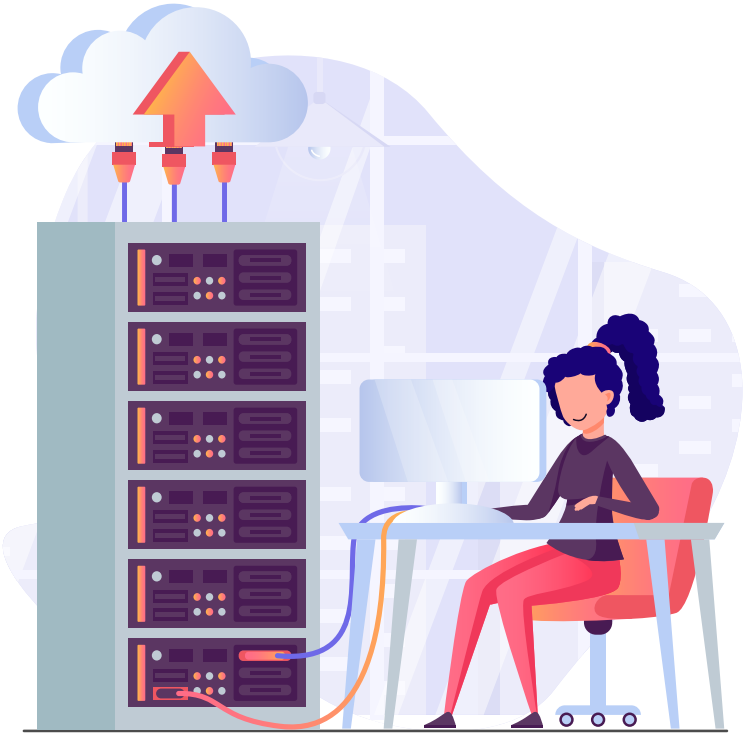
Gestion des accès à privilèges avec un petit plus

La gestion et la surveillance des accès à privilèges – privileged access management (PAM) – ne cessent de gagner en importance à une époque où la cybercriminalité fait rage. WALLIX, spécialiste du PAM, propose une plateforme globale pour la gestion, la sécurisation et la surveillance de tels accès.

L'accès aux systèmes, applications et services – que ce soit par des collaborateurs internes disposant d'autorisations spéciales (par exemple des administrateurs), des prestataires externes ou des composants logiciels entre eux – doit être surveillé et géré de manière particulièrement stricte. En effet, une fois que l'on est «entré» dans un système à privilèges, on peut déployer des activités non seulement utiles mais aussi malveillantes de manière quasiment illimitée. Les solutions de gestion des accès à privilèges veillent à ce que seuls les accès vraiment autorisés aient (ou puissent avoir) lieu, tout en garantissant une traçabilité complète de tous les processus.



Un Bastion contre les accès non autorisés

L'entreprise française de logiciels WALLIX, fondée en 2003, s'est entièrement consacrée à la sécurisation des accès à privilèges sous la devise «PAM4ALL». Spécialiste du PAM depuis la première heure, WALLIX s'est imposé comme le leader européen d'une plateforme PAM globale, avec plus de 1800 collaborateurs et trois centres de recherche et développement en France et en Espagne. WALLIX figure en tant que leader dans le dernier Magic Quadrant 2022 de Gartner pour les solutions PAM.

Le composant clé de la plateforme WALLIX, appelé Bastion, couvre tous les aspects de la gestion des accès à privilèges. En font partie des thèmes tels que la gestion des accès, la gestion des sessions avec support pour le monitoring et l'enregistrement complet des sessions RDP/TSE, VNC, SSH et Telnet, le mode supervision pour le suivi en direct des sessions par les administrateurs ainsi que la gestion des mots de passe avec coffre-fort de mots de passe et l'application des prescriptions en matière de mots de passe, y compris l'actualisation régulière des mots de passe.

Toutefois, les fonctionnalités de Bastion ne s'arrêtent pas là. Grâce à des pistes d'audit fiables et juridiquement valables pour toutes les activités des utilisateurs privilégiés, la solution est parfaitement adaptée pour soutenir la conformité de l'entreprise et les réglementations légales telles que PCI-DSS, Basel III et SOX. En outre, Bastion détecte les activités inhabituelles et suspectes et aide à bloquer ces menaces à temps ou, en cas d'attaque réussie, à les suivre et à les documenter. Et avec le composant AAPM (application-to-application password management), Bastion assure des accès sécurisés, automatisés et cryptés entre les applications et les services via l'API et soutient ainsi les modèles de développement et d'exploitation modernes tels →

que DevOps et RPA (robotic process automation) – aussi bien sur site que dans le cloud, aussi bien pour les environnements IT que pour les environnements IoT et OT.

Protection des points finaux par la gestion des privilèges
Avec l'option WALLIX Bestsafe, WALLIX offre de nombreuses caractéristiques supplémentaires qui servent à la sécurisation et au durcissement des points finaux avec une protection proactive au niveau des processus. Bestsafe ne nécessite pas de mises à jour régulières, n'utilise qu'un minimum de ressources système en tant que service sans agent et neutralise 95 % de tous les logiciels malveillants. Bestsafe agit de manière totalement transparente pour les utilisateurs. La solution est facile à configurer grâce à des listes blanches, grises et noires et permet des réglages de haute granularité – par exemple avec des règles de ransomware sophistiquées.

Services d'identité à partir du cloud
Avec WALLIX Trustelem, le fabricant propose un accès sûr et pratique selon le principe «identity as a service» – ceci au moyen d'une authentification multifacteurs (MFA) basée sur le contexte et de la fédération d'identité avec support pour l'Active Directory, Azure AD, LDAP et Google Workspace. La solution MFA intégrée permet une protection rapide des applications en nuage et une connexion simple (single sign-on) pour tous les utilisateurs. Les solutions de WALLIX, garanties sans backdoors, permettent une gestion globale de la sécurité et des cyberrisques pour la protection de l'entreprise – aussi bien dans le secteur financier, l'industrie de production et le secteur de la santé que dans d'autres infrastructures sensibles. Elles disposent de la certification CSPN de l'ANSSI, l'équivalent français du BSI allemand, contribuent en outre au respect des exigences de conformité et fournissent des informations pour des audits fiables.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch

→ **boll.ch/wallix**