WALLIX
TRACE, AUDIT & TRUST

NOUS PROTÉGEONS VOS ACTIFS SENSIBLES
NOUS COMPRENONS VOS MÉTIERS

FINANCE & ASSURANCE

TRANSITION NUMERIQUE / CLOUD COMPUTING / COMPLIANCE

Avec la dématérialisation, le secteur finance & assurance est particulièrement exposé à la cybercriminalité : l'expansion des réseaux et des technologies, l'ouverture des Systèmes d'Information aux échanges extérieurs et la croissance des transactions électroniques donnent autant de possibilités de voir des attaques, des vols ou des pertes de données se multiplier. **La transition numérique et les services hébergés dans le cloud**, challenges de la transformation métier portés par ce secteur d'activité, **sont également des défis pour la cybersécurité. Tout comme les besoins de compétences et d'externalisation nécessitent de repenser la gouvernance de la sécurité des Systèmes d'Information.**

RÉGLEMENTATIONS

- **NIS**
- **RGPD**
- **PCI-DSS**
- **BALE I, II, III**
- **Sarbanes-Oxley Act - SOX**
- **SOLVABILITÉ 2**
- **ISO-27001/17799**

Les normes et les réglementations auxquelles sont soumises les institutions financières impliquent la garantie d'une protection des Systèmes d'Information contre les manœuvres frauduleuses tant envers les entreprises qu'envers leurs usagers. La séparation des pouvoirs dans le contrôle des comptes à privilèges aide à garantir l'intégrité des dossiers sensibles de l'entreprise et à les prémunir contre toute activité irresponsable ou illégale. Puisque les accès privilégiés permettent à leurs utilisateurs d'avoir accès aux applications tout autant qu'à leur contenu, il est nécessaire de repenser la gouvernance et le contrôle de ces utilisateurs. Il s'agit de protéger à la fois les actifs sensibles, les informations à caractère personnel, les données commerciales et la réputation de l'entreprise.

CAS D'USAGE

Garantir l'intégrité et surveiller les accès des fichiers est un facteur-clé dans la conformité aux normes de sécurité informatique des données financières : la gestion des accès à privilèges est indissociable d'une gouvernance de la sécurité.

- **Garantir la confidentialité des données personnelles des utilisateurs et des clients :** gestion des mots de passe de l'infrastructure, des applications, changement et distribution des mots de passe aux utilisateurs en fonction des usages,
- **Protéger les ordinateurs, les réseaux, les systèmes et bases de données et tous les applicatifs critiques contre les accès imprévus et non autorisés :** sécuriser les identifiants et les mots de passe dans un coffre-fort certifié,
- **Révoquer les accès des personnels non autorisés ou ayant quitté l'organisation et contrôler la politique de sécurité interne et le respect de la réglementations :** imputabilité des connexions et traçabilité des actions,
- **Alimenter des systèmes d'analyse comportementale et de gestion des événements (SIEM) :** anticiper et visualiser les menaces externes et internes.