Valable à partir du	01.06.2016
Valable jusqu'au :	01.10.2028
Próxima revisión :	01.10.2027
Personne(s) responsable(s) :	Olaf Petry, CISO
Confidentialité :	Public

Informations sur la protection des données

Services de sécurité gérés

Groupe Hornetsecurity

Informations sur la protection des données pour les services proposés

I. Coordonnées ... 3
1. Base ... 3
2. Coordonnées ... 3
II. Généralités sur le traitement des données ... 5
1. Portée du traitement des données à caractère personnel ... 5
2. Base juridique pour le traitement des données à caractère personnel ... 5
III. Traitement des données pour le fonctionnement des *services* ... 6
1. Données de base ... 6
a. Données de base ... 6
b. Données de configuration ... 6
2. 365 Permission Manager ... 7
3. 365 Total Backup ... 7
4. 365 Total Protection ... 8
5. 365 Total Protection Enterprise Backup ... 10
6. AI Recipient Validation ... 10
7. Control Panel, connexion au ... 11
8. Hornet.email Webmail, connexion à ... 12
9. Hosted Exchange ... 13
10. IA, utilisation de l'intelligence artificielle ... 13
a. Introduction ... 13
b. Finalité du traitement ... 13
c. Données que nous collectons ... 14
d. Outils d'IA, stockage et conservation des données ... 15
11. Security Awareness Service ... 16
12. Spam and Malware Protection ... 17

a. En option : Advanced Thread Protection (ATP) 18
b. En option : Email Encryption 18
c. En option : Archiving 19
d. En option : Continuity Service 20
e. En option : E-Mail-Signature and Disclaimer 20
f. En option : E-mail made in Germany 21
13. Test-Onboarding 21
14. VM Backup 21
15. Web Filter 22
16. Websafe, Déclaration de confidentialité pour les tiers 22
IV. Possibilité d'opposition et de suppression 23
V. Droits des personnes concernées 23
a. Droit à l'information conformément à l'article 15 du RGPD 23
b. Droit de rectification conformément à l'article 16 du RGPD 23
c. Droit à la suppression conformément à l'article 17 du RGPD 24
d. Droit à la limitation du traitement conformément à l'article 18 du RGPD 24
e. Droit à la portabilité des données conformément à l'article 20 du RGPD 24
f. Droit de recours auprès de l'autorité de surveillance compétente, article 77 du RGPD 24
VI. Destinataires des données 24
VII. Transfert de données vers des pays tiers 24

I. Coordonnées

1. Base

La base d'une protection efficace des données est une information complète sur la collecte, le traitement et l'utilisation de vos données (« traitement des données »). C'est pourquoi nous souhaitons vous informer,

- quand ou lors de quelles actions nous traitons des données,
- quelles données nous traitons et pour quelles raisons
- qui reçoit les données,
- quels sont vos droits en ce qui concerne le traitement des données par nos soins.

Ces informations sur la protection des données ne concernent que l'utilisation des données à caractère personnel dans le cadre des *services*. Vous pouvez télécharger ces informations sur la protection des données de manière permanente et à tout moment à l'adresse suivante : https://www.hornetsecurity.com/service-privacy-statement/

2. Coordonnées

Le responsable du traitement des données dans le cadre des *services* au sens du règlement général sur la protection des données (RGPD) est toujours le client. Hornetsecurity agit en tant que sous-traitant conformément à l'article 28 du RGPD. La prestation de services est également assurée en partie par d'autres sociétés du groupe Hornetsecurity en tant que sous-traitants :

	Sous-traitants	Les prestations sont sous-traitées en interne par
☐	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Téléphone : +49 511 515 464-0 E-mail : info@hornetsecurity.com	-/-
☐	Hornetsecurity Iberia S.L Calle Vía de las Dos Castillas 33, Edificio 3 Ática 3 Planta Tercera D 28224 Pozuelo de Alarcón, Madrid Espagne Téléphone : +34 91 368 77 33 E-mail : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Téléphone : +49 511 515 464-0 E-mail : info@hornetsecurity.com
☐	Hornetsecurity Argentina S.A. Belgrano 53 Piso, PB Dpto : B Tandil, Buenos Aires Argentine Tél : +54 9 249 449 9296 E-mail : info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Tél : +49 511 515 464-0 E-mail : info@hornetsecurity.com

	Sous-traitants	Les prestations sont sous-traitées en interne par
☐	Hornetsecurity Ltd. 82 James Carter Road Mildenhall, Bury Saint Edmunds IP28 7DD Royaume-Uni Tél : +44 203 0869 833 E-mail : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Tél : +49 511 515 464-0 E-mail : info@hornetsecurity.com
☐	Hornetsecurity Ltd BLK LS3, Level 1, Malta Life Sciences Park San Gwann Industrial Estate San Gwann, SGN 3000 Malte Tél : +44 203 0869 833 E-mail : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Tél : +49 511 515 464-0 E-mail : info@hornetsecurity.com
☐	Hornetsecurity Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 États-Unis Tél : +1 (412) 924-5300 E-mail : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Tél : +49 511 515 464-0 E-mail : info@hornetsecurity.com
☒	Hornetsecurity Canada Inc. Suite 500, Park Place Building 666 Burrard Street, Vancouver, BC V6E 3P3 Canada Tél : +1 (514) 527-3232 E-mail : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Tél : +49 511 515 464-0 E-mail : info@hornetsecurity.com
☐	IT-Seal GmbH IT-Seal GmbH Hilpertstr. 31 64295 Darmstadt Allemagne Tél : +49 (0) 6151 / 4938990 E-mail : kontakt@it-seal.de	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Allemagne Tél : +49 511 515 464-0 E-mail : info@hornetsecurity.com

Nous avons également nommé un délégué à la protection des données. Vous pouvez le contacter à l'adresse suivante :
privacy@hornetsecurity.com.

II. Généralités sur le traitement des données

1. Portée du traitement des données à caractère personnel

La fourniture des services nécessite le traitement de différentes données. En outre, l'étendue du traitement des données dépend de votre utilisation des fonctionnalités des services, par exemple des données que vous y traitez ou faites traiter, ou encore de votre consentement au traitement des données.

Dans le cadre du contrat conclu avec Hornetsecurity pour l'utilisation des services, vous êtes tenu de fournir les données à caractère personnel nécessaires à l'exécution du contrat. Le refus de fournir ces données peut constituer un manquement à vos obligations, à la suite duquel vous pouvez être tenu de verser des dommages et intérêts. Vous n'êtes pas obligé de nous fournir des données à caractère personnel. Toutefois, dans la mesure où la mise à disposition de ces données est techniquement liée à l'utilisation de nos services, un refus aura pour conséquence que vous ne pourrez pas utiliser nos services.

Lorsque vous utilisez les services, vous n'êtes pas soumis à une prise de décision automatisée conformément à l'article 22 du RGPD.

2. Base juridique pour le traitement des données à caractère personnel

Les bases juridiques du traitement des données à caractère personnel sont présentées ci-dessous.

Motif de traitement	Base juridique dans le RGPD	Explication
Exécution d'un contrat ou de mesures précontractuelles	Article 6, paragraphe 1, point b)	Le traitement n'a lieu que dans la mesure nécessaire à la perception et à l'exécution des droits et obligations découlant du contrat. Sauf indication contraire explicite, nous ne traitons les données que dans cette mesure.
Intérêt légitime	Article 6, paragraphe 1, point f)	Un traitement a lieu dans la mesure où nous avons un intérêt légitime et où aucun intérêt prépondérant de la personne concernée n'est visible. L'intérêt concret est expliqué dans les présentes informations sur la protection des données dans le cadre de la présentation du traitement.
Obligation légale	Article 6, paragraphe 1, point c)	Un traitement a lieu dans la mesure où il est nécessaire pour remplir des obligations légales allemandes ou européennes.

III. Traitement des données pour le fonctionnement des *services*

Pour que nous puissions vous fournir les *services*, il est nécessaire de traiter certaines données.

La base juridique du traitement de ces informations et données enregistrées est la nécessité d'exécuter la relation contractuelle existante. La durée de stockage se mesure donc en principe à la durée de la relation contractuelle. Toutefois, à l'issue de celle-ci, des bases juridiques alternatives peuvent intervenir, telles que des délais de conservation légaux.

1. Données de base

Le responsable du traitement des données de base et des données de configuration est l'entité du groupe Hornetsecurity indiquée dans la section I, « Coordonnées » (page 3).

a. Données de base

Les données de base du donneur d'ordre (nom, adresse, contact, numéro de téléphone, adresse électronique, service, poste, services réservés, période de facturation, coordonnées bancaires) sont saisies pour la gestion des services et utilisées pour l'exécution des prestations convenues par contrat. Les données personnelles des co-utilisateurs (adresse e-mail) sont saisies et utilisées pour l'exécution des prestations convenues par contrat.

Le traitement des données des co-utilisateurs s'effectue sur du matériel informatique propre, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

Les données de base du donneur d'ordre sont traitées par un sous-traitant sur des systèmes situés dans un pays tiers à des fins de gestion des données de base des clients (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, États-Unis). Le transfert des données s'effectue sur la base de clauses contractuelles types.

Le traitement des données dans le logiciel CRM de Salesforce est effectué sous la responsabilité commune, conformément à l'article 26 du RGPD, des entreprises mentionnées au point I, « Coordonnées ». Les personnes concernées peuvent consulter le contenu essentiel de cet accord sur demande. La base juridique de cette démarche est notre intérêt légitime conformément à l'article 6, paragraphe 1, point f) en vertu de l'article 48 du RGPD à l'amélioration de l'efficacité et à la minimisation des coûts par la création et l'utilisation de structures administratives communes.

En outre, une partie des données de base du donneur d'ordre est transmise à des sous-traitants au sein de l'UE et traitée sur leurs systèmes (PIN Mail AG, Alt-Moabit 91, 10559 Berlin, Allemagne) à des fins de livraison et d'envoi de factures (par lettre ou par e-mail).

b. Données de configuration

La configuration technique de chaque *service* souscrit est enregistrée en relation avec l'adresse électronique de l'utilisateur, l'appartenance d'un utilisateur à un groupe ou le nom de domaine du client.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

Pour VM Backup et 365 Total Backup s'applique également ce qui suit :

Pour la validation de la licence, les données de base nécessaires à une identification unique (adresse électronique) sont transmises aux systèmes de Hornetsecurity Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malte, UE.

2. 365 Permission Manager

365 Permission Manager est un outil logiciel de gestion de la gouvernance, des risque et de la conformité (GRC) qui permet aux utilisateurs d'obtenir une vue et une compréhension complètes de leurs autorisations de fichiers M365 dans leur propre locataire dans Microsoft Azure Cloud pour SharePoint Online, OneDrive for Business, Microsoft Teams et Microsoft 365 Groups.

Le traitement automatique des données comprend la récupération et le traitement des métadonnées des objets stockés dans le locataire M365. Objets dont les métadonnées sont récupérées : fichiers, dossiers, bibliothèques de documents, sites, utilisateurs, groupes. Les métadonnées récupérées et traitées sont les propriétaires des objets (adresse de messagerie, nom d'affichage), les informations sur les objets auxquels des droits d'accès ont été accordés (adresse de messagerie, nom d'affichage, qu'il s'agisse d'objets appartenant ou non à la même organisation), ainsi que les autorisations attribuées.

Il n'est pas possible d'accéder au contenu des objets (contenu des fichiers).

La suppression des métadonnées récupérées et stockées a lieu dès que l'objet correspondant est supprimé dans le cloud Microsoft ou lorsque le service est désactivé pour le client dans le Control Panel.

Le traitement des métadonnées consultées s'effectue sur du matériel informatique propre, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

3. 365 Total Backup

365 Total Backup est une solution de sauvegarde et de restauration fiable, intuitive et facile à gérer pour les boîtes aux lettres Microsoft 365, les comptes OneDrive pour les entreprises, les bibliothèques de documents SharePoint, les chats Teams et les points de terminaison.

365 Total Backup permet au client, via une console multi-locataires, de configurer, de visualiser et de surveiller les droits, les sauvegardes et les objets M365 à sauvegarder en fonction de directives. Toutes les données de sauvegarde sont cryptées à l'aide de clés AES-256 personnalisées.

La gestion des données sécurisées et cryptées est assurée au sein du groupe Hornetsecurity par Hornetsecurity Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malte (« Hornetsecurity Ltd »).

Les données de sauvegarde cryptées sont stockées conformément aux paramètres définis par le client :

- dans le cloud Hornetsecurity, notamment en Allemagne, en France, en Suisse, au Royaume-Uni, au Canada et aux États-Unis (Virginie et Géorgie), hébergé par Hornetsecurity GmbH, Am Listholze 78, 30177 Hannover, Allemagne.
- ou, pour les installations plus anciennes (antérieures à février 2022), dans le cloud Microsoft Azure, zone Europe occidentale – en « stockage à froid » (« Cold Storage ») –, Hornetsecurity Ltd. utilisant la plateforme Microsoft Azure et ses services de conformité. La plateforme et les services Azure Europe occidentale sont certifiés SOC 1 Type 2, SOC 2 Type 2, ISO 9001, ISO 27001, ISO 22301, PCI DSS et HIPAA.

Pendant l'exploitation, la licence logicielle utilisée est comparée en ligne avec la licence achetée enregistrée dans les données de base. Il n'y a pas de transmission ou de traitement des données utiles des services par le contractant.

4. 365 Total Protection

Dans le cadre de Spam and Malware Protection (protection contre le spam et les logiciels malveillants), les e-mails entrants du donneur d'ordre sont filtrés pour détecter les contenus nuisibles (par exemple les virus), les publicités non sollicitées (par exemple les spams) et les publicités légitimes (par exemple les newsletters) sur les systèmes informatiques du donneur d'ordre. Les e-mails sortants sont également filtrés.

Le traitement automatique des données comprend les métadonnées de la transmission des messages (adresse de messagerie de l'expéditeur et du destinataire, objet du message, date/heure de réception et de distribution du message, adresses IP des serveurs impliqués dans la communication, code et texte d'erreur SMTP), le contenu des e-mails et la classification du mail (clean, spam, virus, infomail). Les métadonnées des messages sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. Le mail lui-même est supprimé après une distribution réussie ou un rebond.

Pour l'utilisation de Individual User Signatures, Company Disclaimer et 1-Click Intelligent Ads, l'utilisation d'un service d'annuaire du côté du donneur d'ordre est supposée, lequel peut être interrogé par le contractant via le protocole LDAP. De plus, les groupes du répertoire des utilisateurs doivent être organisés dans le Control Panel. Les messages doivent être envoyés via les relais du contractant.

Le traitement automatique des données comprend l'adresse de messagerie de l'utilisateur, le nom de groupe attribué dans le service d'annuaire, d'autres informations éventuellement liées dans le service d'annuaire telles que l'appartenance à une organisation, le poste, le numéro de téléphone, le numéro de fax et le contenu du pied de page de l'e-mail qui, du côté du donneur d'ordre, est attribué au groupe dans l'annuaire. Les données à caractère personnel extraites de l'annuaire sont supprimées lorsque l'utilisation du service prend fin. Le message traité est supprimé après une distribution réussie ou un rebond.

Global S/MIME & PGP Encryption : Le contractant crypte et signe les e-mails sortants et décrypte les e-mails entrants du donneur d'ordre sur ses propres systèmes informatiques conformément aux directives mises en place. Selon les paramètres des directives, les e-mails sortants sont mis à la disposition du destinataire dans le Websafe protégé.

Le traitement automatique des données comprend l'adresse e-mail de l'expéditeur et du destinataire, les clés S/MIME ou PGP privées et publiques, le contenu des e-mails sortants envoyés à des tiers (Websafe), l'adresse e-mail dans les clés publiques de tiers, le statut du cryptage et le contenu des e-mails. Les données relatives à l'expéditeur, au destinataire et au statut de cryptage sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. Le mail lui-même est supprimé après une distribution réussie ou un rebond.

Archiving : Le contractant archive les e-mails du donneur d'ordre sur ses propres systèmes informatiques de manière à ce qu'ils soient non modifiables

Le traitement automatique des données comprend l'adresse e-mail de l'expéditeur et du destinataire, l'objet de l'e-mail, la date/l'heure de réception de l'e-mail, les adresses IP des serveurs impliqués dans la communication, le contenu des e-mails et, le cas échéant, le nom et le type de pièce jointe.

Les données suivantes sont utilisées pour l'affichage dans le Control Panel : adresse de l'expéditeur et du destinataire, objet de l'e-mail, date/heure, nom et type de pièce jointe. Toutes ces données, y compris le message lui-même, sont stockées selon la durée d'archivage spécifique au client, plus un (1) an, puis supprimées. Un blocage de la suppression à la demande du client peut augmenter la durée de stockage.

Advanced Thread Protection (ATP) : protège le trafic des e-mails du donneur d'ordre contre les attaques ciblées et individuelles, telles que le spear-phishing, les Blended Attacks (attaques mixtes), les Advanced Persistent Threats (menaces persistantes avancées), les ransomwares et la fraude au PDG. Afin de détecter les attaques, les e-mails du donneur d'ordre considérés comme suspects par le contractant sont analysés par des techniques de filtrage avancées.

Pour ce faire, les méta-informations sur le contenu de l'e-mail ainsi que le type, le nom et le contenu de la pièce jointe -sont traités automatiquement. Les méta-informations sur le contenu de l'e-mail sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. L'e-mail est supprimé du système ATP après une analyse réussie.

Contingency Covering : En cas de défaillance du serveur cible, le contractant met à disposition une boîte aux lettres électronique de 10 Go par utilisateur. Les utilisateurs autorisés peuvent accéder aux e-mails de cette boîte aux lettres via une interface webmail ou via IMAP et POP3.

Le traitement automatique des données comprend les métadonnées du message (l'adresse de messagerie de l'expéditeur et du destinataire, la date/l'heure de réception de l'e-mail), le contenu de l'e-mail ainsi que les métadonnées du webmail (nom de connexion, adresse IP, durée de connexion, volume de consultation, protocole). Les métadonnées des messages, les métadonnées du webmail et les messages archivés sont supprimés au plus tard après

14 mois. Les messages dans la boîte aux lettres du webmail sont supprimés au plus tard lorsque le client n'utilise plus le service.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation).

Pour l'utilisation de Single-Sign-On, l'adresse e-mail est transmise à Microsoft lors de l'inscription de l'utilisateur.

Aucune autre donnée n'est transmise à des tiers, l'accès aux données par des tiers est également exclu.

5. 365 Total Protection Enterprise Backup

Ce service regroupe les services

- 365 Total Protection (page 8) et
- 365 Total Backup (page 7).

Veuillez y lire les informations correspondantes.

6. AI Cyber Assistant : AI Email Security Analyst

AI Email Security Analyst indique aux utilisateurs finaux les précautions à prendre lorsqu'ils traitent l'e-mail signalé. De plus, cette fonctionnalité fournit une explication et une évaluation des indicateurs de légitimité ou de malveillance présents dans le message.

Les administrateurs peuvent utiliser AI Email Security Analyst dans le cadre du suivi en temps réel des e-mails, où ils obtiennent à la demande une analyse générique, une évaluation des risques et une classification basée sur l'IA du contenu des e-mails. Aucune information détaillée sur le contenu des e-mails n'est divulguée.

AI Email Security Analyst traite les données via des modèles de langage pré-entraînés (LLM) hébergés dans des environnements MS Azure isolés. Serveurs MS Azure situés dans la région « États-Unis » pour les clients des États-Unis et du Canada, serveurs MS Azure situés dans la région « Europe » pour les clients de l'UE et du reste du monde.

Une fois évalués, les contenus des e-mails ne sont ni stockés dans le système d'IA ni utilisés à des fins d'entraînement. Les résultats de l'évaluation, associés aux retours d'expérience des utilisateurs concernant l'AI Email Security Analyst, peuvent être utilisés pour améliorer les algorithmes de détection.

Le stockage des e-mails s'effectue sur du matériel propre, situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. À l'exception du prestataire et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

7. AI Cyber Assistant : AI Recipient Validation

AI Recipient Validation est un outil qui permet aux utilisateurs finaux d'être avertis par les locataires de M365 dans leur client Outlook lorsqu'un e-mail qu'ils ont envoyé est susceptible d'être mal orienté (par ex. si un faux destinataire a été ajouté à un fil de messagerie) ou contient des informations sensibles (par exemple, des numéros de carte de crédit ou des données à caractère personnel). Les utilisateurs peuvent accepter les conseils ou continuer sans apporter de modifications à l'e-mail. Les suggestions du produit sont mises à jour en fonction du comportement de l'utilisateur.

Le traitement automatique des données dans le cloud comprend l'objet de l'e-mail, l'expéditeur et le destinataire (nom en clair et adresse mail), le type d'e-mail (nouveau, réponse, transfert), l'heure d'envoi de l'e-mail, la langue du client Outlook, tous les utilisateurs et groupes du locataire, le nombre de destinataires dans les listes de distribution, le nombre d'e-mails envoyés, ainsi que les statistiques de performance du module complémentaire Outlook.

Le traitement automatique des données dans le client Outlook local comprend le contenu de l'e-mail.

AI Recipient Validation n'utilise ni IA générative ni grands modèles linguistiques (LLM). L'évaluation repose sur une logique décisionnelle basée sur des règles, sous la forme d'un arbre de décision. Les retours d'information indiquant si un destinataire a été confirmé comme valide ou indésirable dans le contexte de l'e-mail concerné peuvent être utilisés pour ajuster cette logique décisionnelle et ainsi améliorer les évaluations futures. Ce processus n'implique ni entraînement ni réglage fin d'un LLM.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

8. AI Cyber Assistant : Conversational Agent

L'agent conversationnel est accessible via le panneau de contrôle et assiste les utilisateurs au niveau « Partenaire » ainsi que ceux disposant d'une autorisation d'utilisation de l'agent. Il fournit des réponses aux questions relatives à la vente, à l'assistance technique, ainsi qu'aux indicateurs d'utilisation et de performance des services.

L'agent conversationnel utilise un modèle linguistique de grande envergure (LLM) pré-entraîné. Pour répondre aux demandes, le modèle a accès à certaines informations internes issues des services commerciaux, marketing, techniques et d'assistance, ainsi qu'aux métadonnées pertinentes relatives aux clients et à l'utilisation issues du suivi en temps réel des e-mails (Email Live Tracking), dans la limite des autorisations de l'utilisateur.

Les données d'entrée et de sortie sont traitées en tant que contexte lors de l'exécution et ne sont pas utilisées pour l'entraînement du LLM.

À des fins d'assurance qualité, les 50 dernières saisies utilisateur et sorties du LLM sont conservées, mais au maximum pendant 30 jours.

Veuillez noter que les réponses sont générées par l'IA et peuvent, dans certains cas, ne pas être correctes.

Le traitement des données s'effectue sur notre propre matériel, hébergé dans des centres de données loués (colocation). Le traitement et le stockage ont lieu en Allemagne. Pour les utilisateurs situés aux États-Unis, le traitement et le stockage ont lieu aux États-Unis.

9. AI Cyber Assistant : Teams Protection

Teams Protection protège les utilisateurs finaux contre les messages compromettants lors de leurs échanges sur Microsoft Teams en analysant tous les messages contenant des URL. Lorsqu'une menace est détectée, un message d'alerte s'affiche dans l'historique de discussion

via le bot AI Cyber Assistant. En option, les messages contenant des URL potentiellement malveillantes peuvent être supprimés. Teams Protection utilise la base de données et les technologies de détection de Secure Links de Hornetsecurity (qui fait partie d'Advanced Threat Protection, page 18).

Dans le panneau de configuration, les administrateurs disposent d'une vue d'ensemble des discussions contenant des URL malveillantes détectées, avec indication des interlocuteurs concernés et de l'URL en question. Les comptes diffusant des contenus malveillants peuvent être bloqués.

Tous les messages Teams sont traités par nos serveurs situés dans nos propres centres de données. Nous enregistrons les URL malveillantes détectées ainsi que les participants à la communication afin d'alerter nos clients et de leur fournir des détails sur ces menaces.

Le traitement des données s'effectue sur notre propre matériel, hébergé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. À l'exception du prestataire et des représentants désignés du donneur d'ordre, aucun tiers n'a accès à ces données.

10. Control Panel, connexion au

Si vous êtes déjà client de Hornetsecurity, vous pouvez vous connecter via notre site web au Control Panel à partir duquel vous pouvez utiliser et gérer votre prestation. Pour vous connecter, vous avez besoin de votre nom d'utilisateur ou de votre adresse e-mail ainsi que de votre mot de passe. La durée de stockage se mesure donc en principe à la durée de la relation contractuelle. Toutefois, à l'issue de celle-ci, des bases juridiques alternatives peuvent intervenir, telles que des délais de conservation légaux.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

La base juridique du traitement de ces informations et données enregistrées est la nécessité d'exécuter la relation contractuelle existante.

11. Hornet.email Webmail, connexion à

Si vous êtes déjà client de Hornetsecurity, vous pouvez vous connecter via notre site web au Control Panel à partir duquel vous pouvez utiliser et gérer votre prestation. En tant que client Webmail, vous pouvez vous connecter à votre boîte aux lettres via un lien séparé. Pour vous connecter, vous avez besoin de votre nom d'utilisateur ou de votre adresse e-mail ainsi que de votre mot de passe. La durée de stockage se mesure donc en principe à la durée de la relation contractuelle. Toutefois, à l'issue de celle-ci, des bases juridiques alternatives peuvent intervenir, telles que des délais de conservation légaux.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

La base juridique du traitement de ces informations et données enregistrées est la nécessité d'exécuter la relation contractuelle existante.

12. Hosted Exchange

Le donneur d'ordre peut réserver des boîtes aux lettres Hosted Exchange en plus de Spam and Malware Protection s'il ne souhaite pas utiliser son propre serveur de messagerie. Hosted Exchange vous offre, sans effort supplémentaire, le fonctionnement sécurisé d'un serveur Exchange géré de manière professionnelle dans votre domaine de messagerie avec Active Sync, des informations de contact partagées, un calendrier en ligne, une collaboration de groupe et un accès depuis différents clients et plateformes matérielles.

Le traitement automatique des données comprend les e-mails reçus et envoyés, l'adresse e-mail de l'utilisateur, les appartenances à des groupes, la date de création de la boîte aux lettres, les autorisations de/vers d'autres comptes internes du même domaine et les appareils mobiles utilisés pour accéder à la boîte aux lettres. En outre, si elles ont été introduites : entreprise, poste, service, numéro d'employé, supérieur, numéros de téléphone, adresse. Les données sont supprimées au plus tard 90 jours après la résiliation du service.

Les e-mails sont transmis pour traitement et stockage à des serveurs de sous-traitants situés dans l'UE (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Allemagne ou Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Allemagne).

La base juridique du traitement de ces informations et données enregistrées est la nécessité d'exécuter la relation contractuelle existante.

13. IA, utilisation de l'intelligence artificielle

a. Introduction

Ce document explique nos pratiques en matière de collecte, de stockage et de traitement des métadonnées des e-mails et des sujets latents du contenu des e-mails pour nos projets d'apprentissage automatique et d'intelligence artificielle chez Hornetsecurity. Notre approche place la vie privée des utilisateurs au premier plan et est conforme aux directives existantes en matière de protection des données. Bien que nous nous concentrions toujours sur les métadonnées des e-mails, l'identification des objets des e-mails fournit des informations permettant d'affiner les modèles d'apprentissage automatique, notamment pour la classification des e-mails, nécessaire pour des services tels que Targeted Fraud Forensics, Phishing Protection, AI Recipient Validation et les produits et fonctionnalités de filtrage des infomails.

b. Finalité du traitement

Amélioration continue des modèles de classification des e-mails

Nous affinons et améliorons les algorithmes d'apprentissage automatique en utilisant les données des e-mails afin de garantir la précision et la pertinence de leurs prédictions. Cela nous aide à distinguer efficacement les communications authentiques, les spams et les contenus malveillants.

Catégorisation des e-mails

À l'aide des métadonnées des e-mails et des thèmes latents, les e-mails sont classés en différents types, par exemple « publicité » ou « phishing ». Cette approche est étroitement liée à notre produit de filtrage des infomails, qui permet aux utilisateurs de mettre en quarantaine les e-mails indésirables.

Partage d'informations sensibles et fuites de données

Pour nos produits Targeted Fraud Forensics et AI Recipient Validation, il est essentiel de prédire la probabilité de divulgation d'informations sensibles à des personnes non autorisées. À cette fin, nous analysons les métadonnées des e-mails, les graphes sociaux, par exemple les liens entre les expéditeurs et les destinataires des e-mails, ainsi que les thèmes latents, afin de détecter les fuites de données potentielles et les menaces de sécurité.

Amélioration de la convivialité

Les actions des utilisateurs, comme le signalement d'e-mails indésirables ou la modification du contenu des e-mails sur la base de suggestions, influencent l'optimisation de la convivialité des produits Hornetsecurity. Cette optimisation permet de réduire le nombre d'e-mails indésirables et de proposer des alertes et des recommandations d'action plus pertinentes.

Protection du compte et sécurité

L'évaluation des données de messagerie et l'analyse des tendances pour détecter les anomalies ou les menaces de sécurité potentielles, telles que les campagnes de phishing émergentes ou les comptes de messagerie compromis, nous aident à protéger nos utilisateurs et leurs données.

c. Données que nous collectons

Identifiants de base :

- Adresse e-mail de l'expéditeur
- Adresse(s) e-mail du destinataire
- Adresses IP, noms d'hôtes et ASN (Autonomous System Number) des serveurs expéditeurs

Données temporelles :

- Horodatage des livraisons d'e-mails
- Horodatage des retours des utilisateurs et des administrateurs sur les e-mails signalés comme spam, infomail ou inoffensifs

Caractéristiques des messages et statut d'authentification :

- Taille du message
- Format du message (HTML, texte brut et autres détails sur le type de contenu)
- La ou les sommes de contrôle du corps et de l'en-tête du message
- Détails d'authentification et de vérification (entrées pour DKIM, DMARC, SPF Records)

Informations sur l'interaction :

- Réponse à l'e-mail (par ex. signalé comme spam ou inoffensif)
- Actions de réponse aux messages (par ex. répondu, transféré, premier contact)

- Actions en réponse aux alertes et aux notifications (par exemple, décision d'envoyer ou non un e-mail après demande par AI Recipient Validation)
- Métadonnées telles que le nombre de messages, les mots-clés dans l'objet et la répartition de l'horodatage correspondant pour certains destinataires/listes de distribution (AI Recipient Validation)

Métadonnées des pièces jointes :

- Nombre de pièces jointes
- Types de fichiers (par ex. .pdf, .docx, .jpg)
- Taille des fichiers
- Noms de fichiers contenant des données à caractère personnel anonymisées
- Somme(s) de contrôle du/des fichier(s)

Liens et domaines :

- Liens dans un e-mail ou dans des pièces jointes à un e-mail avec des chemins d'URL et des paramètres rendus anonymes
- Domaines des liens extraits et leurs informations DNS (par exemple, les enregistrements A du DNS)

Données d'en-tête :

- Informations contenues dans la section d'en-tête de l'e-mail, y compris :
- De
- À
- Date
- Objet contenant des données à caractère personnel anonymisées
- ID du message
- Données User-Agent et X-Mailer
- Lignes reçues
- Résultats de l'authentification
- En-têtes de message liés au contenu (par exemple « Content-Type »)

Déduction du thème à partir du corps du message :

Afin d'améliorer nos modèles de classification des e-mails, nous extrayons le thème général du contenu des e-mails. Dans ce cas, le texte du message est traité afin d'identifier une catégorie ou un thème supérieur, sans enregistrer de détails concrets ou sensibles du texte du message lui-même.

Exemple : un e-mail contenant des détails sur une vente de marchandises à venir pourrait être généralement classé comme une « promotion » ou un « événement de vente ».

d. Outils d'IA, stockage et conservation des données

Tous les outils et modèles d'IA sont soit développés en interne, soit mis à disposition via des plateformes de confiance comme Azure. Pour le stockage de l'IA, nous utilisons à la fois notre propre infrastructure et les Large Language Models (LLM) hébergés par Microsoft Azure pour fournir des fonctions d'IA avancées. Nos données d'invite ne contiennent que les données personnelles minimales nécessaires à la fourniture du service. Les données ne sont jamais

stockées ou utilisées pour la formation de modèles sans autorisation expresse. Les LLM externes sont entraînés par le fournisseur du LLM sans nos données.

L'infrastructure de stockage et de traitement de l'IA se trouve soit dans le centre de données Hornetsecurity, soit dans l'environnement cloud sécurisé d'Azure. L'accès aux données et aux modèles est strictement contrôlé et surveillé du point de vue de la protection des données. Des tiers ou du personnel non autorisé n'ont pas accès à ces données. Les modèles d'apprentissage automatique sont exclusivement mis à disposition et utilisés via notre infrastructure sécurisée ou via des connexions sécurisées aux services Azure. Chaque transaction de données entre les systèmes des clients et notre API AI/ML est protégée par des procédures de cryptage robustes de bout en bout. Cela garantit la confidentialité et l'intégrité des données pendant leur transfert.

Protocoles de stockage et de conservation

- Les données sont cryptées au repos et pendant la transmission. Les procédures de cryptage sont conformes aux meilleures pratiques du secteur.
- Les données sont conservées aussi longtemps que nécessaire pour atteindre les objectifs de traitement indiqués. Certains fichiers journaux peuvent être conservés jusqu'à 12 mois, conformément à notre politique de conservation des données.
- Toutes les autres données enregistrées pour le fonctionnement ou l'exécution des fonctions d'un produit ou d'un service payant actif sont conservées aussi longtemps que ces données sont nécessaires.
- Les services terminés suivent ensuite une procédure de désactivation.

Anonymisation des informations personnelles identifiables :

- Afin de garantir la vie privée des utilisateurs et de respecter les normes de protection des données, les données à caractère personnel sont systématiquement rendues anonymes avant d'être stockées, dans la mesure du possible.
- L'anonymisation des informations personnelles identifiables (PII) est une mesure prise pour éliminer les biais potentiels dans nos modèles d'apprentissage automatique et pour garantir que les modèles fonctionnent de manière objective.

14. Security Awareness Service

Pour le Security Awareness Service, les données des utilisateurs (nom, service, adresse e-mail, groupe attribué pour l'évaluation) sont saisies par importation CSV, par comparaison avec MS365 ou par synchronisation LDAP. Les données servent à fournir une formation de sensibilisation (vidéos, questionnaires, fiches d'information) et à envoyer des e-mails de phishing simulés à l'utilisateur.

Les résultats des attaques simulées sont évalués statistiquement et édités par groupe et par utilisateur. Lorsque le mode de protection de la vie privée est activé, il n'est pas possible de procéder à une évaluation personnelle. Les informations recueillies permettent de créer un Employee Security Index (ESI®) qui documente les progrès en matière de sensibilisation, mais qui permet également une comparaison directe avec un groupe d'utilisateurs très bien formés.

Pour simuler des scénarios de phishing proches de la réalité, des adresses de messagerie appartenant à l'entreprise sont également utilisées comme adresses d'expéditeur falsifiées. Un utilisateur peut s'opposer à l'utilisation de son adresse électronique à de telles fins.

Pour simuler de manière réaliste des e-mails de spear phishing sur la base d'OSINT (Open Source Intelligence), des données d'entreprises et des données personnelles disponibles publiquement sont également analysées, par ex. les informations provenant de portails d'évaluation d'entreprises tels que Kununu.com ou de sources de réseaux sociaux liées à l'activité, par ex. Xing.com ou LinkedIn.com. De même, dans les niveaux d'entraînement supérieurs, il est possible de se référer à des e-mails antérieurs, réellement reçus ou envoyés, qui n'ont absolument rien à voir avec la simulation de phishing.

Les informations saisies par les utilisateurs dans le cadre de simulations d'e-mails de phishing, par ex. les données d'inscription sur des pages d'inscription générées par nos soins et falsifiées ne sont ni traitées ni enregistrées. Les pièces jointes de documents ouvertes par les utilisateurs dans le cadre de simulations d'e-mails de phishing, par ex. les documents Word ou les feuilles de calcul Excel, ne contiennent pas de code malveillant.

Traitement des messages d'e-mails de phishing potentiels dans Outlook via le bouton de l'add-on Hornetsecurity :

- Dans la mesure où il s'agit d'une simulation d'e-mail de phishing dans le cadre du Security Awareness Service, le message réussi est confirmé à l'utilisateur et fait l'objet d'une saisie statistique.
- S'il ne s'agit pas d'un e-mail de phishing simulé et que le client a également souscrit au service de filtrage des spams et des logiciels malveillants, l'e-mail signalé est envoyé à notre Security Lab pour une analyse plus approfondie.
- Dans la mesure où il ne s'agit pas d'un e-mail de phishing simulé et que le client n'a pas souscrit au service de filtrage des spams et des logiciels malveillants, l'e-mail signalé est envoyé à une boîte aux lettres d'assistance que le client choisit.

Les données client nécessaires à la configuration du service et toutes les évaluations statistiques sont supprimées au plus tard 4 semaines après la fin du contrat.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

15. Spam and Malware Protection

Dans le cadre de Spam and Malware Protection (protection contre le spam et les logiciels malveillants), les e-mails entrants du donneur d'ordre sont filtrés pour détecter les contenus nuisibles (par exemple les virus), les publicités non sollicitées (par exemple les spams) et les publicités légitimes (par exemple les newsletters) sur les systèmes informatiques du donneur d'ordre. Si le donneur d'ordre le souhaite, les e-mails sortants sont également filtrés.

Le traitement automatique des données comprend les métadonnées de la transmission des messages (adresse e-mail de l'expéditeur et du destinataire, objet du message, date/heure de

réception du mail et de distribution du message, adresses IP des serveurs impliqués dans la communication, code et texte d'erreur SMTP), le contenu des e-mails et la classification de l'e-mail (clean, spam, virus, infomail). Les métadonnées des messages sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. Le mail lui-même est supprimé après une distribution réussie ou un rebond.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation).

Aucune autre donnée (en-tête de l'e-mail, expéditeur, destinataire, objet, date, contenu du texte) n'est transmise à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

a. En option : Advanced Thread Protection (ATP)

ATP protège le trafic de messagerie du donneur d'ordre contre les attaques ciblées et individuelles, telles que le spear phishing, les Blended Attacks (attaques mixtes), les Advanced Persistent Threats (menaces persistantes avancées), les ransomwares et la fraude au PDG. Afin de détecter les attaques, les e-mails du donneur d'ordre considérés comme suspects par le contractant sont analysés par des techniques de filtrage avancées.

Pour ce faire, les méta-informations sur le contenu de l'e-mail ainsi que le type de pièce jointe, le -nom et -le contenu sont traités automatiquement. Les méta-informations sur le contenu de l'e-mail sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. L'e-mail est supprimé du système ATP après une analyse réussie.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

b. En option : Secure Links (intégré à l'ATP)

Afin de renforcer la sécurité lors de l'utilisation de nos services de messagerie électronique, nous utilisons la fonction « Secure Links ». Les liens contenus dans les e-mails entrants sont techniquement réécrits et, lorsqu'ils sont ouverts, ils sont d'abord vérifiés via une infrastructure de sécurité.

Dans le cadre de cette vérification, l'adresse de destination et les contenus Web accessibles via celle-ci sont automatiquement analysés à la recherche d'indices de hameçonnage, de logiciels malveillants ou d'autres caractéristiques liées à la sécurité. Pour ce faire, nous utilisons des méthodes basées sur des règles ainsi que des techniques d'apprentissage automatique et d'apprentissage profond. Le contenu des e-mails n'est pas traité par des modèles linguistiques à grande échelle (Large Language Models) ni par une IA générative.

L'analyse de sécurité se limite à l'URL consultée et aux ressources Web accessibles via celle-ci. Le contenu de l'e-mail, les informations relatives à l'expéditeur et au destinataire, ainsi que les pièces jointes, ne sont pas utilisés pour l'entraînement, le réglage fin ou le développement des modèles de détection utilisés.

Dans la mesure où une URL ou la page Web consultée contient elle-même des données à caractère personnel, celles-ci peuvent être traitées techniquement dans le cadre du contrôle de sécurité. Ces données ne sont pas utilisées à des fins d'entraînement ou d'optimisation des modèles de détection sous-jacents.

c. En option : Email Encryption

Le contractant commande et gère des certificats S/MIME, crypte et signe les e-mails sortants et décrypte les e-mails entrants du donneur d'ordre sur ses propres systèmes informatiques conformément aux directives établies. Selon les paramètres des directives, les e-mails sortants sont mis à la disposition du destinataire dans le Websafe protégé.

Le traitement automatique des données comprend l'adresse e-mail de l'expéditeur et du destinataire, la clé privée et publique S/MIME ou PGP, le contenu des e-mails sortants envoyés à des tiers (Websafe), l'adresse e-mail dans les clés publiques de tiers, le statut du cryptage et le contenu de l'e-mail. Les données relatives à l'expéditeur, au destinataire et au statut de cryptage sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. Le mail lui-même est supprimé après une distribution réussie ou un rebond.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation).

Pour la commande de certificats S/MIME, l'adresse e-mail ainsi que le prénom et le nom de la personne qui commande le certificat sont transmis pour traitement à un sous-traitant dans l'UE (InterNetX GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg, Allemagne).

Pour une authentification à deux facteurs (2FA) du destinataire de Websafe, son numéro de téléphone portable est transmis, avec son consentement, à un sous-traitant pour traitement (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, États-Unis). La transmission s'effectue sur la base de clauses contractuelles standard. Là, le numéro de portable est immédiatement supprimé après la fin du processus chez Twilio. Le contractant conserve le numéro de téléphone portable tant que la boîte aux lettres du destinataire existe.

Aucune donnée autre que celles mentionnées pour la commande du certificat S/MIME et la génération d'une clé 2FA n'est transmise à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

d. En option : Archiving

Le contractant archive les e-mails du donneur d'ordre sur ses propres systèmes informatiques de manière à ce qu'ils soient non modifiables

Le traitement automatique des données comprend l'adresse e-mail de l'expéditeur et du destinataire, l'objet de l'e-mail, la date/l'heure de réception de l'e-mail, les adresses IP des serveurs impliqués dans la communication, le contenu des e-mails et, le cas échéant, le nom et le type de pièce jointe.

Les données suivantes sont utilisées pour l'affichage dans le Control Panel : adresse de l'expéditeur et du destinataire, objet de l'e-mail, date/heure, nom et type de pièce jointe. Toutes

ces données, y compris le message lui-même, sont stockées selon la durée d'archivage spécifique au client, plus un (1) an, puis supprimées. Un blocage de la suppression à la demande du client peut augmenter la durée de stockage.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

e. En option : Continuity Service

Le contractant met à disposition les e-mails entrants et sortants du donneur d'ordre dans les archives pendant une période de 3 mois, à condition que ces e-mails soient acheminés via les serveurs de Hornetsecurity.

Le contractant met également à disposition une boîte aux lettres électronique d'une capacité de 10 Go par utilisateur. Les utilisateurs autorisés peuvent accéder aux e-mails de cette boîte aux lettres via une interface webmail ou via IMAP et POP3.

Le traitement automatique des données comprend les métadonnées du message (l'adresse de messagerie de l'expéditeur et du destinataire, la date/l'heure de réception de l'e-mail), le contenu de l'e-mail ainsi que les métadonnées du webmail (nom de connexion, adresse IP, durée de connexion, volume de consultation, protocole). Les métadonnées des messages, les métadonnées du webmail et les messages archivés sont supprimés au plus tard après 14 mois. Les messages dans la boîte aux lettres du webmail sont supprimés au plus tard lorsque le client n'utilise plus le service.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

f. En option : E-Mail-Signature and Disclaimer

L'utilisation de Signature and Disclaimer présuppose l'utilisation d'un service d'annuaire du côté du donneur d'ordre, qui peut être interrogé par le contractant via le protocole LDAP. De plus, les groupes du répertoire des utilisateurs doivent être organisés dans le Control Panel. Les messages doivent être envoyés via les relais du contractant.

Le traitement automatique des données comprend l'adresse électronique de l'utilisateur, le nom de groupe attribué dans le service d'annuaire et d'autres informations éventuellement liées dans le service d'annuaire, telles que l'appartenance à une organisation, le poste, le numéro de téléphone, le numéro de fax et le contenu du pied de page de l'e-mail, qui sont attribués au groupe dans l'annuaire du côté du donneur d'ordre. Les données à caractère personnel extraites de l'annuaire sont supprimées lorsque l'utilisation du service prend fin. Le message traité est supprimé après une distribution réussie ou un rebond.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

g. En option : E-mail made in Germany

Le prestataire permet une connexion de l'infrastructure de messagerie du donneur d'ordre à l'association E-Mail made in Germany (EmiG) et réalise à cet effet la mise en œuvre côté serveur de messagerie, nécessaire pour satisfaire aux exigences d'un cryptage de transport continu des e-mails dans l'association EmiG.

Le traitement automatique des données comprend les métadonnées de la transmission des messages (adresse e-mail de l'expéditeur et du destinataire, objet du message, date/heure de réception du message, adresses IP des serveurs impliqués dans la communication, statut de cryptage) et le contenu des e-mails. Les métadonnées de la transmission des messages sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois. Le mail lui-même est supprimé après une distribution réussie ou un rebond.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

16. Test-Onboarding

Pour tester la performance des services, vous pouvez vous inscrire directement via notre site web. Pour cela, nous avons besoin de différentes informations personnelles vous concernant, d'informations sur le domaine, le serveur et les utilisateurs pour lesquels la prestation est souhaitée, ainsi que sur le service souhaité. Les champs obligatoires sont marqués en conséquence. Toutes les autres informations sont facultatives. La durée de stockage se mesure donc en principe à la durée de la relation contractuelle. Toutefois, à l'issue de celle-ci, des bases juridiques alternatives peuvent intervenir, telles que des délais de conservation légaux.

Les données de base du donneur d'ordre sont traitées à des fins de gestion de la base de données clients par des sous-traitants sur des systèmes situés dans un pays tiers (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, États-Unis). Le transfert des données s'effectue sur la base de clauses contractuelles types.

- La base juridique du traitement est dans ce cas l'exécution de mesures précontractuelles ou la nécessité de l'exécution du contrat.

17. VM Backup

VM Backup est une solution de sauvegarde et de restauration fiable, intuitive et facile à gérer pour les serveurs virtualisés dans les environnements Hyper-V et VMware, ainsi que pour les serveurs physiques Microsoft.

VM Backup permet au client d'effectuer des sauvegardes vers les emplacements définis par le client, à des intervalles de temps définis par le client. Le cryptage des sauvegardes est as-

suré par des clés de cryptage AES-256 (mot de passe) configurées par le client. Toutes les copies hors site sont cryptées en AES-256. Pour les sauvegardes sur site (primaires), le cryptage est facultatif et également pris en charge.

Pour les copies hors site, le stockage des données est effectué en option sur un cloud loué par le client auprès d'un fournisseur tiers (Microsoft Azure Blob Storage, Wasabi Cloud Object Storage, Amazon S3 ou BackBlaze Cloud Storage). Le client agit en tant que donneur d'ordre vis-à-vis des prestataires tiers.

Pendant l'exploitation, la licence logicielle utilisée est comparée en ligne avec la licence achetée enregistrée dans les données de base. Il n'y a pas de transmission ou de traitement des données utiles des services par le contractant.

18. Web Filter

Les appels http/https et ftp sortants du donneur d'ordre sont acheminés via des serveurs proxy du contractant. Le trafic de données est contrôlé à la recherche de contenus potentiellement nuisibles et filtré le cas échéant.

Le traitement automatique des données comprend la date et l'heure de l'appel d'une adresse web, l'adresse IP appelante, l'URL appelée, la catégorie classée de l'objet appelé, l'entité authentifiée : soit l'adresse électronique, éventuellement pseudonymisée, soit l'adresse IP, soit le nom du service d'annuaire et le chemin d'accès à l'objet, soit la chaîne du connecteur de filtrage web (sAM AccountName, ID du domaine, nom de l'ordinateur, IP de l'ordinateur, programme appelant). Les données mentionnées (URL sans chemin d'accès) sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois.

Le traitement des données s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du contractant et des représentants désignés du donneur d'ordre, aucun tiers n'a accès aux données.

La base juridique du traitement de ces informations et données enregistrées est la nécessité d'exécuter la relation contractuelle existante.

19. Websafe, Déclaration de confidentialité pour les tiers

Pour que nous puissions vous fournir ce service, il est nécessaire de traiter certaines données. Le traitement de ces informations et données enregistrées est nécessaire à l'exécution de la relation contractuelle existante avec nos clients. Cela constitue la base juridique du traitement. Lorsque vous utilisez le service Websafe, vous n'êtes pas soumis à une prise de décision automatisée conformément à l'article 22 du RGPD.

Le traitement automatique des données comprend les métadonnées du message (l'adresse e-mail de l'expéditeur et du destinataire, la date et l'heure de réception de l'e-mail), le contenu de l'e-mail, les métadonnées Websafe (nom de connexion, votre adresse IP, durée de la connexion, volume de consultation, protocole) et, le cas échéant, le numéro de votre téléphone portable. Vos e-mails sont conservés pendant 3 mois dans Websafe. Ils sont ensuite supprimés. Votre compte Websafe existe en principe tant que vous y recevez des e-mails. Si vous ne recevez plus d'e-mails, votre compte Websafe sera automatiquement supprimé 12 mois

après la réception du dernier e-mail. Toutes vos données personnelles, et notamment votre numéro de téléphone, seront alors supprimées de nos serveurs.

Pour finaliser votre inscription, nous devons envoyer un code PIN à votre téléphone portable. Vous pouvez également contacter l'expéditeur de votre e-mail pour qu'il vous transmette le code PIN d'une autre manière. Le fournisseur de services Websafe ne prélève pas de frais pour l'utilisation du service Websafe et l'envoi de SMS.

Le sous-traitant chargé d'envoyer les SMS sur votre téléphone portable est la société Twilio Inc., 375 Beale Street, Suite 300, San Francisco, Californie 94105, États-Unis. La transmission du numéro de téléphone portable se fait sur la base de clauses contractuelles standard de l'UE. Le numéro de téléphone portable est immédiatement supprimé après utilisation par Twilio.

Le traitement des données des métadonnées des messages, des métadonnées Websafe et des messages dans la boîte aux lettres Websafe s'effectue sur notre propre matériel informatique, placé dans des centres de données loués (colocation). Ces données ne sont pas transmises à des tiers. En dehors de Hornetsecurity GmbH, aucun tiers n'a accès à ces données.

IV. Possibilité d'opposition et de suppression

Dans la mesure où le traitement des données est basé sur votre consentement ou sur notre intérêt légitime, vous avez le droit de vous opposer à tout moment au traitement ou de révoquer le consentement que vous avez donné. Votre opposition ou votre révocation n'a d'effet que pour l'avenir. Vous pouvez à tout moment vous adresser à datenschutz@hornetsecurity.com pour exercer votre droit d'opposition ou de révocation. Si vous vous opposez à un traitement sur la base de notre intérêt légitime, nous pouvons néanmoins poursuivre le traitement si nous pouvons démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur vos intérêts, vos droits et vos libertés.

V. Droits des personnes concernées

Si des données à caractère personnel vous concernant sont traitées, vous êtes une personne concernée conformément à l'article 4, paragraphe 1, du RGPD. En tant que personne concernée, vous disposez des droits suivants en ce qui concerne vos données à caractère personnel. Pour exercer ces droits, vous pouvez nous contacter aux coordonnées indiquées ci-dessus.

a. Droit à l'information conformément à l'article 15 du RGPD

Vous avez un droit d'accès à vos données à caractère personnel que nous traitons. Il s'agit des informations obligatoires visées à l'article 15 du RGPD.

b. Droit de rectification conformément à l'article 16 du RGPD

Vous avez le droit d'obtenir sans délai la rectification des données à caractère personnel inexactes et de faire compléter les données à caractère personnel incorrectes.

c. Droit à la suppression conformément à l'article 17 du RGPD

Vous avez le droit de demander la suppression de vos données à caractère personnel si l'une des raisons mentionnées à l'article 17 du RGPD s'applique, notamment lorsqu'il n'existe plus de base juridique pour le traitement.

d. Droit à la limitation du traitement conformément à l'article 18 du RGPD

Vous avez le droit d'exiger la limitation du traitement de vos données à caractère personnel si l'une des raisons mentionnées à l'article 18 du RGPD s'applique, notamment à votre demande, au lieu de la suppression des données.

e. Droit à la portabilité des données conformément à l'article 20 du RGPD

Vous avez le droit d'obtenir toutes les données à caractère personnel que nous avons enregistrées à votre sujet dans un format structuré, couramment utilisé et lisible par machine, et de transmettre ces données à un autre responsable sans être empêché par le responsable auquel les données à caractère personnel ont été fournies.

f. Droit de recours auprès de l'autorité de surveillance compétente, article 77 du RGPD

Vous avez le droit, conformément à l'article 77 du RGPD, de déposer une réclamation auprès de l'autorité de contrôle compétente pour vous.

VI. Destinataires des données

Le traitement de vos données à caractère personnel dans le cadre des *services* est également effectué en partie par des sous-traitants. Celles-ci sont traitées exclusivement sur la base d'un accord de traitement des commandes conformément à l'article 28, paragraphe 3, du RGPD.

VII. Transfert de données vers des pays tiers

Les données à caractère personnel que nous collectons auprès de vous dans le cadre de la prestation des *services* ne sont pas transmises à des pays tiers en dehors de l'Espace économique européen.

Pour l'envoi de SMS d'une authentification à deux facteurs, nous utilisons le fournisseur Twilio, dont le siège se trouve aux États-Unis et donc dans un pays tiers conformément à l'article 44 du RGPD. Twilio participe au DPF (Data Privacy Framework) de l'UE et des États-Unis et travaille selon des clauses contractuelles standard, ce qui garantit un niveau de protection des données adéquat.

Pour la gestion de vos données contractuelles, nous utilisons le fournisseur Salesforce dont le siège se trouve aux États-Unis et donc dans un pays tiers conformément à l'article 44 du RGPD. Salesforce participe au DPF (Data Privacy Framework) de l'UE et des États-Unis et travaille selon des clauses contractuelles standard certifiées, ce qui garantit un niveau de protection des données adéquat.

Pour la gestion de votre signature électronique dans le cadre de contrats, nous utilisons le fournisseur Docusign, dont le siège se trouve aux États-Unis et donc dans un pays tiers conformément à l'article 44 du RGPD. Docusign travaille selon des clauses contractuelles standard certifiées, ce qui garantit un niveau de protection des données adéquat.