Une Analyse Approfondie de la Sécurité du Service de Stockage Cloud MEGA.io

Résumé Exécutif

Le service de stockage en ligne MEGA s'est positionné sur le marché comme un bastion de la confidentialité, fondé sur la promesse d'un chiffrement « zero-knowledge » (à divulgation nulle de connaissance) entièrement contrôlé par l'utilisateur.1 Cette approche, qui prétend rendre les données des utilisateurs techniquement inaccessibles même pour le fournisseur de services, constitue son principal argument de vente. Cependant, ce rapport révèle une contradiction fondamentale entre ces affirmations marketing et les conclusions d'une recherche indépendante menée par des cryptographes de l'École Polytechnique Fédérale de Zurich (ETH Zurich) en 2022.

Cette recherche, surnommée « Mega-Awry », a mis en lumière des failles cryptographiques critiques et fondamentales dans l'architecture de MEGA.4 Ces vulnérabilités ne sont pas de simples bogues, mais des défauts de conception qui permettent à un serveur MEGA malveillant ou compromis de déchiffrer progressivement les fichiers des utilisateurs, et même d'injecter des données malveillantes dans leur espace de stockage, brisant ainsi de manière irréfutable la promesse du « zero-knowledge ».8

En réponse, MEGA a déployé des correctifs logiciels pour contrer le vecteur d'attaque le plus direct. Néanmoins, ces mesures sont considérées par la communauté de la sécurité comme insuffisantes, car elles ne s'attaquent pas aux faiblesses architecturales sous-jacentes qui rendent le système intrinsèquement fragile.7 La refonte complète du système, recommandée par les chercheurs, n'a pas été entreprise.

Le verdict de cette analyse est donc nuancé mais sans équivoque : la sécurité de MEGA est fragile et ne peut être considérée comme fiable pour le stockage de données hautement sensibles, en particulier lorsque le fournisseur de services lui-même est inclus dans le modèle de menace. Sa valeur est considérablement diminuée pour les utilisateurs exigeant une confidentialité absolue. Elle peut toutefois rester acceptable pour un usage courant où le principal adversaire n'est pas le fournisseur de services, mais où une protection de base contre la surveillance de masse ou les violations de données tierces est souhaitée.

Section 1 : La Promesse Architecturale : Déconstruction du Modèle de Chiffrement « Zero-Knowledge » de MEGA

1.1 Le Cadre du Chiffrement Contrôlé par l'Utilisateur (UCE)

La proposition de valeur fondamentale de MEGA repose sur son architecture de chiffrement « zero-knowledge », également commercialisée sous le nom de chiffrement de bout en bout contrôlé par l'utilisateur (UCE - User-Controlled Encryption).2 L'affirmation centrale est que seul l'utilisateur détient les clés de déchiffrement de ses données. Par conséquent, personne d'autre, pas même le personnel de MEGA, ne peut accéder, déchiffrer ou lire les fichiers stockés sur ses serveurs.1 Cette caractéristique est présentée comme un différenciateur clé par rapport à des concurrents majeurs tels que Google Drive ou Dropbox, où le fournisseur conserve souvent un accès technique aux clés de déchiffrement des utilisateurs, que ce soit pour des raisons opérationnelles ou de conformité légale.2

Pour renforcer cette promesse, la documentation de MEGA souligne que le mot de passe de l'utilisateur est la « clé de chiffrement principale ». L'entreprise insiste sur le fait qu'elle n'a aucun accès à ce mot de passe et ne le stocke jamais, ce qui explique pourquoi elle est techniquement incapable de proposer une procédure de réinitialisation de mot de passe par e-mail. Si un utilisateur perd son mot de passe et sa clé de récupération, l'accès à ses données est définitivement perdu.2 C'est sur cette base que MEGA demande aux utilisateurs d'établir leur confiance.

1.2 La Hiérarchie des Clés : du Mot de Passe Utilisateur au Chiffrement des Fichiers

Le processus de chiffrement de MEGA est structuré selon une hiérarchie de clés conçue pour sécuriser les données à plusieurs niveaux. Ce modèle, bien que complexe en apparence, peut être décomposé en plusieurs étapes logiques, basées sur la documentation de sécurité et les analyses des chercheurs.8

1. **Génération de la Clé Maîtresse :** Tout commence avec le mot de passe de l'utilisateur. Ce mot de passe n'est pas utilisé directement pour chiffrer les fichiers. Il sert plutôt à dériver une clé de chiffrement qui, à son tour, chiffre une « clé maîtresse » (Master Key) générée de manière aléatoire lors de la création du compte.
2. **Chiffrement du Matériel Cryptographique :** Cette clé maîtresse devient le pivot de la sécurité du compte. Elle est utilisée pour chiffrer tout le matériel cryptographique essentiel de l'utilisateur, qui comprend une paire de clés RSA de 2048 bits (utilisée pour le partage sécurisé de données avec d'autres utilisateurs), une paire de clés Curve25519 (pour l'échange de clés dans la fonction de chat), et une paire de clés Ed25519 (pour la signature numérique des autres clés).8
3. **Clés de Nœud (Node Keys) :** Pour chaque fichier ou dossier individuel téléversé sur MEGA, une nouvelle clé symétrique unique, appelée « clé de nœud », est générée. Cette clé est utilisée pour chiffrer le contenu de cet élément spécifique.8 Cette approche garantit que la compromission d'une clé de fichier ne compromet pas l'ensemble des données de l'utilisateur.
4. **Stockage sur le Serveur :** Le matériel cryptographique chiffré (la clé privée RSA, les clés de nœud, etc.) est ensuite téléversé et stocké sur les serveurs de MEGA. Cette décision architecturale est cruciale : elle permet la synchronisation multi-appareils et l'accès au compte depuis n'importe quel terminal. Cependant, comme l'a révélé l'analyse des vulnérabilités, ce choix de stocker la clé privée de l'utilisateur (même sous forme chiffrée) sur le serveur est devenu le principal point de défaillance du système.8

Cette architecture est un compromis délibéré entre sécurité et commodité. Pour offrir une expérience utilisateur fluide avec une synchronisation transparente et une option de récupération de compte (via la clé de récupération), MEGA a choisi de stocker les clés privées chiffrées de ses utilisateurs sur ses propres serveurs. Un modèle plus sécurisé, mais nettement moins pratique, aurait exigé que l'utilisateur gère ses clés privées entièrement et exclusivement sur ses propres appareils. Ce choix de conception, qui privilégie l'expérience utilisateur au détriment de la sécurité absolue, a créé la surface d'attaque même qui a été exploitée par la suite. L'acte de centraliser le risque en confiant la garde des secrets cryptographiques chiffrés au serveur a fait de la sécurité de l'ensemble du système une simple dépendance à l'honnêteté et à l'infaillibilité de l'infrastructure de MEGA.

1.3 Le Rôle de RSA et AES dans la Chaîne de Sécurité

L'architecture de MEGA s'appuie sur deux primitives cryptographiques standards : AES et RSA. L'AES (Advanced Encryption Standard) est l'algorithme de chiffrement symétrique utilisé pour le chiffrement rapide et efficace du contenu des fichiers et des clés de nœud.8 Le RSA est le cryptosystème asymétrique utilisé principalement pour le partage sécurisé de clés entre utilisateurs.11 Lorsqu'un utilisateur partage un dossier, la clé de ce dossier est chiffrée avec la clé publique RSA du destinataire, garantissant que seul ce dernier peut la déchiffrer avec sa clé privée.

Cependant, le diable se cache dans les détails de l'implémentation. Pour chiffrer le matériel cryptographique (comme la clé privée RSA et les clés de nœud), MEGA a utilisé le mode de fonctionnement AES-ECB (Electronic Codebook). Ce choix est considéré comme un « drapeau rouge » par la communauté cryptographique. L'ECB est le mode le plus simple de l'AES, mais il est notoirement peu sûr pour la plupart des applications car il chiffre des blocs de texte en clair identiques en blocs de texte chiffré identiques, et surtout, il ne fournit aucune protection d'intégrité ou d'authenticité.8 Cette absence de protection est une faiblesse fondamentale qui s'est avérée être la cause première des vulnérabilités découvertes.

1.4 Sécurité Annoncée contre Réalité Architecturale

À première vue, la description de l'architecture de MEGA semble robuste pour un non-spécialiste. L'utilisation de termes comme « chiffrement de bout en bout » et « zero-knowledge » crée un modèle mental puissant mais potentiellement trompeur. Les utilisateurs interprètent ces termes comme signifiant que MEGA est *techniquement incapable* d'accéder à leurs données en toutes circonstances.

La réalité, cependant, est que le modèle de sécurité rend cet accès *procéduralement difficile* et dépend entièrement de l'honnêteté de MEGA en tant que gardien des clés chiffrées. Les choix d'implémentation spécifiques — notamment le stockage de la clé privée chiffrée de l'utilisateur sur le serveur et l'utilisation du mode AES-ECB — créent un système fragile dont la sécurité repose sur l'hypothèse que l'infrastructure du serveur est et restera toujours digne de confiance. Comme la section suivante le démontrera, cette hypothèse s'est avérée fausse, révélant un écart critique entre la perception de sécurité absolue véhiculée par le marketing et la réalité d'une architecture conditionnellement sécurisée.

Section 2 : Failles Fondamentales : Un Examen Approfondi des Vulnérabilités « Mega-Awry »

En juin 2022, une équipe de chercheurs de l'ETH Zurich a publié une étude qui a démantelé la façade de sécurité impénétrable de MEGA. Leur analyse a révélé une série de cinq attaques, collectivement baptisées « Mega-Awry », qui exploitent des failles fondamentales dans la conception cryptographique du service. Ces attaques ne sont pas des exploits théoriques mineurs ; elles permettent, dans des conditions réalisables, une compromission totale de la confidentialité et de l'intégrité des données des utilisateurs.

2.1 La Cause Racine : Chiffrement Malléable et Absence de Protection d'Intégrité

La cause profonde de toutes les vulnérabilités découvertes réside dans un choix de conception cryptographique fondamentalement défectueux : l'utilisation du mode de fonctionnement AES-ECB pour le chiffrement des clés.8 Comme mentionné précédemment, le mode ECB est une « alerte rouge » pour les cryptographes car il ne fournit aucune protection d'intégrité. Cela rend le texte chiffré « malléable », un terme qui décrit la capacité d'un attaquant à modifier un texte chiffré et à influencer de manière prévisible le résultat du texte en clair après le déchiffrement, et ce, sans jamais connaître la clé de chiffrement.12

Cette malléabilité est le catalyseur qui a permis aux chercheurs de concevoir des attaques dévastatrices. En l'absence de vérification d'intégrité (comme celles fournies par des modes de chiffrement authentifiés modernes tels que l'AES-GCM, que les chercheurs ont recommandé), le client MEGA n'a aucun moyen de savoir si le matériel cryptographique qu'il reçoit du serveur a été altéré en transit.8 C'est cette porte ouverte qui a été exploitée.

2.2 Vecteur d'Attaque 1 : Récupération de la Clé Privée RSA

La première et la plus critique des attaques permet à un serveur malveillant (ou à MEGA lui-même) de récupérer la clé privée RSA d'un utilisateur.6

- **Mécanisme :** L'attaque exploite la malléabilité du texte chiffré contenant la clé privée RSA de l'utilisateur, qui est stockée sur les serveurs de MEGA. Un attaquant contrôlant le serveur peut systématiquement altérer ce texte chiffré avant de l'envoyer au client lors d'une tentative de connexion. À chaque connexion, la manière dont le client de l'utilisateur traite cette clé altérée et répond au serveur lors de l'échange d'identifiant de session (SID) divulgue une infime quantité d'information — un seul bit — sur l'un des facteurs premiers de la clé RSA.7
- **Impact :** En répétant ce processus à chaque connexion de l'utilisateur, l'attaquant peut progressivement accumuler suffisamment de bits pour reconstruire la clé privée RSA complète. Initialement, les chercheurs de l'ETH Zurich ont estimé qu'il fallait 512 connexions réussies. Cependant, des recherches ultérieures menées par des chercheurs de l'UCSD ont considérablement amélioré l'attaque, réduisant ce seuil à seulement six connexions.6
- **Conséquence :** La récupération de la clé privée RSA est catastrophique. Elle permet à l'attaquant de déchiffrer toutes les données qui ont été partagées avec l'utilisateur, de se faire passer pour lui auprès d'autres utilisateurs et de préparer le terrain pour des attaques encore plus graves. Cela anéantit complètement le modèle de confidentialité pour toutes les données partagées.

2.3 Vecteur d'Attaque 2 : Récupération de Texte en Clair et Déchiffrement des Fichiers Utilisateur

Une fois la clé privée RSA compromise, l'attaquant peut passer à la phase suivante : le déchiffrement de n'importe quel fichier de l'utilisateur, même ceux qui n'ont jamais été partagés.8

- **Mécanisme :** L'attaquant utilise le même processus de connexion malléable. Cette fois, au lieu de simplement altérer la clé RSA, il peut « couper-coller » des blocs de texte chiffré correspondant aux clés de fichiers (les clés de nœud) dans le flux de données, à l'endroit où le client s'attend à recevoir la clé RSA. Le client, sans se méfier, déchiffre ces clés de fichiers en utilisant la clé maîtresse de l'utilisateur et renvoie des informations qui permettent à l'attaquant de reconstituer la clé de fichier en clair.12
- **Impact :** Cette technique permet à un attaquant de récupérer une clé de fichier par tentative de connexion.12
- **Conséquence :** C'est la violation ultime de la promesse de « zero-knowledge ». Un attaquant contrôlant les serveurs de MEGA peut, avec le temps, acquérir les clés de tous les fichiers d'un utilisateur et ainsi accéder à l'intégralité de son contenu stocké.

2.4 Vecteurs d'Attaque 3 & 4 : Violation d'Intégrité et Injection de Fichiers Malveillants (Attaques de « Framing »)

Les attaques ne se limitent pas à une violation passive de la confidentialité. Les chercheurs ont démontré qu'un attaquant pouvait également passer à une phase active en injectant des fichiers malveillants dans le compte d'un utilisateur.8

- **Mécanisme :** En comprenant la structure de chiffrement des fichiers de MEGA et en ayant la capacité de déchiffrer et de rechiffrer des clés, un serveur malveillant peut forger un fichier entièrement nouveau (par exemple, le fichier hacker-cat.png utilisé dans la preuve de concept) ainsi que sa clé de nœud chiffrée correspondante. Il peut ensuite insérer ce fichier et sa clé dans la liste de fichiers que le serveur envoie à l'utilisateur lorsqu'il se connecte.8
- **Impact :** Du point de vue de l'utilisateur, le fichier malveillant apparaît dans son espace de stockage cloud comme n'importe quel autre fichier. Parce qu'il est accompagné d'une clé de nœud valablement chiffrée (bien que forgée par l'attaquant), il semble parfaitement authentique et se déchiffre correctement sur la machine de l'utilisateur lorsqu'il est ouvert.8
- **Conséquence :** Cette attaque brise l'intégrité des données. Un utilisateur ne peut plus avoir la certitude que les fichiers présents dans son espace de stockage sont bien ceux qu'il a initialement téléversés. Un attaquant pourrait remplacer des documents légitimes par des versions altérées contenant des logiciels malveillants ou de la désinformation, sans que l'utilisateur ne puisse le détecter.

2.5 Vecteur d'Attaque 5 : L'Attaque par Oracle de Remplissage GaP-Bleichenbacher

La dernière attaque identifiée est une variante plus complexe d'une attaque cryptographique classique, qui cible le mécanisme d'échange de clés de l'ancienne fonction de chat de MEGA.7

- **Mécanisme :** Il s'agit d'une attaque par « oracle de remplissage », où un attaquant exploite la manière dont un serveur répond à des messages RSA mal formatés (avec un remplissage incorrect) pour en déduire progressivement le contenu. Bien que décrite comme plus « coûteuse » en termes de calculs, elle reste une voie d'attaque pratique.7
- **Conséquence :** Elle offre une autre méthode à un serveur malveillant pour déchiffrer les données des utilisateurs (dans ce cas, les clés de chat), renforçant ainsi le constat d'une fragilité systémique dans l'architecture cryptographique de MEGA.

Tableau 1 : Affirmations de Sécurité de MEGA contre Résultats de la Recherche Indépendante

Pour synthétiser l'impact de ces découvertes, le tableau suivant met en contraste direct les promesses marketing de MEGA avec la réalité technique révélée par les chercheurs.

Affirmation de MEGA	Réalité (Découverte « Mega-Awry »)	Implication pour la Sécurité de l'Utilisateur
« Personne n'a accès à votre mot de passe à part vous — pas même nous. » 2	Un serveur malveillant peut exploiter les connexions répétées de l'utilisateur pour reconstituer systématiquement sa clé privée RSA. 8	**Perte Totale de Confidentialité pour les Données Partagées.** MEGA (ou un attaquant contrôlant ses serveurs) peut déchiffrer tous les fichiers et dossiers partagés avec l'utilisateur.
« Avec MEGA, vous contrôlez le chiffrement. Vous détenez les clés… » 2	Un serveur malveillant peut tromper le client pour qu'il déchiffre des données arbitraires, y compris les clés de fichiers individuels non partagés. 8	**Perte Totale de Confidentialité pour Toutes les Données.** MEGA peut obtenir l'accès et déchiffrer *tous* les fichiers dans le stockage cloud d'un utilisateur, contredisant directement le principe de « zero-knowledge ».
Les fichiers des utilisateurs sont authentiques et ne peuvent être modifiés que par l'utilisateur.	Un serveur malveillant peut forger et injecter des fichiers arbitraires dans le stockage cloud d'un utilisateur, qui apparaissent comme parfaitement authentiques pour ce dernier. 8	**Perte Totale de l'Intégrité des Données.** Les utilisateurs ne peuvent plus être certains que les fichiers dans leur stockage sont ceux qu'ils ont initialement téléversés. Des documents malveillants ou des logiciels

Affirmation de MEGA	Réalité (Découverte « Mega-Awry »)	Implication pour la Sécurité de l'Utilisateur
		espions pourraient être insérés sans détection.

Section 3 : Gestion de Crise : Évaluation des Mesures d'Atténuation de MEGA et de la Voie à Suivre

Face à la publication de vulnérabilités aussi fondamentales, la réponse de MEGA était très attendue. L'entreprise a réagi en publiant des mises à jour logicielles et en communiquant sur les mesures prises. Cependant, une analyse approfondie de cette réponse révèle un écart significatif entre les correctifs appliqués et les recommandations des experts en sécurité.

3.1 Analyse des Correctifs Déployés et des Mises à Jour Logicielles

Dans un billet de blog publié en juin 2022, MEGA a officiellement reconnu le rapport de l'ETH Zurich et annoncé la publication de mises à jour logicielles pour corriger la « vulnérabilité critique ».9 Le principal correctif visait à neutraliser la première et la plus efficace des attaques : la récupération de la clé privée RSA. La mise à jour a renforcé la manière dont le client MEGA gère la clé RSA chiffrée reçue du serveur, la rendant insensible aux manipulations qui permettaient la fuite d'informations.9

MEGA a également confirmé plus tard que ce correctif était efficace contre l'attaque améliorée (ne nécessitant que 6 connexions) découverte par les chercheurs de l'UCSD, rassurant ainsi les utilisateurs sur le fait que ce vecteur d'attaque spécifique était bien fermé.9

3.2 La Divergence : une Réparation Rapide contre une Refonte Nécessaire

C'est ici que réside le cœur du désaccord entre MEGA et la communauté de la sécurité. La communication de MEGA a présenté la situation comme une faille qui a été identifiée et corrigée, impliquant un retour à la normale.9 En revanche, les chercheurs et d'autres experts ont souligné que les correctifs, bien que nécessaires, étaient largement insuffisants car ils ne s'attaquaient pas aux problèmes architecturaux fondamentaux. Les causes profondes, telles que l'utilisation d'un chiffrement malléable (AES-ECB) et le manque de séparation des clés, demeurent inchangées.4

Le professeur Kenneth Paterson, l'un des auteurs de l'étude, a exprimé publiquement sa déception quant au fait que MEGA ne s'était pas engagé dans une refonte complète de son architecture, qualifiant la cryptographie restante de « plutôt fragile ».7 La recommandation des chercheurs était claire : une refonte complète du système utilisant des primitives modernes et robustes, comme le chiffrement authentifié AES-GCM et des protocoles d'authentification plus sûrs (PAKE augmenté).8

La réponse de MEGA peut être interprétée comme une action de gestion de crise axée sur les relations publiques plutôt qu'une refonte technique guidée par la sécurité. En corrigeant la vulnérabilité la plus spectaculaire et la plus facile à expliquer, l'entreprise a pu déclarer publiquement que « le problème est résolu ». Cependant, elle a évité la tâche beaucoup plus coûteuse et complexe de redessiner son architecture cryptographique, un processus qui aurait pu nécessiter le rechiffrement de pétaoctets de données utilisateur et potentiellement rompre la compatibilité ascendante.9 Ce choix suggère un calcul commercial où le coût et la complexité d'une refonte complète ont été jugés supérieurs au risque perçu d'attaques futures exploitant les faiblesses architecturales restantes.

3.3 Le Programme de Bug Bounty comme Mesure de Sécurité

MEGA dispose depuis longtemps d'un programme de récompense pour la découverte de vulnérabilités (bug bounty), offrant jusqu'à 10 000 € par faille signalée.14 Dans le cadre de ce programme, l'entreprise a versé une « récompense significative » aux chercheurs de l'ETH Zurich, ce qui témoigne d'une certaine bonne foi dans le respect des pratiques de divulgation responsable.9

Le programme invite explicitement à signaler tout ce qui pourrait briser le modèle de sécurité cryptographique de MEGA, tout en excluant certains scénarios comme l'ingénierie sociale ou les attaques nécessitant un client déjà compromis.15 Cependant, bien qu'un programme de bug bounty soit une pratique de sécurité saine, il met également en évidence une

dépendance à l'égard de chercheurs externes pour trouver des failles dans un système qui manque d'audits formels et indépendants. Un bug bounty est une mesure réactive, tandis qu'un audit de sécurité proactif est une mesure préventive. Le fait que des failles de conception aussi fondamentales aient persisté pendant près d'une décennie avant d'être découvertes par des universitaires suggère que le programme de bug bounty a fonctionné comme un substitut, plutôt qu'un complément, à la validation rigoureuse qu'un audit formel aurait fournie.

3.4 Risques Architecturaux Persistants et Préoccupations non Résolues

L'état actuel de la sécurité de MEGA est donc ambigu. Le vecteur d'attaque le plus direct et le plus efficace pour récupérer la clé privée RSA a été corrigé. Cependant, l'architecture sous-jacente, qualifiée de « fragile », demeure. L'utilisation de code hérité et de « raccourcis » cryptographiques datant de près de dix ans est un risque reconnu par MEGA elle-même.9

De plus, le fait que le changement de mot de passe d'un utilisateur ne déclenche pas un rechiffrement des clés ou des fichiers existants est une préoccupation. Cela signifie que si un compte avait été compromis *avant* l'application du correctif, il pourrait théoriquement rester vulnérable à certains égards.8 C'est un point subtil mais important qui souligne que les correctifs ne sont pas rétroactifs pour les dommages potentiellement déjà causés.

Section 4 : L'Équation de la Confiance : Transparence, Audits et Historique Opérationnel

La confiance dans un service de stockage sécurisé ne repose pas uniquement sur son architecture cryptographique, mais aussi sur sa transparence, ses pratiques de vérification et son historique. Sur ces points, l'évaluation de MEGA révèle des forces et des faiblesses significatives.

4.1 L'Illusion du Code Open Source : Pourquoi la Visibilité n'est pas la Vérification

MEGA met en avant la publication du code source de ses applications clientes (web, bureau, mobile) comme une preuve de son engagement envers la transparence.2 Cela permet, en théorie, à n'importe qui d'examiner le code pour s'assurer qu'il fait ce qu'il prétend faire.

Cependant, cette transparence a une limite critique : elle ne s'applique qu'au code côté client. Le code côté serveur, qui est au cœur des attaques « Mega-Awry » et qui gère l'infrastructure, reste propriétaire et fermé.18 Sans la capacité de vérifier le comportement du serveur, la transparence du code client perd une grande partie de sa valeur en matière de protection contre un fournisseur malveillant. Le client est obligé de faire confiance à ce que le serveur lui envoie, ce qui était précisément le point de départ des attaques.

4.2 La Pièce Manquante : L'Absence d'Audits de Sécurité Indépendants

Malgré ses affirmations de haute sécurité, il n'existe aucun audit de sécurité public, indépendant et réalisé par une tierce partie sur l'architecture cryptographique ou l'infrastructure de MEGA.18 C'est une lacune majeure et un signal d'alarme pour tout service qui se veut un leader en matière de sécurité. Il est important de ne pas confondre

mega.io avec mega.ai, une autre entreprise qui, elle, affiche des certifications SOC 2 et ISO 27001.22

Un audit indépendant fournirait la vérification rigoureuse que la simple publication du code client ne peut offrir. L'absence de tels audits signifie que pendant près de dix ans, les failles fondamentales du système n'ont été ni identifiées par des processus internes, ni découvertes par un audit externe, mais ont dû attendre l'initiative d'une équipe de recherche universitaire.

4.3 Un Historique de Controverses et d'Utilisations Abusives

La réputation de MEGA est également façonnée par son histoire. Le service a été lancé par Kim Dotcom en tant que successeur de Megaupload, un site fermé par les autorités pour violation massive des droits d'auteur.14 Bien que Dotcom ait quitté l'entreprise depuis, et ait même conseillé de ne plus l'utiliser suite à des prises de contrôle présumées, cette origine sulfureuse continue de marquer l'image de la marque.14

Au-delà de ses origines, MEGA a connu des incidents de sécurité opérationnels. En 2018, son extension officielle pour le navigateur Chrome a été compromise et modifiée pour voler des cryptomonnaies et des identifiants de sites web, démontrant une faille dans la sécurité de sa chaîne d'approvisionnement logicielle.19

Plus récemment, l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a identifié Mega.io comme un outil utilisé par les opérateurs du rançongiciel Phobos pour l'exfiltration de données volées.23 Cela illustre comment les caractéristiques mêmes qui attirent les utilisateurs soucieux de leur vie privée (chiffrement fort, anonymat perçu) en font également un outil de choix pour les cybercriminels.24 Un service qui promet que même son opérateur ne peut pas voir les données des utilisateurs est la solution d'exfiltration parfaite pour les groupes de rançongiciels. Cela place MEGA dans une position délicate, obligée de lutter contre les abus, comme en témoignent ses rapports de transparence sur les retraits de contenu illégal 25, tout en essayant de préserver sa promesse de confidentialité.

4.4 Analyse de la Réputation du Domaine et de l'Infrastructure

Sur le plan opérationnel, MEGA utilise plusieurs noms de domaine : mega.nz reste le portail principal pour les utilisateurs connectés, tandis que mega.io est utilisé depuis 2021 pour les pages d'entreprise et de produits, une décision motivée par un meilleur référencement international.14 L'analyse du trafic confirme une base d'utilisateurs mondiale et significative.28

Un point positif indéniable de l'infrastructure de MEGA est la localisation de ses centres de données. Les données sont stockées en Europe ou dans des pays jugés adéquats par le RGPD, comme la Nouvelle-Zélande, avec une politique explicite de ne pas stocker de fichiers utilisateur aux États-Unis.21 D'un point de vue de la confidentialité juridictionnelle, c'est un avantage majeur pour les utilisateurs préoccupés par les lois de surveillance américaines comme le CLOUD Act.

Section 5 : Le Cadre Légal et de Confidentialité : Examen des Politiques et de la Conformité

L'évaluation de la sécurité d'un service cloud ne peut être complète sans un examen attentif de son cadre juridique et de ses politiques de confidentialité. Ces documents définissent les règles du jeu en matière de collecte, d'utilisation et de protection des données des utilisateurs.

5.1 Résidence des Données, Risque Juridictionnel et RGPD

Comme mentionné précédemment, la stratégie de MEGA en matière de résidence des données est un atout majeur. En hébergeant les données dans des centres de données sécurisés en Europe et dans des pays reconnus pour leur niveau de protection adéquat, comme la Nouvelle-Zélande, MEGA se positionne favorablement sur le plan de la confidentialité.21 L'évitement délibéré des centres de données américains est une mesure concrète pour protéger les utilisateurs de la portée des agences de surveillance américaines.21

De plus, MEGA a pris l'engagement d'appliquer les protections et les droits conférés par le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne à tous ses utilisateurs dans le monde, et pas seulement à ceux résidant dans l'UE.29 C'est une démarche positive qui renforce son image d'entreprise soucieuse de la vie privée.

5.2 Analyse des Conditions d'Utilisation et de la Politique de Confidentialité

Un examen détaillé des documents juridiques de MEGA révèle des nuances importantes que les utilisateurs doivent comprendre.30

- Politique de Confidentialité 30 :
  Le point le plus crucial est de comprendre ce que MEGA collecte sous forme non chiffrée. Bien que le *contenu* des fichiers soit protégé par le chiffrement « zero-knowledge », une quantité significative de métadonnées ne l'est pas. MEGA collecte et conserve des données de compte (adresse e-mail, historique des adresses IP, type de navigateur et de système d'exploitation), des données d'utilisation (taille des fichiers, relations parent-enfant entre les fichiers, adresses e-mail des contacts, métadonnées des chats comme les heures de début et de fin) et les enregistrements des transactions financières. Cette collecte de métadonnées, bien que nécessaire au fonctionnement du service, nuance fortement la promesse de confidentialité absolue.

- Conditions d'Utilisation 31 :
  Ces conditions révèlent un modèle de confidentialité à plusieurs niveaux. Alors que le service de stockage cloud principal est présenté comme étant entièrement chiffré par l'utilisateur (UCE), d'autres produits de la gamme, comme le stockage objet MEGA S4, ne le sont *pas*. Les conditions stipulent clairement que MEGA peut accéder au contenu des fichiers stockés sur S4 et les fournir aux autorités si la loi l'exige. C'est une distinction critique pour les utilisateurs de l'écosystème MEGA, qui pourraient supposer à tort que la garantie de chiffrement s'applique à tous les produits de la marque.

5.3 Collecte de Données : Ce que MEGA Sait et Conserve

En synthétisant les informations de la politique de confidentialité, on peut dresser un portrait clair de ce que MEGA sait sur ses utilisateurs, même sans pouvoir lire leurs fichiers. MEGA sait : qui vous êtes (via votre e-mail), quand et d'où vous vous connectez (journaux d'adresses IP), avec qui vous communiquez (listes de contacts et de participants aux chats), et comment vos données sont structurées (taille des fichiers, arborescence des dossiers).30

Pour de nombreux modèles de menace, notamment ceux impliquant une surveillance étatique, ces métadonnées peuvent être aussi révélatrices que le contenu lui-même. Une agence gouvernementale munie d'une ordonnance judiciaire pourrait, à partir de ces métadonnées, reconstituer un réseau de contacts, suivre les activités d'un utilisateur et déduire la nature de ses données, même sans jamais les déchiffrer. La promesse de « zero-knowledge » est donc trahie par la richesse des métadonnées collectées.

En ce qui concerne la conservation, MEGA conserve les données personnelles tant que le compte est actif. Après la résiliation d'un compte, les données peuvent être conservées jusqu'à 12 mois pour permettre une éventuelle réactivation, après quoi elles sont anonymisées.30

Section 6 : Verdict Final et Recommandations Stratégiques

6.1 Synthèse des Preuves : Réévaluation de la Valeur de la Sécurité de MEGA

L'analyse menée dans ce rapport dresse un portrait complexe de la sécurité de MEGA. La promesse initiale d'un système de stockage impénétrable, entièrement contrôlé par l'utilisateur, s'est révélée être fondée sur une architecture cryptographique fragile. Les vulnérabilités « Mega-Awry » n'étaient pas de simples bogues, mais les symptômes de défauts de conception fondamentaux qui ont persisté pendant près d'une décennie.

La réponse de l'entreprise, bien que rapide, a consisté à appliquer un pansement sur la blessure la plus visible en corrigeant l'exploit le plus direct, tout en laissant l'architecture sous-jacente vulnérable. Ce choix de privilégier la continuité des activités plutôt qu'une refonte complète de la sécurité est révélateur. De plus, l'absence persistante d'audits de sécurité indépendants constitue une lacune critique en matière de confiance, transformant l'argument de la transparence du code source en une forme de théâtre sécuritaire.

Par conséquent, la « valeur » de la sécurité de MEGA est hautement conditionnelle. Elle dépend entièrement du modèle de menace de l'utilisateur : qui est l'adversaire potentiel et quelle est la sensibilité des données à protéger?

6.2 Profils de Risque et Recommandations d'Utilisation

Sur la base de cette analyse, des recommandations claires peuvent être formulées pour différents types d'utilisateurs.

- **Pour les Utilisateurs Occasionnels (Données non sensibles) :** Pour stocker des photos de famille, des documents non critiques ou partager des fichiers volumineux, où la principale préoccupation est d'éviter l'exploration de données pratiquée par des services comme Google, MEGA est probablement « suffisant ». Les vulnérabilités corrigées rendent une attaque sophistiquée côté serveur moins probable contre une cible de faible valeur. Son offre gratuite généreuse reste un argument de poids.1
- **Pour les Particuliers Soucieux de leur Vie Privée (Données personnelles mais sensibles) :** Pour archiver des documents financiers, des journaux intimes ou des communications sensibles, MEGA représente un choix risqué. La menace principale ici est la possibilité que le fournisseur lui-même (ou un gouvernement le contraignant) devienne un adversaire. Les découvertes de « Mega-Awry » prouvent que c'est un vecteur de menace viable.

    - **Recommandation :** Ne pas utiliser MEGA pour cet usage, à moins d'appliquer une couche de chiffrement supplémentaire côté client *avant* le téléversement. L'utilisation d'un outil tiers, audité et fiable comme Cryptomator ou Veracrypt, transforme MEGA en un simple canal de stockage « stupide », neutralisant ainsi le risque lié à sa cryptographie défaillante.
- **Pour un Usage Professionnel et Commercial (Données hautement sensibles) :** Pour les journalistes, les militants, les avocats ou les entreprises manipulant des secrets commerciaux ou des données clients, MEGA est **fortement déconseillé**. Les failles architecturales démontrées, l'absence d'audits indépendants et le potentiel d'attaques contre l'intégrité des données (injection de fichiers) en font un risque inacceptable dans un contexte professionnel. La possibilité qu'un serveur malveillant compromette à la fois la confidentialité et l'intégrité des données est un facteur rédhibitoire.

6.3 Bonnes Pratiques pour Atténuer les Risques lors de l'Utilisation de MEGA

Pour tout utilisateur qui choisit de continuer à utiliser MEGA, une série de bonnes pratiques doit être rigoureusement appliquée pour minimiser les risques :

1. **Utiliser un mot de passe fort et unique :** C'est la mesure la plus fondamentale, car ce mot de passe est à la base de toute la chaîne de chiffrement.3
2. **Activer l'authentification à deux facteurs (2FA) :** Cela protège le compte contre les attaques par vol d'identifiants et le credential stuffing.1
3. **Conserver la Clé de Récupération en lieu sûr :** La perdre signifie perdre définitivement l'accès au compte et aux données.2
4. **Chiffrer soi-même les données sensibles en amont :** C'est la mesure d'atténuation la plus efficace. Utiliser un logiciel de chiffrement client de confiance comme Cryptomator avant de téléverser des fichiers sur MEGA.
5. **Se méfier des liens de partage :** Ne pas faire aveuglément confiance aux fichiers partagés, car l'attaque contre l'intégrité reste une possibilité théorique.
6. **Vérifier régulièrement l'historique des sessions :** Surveiller toute connexion non reconnue pour détecter une éventuelle compromission du compte.33

Tableau 2 : Résumé des Vulnérabilités « Mega-Awry » et Statut de leur Atténuation

Le tableau suivant résume les vulnérabilités, leur impact et, surtout, l'état actuel de leur correction, en soulignant les risques architecturaux qui justifient les recommandations prudentes de ce rapport.

Nom de la Vulnérabilité	Description	Impact Potentiel	Statut de l'Atténuation et Risque Résiduel	
1. Récupération de Clé RSA	Un serveur malveillant altère la clé RSA chiffrée pour divulguer des informations sur 6+ connexions.	Déchiffrement de toutes les données partagées ; usurpation d'identité de l'utilisateur.	**Corrigé.** La vulnérabilité spécifique côté client qui permettait la fuite d'informations a été corrigée.9	
2. Récupération de Texte en Clair	Un serveur malveillant utilise la clé RSA récupérée pour tromper le client afin qu'il déchiffre les clés de fichiers.	Déchiffrement de *tous* les fichiers de l'utilisateur, partagés ou non.	**Atténué Indirectement.** Cette attaque dépendait de la récupération préalable de la clé RSA. L'attaque 1 étant corrigée, ce vecteur spécifique est bloqué. **Risque Résiduel :** Le mécanisme sous-jacent	

Nom de la Vulnérabilité	Description	Impact Potentiel	Statut de l'Atténuation et Risque Résiduel	
			(chiffrement ECB malléable) demeure.	
3. Attaque de « Framing »	Un serveur malveillant forge et injecte des fichiers malveillants dans le stockage de l'utilisateur.	Perte totale de l'intégrité des données ; l'utilisateur pourrait télécharger et exécuter un logiciel malveillant déguisé en fichier légitime.	**Partiellement Atténué.** MEGA affirme avoir atténué cette attaque.13	**Risque Résiduel :** Les chercheurs soutiennent que l'absence fondamentale de protection de l'intégrité dans le format de fichier rend les attaques de ce type plausibles jusqu'à une refonte complète.
4. Attaque d'Intégrité	Une variante de l'attaque de « Framing », exploitant également l'absence de contrôles d'intégrité.	Perte totale de l'intégrité des données.	**Partiellement Atténué.** Statut identique à l'attaque de « Framing ». **Risque Résiduel :** Le même que ci-dessus. La faille architecturale principale persiste.	
5. GaP-Bleichenbacher	Une attaque par oracle de remplissage contre le mécanisme d'échange de clés de l'ancien chat.	Déchiffrement des clés de chat.	**Non Traité (selon les rapports initiaux).** MEGA a priorisé la correction des failles plus critiques. **Risque Résiduel :** Démontre que plusieurs parties du système cryptographique ont été construites avec des implémentations « fragiles » ou non standard.	

Sources des citations

1. MEGA Cloud Storage: Create a Free Account, consulté le septembre 21, 2025, https://mega.io/storage
2. How MEGA Protects Your Privacy and Data, consulté le septembre 21, 2025, https://mega.io/security
3. MEGA Review (MEGA.IO) [Secure Cloud Storage] - The Latest Backup Software Reviews | BestBackupReviews.com, consulté le septembre 21, 2025, https://www.bestbackupreviews.com/reviews/mega-review/
4. Le chiffrement du Cloud MEGA mis à mal par des chercheurs - Clubic, consulté le septembre 21, 2025, https://www.clubic.com/disque-dur-memoire/stockage-en-ligne/actualite-428061-le-chiffrement-du-cloud-mega-mis-a-mal-par-des-chercheurs.html
5. Is MEGA private and secure? : r/PrivacyGuides - Reddit, consulté le septembre 21, 2025, https://www.reddit.com/r/PrivacyGuides/comments/sffoi2/is_mega_private_and_secure/
6. MEGA Security Flaw: A Full Cloud Storage Security Review in 2025 - Cloudwards, consulté le septembre 21, 2025, https://www.cloudwards.net/mega-security-flaw/
7. Mega's unbreakable encryption proves to be anything but - The Register, consulté le septembre 21, 2025, https://www.theregister.com/2022/06/22/megas_encryption_broken/

8. MEGA: Malleable Encryption Goes Awry, consulté le septembre 21, 2025, https://mega-awry.io/
9. MEGA Security Update June 2022, consulté le septembre 21, 2025, https://blog.mega.io/mega-security-update
10. MEGA: Protect your Online Privacy, consulté le septembre 21, 2025, https://mega.io/
11. How does Mega's encryption work for sharing? - Stack Overflow, consulté le septembre 21, 2025, https://stackoverflow.com/questions/18346054/how-does-megas-encryption-work-for-sharing
12. MEGA: Malleable Encryption Goes Awry - YouTube, consulté le septembre 21, 2025, https://www.youtube.com/watch?v=nJQ-DbntAUs
13. Critical Flaws in MEGA Cloud Storage Let Attacker Decrypt User Data - GBHackers, consulté le septembre 21, 2025, https://gbhackers.com/critical-flaws-mega-cloud-storage/
14. Mega (site web) - Wikipédia, consulté le septembre 21, 2025, https://fr.wikipedia.org/wiki/Mega_(site_web)
15. Bug Bounty: Report Vulnerabilities - MEGA, consulté le septembre 21, 2025, https://mega.io/bug-bounty
16. A curiosity in MEGA's 2022 security whitepaper : r/Bitwarden - Reddit, consulté le septembre 21, 2025, https://www.reddit.com/r/Bitwarden/comments/1asdncm/a_curiosity_in_megas_2022_security_whitepaper/
17. AI flagged some serious crypto concerns about Mega - should I be concerned? - Reddit, consulté le septembre 21, 2025, https://www.reddit.com/r/MEGA/comments/1lhjkq9/ai_flagged_some_serious_crypto_concerns_about/
18. audit - Does MEGA cloud service say ALL the truth? - Information Security Stack Exchange, consulté le septembre 21, 2025, https://security.stackexchange.com/questions/95563/does-mega-cloud-service-say-all-the-truth
19. Mega (service) - Wikipedia, consulté le septembre 21, 2025, https://en.wikipedia.org/wiki/Mega_(service)
20. MEGA Transparency Report 2021, consulté le septembre 21, 2025, https://blog.mega.io/mega-transparency-report-2021
21. MEGA Cloud Storage Review (2025 Test Results) - CyberInsider, consulté le septembre 21, 2025, https://cyberinsider.com/cloud-storage/reviews/mega/
22. Security and Compliance - Safeguarding Data With Highest Priority - Mega AI, consulté le septembre 21, 2025, https://www.mega.ai/security-and-compliance
23. #StopRansomware: Phobos Ransomware | CISA, consulté le septembre 21, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a
24. An Encounter with Ransomeware-as-a-Service: MEGAsync Analysis - Recon InfoSec, consulté le septembre 21, 2025, https://blog.reconinfosec.com/megasync-analysis
25. MEGA Transparency Report, consulté le septembre 21, 2025, https://mega.io/transparency
26. Quels sont les domaines utilisé par MEGA à titre officiel, consulté le septembre 21, 2025, https://help.mega.io/fr/security/data-protection/official-domains
27. Additional Domain for MEGA: mega.io - Reddit, consulté le septembre 21, 2025, https://www.reddit.com/r/MEGA/comments/l08d0s/additional_domain_for_mega_megaio/
28. Trafic du site mega.io, classement et analyse [août 2025] - Semrush, consulté le septembre 21, 2025, https://fr.semrush.com/website/mega.io/overview/
29. Avis MEGA.nz (2025) : stockage cloud sécurisé et confidentiel - Clubic, consulté le septembre 21, 2025, https://www.clubic.com/stockage-en-ligne/avis-352094-mega-nz.html
30. Privacy Policy - MEGA, consulté le septembre 21, 2025, https://mega.io/privacy
31. Terms of Service - MEGA, consulté le septembre 21, 2025, https://mega.io/terms
32. Avis MEGA 2025 : Est-il plus sécurisé que Google Drive, OneDrive et autres services cloud, consulté le septembre 21, 2025, https://www.experte.com/fr/stockage-cloud/mega
33. How do I secure my MEGA account after it has been compromised?, consulté le septembre 21, 2025, https://help.mega.io/security/data-protection/account-compromised
34. How can I check MEGA login sessions and log them out remotely?, consulté le septembre 21, 2025, https://help.mega.io/security/data-protection/login-sessions