La sécurité cloud : l'adoption du modèle Zero Trust

Date de la veille : 24 Avril 2026

Le modèle Zero Trust s'impose en 2026 comme le nouveau standard de sécurité des environnements cloud. Contrairement aux approches traditionnelles qui supposent qu'un utilisateur connecté au réseau de l'entreprise est fiable par défaut, le Zero Trust repose sur un principe fondamental : ne jamais faire confiance, toujours vérifier. Concrètement, chaque accès à une ressource cloud — qu'il provienne d'un employé, d'une application ou d'un appareil — est systématiquement authentifié, autorisé et contrôlé, quelle que soit sa provenance. Les grands fournisseurs cloud (AWS, Azure, Google Cloud) intègrent désormais nativement ces mécanismes dans leurs plateformes, via la gestion des identités et des accès (IAM), le chiffrement de bout en bout et la surveillance continue des comportements anormaux.

Cette approche apporte des bénéfices majeurs aux entreprises opérant dans des environnements multi-cloud et hybrides. Elle réduit considérablement la surface d'attaque en limitant les droits d'accès au strict nécessaire, empêchant ainsi la propagation latérale d'une menace en cas de compromission. Elle améliore également la conformité réglementaire, les principes Zero Trust répondant directement aux exigences de NIS2 et du RGPD en matière de contrôle des accès et de traçabilité. Enfin, l'automatisation des contrôles de sécurité qu'elle implique libère les équipes IT d'une surveillance manuelle coûteuse, tout en offrant une réactivité bien supérieure face aux cybermenaces de plus en plus sophistiquées.

Sources : https://www.lemagit.fr/actualites/366637507/Les-tendances-du-cloud-IaaS-en-2026 https://thrivenextgen.com/top-cloud-trends-in-2026/ https://keytech.io/les-grandes-tendances-it-2026-ce-qui-change-vraiment-pour-les-entreprises/