AWS CONNAIT SA 4ÈME PANNE EN 5 ANS

La panne massive du cloud d'Amazon Web Services (AWS), dont l'origine reste inexpliquée, a provoqué une véritable onde de choc sur le web mondial. En quelques heures, des milliers de sites et services essentiels ont été rendus inaccessibles : un épisode qui illustre la dépendance critique de nos économies numériques à quelques acteurs privés extra-européens.

Suite à cette quatrième panne d'AWS en cinq ans dans la région Est des États-Unis, les commentaires se multiplient. Voici tout d'abord celui de **Brent Ellis, analyste principal chez Forrester**, sur l'impact de cette panne et les dangers liés à une dépendance excessive à un seul fournisseur de cloud.

L'impact de cette panne

« AWS alimente des millions de sites web et d'applications, transformant un simple problème technique en une perturbation mondiale. Cette panne particulière met en évidence les problèmes fondamentaux liés à la résilience du cloud, qui découlent d'une dépendance excessive à des services tels que le DNS, qui n'ont pas été conçus pour répondre aux exigences technologiques de l'ère du cloud. Elle souligne également comment le risque de concentration — un risque systémique dangereusement puissant mais souvent négligé — apparaît lorsque tant d'entreprises de tous les secteurs deviennent dépendantes d'un seul fournisseur de cloud et, plus précisément, d'une seule région couverte par ce fournisseur.

« Mais le problème va au-delà des dépendances régionales internes d'AWS pour toucher les dépendances logiques à travers la plateforme. DynamoDB, le premier service identifié comme étant affecté par les problèmes DNS, joue un rôle central dans d'autres services AWS pour l'analyse, l'apprentissage automatique, la recherche, etc. »

Le modèle de responsabilité partagée d'AWS

« Il est très tentant de faire appel aux géants de la technologie, mais il serait erroné de supposer qu'ils sont trop grands pour faire faillite ou intrinsèquement résilients, comme le prouvent les pannes actuelles et passées.

« En ce qui concerne les promesses de résilience, AWS renvoie ses clients à son modèle de responsabilité partagée afin de mettre en évidence les domaines dans lesquels il assume la responsabilité de la disponibilité des services et ceux dont les clients sont responsables. Mais lorsque des services essentiels tels que le DNS tombent en panne, même les applications bien conçues peuvent devenir instables. AWS s'efforce de réparer son infrastructure, mais de nombreuses entreprises doivent attendre que cela soit fait, même si elles ont suivi les modèles de conception recommandés. Ce problème n'est pas exclusif à AWS, mais il est devenu récurrent, en particulier dans la région Est des États-Unis, où les clients sont laissés pour compte lorsqu'il s'agit de faire face aux conséquences de la panne. »

Risque concentré et dangers liés à l'incapacité à gérer les dépendances imbriquées

« La commodité l'emporte souvent sur la gestion des dépendances complexes et imbriquées dans des environnements hautement concentrés. Malgré les pannes passées, les organisations qui n'ont pas su gérer cette complexité ont été les premières touchées lorsque des problèmes en cascade ont perturbé les systèmes, les processus et les opérations.

« L'ancrage du cloud, en particulier AWS, dans les entreprises modernes, associé à un écosystème interdépendant de services SaaS, de développement logiciel externalisé et d'une visibilité quasi nulle sur les dépendances, n'est pas un bug, mais bien une caractéristique d'un risque hautement concentré où même de petites interruptions de service peuvent avoir des répercussions sur l'économie mondiale. »

Ce que les responsables IT peuvent faire dès maintenant ? « *Du point de vue de la résilience du cloud, les responsables technologiques des entreprises doivent désormais suivre deux lignes d'action : développer des outils pour accroître la fiabilité des systèmes technologiques et traiter les zones d'ombre contractuelles liées aux modèles de responsabilité partagée avec les fournisseurs de cloud (et de SaaS).* »

Quand le cloud d'Amazon tousse, c'est toute l'économie numérique mondiale qui s'enrhume, poursuit **Olivier Lambert, co-fondateur et CEO de Vates**. Et si cet incident n'était pas qu'un dysfonctionnement technique, mais le symptôme d'une vulnérabilité stratégique ?

Une défaillance interne, pas une cyberattaque, rappelle **Darren Guccione de Keeper Security :** « *Si les pannes Internet majeures suscitent souvent des inquiétudes immédiates quant à une cyberattaque, les rapports actuels indiquent que la perturbation importante d'AWS a été causée par une défaillance interne de l'infrastructure, plutôt que par une activité malveillante. Il s'agit d'une distinction importante, car toutes les défaillances des systèmes ne sont pas le résultat d'une faille de cybersécurité, et confondre les deux peut brouiller la compréhension des risques réels.*

Les écosystèmes informatiques modernes sont complexes, interconnectés et fortement dépendants d'une poignée de fournisseurs de cloud critiques. Lorsqu'un incident de cette ampleur se produit, qu'il soit dû à une défaillance technique ou à une mauvaise configuration, son impact sur les opérations mondiales peut être aussi grave qu'une cyberattaque coordonnée.

Pour les entreprises, cela souligne la nécessité d'une résilience qui va au-delà de la prévention des menaces. Les plans de continuité des activités doivent tenir compte à la fois des perturbations cybernétiques et non cybernétiques, en garantissant que les systèmes d'accès privilégié, d'authentification et de sauvegarde restent sécurisés et fonctionnels, même lorsque l'infrastructure centrale est affectée.

Les cadres Zero Trust et les solutions de gestion des accès privilégiés (PAM) sont conçus pour protéger contre les acteurs malveillants, mais ils peuvent également jouer un rôle essentiel dans le maintien de la visibilité et du contrôle pendant les pannes du système, tout en améliorant la résilience et les capacités de réponse aux incidents des clients. La véritable résilience ne consiste pas seulement à prévenir les attaques, mais aussi à garantir la stabilité en cas de défaillance. »

Pour **Thierry Bedos, VP South EMEA de Keepit**, spécialiste danois et européen de la protection, la sauvegarde et la restauration de données et d'applications SaaS, indépendant des hyperscalers cloud mondiaux : « *La panne de service survenue aujourd'hui, qui a affecté de nombreuses plateformes dans le monde à la suite d'un dysfonctionnement d'AWS, illustre de manière frappante un principe fondamental : même lorsque les infrastructures cloud sont dites "hautement disponibles", les entreprises doivent prendre des mesures complémentaires pour protéger leurs données et applications SaaS critiques.*

De telles pannes à grande échelle rappellent qu'un simple hébergement dans le cloud ne suffit pas. L'association "SaaS + sauvegarde SaaS indépendante" constitue désormais un pilier essentiel de la stratégie de résilience des entreprises. Chez Keepit, et en tant qu'acteur européen, nous encourageons les organisations à considérer la sauvegarde SaaS non pas comme une option, mais comme un élément fondamental de leur gouvernance IT, de leur conformité et de leur protection opérationnelle. »

.Source : IT Channel - octobre 2025