), the European cybersecurity champion and a key player in identity, access and privilege management, provides a simple and secure platform enabling organizations to operate freely across digital (IT) and industrial (OT) environments. Today, WALLIX unveils its 2026 outlook, presented by ***Julien Cassignol***, *Chief Product & Technology Officer (CPTO*). Against a backdrop of geopolitical tensions and accelerating digital transformation, four major forces are reshaping cybersecurity: stricter regulations, AI-driven intelligent automation, the exponential growth of digital identities, both human and machine, and the emergence of the post-quantum era.

Regulation, the foundation of trusted digital environments

European cybersecurity regulations continue to evolve, with the goal of creating digital environments where data protection and resilience are central. The NIS2 Directive, DORA Regulation, IEC 62443, Cyber Resilience Act, AI Act, and others now define demanding standards. In an unstable geopolitical context where cyber threats increasingly target the foundations of our economies and daily lives, these frameworks go beyond compliance. They reflect a collective ambition to build trusted digital ecosystems aligned with the interests of governments, organizations, and users.

The challenge is to ensure that sensitive data, particularly personal and industrial data, which represent critical assets, remains protected. It also requires keeping encryption keys under local control and strictly managing digital access within each organization. Achieving this level of operational sovereignty depends on scalable identity and access management platforms. By 2026, these platforms will be compliant by design with international standards and efficient by nature. They must be deployable across all environments, on-premises, hybrid, or cloud, without creating unwanted extraterritorial dependencies.

Digital autonomy is a strategic priority for WALLIX. With its modular WALLIX One platform, the company enables organizations to strengthen control over digital access and both human and non-human identities, while retaining full freedom of deployment. WALLIX is fully aligned with regulators' vision of resilient, interoperable, and trusted digital ecosystems.

Machine identity management: controlling access at scale

The number of digital identities is growing exponentially. Beyond human users, non-human identities (machines and agentic systems) are becoming a major security challenge. Service accounts, PLCs, robots, medical devices, and an estimated 30 billion connected objects by 2030 (according to Gartner) represent invisible identities that can cause significant breaches if left unmanaged. This issue is critical to the reliability of industrial environments and the resilience of essential and critical organizations.

By 2026, Machine Identity Management will be a core security discipline, applying the same rigorous controls to machines as to human users. Every secret, certificate, and key must be inventoried, protected, and automatically renewed. However, securing secrets alone is not enough. Each process using those secrets must also be identified, verified, and authorized. Even frequently rotated credentials cannot ensure security if the legitimate process using them has been compromised or replaced with malicious code.

WALLIX is fully committed to this approach, delivering open and innovative solutions to manage machine identities at scale. In particular, the company has joined **the OpenBao** open-source community, which pools efforts to secure secrets across hybrid and multi-cloud environments. This open approach enables organizations to retain control over their keys and access without dependence on a single proprietary vendor—and, most importantly, to scale securely. It reflects WALLIX's commitment to open standards as a foundation for trust, interoperability, and long-term freedom.

Agentic AI: towards autonomous Cyber Defense

As threats become faster and more sophisticated, intelligent automation is emerging as a key pillar of cybersecurity. While attackers increasingly leverage generative AI to enhance their techniques, defenders are turning to **agentic AI** capable of operating autonomously in complex environments. Embedded within Security Operations Centers (SOCs), this technology analyzes incidents end-to-end, prioritizes alerts, and frees teams from constant manual monitoring.

Cybersecurity is shifting from a reactive posture to proactive defense, capable of responding within seconds or even anticipating attacks. Intelligent automation makes it possible to manage what was previously unmanageable, such as millions of continuously evolving access rights. By combining machine learning for anomaly detection with large-scale data analysis across millions of events, AI can instantly identify abnormal behavior from a compromised or unsafe service account and neutralize it before a breach occurs, where it once took days to detect.

WALLIX continues to invest in combining AI with human expertise to deliver truly proactive defense. Agentic AI requires strict governance: it must only access the data necessary for its mission. This reinforces the strategic importance of Machine Identity Management in controlling non-human identities and permissions. **The recent acquisition of Malizen strengthens WALLIX's capabilities** in detecting anomalous behavior and automating data analysis, helping organizations stay ahead of increasingly rapid and sophisticated attacks.

Preparing for the post-quantum era: building cryptographic autonomy

Quantum computing represents a long-term strategic risk to data security, industrial systems, IoT networks, and other interconnected environments. Its ability to break current cryptographic algorithms means that data encrypted today could be exposed tomorrow if organizations fail to prepare. This includes industrial networks, hospital medical devices, and smart buildings.

The transition to post-quantum cryptography is therefore both a technical and strategic priority. Organizations must adopt a crypto-agility approach now, enabling them to evolve encryption mechanisms and security policies as standards mature.

Through its WALLIX One platform, WALLIX will integrate post-quantum encryption standards to support quantum-resistant algorithms. This includes securing backups, internal communications, and privileged

access with encryption designed to withstand future quantum attacks. By supporting organizations in migrating their keys, certificates, and protocols to these new standards, WALLIX continues to contribute to building European cryptographic autonomy.

About WALLIX

WALLIX (Euronext: ALLIX, listed since 2015) is a European cybersecurity publisher, leader in privileged access management (PAM), which helps organizations strengthen their security and digital sovereignty. Rooted in the European values of security and freedom, and recognized for the technological excellence of its WALLIX One platform by the largest analyst firms, WALLIX supports more than 4,000 organizations around the world. Its mission is simple: to protect identities, access, and privileges across all IT and OT environments, giving organizations the freedom to confidently move in a more secure digital world.
www.wallix.com | **info@wallix.com**

FINANCIAL COMMUNICATION CONTACTS

ACTUS Finance & Communication
Investor Relations - Hélène de Watteville
+33 (0)1 53 67 36 33 / **WALLIX@actus.fr**

Press Relations – Déborah Schwartz+33 (0)6 27 09 05 73 / **dschwartz@actus.fr**