

HOSTED EMAIL SECURITY  
HÄUFIG GESTELLTE FRAGEN

<b>ÜBERBLICK UND VORTEILE</b> .....	<b>3</b>
1. WAS IST HOSTED EMAIL SECURITY?.....	3
2. WELCHE EINZIGARTIGEN VORTEILE BIETET HOSTED EMAIL SECURITY? .....	3
3. WARUM SOLLTE MAN STATT EINES LOKAL INSTALLIERTEN E-MAIL-SICHERHEITSPRODUKTS EINE GEHOSTETE LÖSUNG VERWENDEN? .....	3
4. WARUM SOLLTE MAN EINE GEHOSTETE LÖSUNG VON TREND MICRO ERWERBEN?.....	4
5. EIGNET SICH HOSTED EMAIL SECURITY FÜR UNTERNEHMEN? .....	4
6. BRAUCHT EIN UNTERNEHMEN, DAS BEREITS SCANMAIL ODER EIN ANDERES LOKAL INSTALLIERTES SICHERHEITSPRODUKT VERWENDET, HOSTED EMAIL SECURITY? .....	4
<b>SERVICE LEVEL AGREEMENT</b> .....	<b>5</b>
7. WAS IST DAS HOSTED EMAIL SECURITY SERVICE LEVEL AGREEMENT (SLA)? .....	5
8. GIBT ES EIN MUSTER DES SLA, AUF DAS MAN JEDERZEIT LEICHT ZUGREIFEN KANN? .....	5
9. WIE KOMMT DAS SLA ZUM KUNDEN?.....	5
10. IST DAS SLA VERBINDLICH? .....	5
11. GILT DAS SLA AUCH, WENN KUNDEN HOSTED EMAIL SECURITY ALS BESTANDTEIL VON TREND MICRO™ WORRY-FREE™ BUSINESS SECURITY VERWENDEN?.....	5
12. HABEN KUNDEN PRO MONAT ANSPRUCH AUF MEHRERE ANFRAGEN IN DEN VERSCHIEDENEN SERVICE-LEVELS? .....	5
<b>PRODUKTMERKMALE UND IHRE FUNKTION</b> .....	<b>6</b>
13. WORIN BESTEHT DER UNTERSCHIED ZWISCHEN HOSTED EMAIL SECURITY UND HOSTED EMAIL SECURITY – INBOUND FILTERING? .....	6
14. WIE STOPPT HOSTED EMAIL SECURITY SPAM UND ANDERE E-MAIL-BASIERTE BEDROHUNGEN? .....	6
15. WIE FUNKTIONIERT EMAIL REPUTATION? .....	6
16. WELCHE ARTEN DER BEDROHUNGSSUCHE FÜHRT HOSTED EMAIL SECURITY DURCH? .....	7
17. WELCHE ART VON MALWARE-SCHUTZ BIETET HOSTED EMAIL SECURITY? .....	7
18. WELCHE TECHNOLOGIEN KOMMEN BEI DER KOMBINIERTEN ANTI-SPAM-ENGINE VON TREND MICRO ZUM EINSATZ?.....	7
19. WELCHE CONTENT-FILTERFUNKTIONEN WERDEN GEBOTEN?.....	7
20. WELCHE OPTIONEN ZUR E-MAIL-VERSCHLÜSSELUNG STEHEN KUNDEN VON HOSTED EMAIL SECURITY ZUR VERFÜGUNG?.....	8
21. WIE WERDEN SIE VON TREND MICRO BEI DER DURCHSETZUNG VON RICHTLINIEN UND DER VERMEIDUNG VON DATENVERLUSTEN UNTERSTÜTZT?.....	8
22. BESTEHT DIE GEFAHR, DASS RECHTMÄßIGE E-MAILS VERSEHENTLICH GESPERRT WERDEN? .....	8
23. KÖNNEN ENDBENUTZER MIT HOSTED EMAIL SECURITY IHRE EIGENEN SPAM-QUARANTÄNE-ORDNER VERWALTEN? .....	8
<b>INFORMATIONEN ÜBER AKTIVIERUNG, UPGRADE UND KAUF</b> .....	<b>9</b>
24. WAS IST IM LIEFERUMFANG VON HOSTED EMAIL SECURITY ENTHALTEN? .....	9
25. WO ERHALTE ICH GENAUE PREISINFORMATIONEN? .....	9
27. WIE KOMPLEX IST DIE EINRICHTUNG VON HOSTED EMAIL SECURITY? .....	9
28. VOR DER ERSTEN VERWENDUNG MUSS DER KUNDE DIE MX-EINTRÄGE AN TREND MICRO UMLEITEN. WAS IST EIN MX-EINTRAG? .....	9
29. KANN MAN EIN UPGRADE VON HOSTED EMAIL SECURITY – INBOUND FILTERING AUF DAS VOLLSTÄNDIGE HOSTED EMAIL SECURITY DURCHFÜHREN? .....	10
30. WELCHE VORAUSSETZUNGEN SIND FÜR EIN UPGRADE AUF NEUE VERSIONEN VON HOSTED EMAIL SECURITY ERFORDERLICH? .....	10

<b>DATENSCHUTZ, SUPPORT UND KONTROLLE .....</b>	<b>10</b>
<b>31. IST BEI TREND MICRO DER DATENSCHUTZ VON E-MAIL-INHALTEN GEWÄHRLEISTET?.....</b>	<b>10</b>
<b>32. WELCHE WIEDERHERSTELLUNGSOPTIONEN SIND VERFÜGBAR?.....</b>	<b>10</b>
<b>33. GIBT ES BEI TREND MICRO EIN SPEZIELLES TEAM, DAS SICH UM DIE ÜBERWACHUNG UND VERWALTUNG VON LÖSUNGEN WIE HOSTED EMAIL SECURITY KÜMMERT? .....</b>	<b>10</b>
<b>34. VERLIEREN KUNDEN DIE KONTROLLE ÜBER IHRE MX-EINTRÄGE, WENN DIESE AUF TREND MICRO VERWEISEN? .....</b>	<b>10</b>
<b>35. WERDEN E-MAILS VON KUNDEN AUF DEN SERVERN VON TREND MICRO GESPEICHERT? .....</b>	<b>10</b>
<b>36. HANDELT ES SICH BEI HOSTED EMAIL SECURITY UM EINEN „AUSGELAGERTEN SERVICE“?.....</b>	<b>11</b>

## ÜBERBLICK UND VORTEILE

### **1. Was ist Hosted Email Security?**

Trend Micro Hosted Email Security stoppt über 99 % aller Spam-Nachrichten und andere E-Mail-Bedrohungen, bevor sie das Netzwerk erreichen. Dadurch werden die Netzwerkressourcen und das IT-Personal im Unternehmen entlastet, und die Produktivität der Mitarbeiter steigt. Hosted Email Security filtert außerdem den ausgehenden Datenverkehr und bietet optionale Verschlüsselungsfunktionen, um Richtlinien durchzusetzen und Datenlecks zu verhindern. Da Hosted Email Security eine gehostete Lösung ist, kann sie in weniger als 48 Stunden ohne jeden Einsatz von Hardware oder Software implementiert werden. Trend Micro führt alle Wartungsarbeiten inklusive Updates, Patches, Hotfixes und Anwendungstuning durch. So wird sichergestellt, dass Hosted Email Security stets optimale Leistung bringt, obwohl kein oder kaum Wartungsbedarf durch den Kunden erforderlich ist.

[Zurück zum Anfang](#)

### **2. Welche einzigartigen Vorteile bietet Hosted Email Security?**

Hosted Email Security erzielte in unabhängigen Vergleichstests die höchste Spam-Abwehrquote.<sup>1</sup> Die verschiedenen Schutzschichten zur Abwehr von Spam enthalten eine erweiterte Email-Reputation-Filtertechnologie, die Teil des Trend Micro™ Smart Protection Network™ ist. Das Smart Protection Network verknüpft Bedrohungsdaten aus E-Mail-, Web- und File-Reputation-Datenbanken miteinander und stoppt damit Bedrohungen, bevor sie das Netzwerk erreichen. Wird beispielsweise eine bösartige Website von unserer Web-Reputation-Technologie erkannt und ein Link zu dieser Website in einer E-Mail gefunden, so wird diese E-Mail gesperrt.

Hosted Email Security bietet Antiviren-Technologie, die in unabhängigen Tests in der Kategorie Malware-Abwehr den ersten Platz belegte.<sup>2</sup> Trend Micro ist sowohl Entwickler als auch alleiniger Eigentümer dieser Technologie, wodurch unsere Kunden permanenten Echtzeitschutz vor sich schnell entwickelnden Spam-Varianten und den komplexen neuen Internet-Bedrohungen von heute erhalten.

Außerdem sparen die Mitarbeiter Ihrer IT-Abteilung mit Hilfe der benutzerfreundlichen Verwaltungstools von Hosted Email Security auf einzigartige Weise Zeit. Zu diesen Tools gehören z. B. die erneute Überprüfung der E-Mail-Nachrichten in Quarantäne, die automatische Benachrichtigung von Endbenutzern bei Verstößen gegen die E-Mail-Inhaltsrichtlinien, kombinierte „und/oder“-Regeln zur Optimierung der Spam-Abwehrquote und zur Senkung der Fehlalarmquote sowie Content-Filter für E-Mails, die selbst komprimierte, eingebettete und kennwortgeschützte Dateien durchsuchen können.

<sup>1</sup> West Anti-Spam Comparative Test von Coast Labs, Januar 2009

<sup>2</sup> Testergebnisse des Endpoint Security Socially-Engineered Malware Protection Comparative Tests von NSS Labs, September 2009

[Zurück zum Anfang](#)

### **3. Warum sollte man statt eines lokal installierten E-Mail-Sicherheitsprodukts eine gehostete Lösung verwenden?**

Unternehmen, die eine gehostete E-Mail-Sicherheitslösung, und kein lokal installiertes Produkt verwenden, haben folgende Vorteile:

- Stoppt Spam und andere E-Mail-Bedrohungen, bevor sie das Netzwerk erreichen
- Ermöglicht dem Kunden, IT-Arbeitszeit, Mitarbeiterproduktivität, Mail-Server-Speicher, Prozessorkapazität, Bandbreite und andere wertvolle Ressourcen zurückzugewinnen
- Erfordert keine Hardware oder Software, und es gibt nur wenig oder keinen Wartungsaufwand
- Lässt sich in weniger als 48 Stunden implementieren
- Trend Micro kümmert sich um alle Wartungsarbeiten, einschließlich Updates und Anwendungstuning, so dass für den Kunden kein oder nur minimaler Wartungsaufwand anfällt.

- Unternehmen mit hohem Verteilungsgrad wird ein konsistentes Sicherheitsprofil ermöglicht. Da der neueste Schutz jederzeit für alle Benutzer an allen Standorten verfügbar ist, müssen Software-Upgrades nicht an verschiedenen Standorten durchgeführt werden.
- Niedrigere Gesamtbetriebskosten als bei herkömmlichen Hardware- und Software-Produkten
- Flexibilität bei der Kapazitätsplanung: Unbegrenzte E-Mail- und Spam-Filterfunktionen zum Festpreis pro Benutzerlizenz, ohne dass bei Änderungen der Benutzerzahl zusätzliche Hardware-Kosten entstehen, wie es bei lokal installierten E-Mail-Sicherheitsprodukten normalerweise der Fall ist.

[Zurück zum Anfang](#)

#### **4. Warum sollte man eine gehostete Lösung von Trend Micro erwerben?**

Trend Micro schützt mit seiner Hosted Email Security zurzeit täglich mehr als 30.000 Kunden in über 120 Ländern der Welt. Außerdem ist Trend Micro ein weltweit führender Anbieter im Bereich Content-Security und Bedrohungsbewältigung. Im Gegensatz zu vielen anderen Anbietern von gehosteten Lösungen ist Trend Micro ein etabliertes, zuverlässiges Unternehmen. Trend Micro verfügt über mehr als 20 Jahre Erfahrung im Bereich Sicherheit und überwacht derzeit mehr als 20 Milliarden Websites, E-Mails und Dateien täglich sowohl in gehosteten als auch in lokalen Umgebungen. Außerdem sammelt das Smart Protection Network im Internet aus allen Trend Micro Produkten und Services Daten über Bedrohungen und verknüpft sie miteinander, um noch schneller und intelligenter reagieren zu können.

[Zurück zum Anfang](#)

#### **5. Eignet sich Hosted Email Security für Unternehmen?**

Ja. Hosted Email Security passt sich durch seine hohe Skalierbarkeit an die Bedürfnisse von Unternehmen jeder Größe an, von kleinen Firmen mit fünf Mitarbeitern bis hin zu Großkonzernen und ISPs. Bei der Mail-Nachverfolgung werden die Inhalte von Protokollen miteinander verknüpft, damit Administratoren schnell den Status einer bestimmten E-Mail ermitteln und feststellen können, welche Auswirkungen Richtlinien auf die E-Mail und den aktuellen Speicherort hatten. Gleichzeitig vereinfachen detaillierte Berichte den Administratoren den Zugriff auf Informationen zu Prüfzwecken und ermöglichen ihnen eine schnelle Überprüfung des Service-Wertes. Darüber hinaus können Administratoren die E-Mails des Unternehmens durch Regeln zur E-Mail-Nutzung und Content-Filter gezielt kontrollieren.

Ein branchenführendes Service Level Agreement sowie Wiederherstellungs- und Datenschutzfunktionen unterstützen zusätzlich die E-Mail-Sicherheit für Unternehmen. Hosted Email Security bietet Unternehmen alle Vorteile einer gehosteten Lösung, entlastet das Netzwerk und verringert den Bedarf an IT-Ressourcen. Dennoch behalten die Administratoren – wie bei einer lokal installierten Lösung – die Kontrolle über den E-Mail-Verkehr des Unternehmens.

Außerdem ist Hosted Email Security ideal für große Unternehmen mit hohem Verteilungsgrad, für die regelmäßige Software-Upgrades an verschiedenen Standorten zu zeitaufwändig und teuer sind. Mit Hosted Email Security verfügen Unternehmen stets über eine aktuelle und optimale Sicherheit, die den sofortigen Schutz des Mailverkehrs bei geringem Aufwand gewährleistet.

[Zurück zum Anfang](#)

#### **6. Braucht ein Unternehmen, das bereits ScanMail oder ein anderes lokal installiertes Sicherheitsprodukt verwendet, Hosted Email Security?**

Ja. Der Schutz von E-Mails an mehreren verschiedenen Punkten im Netzwerk hat viele Vorteile. ScanMail lässt sich in den Mail-Server (Microsoft Exchange oder IBM® Lotus® Domino™) integrieren und schützt das Netzwerk ab dem Gateway mit Schwerpunkt auf unternehmensinternen E-Mails, schützt den Mail-Speicher, durchsucht E-Mails von Remote-Benutzern und bildet die erste Kontrollinstanz für ausgehende E-Mails. ScanMail for Microsoft Exchange bietet außerdem EUQ-Funktionen in Outlook, die in Hosted Email Security integriert werden können, damit Endbenutzer ihre Spam-Mails in einem entsprechenden Ordner in Outlook anzeigen können. Der Schutz auf Client-Ebene stellt eine weitere, speziell auf die einzelnen Desktops ausgerichtete Schutzschicht dar. Der Schutz an allen Schwachstellen vom Gateway bis zum Desktop ist notwendig, um Bedrohungen dort zu stoppen, wo sie entstehen.

[Zurück zum Anfang](#)

**SERVICE LEVEL AGREEMENT**

**7. Was ist das Hosted Email Security Service Level Agreement (SLA)?**

Im Lieferumfang von Hosted Email Security ist ein vertraglich zugesichertes Service Level Agreement enthalten, das Folgendes garantiert: 100 % Service-Verfügbarkeit, maximal eine Minute Latenz bei der E-Mail-Zustellung, mindestens 99 % Wirksamkeit der Spam-Abwehr, eine Fehlalarmquote von höchstens 0,0003 %, keine Vireninfectionen und reaktionsschnellen Support. Werden diese Vorgaben in einem bestimmten Monat nicht eingehalten, erhalten Kunden ihr Geld zurück.

<b>Bestimmungen des Service Level Agreements</b>	<b>Hosted Email Security</b>	<b>Hosted Email Security - Inbound Filtering</b>
Verfügbarkeit	100 % Verfügbarkeit	100 % Verfügbarkeit
Viren	Keine E-Mail-basierte Vireninfection	Keine E-Mail-basierte Vireninfection
Wirksamkeit der Spam-Abwehr	99 % oder höher	n. v.
Fehlalarme	Maximal 0,0003 %	n. v.
Reaktionszeit des Supports	Entsprechend des jeweiligen Schweregrads	Entsprechend des jeweiligen Schweregrads
Latenz bei der E-Mail-Zustellung	Maximal eine Minute	Maximal eine Minute

[Zurück zum Anfang](#)

**8. Gibt es ein Muster des SLA, auf das man jederzeit leicht zugreifen kann?**

Ja. Ein Muster des SLA kann nach der Anmeldung auf der Hosted Email Security Konsole im Bereich Administration eingesehen werden. Wählen Sie einfach die jeweilige Region/Sprache aus dem Listenfeld aus.

[Zurück zum Anfang](#)

**9. Wie kommt das SLA zum Kunden?**

Beim Kauf von Hosted Email Security ist das SLA im Lieferumfang enthalten.

[Zurück zum Anfang](#)

**10. Ist das SLA verbindlich?**

Ja. Ebenso wie die Endbenutzer-Lizenzvereinbarung (EULA) ist das SLA ein fester Bestandteil von Hosted Email Security. Besteht ein Widerspruch zwischen den Bestimmungen dieser beiden Dokumente, haben die Bestimmungen des SLA Vorrang. Sowohl Trend Micro als auch der Kunde sind für die Einhaltung der Bestimmungen des SLA verantwortlich. Bitte beachten Sie: SLA und EULA können von Zeit zu Zeit geändert oder aktualisiert werden.

[Zurück zum Anfang](#)

**11. Gilt das SLA auch, wenn Kunden Hosted Email Security als Bestandteil von Trend Micro™ Worry-Free™ Business Security verwenden?**

Ja, das SLA gilt für die Komponente Inbound Filtering von Hosted Email Security, die in Worry-Free Business Security enthalten ist.

[Zurück zum Anfang](#)

**12. Haben Kunden pro Monat Anspruch auf mehrere Anfragen in den verschiedenen Service-Levels?**

Ja. Kunden können in einem Kalendermonat mehrmals die Wiederherstellung des Service-Levels beantragen. Bei einigen Service-Levels ist nur eine Anfrage pro Monat zulässig, dazu gehören:

- Verfügbarkeit
- Latenz
- Fehlalarme
- Virenschutz

Bei anderen Service-Levels sind mehrere Einsendungen pro Monat möglich (dazu gehören die Service-Levels Anti-Spam und Technischer Support). Kunden haben außerdem die Möglichkeit, innerhalb eines Monats die Wiederherstellung verschiedener Service-Levels zu beantragen.

[Zurück zum Anfang](#)

## **PRODUKTMERKMALE UND IHRE FUNKTION**

### **13. Worin besteht der Unterschied zwischen Hosted Email Security und Hosted Email Security – Inbound Filtering?**

Sowohl Hosted Email Security als auch die Komponente Inbound Filtering von Hosted Email Security verfügen über eine äußerst wirksame Technologie zur Spam-Abwehr, webbasierte EUQ-Verwaltung, umfangreiche Protokoll-, Bericht- und Benachrichtigungsfunktionen und unterliegen den Bestimmungen des Service Level Agreements.

**Hosted Email Security:** Bietet eine Option zum Filtern ausgehender sowie eingehender E-Mails. Mit der erweiterten Option können Administratoren die voreingestellten E-Mail-Bedrohungsrichtlinien ändern, um die Fehlalarmquote zu verringern und die Spam-Abwehr sowie die Abwehr anderer Bedrohungen zu verbessern. Administratoren können weiterhin Regeln zur Durchsetzung von E-Mail-Nutzungsrichtlinien einrichten, einschließlich einer Begrenzung der E-Mail-Größe und der Anzahl der Empfänger, oder Content-Filterregeln für die Kopfzeile, den Betreff, den Text und Anhänge der E-Mail (PDF-Dateien und Microsoft Dokumente) erstellen, um die Einhaltung der Richtlinien durchzusetzen und Datenverluste zu verhindern. Vordefinierte Wortlisten und Datenformatwörterbücher, z. B. mit Kreditkarten- und Sozialversicherungsnummern, sind ebenfalls verfügbar. Hosted Email Security umfasst auch ein Add-on zur identitätsbasierten E-Mail-Verschlüsselung.

**Hosted Email Security – Inbound Filtering:** Die Komponente Inbound Filtering ist eine funktionsreduzierte Version von Hosted Email Security. Sie überprüft eingehende E-Mails zur Abwehr von Spam und anderen E-Mail-basierten Bedrohungen über Standard-Schutzrichtlinien. Administratoren können Aktionen für Spam-Mails festlegen, wie z. B. „Löschen“, „Quarantäne“ oder „Kennzeichnen und Zustellen“, sie haben jedoch keine Berechtigung, die Standardrichtlinien zu ändern.

Die Verwaltung beider Services erfolgt über eine webbasierte Konsole, wobei alle Updates, Hotfixes, Patches und das gesamte Anwendungstuning von Trend Micro durchgeführt werden.

[Zurück zum Anfang](#)

### **14. Wie stoppt Hosted Email Security Spam und andere E-Mail-basierte Bedrohungen?**

Hosted Email Security durchsucht E-Mails in drei Phasen:

- a. Email Reputation
- b. Bedrohungssuche
- c. Content-Filter (nur Hosted Email Security)

Email Reputation stoppt E-Mail-Bedrohungen gemäß der Vertrauenswürdigkeit des Absenders. Bei der Suche nach Bedrohungen durchsucht eine Bedrohungs-Engine den Inhalt der E-Mail, um Bedrohungen zu erkennen und zu sperren. Content-Filter ermöglichen Kunden die Anwendung von E-Mail-Nutzungsrichtlinien zur Durchsetzung von behördlichen, branchenüblichen und internen Auflagen.

[Zurück zum Anfang](#)

### **15. Wie funktioniert Email Reputation?**

Email Reputation verwendet zur Abwehr von E-Mail-Bedrohungen zwei Arten von Reputation Services. Der erste vergleicht die IP-Adressen der eingehenden E-Mails mit den Einträgen der umfassendsten und zuverlässigsten Reputationsdatenbank der Welt. Der zweite ist ein dynamischer Service, der die Quellen neuer E-Mail-Bedrohungen erkennt und sogar Zombies und Bot-Netze schon beim ersten Auftreten stoppt. Mit Email Reputation werden die Reputationswerte auf der Grundlage bisheriger Spam- und Bedrohungsverläufe und E-Mail-Stichproben überwacht und gegebenenfalls aktualisiert, damit der jeweilige Reputationsstatus stets prüffähig und auf dem neuesten Stand ist.

Dieser Reputation Service ist Teil des Trend Micro Smart Protection Network, auf dem die Produkte und Services von Trend Micro aufbauen. Das Smart Protection Network verknüpft Bedrohungsdaten aus E-Mail-, Web- und File-Reputation-Datenbanken miteinander.

[Zurück zum Anfang](#)

#### **16. Welche Arten der Bedrohungssuche führt Hosted Email Security durch?**

Trend Micro setzt zur Bedrohungssuche die neuesten Techniken auf Grundlage aktueller Entwicklungen ein. Mit zwei Scan Engines werden die E-Mails nach bösartigen Bedrohungen durchsucht. Die erste Scan Engine sucht nach Viren, Spyware und anderer Malware, während die Anti-Spam-Engine von Trend Micro nach Spam und Phishing sucht.

[Zurück zum Anfang](#)

#### **17. Welche Art von Malware-Schutz bietet Hosted Email Security?**

Die Produkte von Trend Micro enthalten Web-Reputation-Funktionen zum Ausfiltern bösartiger URLs in E-Mails. Außerdem ist Hosted Email Security mit einer Anti-Malware-Technologie ausgestattet, die bei unabhängigen Tests verschiedener Sicherheitsanbieter von NSS Labs als Nummer 1 bewertet wurde. Der mit Bestnoten bewertete und preisgekrönte Virenschutz von Trend Micro umfasst die Erkennung von Pattern-Dateien bekannter Viren sowie den Schutz vor Zero-Day-Angriffen. Um Schutz vor Zero-Day-Angriffen zu gewährleisten, suchen wir mit heuristischen Verfahren nach Virenanzeichen. Spezielle Pattern-Dateien sind dafür nicht erforderlich. Mit Hilfe von Prognosetechniken wehrt dieser heuristische Ansatz auch unbekannte Viren ab. Hosted Email Security bietet darüber hinaus Schutz vor Spyware und anderen Arten von Malware.

[Zurück zum Anfang](#)

#### **18. Welche Technologien kommen bei der kombinierten Anti-Spam-Engine von Trend Micro zum Einsatz?**

In der kombinierten Anti-Spam-Engine sind die folgenden Technologien integriert:

- Durch statistische Analyse werden Spam-Anzeichen erkannt und die „Spam-Wahrscheinlichkeit“ bewertet (anhand festgelegter Schwellenwerte wird entschieden, ob es sich bei der E-Mail um Spam handelt).
- Eine erweiterte Heuristik entwickelt aus dem Verhalten bei Bedrohungen intelligente Regeln.
- Eine gezielte Heuristik erkennt Spam in E-Mail-Anhängen.
- Signaturfilter schützen vor bestimmten bekannten Spam-Mails.
- Listen mit gesperrten und zulässigen Absendern
- Die Erkennung eingebetteter URLs sperrt E-Mails mit Links auf bösartige Websites.
- Bild-Spam-Erkennung
- Spam-Erkennung für viele verschiedene Sprachen
- Anti-Phishing-Technologie verwendet spezielle heuristische Regeln, Signaturen und die Erkennung eingebetteter URLs zur gezielten Abwehr von Phishing-Mails.

[Zurück zum Anfang](#)

#### **19. Welche Content-Filterfunktionen werden geboten?**

Unsere Content-Filter sind extrem flexibel, wobei sich die Filterregeln leicht über die intuitive Benutzeroberfläche erstellen lassen. Administratoren können Regeln für Kopfzeile, Betreff und Text der E-Mail sowie für bestimmte Arten von Anhängen (z. B. PDF-Dateien und Microsoft-Dokumente) erstellen. Anhand dieser Regeln können die Administratoren verschiedenste Arten von Inhalten durchsuchen und entsprechend kennzeichnen. Vordefinierte Wortlisten und Datenformatwörterbücher, z. B. mit Kreditkarten- und Sozialversicherungsnummern, erleichtern die Regelerstellung. Administratoren haben außerdem die Möglichkeit, Regeln zur Durchsetzung von E-Mail-Nutzungsrichtlinien festzulegen, einschließlich einer Begrenzung der E-Mail-Größe oder Empfängeranzahl.

Die Regeln können auf die ein- oder ausgehenden E-Mails angewendet werden, und Administratoren können durch die Auswahl bestimmter Absender oder Empfänger (bzw. die Definition von Ausnahmen) bestimmen, ob die Regeln auf das gesamte Unternehmen oder nur auf einzelne Abteilungen, Gruppen oder Benutzer angewendet werden.

Unternehmen können auch die Maßnahmen festlegen, die bei einem Verstoß gegen eine Richtlinie ergriffen werden. Hierfür stehen flexible Optionen zur Verfügung, z. B. das Einfügen eines

Haftungsausschlusses in den Text der E-Mail. Mit zusätzlich erworbenem E-Mail-Verschlüsselungsservice kann die E-Mail auch verschlüsselt werden.

[Zurück zum Anfang](#)

## **20. Welche Optionen zur E-Mail-Verschlüsselung stehen Kunden von Hosted Email Security zur Verfügung?**

Für Hosted Email Security ist die Hosted Email Encryption von Trend Micro als optionaler Service erhältlich. Trend Micro verwendet identitätsbasierte Verschlüsselung, eine benutzerfreundliche Lösung sowohl für Absender als auch für Empfänger. Die E-Mail-Verschlüsselung ist in die Content-Filterfunktionen von Hosted Email Security integriert und kann einfach durch die Aktivierung der Verschlüsselung in den Filtereinstellungen für ausgehende E-Mails eingestellt werden. Administratoren können unsere richtlinienbasierte Verschlüsselung durch die Erstellung von Regeln einfach konfigurieren: Sind die Regelkriterien erfüllt, wird die Verschlüsselung aktiviert.

Weiterhin enthält Hosted Email Security einen Schutz der Transportschicht (TLS), der die E-Mail-Pipeline (nicht die E-Mail selbst) verschlüsselt, falls Absender und Empfänger der E-Mail TLS aktiviert haben. Die Verwendung von TLS garantiert jedoch nicht, dass alle anderen E-Mail-Empfänger auch TLS verwenden. Außerdem werden E-Mails auf ihrem Weg zum Zielempfänger oft über mehrere Internet-Service-Provider (ISP) geleitet. Dies erschwert den kontinuierlichen Schutz der E-Mail auf ihrem gesamten Weg vom Sender zum Empfänger.

TLS ist eine sinnvolle Ergänzung für Hosted Email Encryption, da es die E-Mail-Pipeline vom Kundennetzwerk bis hin zum Hosted Email Security Service schützt. Dort kann dann direkt eine inhaltsbasierte Verschlüsselung der E-Mails erfolgen.

[Zurück zum Anfang](#)

## **21. Wie werden Sie von Trend Micro bei der Durchsetzung von Richtlinien und der Vermeidung von Datenverlusten unterstützt?**

Zusätzlich zur Email Encryption bietet Trend Micro eine umfassende Strategie zum Datenschutz und zum Schutz der Privatsphäre. So bewahrt beispielsweise der Virenschutz von Trend Micro ihre Daten vor Schäden, indem er das Eindringen von Viren verhindert. Einige Auflagen verlangen von Unternehmen ausdrücklich den Einsatz eines umfassenden Virenschutzes. Außerdem verhindern Anti-Spyware und Anti-Phishing Datendiebstahl, und Content-Filter sorgen dafür, dass vertrauliche Daten nur von den vorgesehenen Empfängern gelesen werden.

[Zurück zum Anfang](#)

## **22. Besteht die Gefahr, dass rechtmäßige E-Mails versehentlich gesperrt werden?**

Bei allen E-Mail-Sicherheitslösungen kann es vorkommen, dass rechtmäßige E-Mails versehentlich gesperrt werden. Ein solcher Fall wird als „Fehlalarm“ bezeichnet. Wenn Sie Hosted Email Security verwenden, wird Ihnen vertraglich eine Fehlalarmquote von maximal 0,0003 % sowie eine Spam-Abwehrquote von mindestens 99 % zugesichert.

Überschreitet in einem Monat die Fehlalarmquote die zugesicherte Obergrenze von 0,0003 % (oder liegen die Spam-Abwehrquoten dauerhaft unter 99 %), hat der Kunde unter Umständen Anspruch auf eine Rückerstattung von bis zu 100 % der monatlichen Kosten für Hosted Email Security.

Trend Micro hält die Zustellung von E-Mails für jedes Unternehmen für geschäftskritisch. Daher stellen wir Ihnen außerdem eine breite Palette von einzigartigen Verwaltungstools zur Verfügung, um E-Mails, die fälschlicherweise als Spam in den Quarantäne-Ordner verschoben wurden, schnell zu finden und zuzustellen. Zu diesen Tools zählen die automatische erneute Überprüfung der E-Mails in Quarantäne, eine zentrale Protokollverwaltung, die Nachverfolgung der E-Mails zwischen den Endpunkten sowie benutzerfreundliche webbasierte Tools, mit denen Endbenutzer ihre eigenen Quarantäne-Ordner verwalten können.

[Zurück zum Anfang](#)

## **23. Können Endbenutzer mit Hosted Email Security ihre eigenen Spam-Quarantäne-Ordner verwalten?**

Ja. Eine Komponente von Hosted Email Security ist das webbasierte Tool „End User Quarantine“ (EUQ), mit dem Endbenutzer ihre eigenen Spam-Quarantäne-Ordner verwalten können, um die IT-Abteilung zu entlasten. Kunden können sich auch für die optionale Funktion „Kennzeichnen und

Zustellen“ entscheiden. In diesem Fall werden auf dem E-Mail-Client Regeln zum Erstellen eines Quarantäne-Ordners für Endbenutzer festgelegt. Benutzer, die zusätzlich ScanMail™ for Microsoft® Exchange einsetzen, können den Quarantäne-Ordner in Outlook verwenden, damit alle Spam-Mails beim Endbenutzer in einen einzigen Ordner gelangen, unabhängig davon, von welcher Lösung die Spam-Mails erkannt wurden.

[Zurück zum Anfang](#)

## **INFORMATIONEN ÜBER AKTIVIERUNG, UPGRADE UND KAUF**

### **24. Was ist im Lieferumfang von Hosted Email Security enthalten?**

Hosted Email Security wird als Jahresabonnement zum Festpreis pro Endbenutzerlizenz verkauft. Wartungs- oder Garantiegebühren fallen nicht an. Im Abonnementpreis ist die Überprüfung von E-Mails und das Filtern von Spam in unbegrenztem Umfang enthalten. Es müssen mindestens fünf Benutzerlizenzen erworben werden. Kunden können entweder Hosted Email Security – Inbound Filtering oder die vollständige Version von Hosted Email Security erwerben. Für Kunden, die Hosted Email Security erworben haben, ist zusätzlich der Add-on-Service Hosted Email Encryption erhältlich.

Außerdem ist Hosted Email Security – Inbound Filtering beim Kauf des Trend Micro™ Worry-Free™ Business Security Advanced Pakets im Lieferumfang enthalten. Kunden, die bereits Hosted Email Security – Inbound Filtering und/oder Worry-Free Business Security Advanced besitzen, können auch ein Upgrade auf Hosted Email Security erwerben.

[Zurück zum Anfang](#)

### **25. Wo erhalte ich genaue Preisinformationen?**

Ausführliche Preisinformationen erhalten Sie von einem Channel-Partner oder Vertriebsmitarbeiter in Ihrer Region.

[Zurück zum Anfang](#)

### **26. Wie können Kunden, die Hosted Email Security erworben haben, das Produkt aktivieren und verwenden?**

Der Registrierungs- und Aktivierungsprozess von Hosted Email Security ist je nach Region verschieden. In einigen Regionen ist eine Online-Registrierung möglich. Der Kunde ruft den angegebenen Link auf und gibt einen Registrierungsschlüssel ein, der an einen Zentralserver gesendet wird. Daraufhin sendet der Server eine E-Mail mit einem oder mehreren Aktivierungs-codes (AC) und einer Aktivierungsanleitung an den Kunden.

In anderen Regionen erhält der Kunde den Aktivierungscode vom Händler. Diesen Code muss der Kunde dann an der dafür vorgesehenen Stelle in die Verwaltungskonsolle von Hosted Email Security eingeben.

Unabhängig davon, welche Methode Anwendung findet, erhält der Kunde anschließend eine E-Mail mit einer Anleitung, wie IP-Adresse(n) und Domain-Name(n) seines Mail-Servers eingetragen werden müssen. Außerdem folgt eine Anleitung zur ersten Verwendung des Services durch die Umleitung des MX-Eintrags an Trend Micro.

[Zurück zum Anfang](#)

### **27. Wie komplex ist die Einrichtung von Hosted Email Security?**

Die Bereitstellung des Hosted Email Security Kontos dauert keine 30 Minuten. In Zusammenarbeit mit dem Kunden überprüft Trend Micro den Eigentümer der E-Mail-Domain und testet, ob die E-Mails ordnungsgemäß zugestellt werden. Nachdem Kontoinformationen und IP-Adresse sowie die Domain des Mail-Servers bereitgestellt wurden, muss der Kunde nur noch den Mail Exchange (MX)-Eintrag an Trend Micro umleiten.

[Zurück zum Anfang](#)

### **28. Vor der ersten Verwendung muss der Kunde die MX-Einträge an Trend Micro umleiten. Was ist ein MX-Eintrag?**

Der Mail-Exchange- bzw. MX-Eintrag ist ein Eintrag in einer Datenbank für Domain-Namen, über den der für diese Domain zuständige Mail-Server identifiziert wird (ähnlich einer Lieferanschrift). Bei Hosted Email Security leiten die Kunden die MX-Einträge an Trend Micro um, so dass alle E-Mails

zuerst an Trend Micro zugestellt und von Hosted Email Security gefiltert werden, bevor sie an die Mail-Server der Kunden und schließlich an die Endempfänger gehen.

[Zurück zum Anfang](#)

**29. Kann man ein Upgrade von Hosted Email Security – Inbound Filtering auf das vollständige Hosted Email Security durchführen?**

Ja, Kunden können ein Upgrade von Hosted Email Security – Inbound Filtering auf das vollständige Hosted Email Security durchführen. Genaue Einzelheiten hierzu erhalten Sie vom zuständigen Vertriebsmitarbeiter.

[Zurück zum Anfang](#)

**30. Welche Voraussetzungen sind für ein Upgrade auf neue Versionen von Hosted Email Security erforderlich?**

Hosted Email Security ist nicht versionsgebunden. Da es sich um eine gehostete Lösung handelt, kann Trend Micro seinen Kunden neue Funktionen umgehend zur Verfügung stellen. Trend Micro führt alle Updates selbst durch, um den IT-Aufwand für die Kunden zu minimieren.

[Zurück zum Anfang](#)

**DATENSCHUTZ, SUPPORT UND KONTROLLE**

**31. Ist bei Trend Micro der Datenschutz von E-Mail-Inhalten gewährleistet?**

Ja. Alle gültigen E-Mails werden vollautomatisch verarbeitet. E-Mails sind nicht für Trend Micro Mitarbeiter zugänglich und werden nur gespeichert, wenn das System des Kunden ausfällt, damit sie im Notfall wieder verfügbar sind. Eine Speicherung auf Festplatte erfolgt nur auf ausdrücklichen Kundenwunsch.

[Zurück zum Anfang](#)

**32. Welche Wiederherstellungsoptionen sind verfügbar?**

Hosted Email Security ist derzeit in drei Datenzentren untergebracht – zwei befinden sich in den USA und eins in Deutschland. Diese Datenzentren bieten umfassende Funktionen zur Wiederherstellung über eine verteilte Architektur mit Lastenausgleich.

Bei einem Ausfall des Mail-Servers auf Kundenseite speichert Trend Micro die E-Mails bis zu fünf Tage lang in einer Warteschlange, wenn das E-Mail-System des Kunden nicht verfügbar ist. Ist das System des Kunden wieder verfügbar, werden die E-Mails mittels intelligenter Datenflusssteuerung zugestellt, um eine Überlastung des Systems zu vermeiden.

[Zurück zum Anfang](#)

**33. Gibt es bei Trend Micro ein spezielles Team, das sich um die Überwachung und Verwaltung von Lösungen wie Hosted Email Security kümmert?**

Ja. Zusätzlich zu TrendLabs, unserem globalen Team von Sicherheitsexperten, verfügen wir über ein Team, das sich rund um die Uhr um die Überwachung und Verwaltung von Lösungen wie Hosted Email Security kümmert. Außerdem sichern wir von Trend Micro unseren Kunden in unserem kompromisslosen Service Level Agreement (SLA) vertraglich Folgendes zu: 100 % Service-Verfügbarkeit, eine E-Mail-Zustellungslatenz von maximal einer Minute im Durchschnitt, eine Spam-Abwehr mit mindestens 99 % Wirksamkeit, eine Fehlalarmquote von maximal 0,0003 %, keine Virenfektionen und einen reaktionsschnellen Support.

[Zurück zum Anfang](#)

**34. Verlieren Kunden die Kontrolle über ihre MX-Einträge, wenn diese auf Trend Micro verweisen?**

Nein. Die Kontrolle über die MX-Einträge bleibt stets beim Kunden. Kunden haben jederzeit die Möglichkeit, die MX-Einträge wieder so zu konfigurieren, dass sie auf ihre eigenen Mail-Server verweisen.

[Zurück zum Anfang](#)

**35. Werden E-Mails von Kunden auf den Servern von Trend Micro gespeichert?**

Im Gegensatz zu einigen anderen Anbietern gehosteter E-Mail-Sicherheitslösungen verwendet Trend Micro zum Filtern von Nachrichten keinen mehrstufigen Prozess, bei dem Ihre E-Mails nach dem Eingang auf Servern gespeichert, durchsucht und anschließend weitergeleitet werden. Stattdessen filtert Hosted Email Security Ihre E-Mails in Echtzeit, wobei gültige E-Mails vollautomatisch weitergeleitet werden. E-Mails werden nur (im Notfall) zur Wiederherstellung gespeichert, wenn das

System des Kunden nicht verfügbar ist, und sind nicht für Trend Micro Mitarbeiter zugänglich. Eine Speicherung auf Festplatte erfolgt nur auf ausdrücklichen Kundenwunsch.

[Zurück zum Anfang](#)

**36. Handelt es sich bei Hosted Email Security um einen „ausgelagerten Service“?**

Nein. Wenn Sie sich für Hosted Email Security entscheiden, geben Sie die Verwaltung Ihrer Mail-Server nie aus der Hand und überlassen auch keinem externen Unternehmen Ihre E-Mail-Richtlinien oder die Verwaltung Ihrer E-Mail-Richtlinien. Ihre E-Mails bleiben immer unter Ihrer Kontrolle.

[Zurück zum Anfang](#)