



---

## Spécification de performance

### 365 Extended Email Protection

365 Extended Email Protection offre une couche de sécurité supplémentaire pour protéger le trafic de messagerie des clients de Microsoft 365 grâce à son approche Integrated Cloud Email Security. Les filtres antispam et anti-malware d'Hornetsecurity, alimentés par l'IA, analysent en temps réel le trafic de messagerie entrant pour détecter les cybermenaces avancées et supprimer de manière fiable les spams et les courriels malveillants des boîtes de réception des utilisateurs en l'espace de quelques secondes. L'intégration entièrement automatisée et transparente du service avec la plateforme Microsoft 365 permet une surveillance continue de toutes les boîtes aux lettres et s'appuie sur l'intelligence des menaces 24 heures sur 24 d'Hornetsecurity pour garantir la protection la plus récente.

La condition préalable à l'utilisation du service est l'utilisation de licences Microsoft Cloud avec la fonctionnalité Exchange activée par Microsoft.

Les services suivants sont inclus dans le produit 365 Extended Email Protection :

#### 1. Embarquement facile

- a. L'installation de 365 Extended Email Protection est automatisée. Tous les domaines, boîtes aux lettres et groupes du client sont transférés directement de Microsoft 365 vers le panneau de contrôle Hornetsecurity.
- b. La condition préalable à l'utilisation des services Hornetsecurity pour Microsoft 365 implique l'activation de l'App ID Hornetsecurity pour le locataire Microsoft 365 par un utilisateur administratif du client. Cette opération est réalisée une fois au cours du processus d'accueil.
- c. Il n'est pas nécessaire de modifier les enregistrements MX pour utiliser le service, car 365 Extended Email Protection s'intègre de manière transparente à la plateforme 365 via l'interface API. Tous les courriels entrants du client sont copiés au moyen de la journalisation des courriels et filtrés par les filtres de courriels avancés de Hornetsecurity.
- d. L'embarquement peut être effectué directement dans le panneau de contrôle ou via un lien externe d'accueil.

#### 2. Signature unique

- a. Tous les utilisateurs disposant d'un accès administratif peuvent s'authentifier à Hornetsecurity à l'aide de leurs identifiants administratifs Microsoft 365.
- b. Si les utilisateurs sont déjà connectés à Microsoft 365, ils n'ont pas besoin de s'authentifier à nouveau auprès de Hornetsecurity.



---

### 3. Menaces détectées

- a. Les courriers électroniques détectés comme des menaces sont présentés aux utilisateurs et supprimés des boîtes aux lettres dans une vue d'ensemble configurable et filtrable. En outre, des informations détaillées sur chaque courrier sont affichées.
- b. Les courriels du client qui sont reçus par le biais de la journalisation des courriels sont analysés par Hornetsecurity à la recherche de contenu malveillant (par exemple, des virus) et de publicités non désirées (par exemple, du spam). Les courriels malveillants et les publicités indésirables sont automatiquement supprimés des boîtes aux lettres du client final.
- c. Les utilisateurs peuvent récupérer les courriels à partir de l'aperçu et les remettre au destinataire.
- d. Les courriels supprimés sont stockés en quarantaine pendant trois mois afin que les utilisateurs puissent les consulter et les récupérer.
- e. Le taux de détection des spams et des menaces est d'au moins 99,9 % en moyenne mensuelle, sur la base du nombre de courriels atteignant les systèmes de Hornetsecurity pour les domaines du client au cours de la période mesurée.
- f. Le taux de faux positifs est inférieur à 0,00015 en moyenne mensuelle, sur la base du nombre de courriels propres parvenus aux systèmes de Hornetsecurity pour les domaines du client au cours de la période mesurée.

### 4. Tableau de bord

Le tableau de bord fournit à l'utilisateur une vue d'ensemble des services de Hornetsecurity réservés.

### 5. Rapports et conformité

- a. Le client reçoit des informations et des statistiques détaillées sur son statut de sécurité actuel.
- b. Il s'agit notamment de statistiques sur le courrier électronique et sur les menaces avancées :
  - Somme totale des courriels scannés
  - Somme totale des menaces détectées
  - Les courriels électroniques classés par menace au fil du temps
  - Les 100 premières boîtes aux lettres attaquées
  - Les attaques au fil du temps
  - Menaces par type et vecteur d'attaque
  - Les vecteurs d'attaque au fil du temps



- 
- c. Les activités effectuées par les utilisateurs du panneau de contrôle sont consignées dans un journal d'activité, par exemple la récupération d'un courriel ou l'installation réussie d'un autre service.

## 6. Politique sur l'utilisation raisonnable

- a. La bande passante, le stockage, l'infrastructure et les ressources nécessaires pour utiliser la solution et que nous mettons à disposition à cet égard sont partagés entre tous nos clients. Par conséquent, nous avons le droit de prendre des mesures pour nous assurer que tous les clients utilisent la solution de façon raisonnable et équitable afin que cette utilisation ne nuise pas ou n'empêche pas le service normal offert aux autres clients.
- b. Nous avons décidé de ne pas définir au préalable des indicateurs qui déterminent l'utilisation excessive ou déraisonnable, puisque, à notre discrétion, nous pouvons choisir de préserver nos niveaux de service normaux en réaffectant les ressources réservées à d'autres utilisateurs et non utilisées à ce moment particulier ou à une autre échelle. Vous comprenez que si nous décidons de ne pas appliquer activement notre politique sur l'utilisation raisonnable, vous ne devez pas en conclure que nous avons renoncé à notre droit de le faire et que nous refusons que vous continuiez à utiliser nos services au même niveau que celui de votre niveau actuel.
- c. Pour bénéficier de nos services, vous devez acquérir des unités facturables. Le nombre d'unités facturables dont vous avez besoin dépend d'un certain nombre de critères, tels que la taille de votre organisation, le nombre d'utilisateurs, la taille de stockage des données des sources particulières, etc.
- d. Peu importe le nombre d'unités facturables que vous avez acquises, vous devez utiliser nos services de façon raisonnable, et plus particulièrement d'une manière qui ne nous oblige pas à affecter des ressources de façon disproportionnée. Pour ce faire, nous comparerons votre utilisation de nos ressources (par exemple, les besoins en mémoire, le nombre de connexions parallèles) à celle du client moyen. Pour déterminer le taux d'utilisation du client moyen, nous excluons celui des 5 % de clients ayant le taux le plus élevé et des 5 % ayant le taux le plus bas du service concerné et calculons ensuite la moyenne du montant entre tous nos clients actifs.
- e. Il importe d'exclure les caractéristiques particulières liées à l'industrie dans laquelle vous exercez vos activités pour déterminer si l'utilisation est jugée raisonnable ou non.
- f. Si nous, agissant raisonnablement et de bonne foi, considérons que votre utilisation de notre solution n'est pas raisonnable ou contraire à cette politique, nous prendrons, à notre entière discrétion, l'une des mesures suivantes :
  - i. Vous permettre de continuer à utiliser nos solutions, mais sous réserve du paiement de frais supplémentaires et du respect des modalités que nous pourrions juger raisonnables dans les circonstances.
  - ii. Vous informer que votre compte sera résilié dans un délai raisonnable, à notre discrétion. Pendant ce temps, tous les services et/ou opérations seront suspendus.



- g. Si nous exerçons notre droit de résilier votre compte comme indiqué ci-dessus :
  - i. Toutes les données (métadonnées, données de sauvegarde ou autres) seront supprimées à la fin du délai fixé dans la notification que nous vous enverrons, malgré toute disposition contraire prévue dans les conditions générales.
  - ii. Vous recevrez un remboursement des frais payés à l'avance pour les jours restants de votre période d'abonnement.