Performance Specification

365 Total Protection

1.1 365 Total Protection Business

Through the managed security services of Hornetsecurity, Hornetsecurity 365 Total Protection Business extends the email services of Microsoft 365.
In order to use the 365 Total Protection Business product, you must have Microsoft Cloud Licenses with Exchange functionality activated by Microsoft. The following services are included in 365 Total Protection Business:

1. Easy Onboarding:
   365 Total Protection Business is set up automatically. All the customer's domains, mailboxes and groups are transferred directly from Microsoft 365 to the Hornetsecurity control panel.
   To use Hornetsecurity services for Microsoft 365, one of the customer's administrators must enable the Hornetsecurity app ID for the Microsoft 365 tenant. This is done once during the onboarding process.
   Emails to the customer are forwarded by the service to the Hornetsecurity servers by changing the MX records for the customers' domains that are to be filtered. Hornetsecurity is not responsible for changing the MX records. If the customer wishes, outgoing emails can also be filtered.

2. Single Sign-on:
   All of the customer's users with a valid license for Microsoft 365 can sign on to Hornetsecurity with their Microsoft 365 user details.
   If users are already signed in to Microsoft 365, they do not have to do so again for Hornetsecurity.

3. Email Live Tracking:
   All incoming and outgoing emails are displayed to the client in an overview that can be set and filtered individually. Detailed information is also provided about each email, e.g. the encryption type.
   Depending on the classification of the email (valid, information, spam, content, Threat, AdvThreat, rejected), emails can be released from the display by authorized users and delivered to their recipients. Activities such as allow listing or deny listing can also be carried out.

4. Infomail-Handling:
   Delivery of newsletters and advertising emails can be prevented by rules set up individually by the customer.

   .

5. Content-Control:
   Incoming and outgoing emails are filtered according to established rules regarding their file attachments. Depending on the settings, emails that do not meet the rules are:
   a. rejected with a corresponding error message (incoming),
   b. delivered without their attachment and put into quarantine with their attachment, from where they can be delivered to the recipient by administrators (incoming) and/or

   c. rejected with a corresponding error message (outgoing).

The rules for content filtering can be set by the customer's users who are authorized to do so on the Hornetsecurity control panel.

6. Compliance filter:
   Incoming and outgoing emails are filtered according to defined rules. Depending on the settings, emails that do not meet the rules are:
   a. delivered to the recipient's mailbox (incoming),
   b. rejected with a corresponding error message (incoming),
   c. marked as spam or virus (incoming),
   d. extended to include one or more BCC recipients (incoming and outgoing),
   e. diverted to one or more email addresses (incoming and outgoing),
   f. sent by a different route (incoming and outgoing)
      and/or
   g. delivered, and the sender is notified (outgoing).

   The rules for compliance filtering can be set by the customer's users who are authorized to do so on the Hornetsecurity control panel.

7. Spam and Malware Protection:
   Hornetsecurity filters the customer's incoming emails for harmful content (e.g. viruses) and unsolicited advertising (e.g. spam) on its own IT systems. Incoming emails are:
   a. blocked (rejected) if they are identified with a high degree of certainty as undesirable while the data connection with the Hornetsecurity servers is still in place,
   b. either put into quarantine or delivered with a flag in the subject line, if they are recognized as undesirable after complete acceptance of the email by the Hornetsecurity servers and/or
   c. delivered or made available for collection if they are recognized as desirable emails.

   Emails in quarantine are stored for three months for inspection by the customer's authorized users. At the request of the customer, users are notified of new emails in quarantine (usually once a day).

8. Outlook-based allow and deny listing:
   Hornetsecurity provides the customer with an add-in for Outlook, by means of which the customer has the option to allow list and deny list senders directly in Outlook.

9. Individual user signatures:
   a. Utilization of user-based individual signatures requires the customer to activate sending of emails via Hornetsecurity.
   b. With user-based individual signatures, the customer can create signatures for user groups. These are attached automatically when emails are sent via Hornetsecurity.
   c. A template for a signature can be selected for each user group.
   d. Access for authorized users is via a web interface in which templates for signatures can be created with the aid of a WYSIWYG editor and selectable attributes for the directory service. HTML source code can also be inserted directly.
   e. A preview function enables users in the selected group to see a preview of the template populated with data.

f. Once created, templates are saved by the customer and can be selected for various user groups. All users that are not assigned to a group and groups to which no template has been assigned are brought together in a standard group.

g. Once it has been set up, the signature is attached to outgoing emails when they are sent via Hornetsecurity. This applies to emails sent both externally and internally, provided that they are routed via the contractor.

10. **1-click intelligent ads:**
    1-click intelligent ads extends user-based individual signatures to include display of ads in the signatures at group or company level.
    The customer's authorized users can create sub-signatures centrally and embed them in existing signatures.
    They can be activated or deactivated for groups or for the entire domain with one click.

11. **Company disclaimer:**
    In addition to user-based individual signatures, the customer has the option to create mandatory information either for the entire company or for individual groups.
    a. The mandatory information is attached automatically when emails are sent via Hornetsecurity.
    b. Existing mandatory information can be imported.

12. **Global SMIME/PGP encryption:**
    a. Hornetsecurity encrypts and signs outgoing emails and encrypts the customer's incoming emails on its own IT systems in accordance with the rules set.
    b. Outgoing emails are signed by S/MIME, provided that the private key required for this is present in the certificate store.
    c. The rules for encryption of outgoing emails can be set by the customer's users who are authorized to do so on the Hornetsecurity control panel.
    d. Depending on the rule settings, outgoing emails are:
        i. sent in encrypted form by S/MIME or PGP with the public key of the recipient,
        ii. sent unencrypted via a TLS encrypted channel,
        iii. sent via a DANE-tested and encrypted channel,
        iv. kept in the protected Hornetsecurity Websafe for the recipient and/or
        v. sent unencrypted.
    e. Rules can be set by authorized users on the Hornetsecurity control panel. Users can also ensure email encryption by sending messages with a subject line addition ("tag").
    f. If the rule makes encrypted transmission mandatory but the recipient's public key required for this is not in the certificate store, and transmission by TLS is not supported by the receiving server, outgoing emails to this recipient are rejected and not transmitted.
    g. Incoming emails encrypted by S/MIME or PGP are automatically decrypted if the recipient's private key required for the purpose is present in the certificate store.
    h. Public keys are automatically extracted from signatures of incoming emails and stored in the certificate store.
    i. S/MIME certificates for the client's users can be ordered via the control panel as part of the S/MIME User Subscription. Alternatively, PGP keys can be generated for the client's users or existing S/MIME certificates and PGP keys can be stored in the certificate memory by Hornetsecurity Support. For the use of certificates and keys, Hornetsecurity

charges an annual fee per user certificate and key according to the current price list. This subscription is automatically renewed if it is not deactivated 3 months before expiration and includes the automatic reordering of certificates and keys if required.

j. Hornetsecurity provides support for authorized users insofar as it relates to Hornetsecurity systems. Support for customer systems is not a part of the contract.

13. Hornetsecurity guarantees the confidentiality of the customer's private keys stored in the certificate store. The confidentiality obligation also continues to apply after the contract has come to an end.

14. Secure Cipher Policy Control:
With the secure cipher policy control, the customer can control the trust settings for certification bodies itself.
The customer's authorized users can:
    a. define trust settings for certification bodies and cipher suites in detail on the basis of users and domains.
    b. import self-signed certificates together with the entire trust chain

15. Websafe:
Hornetsecurity makes it possible for the customer to send emails in encrypted form, even if the communication partner has no way of encrypting them at their end.
    a. Emails to customers without an encryption option are delivered to an https and password-protected Websafe mailbox.
    b. A message is sent to the personal Websafe mailbox of the communication partner.
    c. The customer's user is responsible for secure delivery of the access password to the communication partner.
    d. Future emails to the communication partner are sent encrypted to the Websafe mailbox.

1.2 365 Total Protection Enterprise

In order to use the 365 Total Protection Enterprise product, you must have Microsoft Cloud Licenses with Exchange functionality activated by Microsoft.
Hornetsecurity 365 Total Protection Enterprise includes all of the services of 365 Total Protection Business; the service description for 365 Total Protection Business also applies to 365 Total Protection Enterprise.
The following additional services are also included:

1. Email archiving:
    a. Hornetsecurity archives customer emails securely for audit on its own IT systems. The archiving period and archiving exceptions can be defined on the domain, group or user level.
    b. Authorized users can mark emails as "private". Emails marked as "private" are no longer accessible from the archive.
    c. Specially authorized users can set up special access, which allows them to access all archived emails in a specific period (test access, e.g. for the purpose of an audit). Set-up and use of test access is logged.
    d. Archiving is done for emails which
        i. are sent by the customer to third parties via the Hornetsecurity servers (outgoing external emails),

   ii. are sent to the customer by third parties via the Hornetsecurity servers (incoming external emails) and/or
   iii. the customer makes available for archiving by Hornetsecurity via agreed interfaces with Hornetsecurity (internal emails, optional).

e. Hornetsecurity provides support for authorized users insofar as it relates to Hornetsecurity systems. Support for customer systems is not a part of the contract.
f. An inclusive volume of 25 GB is provided for each mailbox. Storage space is calculated as an average over all the customer's mailboxes. A separate charge is made for any usage beyond the inclusive volume.
g. Hornetsecurity offers post-import of existing archive data as an option. Archive data must be delivered in a defined format. Technical prerequisites and framework conditions can be requested from Hornetsecurity. Post-import of existing archive data is subject to charge.
h. On request, Hornetsecurity will export existing archive data to an external data carrier. The export is carried out in EML format onto an encrypted data storage device, which is then sent to the customer. Export of archive data is subject to charge.
   With Aeternum Export Manager, it is also possible to export archived emails on a self-service basis by mailbox and then to download them. The formats PST, EML and MBOX are available. Export of archive data with Aeternum Export Manager is subject to charge.

2. Archiving satisfies the current statutory requirements in Germany regarding electronic archiving of emails. Hornetsecurity will do everything in its power to ensure compliance with these statutory requirements if they change.

3. Hornetsecurity ensures the confidentiality of the archived data and other secrets of the customer that become known within the framework of this contract in respect of third parties. The confidentiality obligation also continues to apply after the contract has come to an end.

4. 10-Years email retention:
   The customer's authorized users can:
   a. access the email archive and
   b. arrange for delivery of archived emails to the customer's systems interactively.

5. Hornetsecurity guarantees the availability of the archived emails for the customer for 10 years from the end of the year in which the archived email in question was sent or received. The prerequisite is the continuation of the contract and fulfillment of the contractual obligations by the customer. If this contract comes to an end, continued availability requires conclusion of a follow-up contract for continuation of data storage.

6. eDiscovery:
   Archived emails can be searched according to certain criteria and content to find specific emails in the archive.

7. Hornetsecurity normally guarantees the access options for authorized users to the archived emails 24 hours a day every day of the year. Maintenance periods are excepted.

8. Forensic analyses:

Heuristic filters for detecting targeted attacks, including verification of authenticity and integrity of metadata and email content, detection and blocking of fake sender identities, detection of fake content, detection of attacks on particularly sensitive data, in particular data concerning payment flows (e.g. credit card data, invoices, payment instructions), detection of targeted attacks on particularly exposed customer employees (e.g. Accounting, CFO, CEO, Controlling).

a. Potentially harmful emails are quarantined by Hornetsecurity.
b. The customer can access quarantined emails via Hornetsecurity's control panel.

9. ATP sandbox:
Suspicious email attachments are opened or executed in several separate, protected environments, and their behavior is checked for possible harmful effects. In particular, attachments found to contain executable code are classified as suspicious.
    a. Potentially harmful emails are quarantined by Hornetsecurity.
    b. Emails with suitable attachments in quarantine can be reviewed by Client administrators from the control panel by using the Sandbox engine. Detailed results of the review can be accessed via the control panel.
    c. Customer security officers are informed directly by email if any threats are detected (real-time alerts).
    d. Email delivery may be delayed due to additional complex filtering. The delay is no longer than 15 minutes per email.

10. URL malware control:
    a. Link scanning: URLs contained in emails or email attachments are activated and the resulting behavior is analyzed.
    b. Link rewriting: URLs in emails are replaced by other URLs that, when activated, retrieve the respective content via the Hornetsecurity Web Filter. Where applicable, the downloaded information is analyzed for suspicious behavior using the Sandbox engine. The Web Filter blocks content that has been flagged as harmful. URLs with no apparent threat after a scan, as well as URL entries on a whitelist, are not replaced.

11. Realtime Threat Report:
The customer has an overview of all booked Hornetsecurity services and can access extensive information and statistics about the current security status.

12. Malware ex-post alert:
If malicious emails have already been delivered, customer security officers are automatically informed by email (ex-post alarm) immediately after the incident is detected (e.g. by filter updates).

13. Malware Ex-Post Deletion:
If Hornetsecurity Artificial Intelligence algorithms detect obfuscated malicious emails after they have been delivered, authorized security officers and administrators can search for the affected mails via the Control Panel and delete them directly from the users' mailboxes.

14. Email Continuity Service:
    a. Hornetsecurity stores incoming and outgoing emails of the customer for three months on its own IT systems, provided that those emails are directed through the Hornetsecurity servers.

b. Authorized users can access the stored emails on the Internet. Stored emails can be searched according to certain criteria and content to find specific emails in the data store. Authorized users can arrange interactively for redelivery of stored emails to the customer's systems.
c. If the Microsoft 365 email server crashes, Hornetsecurity will make one of its own email servers (backup server) available in the Hornetsecurity computer center, to which incoming emails can be redirected and from which outgoing emails can be sent.
d. Redirection of incoming emails to the backup server can be carried out on request or automatically, as preferred. The corresponding setting (manual or automatic) is activated by Hornetsecurity support at the request of the customer.
e. While the customer's email server is down, emails on the backup server can be accessed by the customer's authorized users via POP3, IMAP or Webmail interface.
f. Emails on the backup server are automatically sent to the customer's email server as soon as it is available again, provided that the emails have not already been moved to other folders or deleted via POP3, IMAP or web interface. Emails are deleted from the backup server once they have been transferred to the customer's email server.
g. Hornetsecurity provides support for authorized users insofar as it relates to Hornetsecurity systems. Support for customer systems is not a part of the contract.

15. Content Preview: Authorized users of the client can view attachments of emails, that have been blocked by Content Control policies, in a static preview within a secure environment. This simplifies the process for administrators to approve appropriate email attachments by allowing users to independently request non malicious attachments via the Outlook Web App. The Content Preview is applied to file formats that are suitable for sandbox analysis, assuming that a rule for removing the attachment has been set for them in the Content Control Security Settings.
16. For forensic analyses, ATP sandbox, URL malware control and malware ex-post alerts, 99.9% availability is guaranteed, except during announced maintenance periods.

17. Fair Use Limits
    a. The bandwidth, storage, infrastructure and resources that are required to use the Solution and which we make available in this respect are shared across all our clients. As a result, we have the right to take measures to ensure that all clients use the Solution reasonably and fairly so that such use does not interfere with or prevent normal service performance for other clients.
    b. We have decided not to set any pre-established benchmarks that determine excessive or unreasonable use, since at our discretion, we may choose to preserve our normal service levels by reallocating resources reserved to other users that are at that particular moment not being utilized, or to otherwise scale resources. You understand that if we decide not to actively enforce our Fair Use policy, we shall not be considered as having waived our right to do so, nor have we consented to you continuing to use our services at the same level as you have been at any moment in time.
    c. To benefit from our Services, you are required to acquire Billable Units. The number of Billable Units that you require depend on a number of criteria, such as the size of your organization, the amount of users and the storage size of the particular Sources. You may have established the number of Billable Units that you require by following our guidance documents, which we have uploaded on our Fees and Billing Page, or through the assistance of our sales team.

d. Irrespective of the amount of Billable Units you have acquired, you must use our Services reasonably and specifically in a way that does not require us to allocate resources disproportionately. In determining this, we will benchmark your use of our resources and storage use against that of the average client. We determine the average client by disregarding the highest 5% and lowest 5% of clients of the particular resource and then averaging the remaining amount used by all our active clients.

e. Any specific characteristics related to the industry that you operate in shall be disregarded in establishing whether the use thereof is considered to be reasonable.

f. If we, acting reasonably and in good faith, consider your use of our Solution is not reasonable or is in violation of this policy, we will, at our sole discretion take any of the following measures:

   i. Allow you to continue to use our Solutions but subject to payment of additional fees and complying with any terms that we may consider reasonable in the circumstances.

   ii. Notify you that your account will be terminated within a reasonable timeframe set at our discretion. During such time, Backups will be suspended.

g. If we exercise our right to terminate your account as previously stated:

   i. Your Backup Data will be deleted at the end of the timeframe set out in the notification we will send you, notwithstanding anything to the contrary set out in the Terms and Conditions.

   ii. You will be provided with a refund of any fees paid in advance for the remaining days of your subscription period.