COMPARAISON DES CAPACITÉS & FICHE TECHNIQUE

Unlimited | Secure Email

GFI™
Aurea SMB Solutions

Unlimited | Secure Email - Comparaison des capacités

	Unlimited | Secure Email	Microsoft 365	Google workspace	Barracuda	Sophos	Mailstore
Plate-forme de messagerie sécurisée (calendrier, messagerie instantanée, tâches et notes)	•	•	•			
Cryptage du domaine, de la messagerie et de la connectivité	•	•	•			
Gestion des accès intégrée et sécurisée	•	•	•			
Prise en charge de plusieurs clients et périphériques	•	•	•			
Délégation d'e-mails en libre-service	•	•	•			
Quarantaine en libre-service	•	•	•	•	•	
Multimoteur - Protection antivirus et contre les programmes malveillants	•					
Mises à jour de la détection avancée des menaces	•	*	•	•	•	
Filtrage du contenu et des courriers indésirables basé sur des règles	•			•	•	
Gestion automatisée des archives	•	*	*	•		•
Archivage inviolable	•	*	*	•		•
Recherche avancée et détection électronique	•	*	*	•		•
Archivage des e-mails hébergés		*	*	•		
Sécurité des e-mails hébergée	*	•	•	•	•	

*: disponible mais dans des offres séparées ou des forfaits premium

Ce que vous recevez pour un tarif unique

- Messagerie et collaboration : Messagerie, calendrier, messagerie instantanée et notes, tâches et contacts partagés.
- Trafic sécurisé : Logiciel de protection contre les virus, le phishing et les programmes malveillants que vous pouvez installer à l'intérieur ou à l'extérieur du réseau. Il est compatible avec plusieurs systèmes de messagerie électronique, dont Microsoft, Apple, Google et le produit GFI Kerio Connect.
- Archivage sécurisé : Offre un archivage sécurisé pour la conformité et la gestion

À partir de 39,90 USD par utilisateur/nœud et par an, vous pouvez protéger vos communications et votre réseau à votre propre rythme sans les coûts supplémentaires associés au recours à plusieurs fournisseurs de solutions uniques.

Voici un aperçu de certaines des capacités les plus essentielles :

Unlimited | Secure Email - Fiche technique des fonctionnalités de protection

Cryptage du domaine, de la messagerie et de la connectivité

Prend en charge la configuration de plusieurs domaines, ainsi que l'authentification DKIM pour chaque domaine, la détection du spoofing au niveau de l'expéditeur et l'authentification utilisateur avec Active Directory Integration (NTLM), Open Directory Integration ou en mode intégré (Digest et CRAM MD5). Le chiffrement des données peut être activé dans les stores des emails et, enfin, le protocole TLS 1.3 est utilisé pour la transmission. Avec l'accès, les données et la transmission entièrement cryptés, vous pouvez disposer d'un système sécurisé de bout en bout pour toutes les communications.

Gestion des accès intégrée et sécurisée

Les services Active Directory et d'autres services alternatifs sont disponibles pour gérer les utilisateurs et les groupes, ainsi que définir les autorisations et les accès. En outre, des outils de sécurité tels que les règles d'expiration et de complexité des mots de passe, ainsi que des paramètres de prévention de la détection des mots de passe sont également disponibles.

Prise en charge de plusieurs clients et périphériques

La communication par e-mail, la mise en quarantaine des courriers indésirables et l'archivage des données utilisateur sont tous disponibles via les clients existants (tels qu'Outlook ou Apple) pouvant être utilisés, ainsi que via la prise en charge des périphériques Web et mobiles. Clients natifs avec plus de 10 langues prises en charge.

Délégation d'e-mails en libre-service et quarantaine

La délégation des e-mails aux utilisateurs, les boîtes aux lettres et calendriers partagés, ainsi que la gestion automatique des menaces par e-mail, permettent aux utilisateurs de contrôler leur messagerie et d'éviter les requêtes excessives au service informatique. En les associant à des outils en libre-service supplémentaires tels que l'accès aux clients d'archivage et les filtres antispam d'apprentissage automatique, les administrateurs informatiques peuvent se concentrer davantage sur l'amélioration des opérations.

Protections multiples contre les virus et les programmes malveillants

Protection avancée contre les menaces par e-mail à l'aide de quatre moteurs antivirus (optimisés par les chefs de file du secteur : Bitdefender, Avira, Kaspersky et Cyren).

Mises à jour de la détection avancée des menaces

Les moteurs antivirus multiples et les définitions de spam sont mis à jour fréquemment pour vous assurer d'être protégés contre les menaces les plus récentes, y compris celles apparaissant dans l'heure écoulée. Les moteurs antivirus peuvent être configurés pour rechercher automatiquement les mises à jour selon la fréquence sélectionnée.

Filtrage du contenu et des courriers indésirables basé sur des règles

Le contenu du trafic des e-mails est filtré à l'aide de quatre moteurs de filtrage de pointe. Les règles de filtrage avancées basées sur l'utilisateur permettent un tri flexible et granulaire de n'importe quelle partie de l'e-mail : en-têtes de message, objet, corps, nom de pièce jointe et contenu de pièce jointe à l'aide de différents types de méthodes de correspondance de modèle, y compris les expressions régulières.

Gestion automatisée des archives

Créez et sélectionnez vos archives et gérez-les facilement. Les options de stockage incluent les fichiers MS SQL+, MS SQL, MS SQLExpress, avec la possibilité de tester une base de données intégrée. Vous pouvez ensuite planifier et automatiser vos transferts de stockage/d'archives.

Archivage inviolable

Configurez une base de données d'activités d'audit, de sorte que seul le serveur SQL dispose des autorisations nécessaires pour apporter des modifications aux données, et enregistre les fichiers de trace qui sont également sécurisés avec un accès limité aux services, ainsi que les rapports d'audit complets pour assurer la conformité

Recherche avancée et détection électronique

La recherche inclut l'utilisation de caractères génériques, de filtres imbriqués, disponibles pour les recherches à l'intérieur des pièces jointes d'e-mail. Ainsi, vous n'êtes pas limité au simple texte d'un e-mail. Utilisé à partir des outils de détection électronique en masse, de la console Web d'administration ou des clients utilisateurs finaux.