WALLIX BASTION 9.0: TOWARDS A MORE ROBUST DATA PROTECTION SOLUTION THAT ADDRESSES EMERGING PANDEMIC-RELATED CYBERSECURITY ISSUES

- *WALLIX Bastion is one of the best Privileged Access Management (PAM) solutions, according to Gartner and KuppingerCole Analysts.*

- *WALLIX Bastion 9, the latest version of the ideal solution for securing new digital challenges related to the pandemic: widespread adoption of remote work and cloud services*

- *WALLIX Bastion 9 strengthens the cybersecurity of hospitals, which remain a major target of hackers*

Paris, November 8, 2021 – **WALLIX** (Euronext ALLIX), a European software company providing cybersecurity solutions and the specialist in identity and access security, launches WALLIX Bastion 9, the new version of its flagship Privileged Access Management (PAM) solution.

The pandemic has acted as a driver of the world's digital transformation, a process that began several decades ago encompassing widespread remote work, adoption of cloud services, telemedicine, distance learning, significant increase in the number of mobile devices, and so on. These new uses significantly increase the number of access points into companies' IT infrastructures. These many new potential entry points for hackers must be secured in order to protect data. In fact, although 2021 is not yet over, it has already become known for being a year of major cyberattacks and vulnerabilites, including PrintNightmare, Pegasus, and the Colonial Pipeline.

WALLIX Bastion, one of the best Privileged Access Management (PAM) solutions according to analysts Gartner and KuppingerCole.
When accessing a company's IT infrastructure, employees log in from their computer or mobile device with a username and password. Each employee has an account with access rights to specific resources. However, some employees, such as admins, have elevated rights allowing them access to all the company's resources. These are called privileged accounts. This makes them a primary target for hackers, who seek to penetrate a company's systems to gain access and steal sensitive data. WALLIX Bastion protects privileged account passwords by storing them in a password vault, monitors the activity of users holding these privileged accounts, and blocks their access in case of suspected identity theft. WALLIX Bastion also enables compliance with data protection regulation requirements (GDPR).

WALLIX Bastion 9, a new state-of-the-art version offering a higher security level
WALLIX has developed new features to make WALLIX Bastion an even more robust solution that drastically improves their customers' cybersecurity level and addresses current challenges:

✓ Increased protection for hospitals

Hospitals are a prime target for hackers, due to their lack of cybersecurity maturity and limited means to modernize and secure IT infrastructure. Cyberattacks on the sector regularly make headlines and the situation has worsened during the pandemic, including attacks on Vermont Medical Center, Sonoma Valley Hospital, Düsseldorf's University Hospital, and the UK's National Health Service, among others. In the midst of the pandemic, many healthcare organizations suffered cyberattacks on their Microsoft Active

Directory (AD), prompting ANSSI, the French National Agency for Information Systems Security, to emphasize the importance of strengthening AD security in hospitals.

In healthcare as in other sectors, the AD is a significant target for hackers as it contains the logins and passwords of all privileged accounts. WALLIX Bastion, and now WALLIX Bastion 9, is one of the only PAM solutions on the market capable of strengthening Active Directory security. WALLIX already secures the AD of 1,300 organizations worldwide, including many hospitals, essential service operators, and administrations.

✓ Improved remote work security

WALLIX Bastion is the ideal solution to secure remote work, especially when done from personal computers, mostly unsecured, as was the case with Bordeaux Airport in the midst of the lockdown. WALLIX Bastion enables secure remote access to the company's IT infrastructure, as well as management and monitoring of all IT activity. If WALLIX Bastion detects a cyberattack, the IT team analyzes each action performed and then establishes a remediation plan. With WALLIX Bastion 9, analysis reports are created automatically and in real time, and can be consulted from a dashboard, optimizing the speed of response to cyberattacks.

✓ Advanced security for cloud services

With now-widespread and standardized remote work in the wake of the health crisis, today many companies have shifted to fully remote or hybrid work models. The use of cloud services (online messaging, document sharing applications, etc.) will therefore continue to grow as companies find new ways of working. However, these services often have little or no security, thus creating new vulnerabilities for IT infrastructures. WALLIX Bastion secures access to any cloud service, as defined by the IT team. With WALLIX Bastion 9, the solution now automatically detects connections to any cloud service and secures access.

✓ Equal security for both corporate applications and users

Privileged accounts include both "human" and "non-human" accounts, such as corporate applications (Salesforce, Oracle, SAP, etc.) that can hold highly sensitive data. They, too, have logins and passwords to connect to the company's IT infrastructure through what are known as service accounts. WALLIX Bastion, thanks to AAPM (Application-to-Application Password Management) technology, protects service account passwords upstream via encryption. WALLIX Bastion 9 ensures that these passwords are changed regularly, for greater cybersecurity.

"*WALLIX Bastion 9 is a real step forward in terms of innovation at WALLIX. In fact, it is this version of our flagship WALLIX Bastion solution that has enabled us to move up from "Niche" player to "Challenger" in Gartner's 2021 Magic Quadrant, as well as being recognized as the European leader in PAM by KuppingerCole Analysts. We have leveraged all our expertise in access and identity security to develop features perfectly adapted to the market's current needs, which have enabled us to provide an effective response to the cybersecurity challenges resulting from the pandemic*" **says Emmanuel Pierre, Product Director at WALLIX**.

ABOUT WALLIX

A software company providing cybersecurity solutions, WALLIX is the European specialist in Identity and Access Security. WALLIX's unified solutions portfolio enables companies to respond to today's data protection challenges. WALLIX solutions guarantee detection of and resilience to cyberattacks, which enables business continuity. The solutions also ensure compliance with regulatory requirements regarding access to IT infrastructures and critical data. The portfolio of unified solutions is distributed through a network of more than 316 resellers and integrators worldwide. Listed on Euronext (ALLIX), WALLIX supports more than 1,500 organizations in securing their digital transformation. WALLIX is a founding member of the HEXATRUST group and has been included in the Futur40, the first ranking of fast-growing companies on the stock exchange published by Forbes France and is part of the Tech 40 index.

WALLIX affirms its digital responsibility and is committed to contributing to the construction of a trusted European digital space, guaranteeing the security and confidentiality of data for organizations as well as for individuals concerned about the protection of their digital identity and privacy. Digital technology, whether for professional or personal use, must be ethical and responsible in order to pursue a secure societal digital transformation that respects individual freedoms.

www.wallix.com | info@wallix.com

PRESS CONTACT

LEWIS
Eva ALLAVENA
06 18 10 80 12 / wallixfrance@teamlewis.com

FINANCIAL COMMUNICATION CONTACTS

ACTUS Finance & Communication

Investor Relations - Olivier LAMBERT
01 53 67 36 33 / wallix@actus.fr

Media Relations - Déborah SCHWARTZ
01 53 67 36 35 / dschwartz@actus.fr