DIGITALE DENKART

Managed Services

Anwendung Hornetsecurity

Marken

Produktnamen werden nur zur Identifikation der Produkte verwendet und können eingetragene Marken der entsprechenden Hersteller sein.

Eigentumshinweis

Anwendungseinschränkungen und Offenlegung der Vorschlags- und Angebotsdaten.

Die in diesem Vorschlag bzw. Angebot auf allen Seiten enthaltenen Informationen (Daten) sind Unternehmensgeheimnisse und/oder unternehmensinterne bzw. finanzielle Informationen, die vertraulich oder nur für einen bestimmten Personenkreis vorgesehen sind. Sie werden unter der Voraussetzung der Geheimhaltung zur Verfügung gestellt und dürfen nicht ohne Genehmigung des Bevollmächtigten zu anderen Bewertungszwecken verwendet oder offen gelegt werden. Kommt jedoch ein Auftrag auf Basis dieses Vorschlages bzw. Angebots zustande, hat der Kunde das Recht, diese Informationen (Daten) in dem im Vertrag festgelegten Umfang zu verwenden und offen zu legen. Diese Einschränkung bezieht sich nicht auf das Recht vom Kunden diese Informationen (Daten) zu verwenden oder offen zu legen, wenn sie von einer anderen Quelle ohne Einschränkung zur Verfügung gestellt werden.

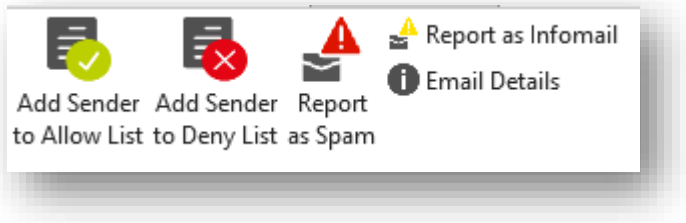
Revision

lfd. Nr.	Bemerkung	Datum	Mitarbeiter
1	Erstellung Dokument	21.07.2025	LB
2			
3			
4			
5			
6			
7			
8			
9			
10			

Inhalt

1. Funktionen im Überblick

Der Hornetsecurity-Button



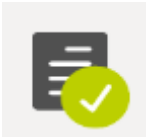
1.1 Funktionen für den Versand von E-Mails

Die folgenden Funktionen können beim Versand von E-Mails ausgeführt werden. Diese Funktionen sind nur während der Erstellung von neuen E-Mails sichtbar:

Abbildung	Funktion	Beschreibung
	E-Mails mit Erinnerung versenden	Es wird eine automatische Erinnerung eingerichtet, die dem Empfänger zugestellt wird, falls er innerhalb eines festgelegten Zeitraums nicht auf die E-Mail antwortet.

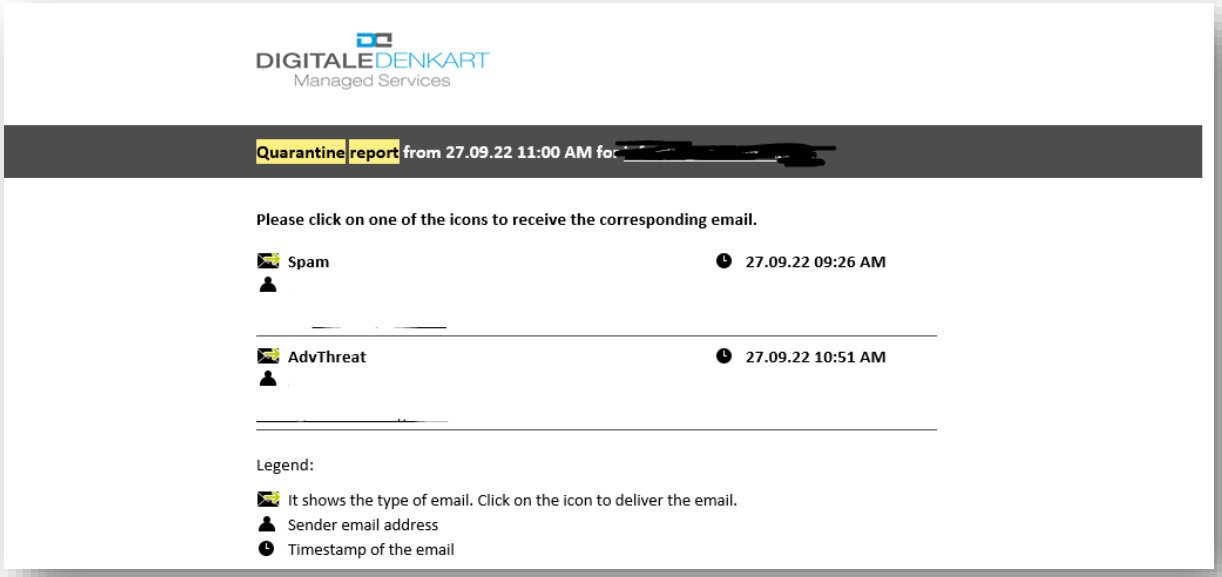
1.2 Funktionen für empfangene und versendete E-Mails

Die folgenden Funktionen können für empfangene und versendete E-Mails ausgeführt werden. Diese Funktionen sind sowohl im „Posteingang“ als auch unter „gesendete Elemente“ freigeschaltet.

Abbildung	Funktion	Beschreibung
	*Spam* melden	Die ausgewählte E-Mail wird als Spam gemeldet.
	*Infomail* melden	Die ausgewählte E-Mail wird als Infomail gemeldet (z. B. *Newsletter*).
	Absender auf *Blacklist* setzen	Der Absender der ausgewählten E-Mail wird auf Ihre persönliche Blacklist gesetzt. Dadurch erhalten Sie keine E-Mails mehr von diesem Absender.
	Absender auf *Whitelist* setzen	Der Absender der ausgewählten E-Mail wird auf Ihre persönliche Whitelist gesetzt. E-Mails von diesem Absender landen zukünftig nicht mehr in der *Quarantäne*, sondern werden Ihnen direkt zugestellt. **WICHTIG:** Für E-Mails von Absendern auf der Whitelist werden keine weiteren Filterregeln angewendet.
	E-Mail-Details anzeigen	Je nach E-Mail-Richtung (eingehend oder ausgehend) werden verschiedene Informationen angezeigt (siehe E-Mail-Details). Falls die E-Mail Anhänge enthält, die mit Advanced *Threat* Protection analysiert worden sind, wird unterhalb der E-Mail-Details zusätzlich die Anhangsvorschau angezeigt (siehe Anhangsvorschau).

1.3 Quarantäne-Bericht

Sie erhalten in regelmäßigen Abständen Ihren persönlichen Quarantäne-Report. In diesem Bericht werden alle als Spam und Infomail kategorisierten Mails aufgeführt. Ebenfalls enthält der Bericht eine Auflistung der Mails, welche nicht zugestellt wurden, sondern in der Quarantäne gespeichert wurden. Diese können dann nachträglich zum Versenden aufgefordert werden.



2 Control Panel

Link zu Ihrem persönlichen Control-Panel: https://cp.digitaledenkart.de/

Nur bei dem Security Awareness Service

In der Abbildung ist eine Übersicht der Services und Tools sowie der Einstellungsmöglichkeiten

- E-Mail Live Tracking
- E-Mail-Statistik
- Black & Whitelists

2.1 E-Mail Live Tracking

Im Controll Panel können Sie Ihr E-Mail Live Tracking einsehen und haben somit die Möglichkeit Ihren E-Mail-Verkehr zu überwachen. Auch werden die E-Mails in Kategorien zugeordnet:

Gültig	Bei diesen E-Mails wird angenommen, dass sie vom Empfänger erwünscht sind und keine Gefahr für ihn darstellen.
Infomail	Diese E-Mails sind werblich. *Infomails* umfassen auch *Newsletter*, die per E-Mail versandt werden.
Spam	Diese E-Mails sind unerwünscht und haben häufig einen werblichen oder betrügerischen Charakter. Die E-Mails werden gleichzeitig an eine große Anzahl von Empfängern verschickt.
Content	Diese E-Mails haben einen ungültigen *Anhang*.
Threat	Diese E-Mails enthalten gefährliche Inhalte wie bösartige Anhänge oder Links oder werden zur Begehung von Straftaten wie *Phishing* verschickt.
AdvThreat	Bei diesen E-Mails hat Advanced *Threat* Protection eine Bedrohung erkannt. Die E-Mails werden für illegale Zwecke eingesetzt und nutzen ausgeklügelte technische Mittel, die nur mithilfe von fortgeschrittenen dynamischen Verfahren abgewehrt werden können.
Abgelehnt	Diese E-Mails werden aufgrund externer Merkmale, die z. B. die Identität des Absenders betreffen können, im Laufe des SMTP-Dialogs direkt von unserem *E-Mail-Server abgelehnt* und nicht weiter analysiert.

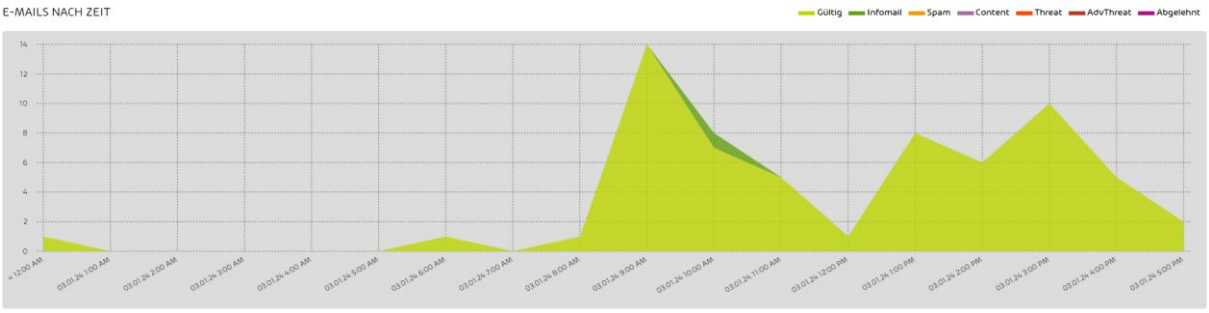
2.2 E-Mail-Statistik

Über das Modul E-Mail-Statistik können Sie eine Statistik über Ihre eigenen E-Mail-Verkehr einsehen. Sie haben die Möglichkeit auszuwählen auf welchen Datumsbereich und auf welche E-Mail-Richtung sich die Statistik im Modul beziehen soll.

Ihnen werden die folgenden beiden Kategorien angezeigt:

1. Aufteilung der E-Mails auf die E-Mail Kategorie

2. Aufteilung der Emails nach der zeitlichen Verteilung



2.3 Einstellungen

Im Modul Einstellungen haben Sie die Möglichkeit ihr Passwort, Zeitzone und Sprache und ggf. Einstellungen zu Ihrem Security Awareness Service zu treffen.

Oft sind Einstellungen schon voreingestellt. Bei Fragen hierzu wenden Sie sich bitte an

+49 (0) 800 5380000

2.4 Black- und Whitelists

Auch sehen Sie hier das Modul Black- und Whitelists. Hier haben Sie die Möglichkeit diese zu bearbeiten.

Eine **Blacklist** ist eine Liste, auf der unerwünschte E-Mail-Adressen eingetragen werden. Eine **Whitelist** ist eine Liste mit zulässigen E-Mail-Adressen, also Mails, die als vertrauenswürdig eingestuft werden.

Die Inhalte der Black- und Whitelists werden auch teilweise durch die Festlegung durch den Hornetsecurity Button festgelegt.