Performance Specification
365 Extended Email Protection

365 Extended Email Protection provides an additional layer of security to protect Microsoft 365 customers' email traffic through its Integrated Cloud Email Security approach. Hornetsecurity's AI-powered anti-spam and malware filters analyze incoming email traffic in real time for advanced cyber threats and reliably remove spam and malicious emails from users' inboxes within seconds. The service's fully automated and seamless integration with the Microsoft 365 platform enables continuous monitoring of all mailboxes and relies on Hornetsecurity's 24/7 threat intelligence to ensure the most up-to-date protection.

The prerequisite for using the service is the use of Microsoft Cloud licenses with Exchange functionality enabled by Microsoft.

The following services are included in the 365 Extended Email Protection product:

1. Easy Onboarding
    a. The setup of 365 Extended Email Protection is automated. All domains, mailboxes and groups of the client are transferred directly from Microsoft 365 to the Hornetsecurity Control Panel.
    b. The prerequisite for using Hornetsecurity Services for Microsoft 365 involves the enablement of the Hornetsecurity App ID for the Microsoft 365 tenant by an administrative user of the customer. This is done once during the onboarding process.
    c. There is no need to change MX Records to use the service, as 365 Extended Email Protection integrates seamlessly with the 365 platform via API interface. All incoming emails from the client are copied by means of email journaling and filtered by Hornetsecurity's advanced email filters.
    d. Onboarding can be performed either directly in the Control Panel or via an external onboarding link.

2. Single Sign-on
    a. All users with administrative access can authenticate to Hornetsecurity using their administrative Microsoft 365 user credentials.
    b. If the users are already logged in to Microsoft 365, they do not need to authenticate again to Hornetsecurity.

3. Detected Threats

a. Emails detected as threats are shown to users and removed from mailboxes in an individually configurable and filterable overview. In addition, detailed information about each email is displayed.
b. The client's emails that are received through email journaling are analyzed by Hornetsecurity for malicious content (e.g., viruses) and unwanted advertisements (e.g., spam). Malicious emails and unwanted advertisements are automatically removed from the end client's mailboxes.
c. Users can recover emails from the overview and deliver them to the recipient.
d. Removed emails are stored in quarantine for three months for viewing and recovery by users.
e. Spam and threat detection rate is at least at 99.9% on a monthly average, based on the number of all emails reaching Hornetsecurity's systems for domains of the client in the measured time period.
f. The false positive rate is less than 0.00015 on a monthly average, based on the number of all clean emails reaching Hornetsecurity's systems for domains of the client in the measured time period.

4. Dashboard

The dashboard provides the user with an overview of the booked Hornetsecurity services.

5. Reporting & Compliance

a. The client receives extensive information and statistics on his current security status.
b. This includes email statistics and advanced threat statistics:
    - Total sum of scanned emails
    - Total sum of detected threats
    - Emails classified by threat over time
    - Top 100 mailboxes attacked
    - Attacks over time
    - Threats by type and attack vector
    - Attack vectors over time
c. The activities performed by users of the Control Panel are logged into an Activity Log, e.g., the recovery of an email or the successful setup of another service.

6. Fair Use Policy

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 which determines 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 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 using our services at the same level that you are doing 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, data storage size of the particular Sources, etc.

d. Irrespective of the amount of billable unit you have acquired, you must use our services sensibly, and specifically in a way which does not require us to allocate resources disproportionately. In determining this, we will benchmark your use of our resources (e.g., memory requirements, number of parallel connections) against that of the average client. We determine the average client by disregarding the 5% highest clients and the 5% lowest clients of the particular resource and averaging the amount between 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 sensible or against 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 timeframe reasonably set at our discretion. During such time, all services and/or operations will be suspended.

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

   i. Any data (metadata, backup data, or otherwise) will be deleted at the end of the timeframe set out by us in the notification sent by us in this respect, notwithstanding anything to the contrary set out in the Terms and Conditions.

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