E-Mail-Sicherheit / HornetSecurity / Benutzerlogin und Verwaltung

Kurzbeschreibung: Dieser Artikel zeigt, wie Sie sich als Benutzer bei HornetSecurity anmelden und welche Hauptfunktionen (E-Mail Live Tracking, Filter & Reports, Black- & Whitelists) Ihnen nach dem Login zur Verfügung stehen.

Für wen relevant?

- Alle Benutzer, deren Postfach über HornetSecurity abgesichert wird und die sich im HornetSecurity-Portal anmelden und dort verwalten möchten (z. B. Quarantäne, Absenderlisten).

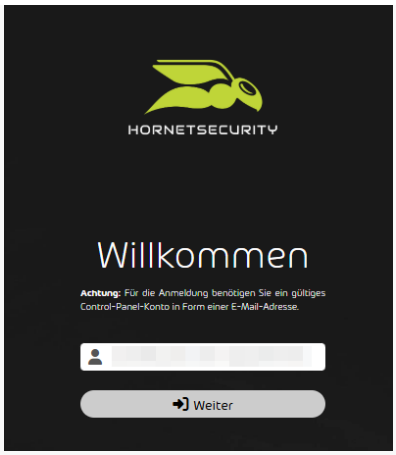
1. Anmeldung bei HornetSecurity

Um sich als Benutzer bei HornetSecurity anzumelden, besuchen Sie folgende Webseite:

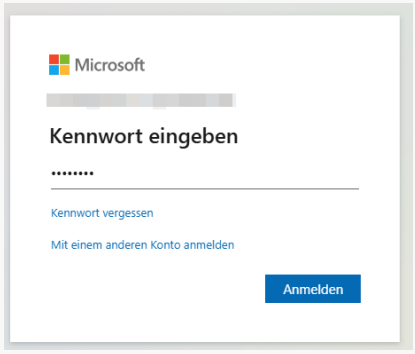
HornetSecurity Login

Schritte zur Anmeldung:

1. Geben Sie Ihre E-Mail-Adresse als Benutzernamen ein.



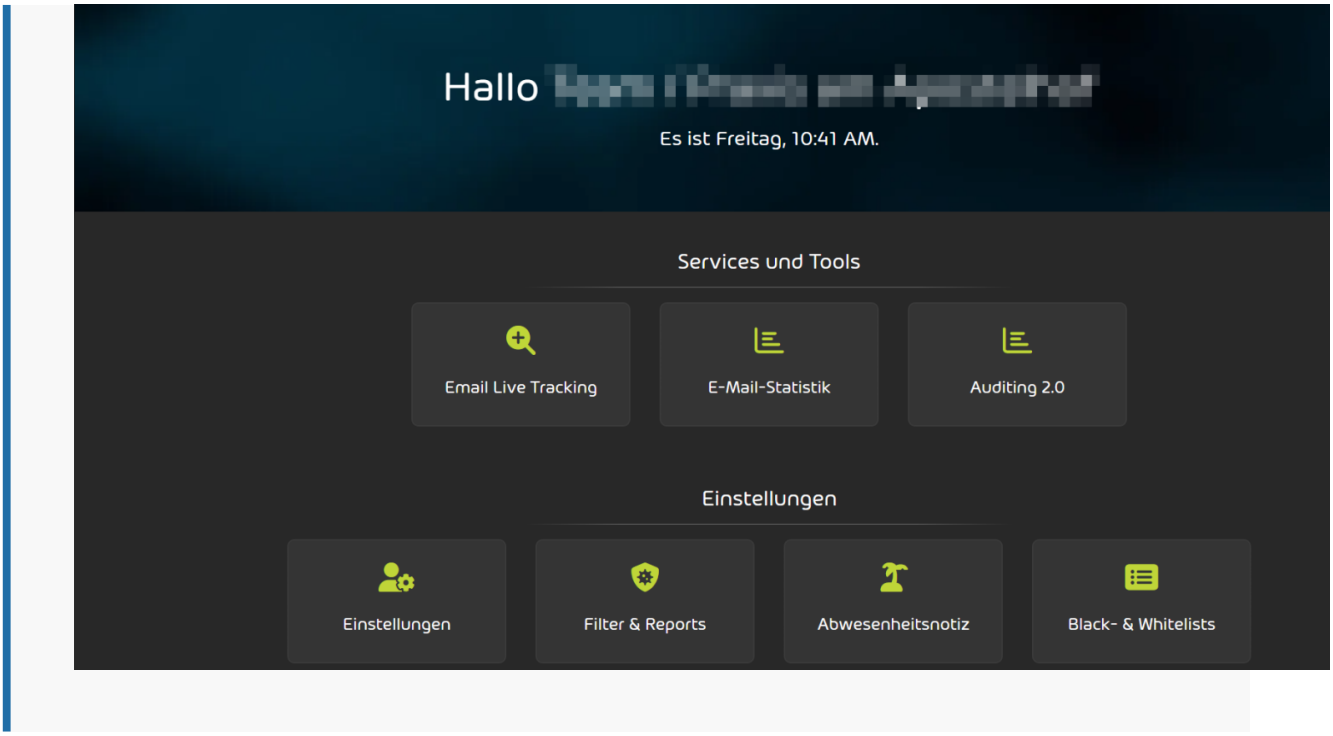
2. Sie werden zur Microsoft-Anmeldeseite weitergeleitet.



3. Geben Sie das zugehörige Passwort ein.
4. Nach erfolgreicher Authentifizierung gelangen Sie auf die Startseite von HornetSecurity.

2. Navigation in der Weboberfläche

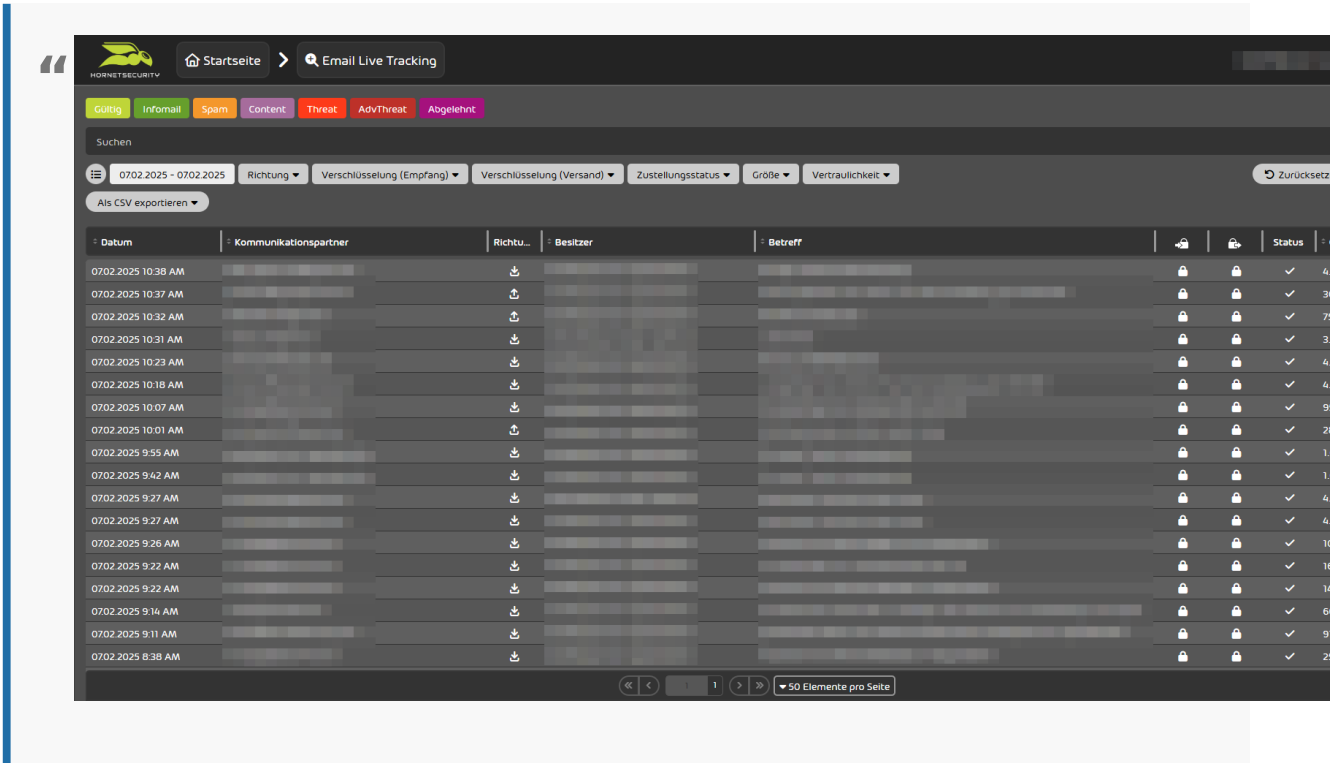
Nach dem Login stehen Ihnen folgende Hauptfunktionen zur Verfügung:



- **E-Mail Live Tracking** – Überwachung des ein- und ausgehenden E-Mail-Verkehrs.
- **Filter & Reports** – Verwaltung von Quarantäne-Berichten und Sicherheitsfiltern.
- **Black- & Whitelists** – Verwaltung der zugelassenen und blockierten Absender.

2.1 E-Mail Live Tracking

Im E-Mail Live Tracking können Sie den Verlauf eingehender und ausgehender E-Mails überprüfen.



- **Suchleiste**: Ermöglicht die gezielte Suche nach Mails anhand des Absendernamens oder eines Begriffs aus dem Betreff.

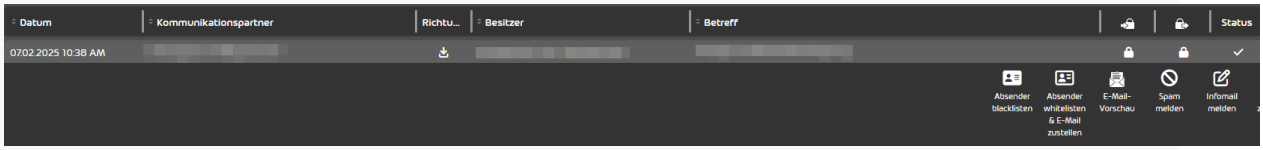
- **Symbole:**
  - Eingehende E-Mails

    > 

  - Ausgehende E-Mails

    > 

- **Aktionen:**

  > 
  >

- **Mails aus Quarantäne zustellen:** Durch Klick auf den Pfeil rechts wird die E-Mail ausgeklappt und kann bearbeitet werden.
- **Absender blockieren (Blacklist):** Blockiert den Absender, sodass dieser keine E-Mails mehr senden kann.
- **Absender freigeben & Mail zustellen (Whitelist):** E-Mails dieses Absenders werden zukünftig nicht mehr als Spam markiert.
- **E-Mail-Vorschau:** Zeigt den Inhalt der E-Mail in einem separaten Fenster an.
- **Spam melden:** Markiert die E-Mail als Spam.
- **Infomail melden:** Kennzeichnet die E-Mail als Newsletter oder Werbemail.
- **Als privat markieren:** Markiert die E-Mail als vertraulich (wichtig für die Archivierung).
- **Technische Informationen anzeigen:** Zeigt wichtige Details für Administratoren.

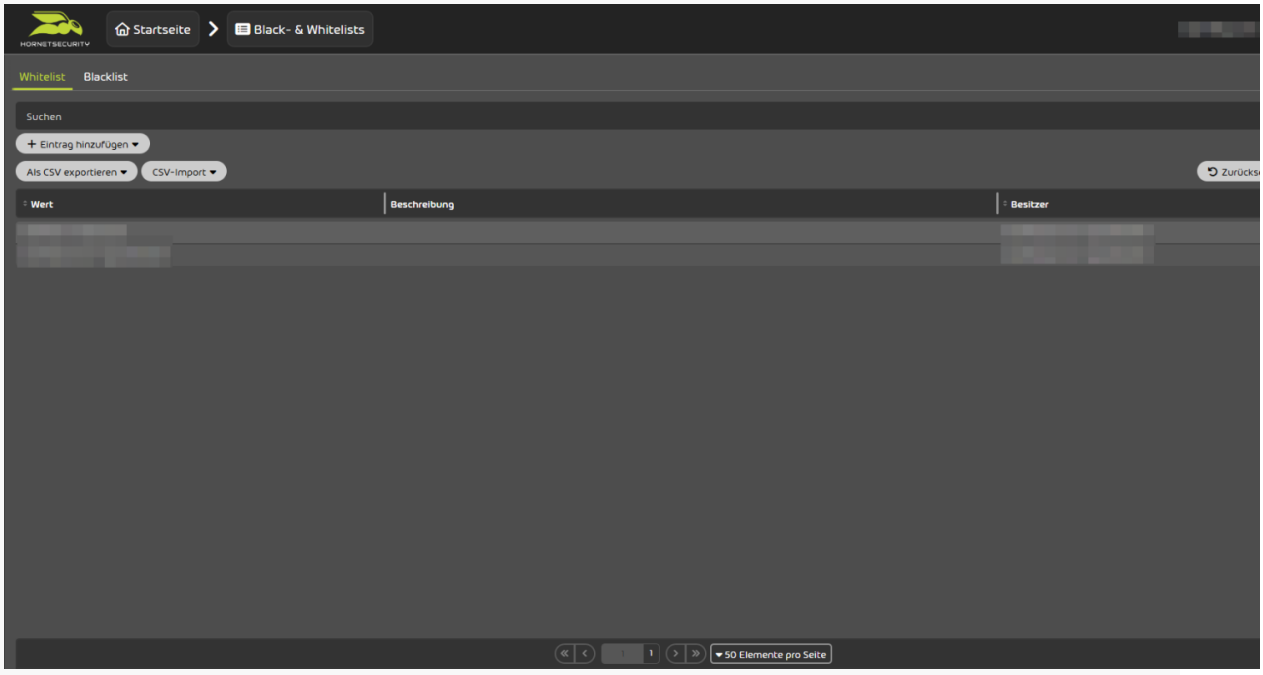
Achtung Von der Nutzung von **„Absender freigeben & Mail zustellen (Whitelist)"** raten wir ausdrücklich ab, da dies die Sicherheit der E-Mails massiv reduziert.

2.2 Filter & Reports

Hier können Benutzer individuelle Einstellungen für Quarantäne-Berichte und Filteroptionen vornehmen.

2.3 Black- & Whitelist

Diese Sektion bietet eine Übersicht über blockierte (Blacklist) und freigegebene (Whitelist) Absender. Neue Einträge können manuell hinzugefügt oder bestehende Einträge bearbeitet werden.



Achtung Auch hier gilt: Wir empfehlen die Nutzung des Whitelistings **nicht**, da es die Sicherheit von E-Mails massiv reduziert.

Kurze Checkliste

- Anmeldung über https://cp.hornetsecurity.com/ mit E-Mail-Adresse und anschließender Microsoft-Authentifizierung erfolgreich?
- Gewünschte E-Mails über das E-Mail Live Tracking gefunden und ggf. bearbeitet?
- Quarantäne-Berichte und Filteroptionen unter „Filter & Reports" bei Bedarf angepasst?
- Blacklist-Einträge zur Blockierung unerwünschter Absender genutzt (statt Whitelisting)?

FAQ – kurz & knapp

- Mit welchen Zugangsdaten melde ich mich bei HornetSecurity an?
  - Mit Ihrer E-Mail-Adresse als Benutzername; die eigentliche Authentifizierung erfolgt anschließend über Ihr Microsoft-365-Konto.
- Warum sollte ich Absender nicht auf die Whitelist setzen?
  - Weil dadurch E-Mails dieses Absenders zukünftig nicht mehr auf Spam/Schadinhalt geprüft werden – das reduziert die E-Mail-Sicherheit massiv. Blockieren (Blacklist) einzelner Absender ist hiervon nicht betroffen und unbedenklich.
- Was bedeutet „Als privat markieren" im Live Tracking?
  - Die E-Mail wird als vertraulich gekennzeichnet, was insbesondere für die revisionssichere Archivierung relevant ist.
- Wo finde ich Quarantäne-Berichte und Filtereinstellungen?
  - Unter dem Menüpunkt „Filter & Reports" im HornetSecurity-Portal.

Fußzeile Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-hornetsecurity-login-verwaltung

---

Created 2026-07-29 06:53:53 UTC by CSGJRAdmin
Updated 2026-07-29 06:59:18 UTC by CSGJRAdmin