Acronis

LIVRE BLANC

Six risques majeurs pour les données G Suite et comment les maîtriser

UNE PROTECTION TRÈS LIMITÉE CONTRE LES PERTES DE DONNÉES

Si votre entreprise utilise G Suite, vous pouvez compter sur un accès fiable à ses applications, avec un haut niveau de disponibilité. Cela étant, de nombreux professionnels de l'informatique s'imaginent à tort que Google offre une protection complète et une conservation à long terme des données G Suite.

En réalité, les e-mails, pièces jointes, événements de calendrier, contacts et fichiers partagés stockés dans G Suite ne bénéficient d'aucune protection contre les pertes de données les plus courantes et les plus graves (suppressions accidentelles, attaques de malwares, etc.).

Dans bon nombre d'entreprises, l'utilisation de G Suite crée donc une faille dans la protection des données, ce qui peut leur causer de mauvaises surprises en cas d'incident. Ce n'est que trop tard qu'elles s'apercevront que Google ne propose que des fonctionnalités limitées pour la restauration de données G Suite perdues, détruites ou endommagées — bien loin des solutions de sauvegarde et de sécurité performantes qu'utilisent la plupart des organisations pour protéger leurs autres applications critiques.

> Ce livre blanc explique diverses limitations dans les fonctions de protection des données de Google qui peuvent facilement passer inaperçues et indique comment remédier aux vulnérabilités de G Suite.

LES SIX PRINCIPALES MENACES POUR LA SÉCURITÉ DES DONNÉES ASSOCIÉES À L'UTILISATION DE G SUITE

Google a investi massivement dans le matériel, les logiciels, les réseaux, la sécurité et les opérations de ses centres de données pour offrir à G Suite un niveau élevé de performance, d'accès et de disponibilité. Ses priorités sont la résilience de l'infrastructure de base, la capacité de reprise en cas de catastrophe naturelle majeure (p. ex. inondation, tremblement de terre, ouragan) et la restauration limitée et à court terme des données G Suite perdues ou corrompues.

Google peut détecter et surmonter rapidement ses propres erreurs opérationnelles, pannes de site, défaillances matérielles et problèmes réseau survenus dans ses centres de données Cloud conformément à ses accords de niveau de service qui sont axés sur la disponibilité des applications. Ces mesures ne protègent néanmoins pas votre entreprise contre les nombreux problèmes courants de pertes de données avec G Suite, tels que la suppression accidentelle ou malveillante de données par des employés ou les tentatives externes de compromission par le biais de malwares ou de ransomwares. Par ailleurs, il arrive souvent que les administrateurs informatiques définissent des périodes de rétention trop courtes pour les messages Gmail : les e-mail sont alors supprimés très rapidement, et impossibles à restaurer en cas de besoin.

> Google est capable de restaurer la plupart des données G Suite pendant une courte période suivant leur suppression par un utilisateur ou un administrateur (par défaut, 25 jours pour les messages Gmail et les fichiers Drive, 20 jours pour les profils utilisateurs). Vous pouvez avoir soudain besoin d'e-mails ou de fichiers d'un ancien employé ou d'un projet resté longtemps inactif et découvrir après des recherches laborieuses que Google n'a conservé aucune copie que vous pourriez restaurer.

LES ADMINISTRATEURS G SUITE DOIVENT MAÎTRISER LES RISQUES POUR LES DONNÉES DANS SIX DOMAINES MAJEURS

1. Suppressions accidentelles

RISQUE POUR LES DONNÉES : Au cours d'une journée de travail, il arrive fréquemment qu'administrateurs ou utilisateurs suppriment des profils utilisateur G Suite, des e-mails et pièces jointes Gmail, des événements de calendrier, des contacts et des fichiers Google Drive. Ces suppressions peuvent être accidentelles, ou délibérées puis regrettées. (Il nous est déjà tous arrivé d'avoir besoin de nous référer à un e-mail que nous avions supprimé la veille.)

POINT FAIBLE DE GOOGLE : Les suppressions de ce type sont répliquées au niveau du réseau. L'ancienneté des ressources aggrave le problème : les données plus anciennes risquent être définitivement supprimées et irrécupérables. Les suppressions plus récentes de ressources moins anciennes sont moins problématiques ; en effet, les fichiers et les e-mails supprimés de façon réversible peuvent être récupérés à court terme dans la Corbeille ou le dossier Éléments supprimés.

2. Utilisateurs malveillants

RISQUE POUR LES DONNÉES : Les ressources G Suite doivent être protégées non seulement contre les suppressions ordinaires non malveillantes, mais également contre toute altération ou destruction malveillante des données par des employés, sous-traitants ou partenaires mal intentionnés.

POINT FAIBLE DE GOOGLE : À l'exception des suppressions de ressources relativement récentes, Google ne dispose d'aucune protection contre la destruction ou l'altération malveillante en interne des données G Suite. Après tout, le fournisseur de services n'a aucun moyen de savoir ce qui constitue une menace ou non.

3. Cybermenaces

RISQUE POUR LES DONNÉES : Les données G Suite sont exposées à la destruction ou à la modification par différents malwares, notamment par des ransomwares, qui chiffrent les données des utilisateurs et les prennent en otage contre rançon payée en ligne. Ces attaques peuvent être lancées par des pirates, des cybercriminels ou des États hostiles.

POINT FAIBLE DE GOOGLE : Google offre des protections très limitées contre les attaques par malware (comme les ransomwares) et une capacité limitée à restaurer la version antérieure à l'attaque des fichiers chiffrés ou modifiés par les malwares.

4. Employés quittant la société

RISQUE POUR LES DONNÉES : Les entreprises commettent souvent l'erreur de fermer les comptes G Suite des employés qui quittent la société ou sont licenciés, sans en sauvegarder les données.

POINT FAIBLE DE GOOGLE : À l'exception des comptes G Suite fermés récemment (au cours des 20 derniers jours), Google ne peut pas restaurer les données G Suite d'un utilisateur supprimé.

5. Failles des règles de rétention

RISQUE POUR LES DONNÉES : Un changement ou l'inadéquation des priorités dans les règles de rétention de G Suite peut entraîner une suppression définitive des données alors qu'elles pourraient encore être utiles. Pour remédier à ce problème, il faut vérifier et mettre à jour régulièrement les règles de rétention.

POINT FAIBLE DE GOOGLE : Les clients G Suite sont responsables de la gestion des règles de rétention. Si, pour quelque raison que ce soit, une suppression définitive se produit en raison de l'obsolescence des règles de rétention existantes, Google n'a pas la possibilité de récupérer la ressource supprimée.

6. Problèmes juridiques et de conformité

RISQUE POUR LES DONNÉES : Les obligations réglementaires (notamment la conservation des documents fiscaux pendant une période définie) et les problèmes juridiques peuvent augmenter les coûts engendrés par les pertes de données non protégées que nous évoquions ci-dessus. La perte définitive de données G Suite peut exposer l'entreprise à des problèmes importants : amendes réglementaires nationales ou sectorielles ; sanctions pénales (dommages et intérêts, procès perdu si l'entreprise est incapable de produire les preuves numériques demandées) ; pertes de revenus et chute du cours des actions ; perte de confiance des clients ; atteinte à l'image de marque.

POINT FAIBLE DE GOOGLE : Compte tenu de tous les risques de pertes de données associés décrits ci-dessus, Google peut difficilement protéger les entreprises qui utilisent G Suite contre les différents risques de non-conformité et vulnérabilités juridiques. Par exemple, après une attaque par ransomware, une société qui stocke dans G Suite les données personnelles de ses clients résidents de l'Union, risque de ne pas pouvoir répondre aux demandes de copies de ces données, et donc de contrevenir au RGPD.

EN CONCLUSION

Une fois que l'on appréhende correctement les divers points faibles de Google en matière de protection des données G Suite, il faut rechercher des solutions qui permettent de combler ces lacunes. Les enjeux sont élevés : l'absence de protection contre les pertes de données G Suite peut avoir de lourdes conséquences, notamment sur une carrière.

ACRONIS BACKUP OFFRE DES SAUVEGARDES DANS LE CLOUD SIMPLES, EFFICACES ET SÉCURISÉES POUR G SUITE

SOLUTION CONVIVIALE DE SAUVEGARDE CLOUD À CLOUD POUR G SUITE

Acronis Backup protège les données G Suite grâce à une sauvegarde directe sans agent depuis les centres de données Google vers le réseau mondial de centres de données Acronis. L'agent d'Acronis Backup s'exécute dans le Cloud Acronis sécurisé et non sur site, ce qui optimise et simplifie le processus de configuration et de maintenance.

RESTAURATION GRANULAIRE POUR G SUITE

Acronis Backup offre une série de fonctionnalités de restauration avancées qui facilitent la restauration rapide d'un grand nombre d'éléments G Suite. Ces fonctions de restauration granulaires permettent de télécharger un fichier directement depuis la sauvegarde, de télécharger une version d'un document parmi plusieurs versions (et pas seulement la plus récente) et de restaurer tout élément de donnée vers son emplacement d'origine ou une nouvelle destination.

FONCTIONS DE RECHERCHE AVANCÉES

Les fonctionnalités de recherche simples et pratiques vous permettent de trouver rapidement les données que vous recherchez, par exemple les e-mails d'un employé qui a quitté la société ou un ancien document dont vous avez besoin pour régler un problème juridique. Pour Gmail, les clients peuvent avoir recours à la recherche par métadonnées pour les boîtes aux lettres (recherche par objet, destinataire, expéditeur, nom de fichier joint ou date), ou utiliser la recherche en texte intégral pour rechercher des données dans le corps du message. Dans le cas de Drive, Contacts et Agenda, les clients peuvent lancer une recherche par métadonnées, par exemple sur les noms de fichier.

FONCTIONNALITÉ UNIQUE DE NOTARISATION PAR BLOCKCHAIN POUR LES DONNÉES GOOGLE DRIVE

Les entreprises qui sauvegardent leurs données Google Drive à l'aide d'Acronis Backup peuvent profiter du service Acronis Notary intégré, qui utilise la technologie Blockchain pour apporter la preuve que les sauvegardes Google Drive n'ont pas été altérées. Cette capacité à attester de l'intégrité de vos sauvegardes Google Drive est particulièrement utile pour les documents juridiques, contrats, fichiers multimédias, images de caméras de surveillance, dossiers médicaux, contrats de location ou accords de prêt.

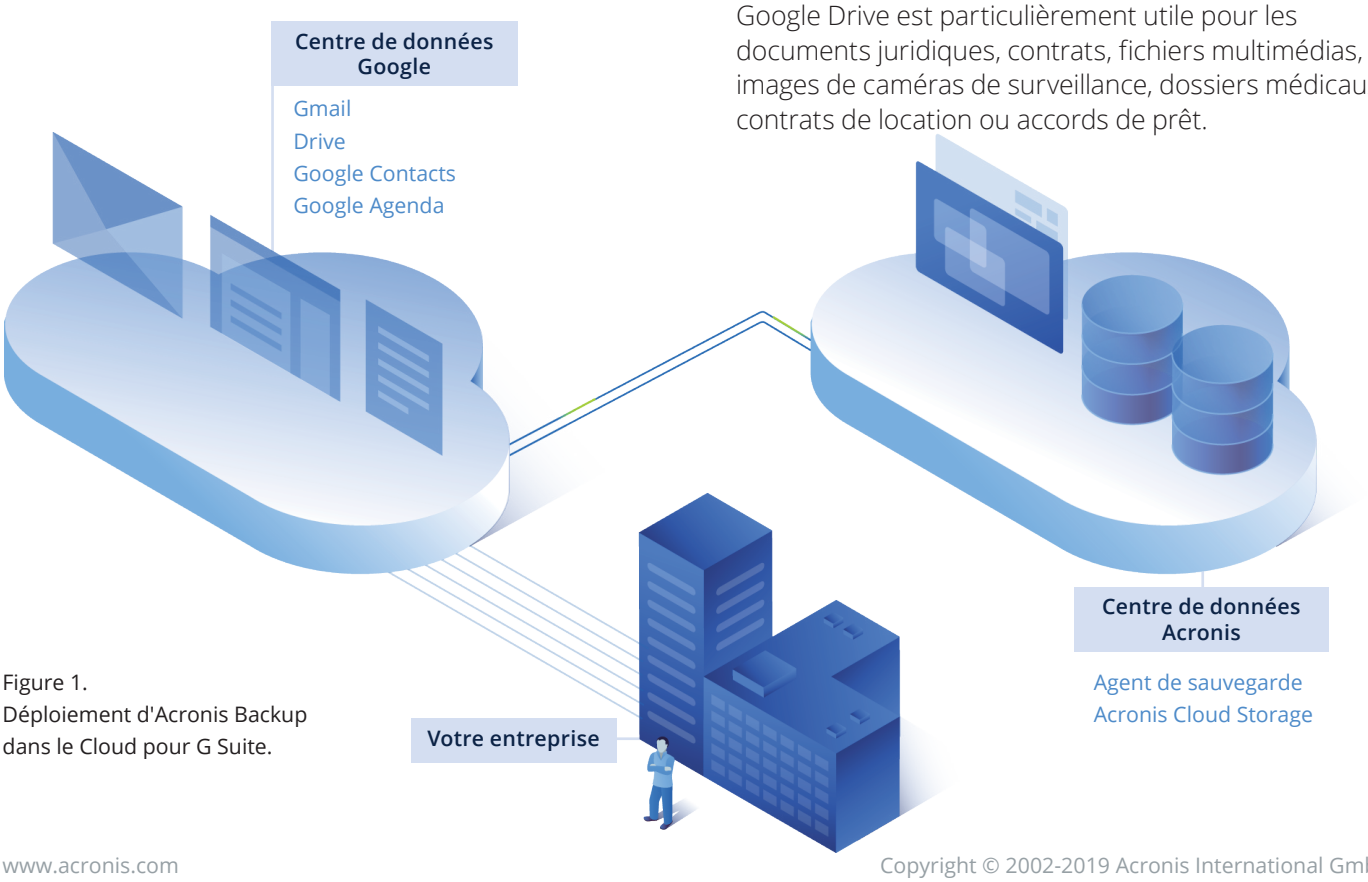

Figure 1.
Déploiement d'Acronis Backup dans le Cloud pour G Suite.

CONFIDENTIALITÉ DES DONNÉES RENFORCÉE

Acronis Backup protège les données contre les intrus grâce à un chiffrement multiniveau des sauvegardes renforcé par des transferts de données sur le réseau avec chiffrement TLS, stockage en centre de données avec chiffrement de haute qualité au niveau du disque et chiffrement par archive avec AES-256.

DÉTECTION AUTOMATIQUE DES NOUVEAUX UTILISATEURS G SUITE ET DES TEAM DRIVES

Une fois le plan de sauvegarde de groupe initial configuré et activé pour un environnement G Suite, le personnel informatique n'a pas besoin de le modifier à chaque ajout d'utilisateur ou de Team Drive. Acronis Backup les détecte automatiquement et met à jour le plan de sauvegarde pour les y intégrer.

PRISE EN CHARGE DE L'AUTHENTIFICATION MULTIFACTEUR GOOGLE

Acronis prend en charge l'authentification multifacteur Google pour permettre l'utilisation de mesures d'authentification supplémentaires comme les appareils approuvés ou les empreintes digitales. En l'absence d'authentification multifacteur, seul un mot de passe est requis pour la vérification.

OUTILS PUISSANTS DE GÉNÉRATION DE RAPPORTS ET DE SURVEILLANCE D'ÉTAT

Acronis offre des fonctions avancées de génération de rapports et de surveillance de l'état des sauvegardes pour aider le personnel du service informatique à améliorer son efficacité et sa réactivité. Le portail de gestion Acronis propose des widgets compacts et conviviaux contenant toutes les statistiques de sauvegarde et de restauration, ainsi que des rapports, des notifications et des alertes pour les événements critiques.

CLOUD ACRONIS HAUTEMENT SÉCURISÉ

Acronis sauvegarde les données G Suite directement vers Acronis Cloud, un réseau international de centres de données sécurisés par un programme complet de sécurité et de conformité qui comprend des contrôles administratifs, physiques et techniques basés sur une évaluation continue des risques.

Nos règles et processus de sécurité des informations reposent sur des normes de sécurité internationales largement acceptées, comme les normes ISO 27001 et NIST (National Institute of Standards and Technology). Ils tiennent compte des exigences des cadres réglementaires locaux en la matière, comme le règlement général sur la protection des données (RGPD) de l'Union européenne et la loi HIPAA (Health Insurance Portability and Accountability) américaine. Parmi les fonctions de sécurité d'Acronis Cloud :

- **Contrôle d'accès au niveau de l'entreprise** basé sur des ID utilisateurs uniques et mots de passe forts, des protocoles d'authentification sécurisée (LDAP, Kerberos, SSH), une authentification à deux facteurs et l'utilisation de pare-feux pour application Web
- **Sécurité des données multiniveau et en zones** renforcée par un chiffrement en temps réel des données en transit et au repos, un transfert sécurisé des données sur HTTPS (TLS), un chiffrement AES-256 pour les données client et la technologie Acronis Cloud RAID pour une disponibilité maximale des données
- **Sécurité physique garantie par des clôtures élevées** avec un accès contrôlé par analyse biométrique de la géométrie de la main et une carte de proximité, une vidéosurveillance renforcée par un archivage sur 90 jours et une équipe de sécurité présente 24 h/24, 7 j/7 et 365 jours par an
- **Infrastructure de centre de données redondante à haute disponibilité** protégée par des systèmes d'alimentation de secours (UPS) et des générateurs diesel, un système de conditionnement d'air, un réseau informatique et des systèmes d'alimentation électrique de secours redondants, un système d'échantillonnage de l'air VESDA et de pré-action sur deux zones, ainsi qu'un dispositif de surveillance de la température et de l'humidité

ACRONIS PROTÈGE VOTRE ENVIRONNEMENT G SUITE (ET TOUT LE RESTE)

Acronis Backup est une **solution complète de protection des données pour l'ensemble de votre environnement informatique**, que vos ressources se trouvent sur site ou hébergées dans des Clouds privés ou publics.

Elle protège un **large éventail de plates-formes** et d'applications, notamment des environnements physiques, virtuels et Cloud, ainsi que des serveurs exécutant d'autres systèmes d'exploitation et hyperviseurs courants, de nombreuses applications et bases de données courantes et des systèmes d'exploitation d'ordinateurs de bureau (dont macOS) et de terminaux mobiles comme iOS et Android.

Cette plate-forme unique de protection des données pour l'ensemble de votre environnement informatique évite les incompatibilités entre les solutions de sauvegarde sur site et dans le Cloud. Elle permet également de réduire le coût des licences, de la formation et de l'intégration. La figure 2 présente les différentes plates-formes protégées par **Acronis Backup**.

De plus, l'interface utilisateur Acronis Backup est suffisamment simple pour être utilisée par des non-spécialistes, ce qui permet aux nouvelles recrues de l'équipe de protection des données de démarrer rapidement. Vous allez en outre économiser sur les coûts d'implémentation, de maintenance et d'exploitation.

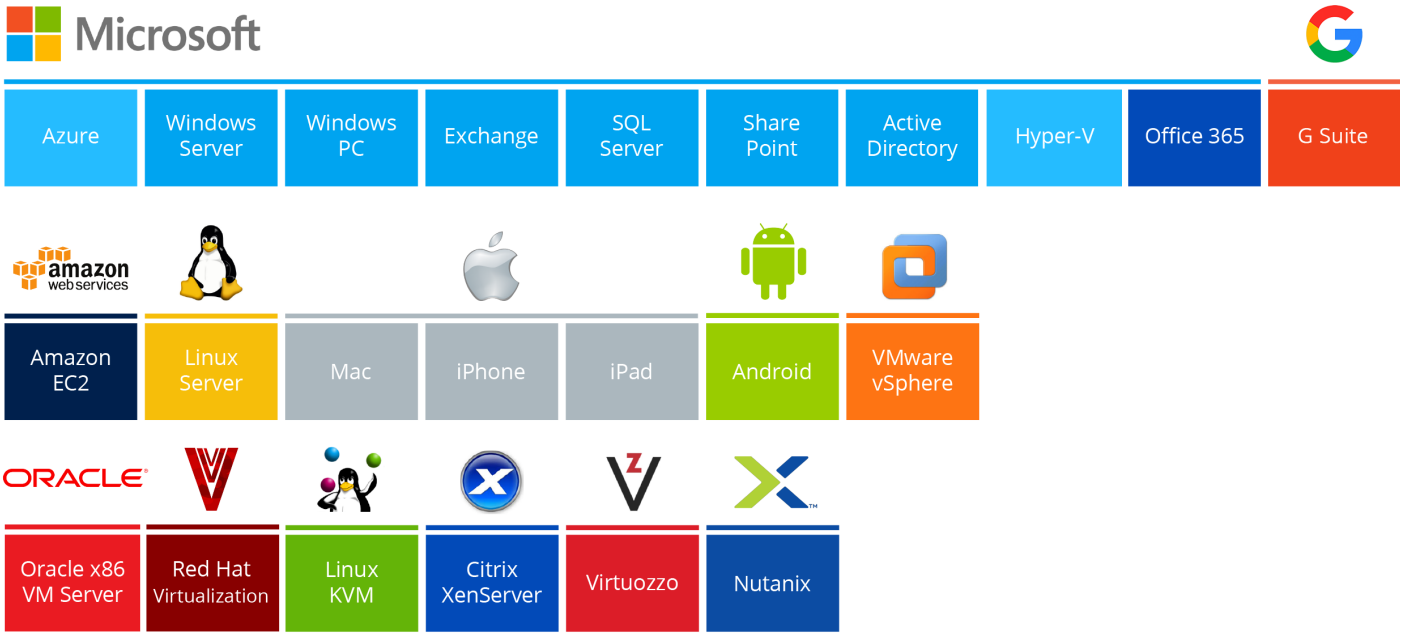

Figure 2. Plates-formes protégées par Acronis Backup.

CONCLUSION

Si votre entreprise utilise G Suite, vous devez compléter les fonctions limitées de protection des données proposées par Google avec Acronis Backup, la solution de sauvegarde la plus fiable et la plus facile à utiliser par les entreprises de toutes tailles.

Pour découvrir comment **Acronis Backup peut améliorer**, simplifier et réduire le coût de protection de vos données G Suite, profitez d'un essai gratuit de 30 jours ici ou trouvez un revendeur Acronis ici.