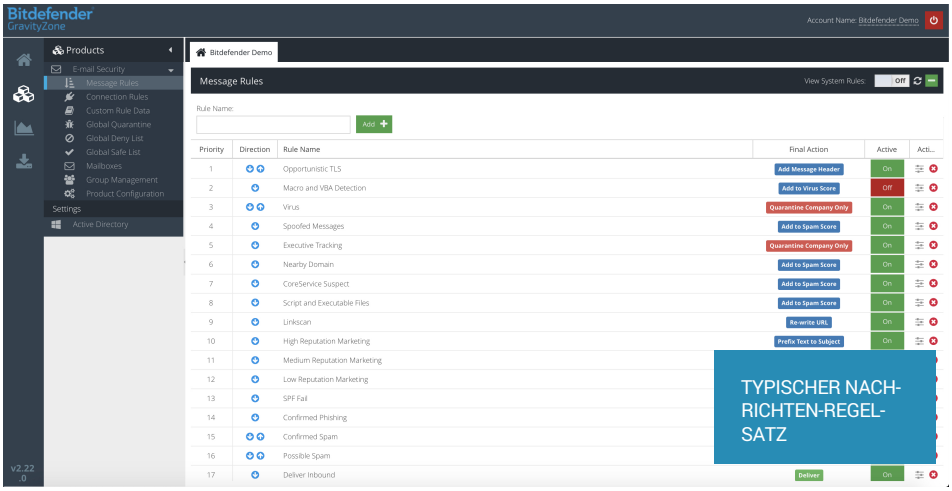
# Bitdefender GravityZone Email Security for MSPs

Führende cloudbasierte E-Mail-Sicherheit, Bestandteil der Bitdefender MSP Security Suite

Allen Benutzerschulungen und E-Mail-Filterlösungen zum Trotz bleiben E-Mails auch weiterhin der wichtigste Angriffsvektor für Cyberkriminelle und von E-Mail-Ransomware und Phishing-Angriffen geht nach wie vor eine große Gefahr aus.

Mit Bitdefender GravityZone Email Security können MSPs E-Mail-Postfächer vor Spam, Phishing und Malware sowie vor komplexen und gezielten Angriffen schützen. Die Lösung verhindert auch Angriffe mit falschen Identitäten und Betrug und nutzt gleich mehrere führende Sicherheits-Engines und Technologien zur Verhaltensanalyse, um ein- und ausgehende E-Mail-Inhalte, URLs oder Anhänge zu analysieren.




**Sorgen Sie mit gleich mehreren Scan-Engines für beispiellose Sicherheit**
Umfassender Technologie-Stack, verschiedene Engines und Verhaltensanalysetechnologien für zuverlässigen Schutz

**Lassen Sie CEO-Betrug/Business E-Mail Compromise keine Chance**
Erkennt Bedrohungen, auch wenn keine Malware vorliegt, so zum Beispiel im Falle von Credential Phishing und Hochstapler-E-Mails.

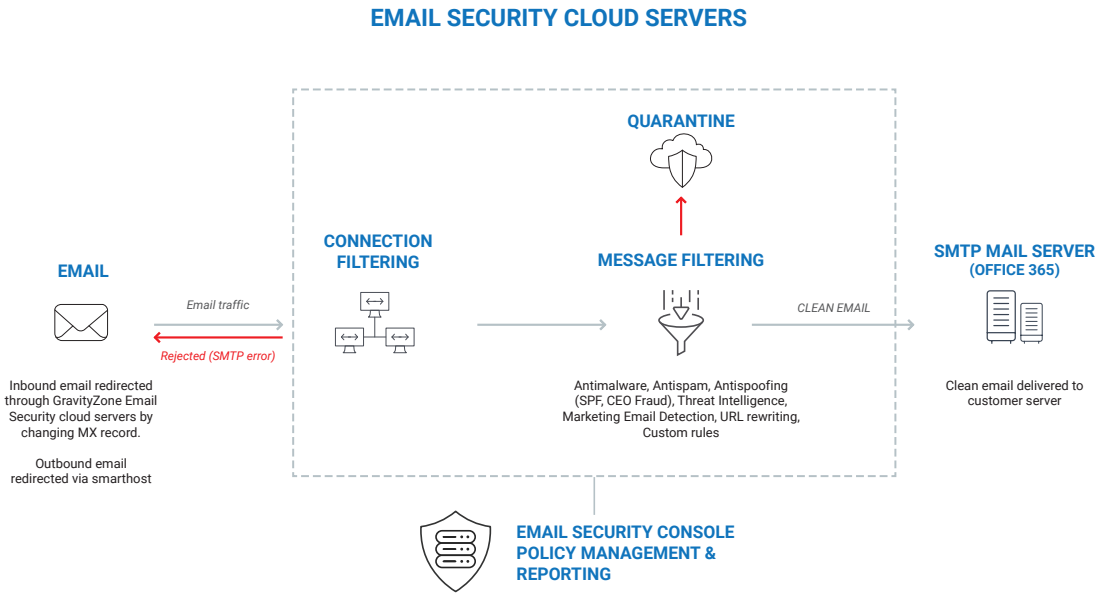
**Speziell für MSPs und ihre Sicherheitsanforderungen entwickelt**
Optimierte Aufgabenerledigung durch Mandantenfähigkeit & konsolidierte Benutzerverwaltung sowie monatliche Lizenzierung für die Endpunkt- und E-Mail-Sicherheit

## Hauptmerkmale und Vorteile:

- Herkömmliche Abgleiche von Mustern, Nachrichtenattributen und Merkmalen werden durch algorithmische Analysen ergänzt, um eine **optimale Bedrohungserkennung ohne Beeinträchtigung der Genauigkeit zu gewährleisten.**.
- **Allein die Verhaltensanalyse** umfasst mehr als 10.000 Algorithmen, die mehr als 130 Variablen in jeder E-Mail analysieren.
- **Die Kombination verschiedener signatur- und verhaltensbasierter AV-Engines** bietet Schutz vor allen Formen von Malware, einschließlich Zero-Day-Varianten:
  - 99,999 % Spam-Erkennung mit einer Fehlalarmquote, die gegen Null geht
  - 100-prozentiger Schutz vor Viren
- **Eine ausgeklügelte Richtlinien-Engine**, über die IT-Administratoren den eingehenden und ausgehenden E-Mail-Verkehr in allen Einzelheiten steuern können. Die Engine ist in der Lage, E-Mails auf verschiedenste Aspekte hin zu überprüfen, so z. B. auf Größe, Inhalt, Anhänge, Header, Absender und Empfänger, um dann geeignete Maßnahmen zu ergreifen, wie z. B. Zustellung, Quarantäne, Unternehmensquarantäne, Umleitung, Benachrichtigung oder Ablehnung.
- **GravityZone Email Security ist sowohl eine fortschrittliche E-Mail-Sicherheitslösung als auch eine vollwertige cloudbasierte E-Mail-Routing-Engine** mit funktionsreicher individueller und unternehmensweiter Quarantäne für die E-Mail-Verwaltung. Die detaillierte Kategorisierung - so zum Beispiel die Unterscheidung zwischen professionellem Marketing-E-Mails und verdächtigen Massen-E-Mails - ermöglicht flexible Richtlinien, die genauen Aufschluss darüber geben, wie verschiedene Arten von Nachrichten verarbeitet und gekennzeichnet werden.
- **Eine detaillierte Nachrichtenverfolgung** ist für E-Mail-Administratoren von unschätzbarem Wert. So können Sie genau nachvollziehen, warum eine E-Mail zugestellt oder abgelehnt wurde. Die umfasst z. B. auch den E-Mail-Header und die gesamte Kommunikation mit dem Remote-E-Mail-Server.
- **Mandantenfähige E-Mail-Sicherheit für MSPs, in GravityZone integriert**: Die mandantenfähige E-Mail-Sicherheitslösung wurde

speziell für MSPs entwickelt, um die Benutzerverwaltung, die Bereitstellung und die monatliche nutzungsabhängige Lizenzierung zu optimieren und zu automatisieren. Möglich wird dies, durch die Konsolidierung dieser Aufgaben für die Endpunkt- und E-Mail-Sicherheit in der zentralen GravityZone-Konsole.

# Aufbau der GravityZone-E-Mail-Sicherheit




## SCHUTZFUNKTIONEN

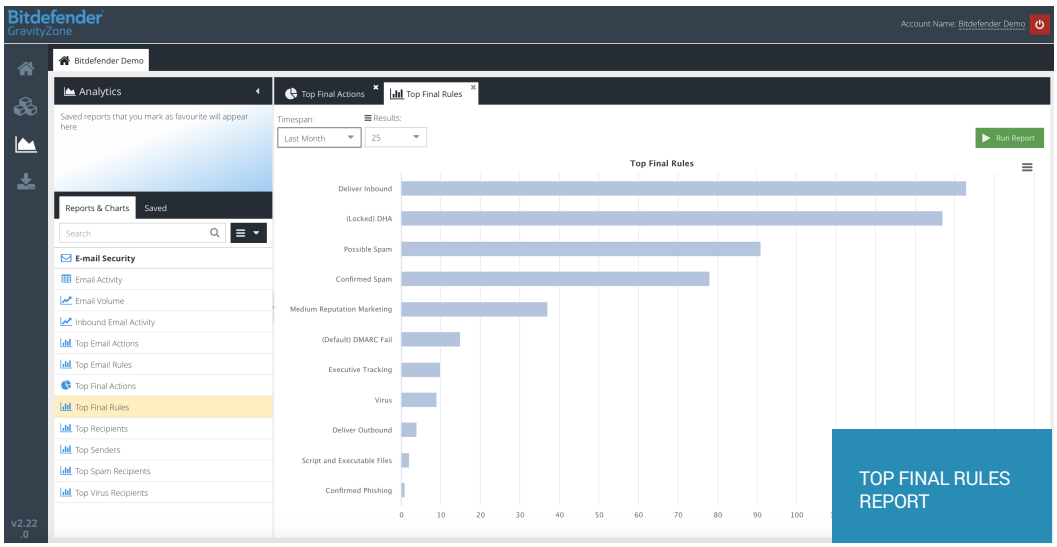
- Anti-Spam: Gleich mehrere Engines kombinieren verschiedene Technologien, um sowohl Spam als auch komplexere gezielte Phishing-Versuche und Angriffe mit falschen Identitäten zu erkennen.
- Malware-Schutz: Verschiedene herkömmliche signatur- und verhaltensbasierte AV-Engines zur Erkennung von Malware.
- "Time-of-Click"-Schutz: Schreibt URLs in E-Mails neu und nutzt verschiedenen Reputationsdienste, um Benutzer zum Zeitpunkt des Klicks zu schützen.
  - Optionen wie automatische Weiterleitung, Klick zum Fortfahren, Blockieren bei Bedrohung und Ziel-URL anzeigen/verbergen.
  - Option zum Scannen von Links zum Zeitpunkt der Nachrichtenzustellung sowie zum Zeitpunkt des Klicks.
- Safe-Deny-Listen: Erstellen Sie unternehmensweite und benutzerspezifische Safe- uns Deny-Listen.
- TLS / opportunistische TLS:
  - Erzwingen von TLS-Verschlüsselung und Einschränkung der Kommunikation mit anderen E-Mail-Servern, die das TLS-Protokoll nicht unterstützen.
  - Option zur Aktivierung von opportunistischer TLS mit der Möglichkeit zum Ausweichen auf Nur-Text, wenn TLS vom empfangenden Mailserver nicht unterstützt wird.
- E-Mail-Authentifizierung: Unterstützung von SPF, DKIM und DMARC.
- Listen zur Identifikation von Führungskräften: Details, die aus Active Directory synchronisiert werden, ermöglichen die automatische Erkennung der echten Namen von Benutzern in Header- und Umschlagadressfeldern. Dies dient dem Schutz vor CEO-Betrug und Angriffen mit falschen Identitäten.
- Ähnliche Domänennamen (Cousing Domains):
  - Absenderdomänen werden mit echten Domänennamen abgeglichen, um so genannte Cousin Domains (welche nur wenige Zeichen vom tatsächlichen Domänennamen abweichen) zu erkennen.
  - Schutz vor Angriffen mit falschen Identitäten / CEO-Betrug.
- Betreff-Tagging und Kopfzeilen:
  - Füge Tags wie [EXTERN] oder [MARKETING] zu den Betreffzeilen von Nachrichten hinzu.
  - Fügt eingehenden Nachrichten HTML- oder Nur-Text-Header hinzu, um Benutzer auf mögliche Risiken hinzuweisen.
- E-Mail-Anhänge:
  - MIME-Typ-Prüfung von Dateianhängen mit der Möglichkeit, gefährliche Dateitypen zu blockieren.
  - Erkennt passwortgeschützte Archive.
- Stichwortlisten: Erstellung beliebig vieler Stichwortlisten. Festlegung von Analyseregeln für E-Mails und von Aktionen für vertrauliche oder sensible Inhalte.
- Mail-Queuing: E-Mails werden bei Ausfällen oder Störungen des primären E-Mail-Dienstes/Servers automatisch für 7 Tage in die Warteschlange gestellt.
- Überwachung des Sendelimits: Automatischer Schutz vor Versuchen, große Mengen an ausgehenden Nachrichten zu senden, um ein Domain-Blacklisting zu verhindern.
- Verhinderung von Directory-Harvest-Angriffen: Verwerfen von E-Mails, die an ungültige oder gefälschte E-Mail-Adressen gerichtet sind.

# VERWALTUNGSFUNKTIONEN

- Richtlinien-Engine: Über 20 bedingte Auslöser zur Steuerung der E-Mail-Zustellung und zur Filterung von Nachrichten basierend auf Größe, Stichwörtern, Spam-Score, Zeit, Quelle, Ziel, Größe des Anhangs, Header, AD-Attributen und mehr.
- Benutzersynchronisierung: Der Active Directory-Synchronisierungsdienst stellt sicher, dass Änderungen repliziert werden. Bei Bedarf Anwendung von Regeln anhand der AD-Gruppenzugehörigkeit.
- Vereinfachte Verwaltung dank Integration mit GravityZone: Konsolidieren Sie Endpunkt- und E-Mail-Sicherheitsaufgaben wie Bereitstellung, Benutzerverwaltung und Lizenzierung über eine zentrale Konsole.
- Web-Oberfläche: Vollständig über die GravityZone Email Security-Konsole bereitgestellt und verwaltet.
- Quarantäne: Option zum Verschieben von E-Mails in eine unternehmensweite oder benutzerspezifische Quarantäne.
- Quarantäne-Digest: Versand von Digest-E-Mails mit allen Nachrichten in der Quarantäne des Benutzers mit der Möglichkeit zur Vorschau, Freigabe oder Blockierung von Nachrichten. Über die Digest-E-Mails können Benutzer zudem Ihre eigenen Safe- und Deny-Listen verwalten. Benutzer können die Häufigkeit und die Tage für den Versand von Digest-E-Mails festlegen.
- Disclaimer: Fügen Sie allen ausgehenden E-Mails einen HTML- und/oder Nur-Text-Disclaimer hinzu. Festlegung von verschiedenen Disclaimern für verschiedene Domains.

# BERICHTSFUNKTIONEN

- Echtzeit-Einblicke: Diagramme für detaillierte Einblicke in den eingehenden und ausgehenden E-Mail-Verkehr, die ausgelösten Regeln und die ergriffenen Maßnahmen. Dabei besteht die Möglichkeit zum Drilldown von übergeordneten Diagrammen bis hin zu detaillierten Berichten.
- Report Builder: Administratoren können ihre eigenen Berichte anhand von Feldnamen und Kriterien konfigurieren. Berichte können gespeichert und exportiert werden. Auditberichte können anhand von Kriterien wie Zeit, Benutzer, Absenderadresse, Betreff, Absender-IP, Empfänger, Richtung, endgültige Aktion, Regelname durchsucht werden. Berichte, die als "Favoriten" markiert sind, werden einem Schnellzugriff hinzugefügt.
- Zeitpläne und Benachrichtigungen: Zeitplangesteuerte Berichte und Zustellung von Berichten nur, wenn Inhalte verfügbar sind (Benachrichtigungsmodus). Benachrichtigungen basierend auf Regeln, Aktionen, Inhalten etc.
- Top-Trendberichte: Eine Auswahl an vordefinierten Trendberichten mit Diagramm- und Tabellendaten. Trendberichte können als PDF exportiert und per E-Mail an verschickt werden.
- Verschiedene Ansichten: Analysen und Berichte anhand von Zeit, Benutzer, Absenderadresse, Betreff, Absender-IP, Empfänger, Richtung, endgültige Aktion, Regelname.
- Detailliertes Audit (Nachrichtenverfolgung): Detailansichten von Nachrichtenanalysen mit dem genauen Grund, warum eine E-Mail zugestellt oder abgelehnt wurde. Die umfasst auch den E-Mail-Header und die gesamte Kommunikation mit dem Remote-E-Mail-Server.
- Protokollaufbewahrung & automatische Archivierung: Die Protokolldaten von GravityZone Email Security werden nach 90 Tagen automatisch archiviert und stehen für weitere 12 Monate zum Download aus der Konsole zur Verfügung.
- Schnelle und einfache Bereitstellung: Einfache Umleitung der MX-Einträge einer Domäne an die GravityZone Email Security Cloud.
- Unterstützung aller E-Mail-Anbieter: Funktioniert unabhängig vom E-Mail-Dienstleister. Zustellung von E-Mails an verschiedene Anbieter auf der Grundlage der AD-Gruppenzugehörigkeit des Benutzers - Unterstützung hybrider Umgebungen unter Verwendung von Exchange On-Premises mit Office 365 Exchange Online oder Gmail.



# Bitdefender MSP Security Suite

Text: Email Security ist Bestandteil der umfassendsten, mehrstufigen MSP Security Suite Leisten Sie mehr als Viren- und Malware-Schutz, steigern Sie Ihre Umsätze und optimieren Sie Verwaltungsaufgaben mit einer zentralen Lösung, die alle relevanten Sicherheitsebenen für Risikoanalyse, Härtung, Prävention, Erkennung und Reaktion abdeckt.


**Testen Sie Email Security** und die Bitdefender MSP Security Suite unter: **www.bitdefender.de/msp**

Bitdefender ist ein globales Sicherheits-Technologie-Unternehmen und bietet wegweisende End-to-End Cyber-Security-Lösungen sowie Advanced Threat Protection für über 500 Millionen Nutzer in über 150 Ländern. Seit 2001 ist Bitdefender ein innovativer Wegbereiter der Branche, indem es preisgekrönte Sicherheitslösungen für Privat- und Geschäftsanwender integriert und entwickelt. Zudem liefert das Unternehmen Lösungen sowohl für die Sicherheit hybrider Infrastrukturen als auch für den Endpunktschutz. Als führendes Security-Unternehmen pflegt Bitdefender eine Reihe von Allianzen sowie Partnerschaften und betreibt eine umfassende Forschung & Entwicklung. Weitere Informationen sind unter www.bitdefender.de verfügbar.



BD-NGZ-Apr 13 2020-TH
Bitdefender-MSP-EmailSecurity-Datasheet-CREA7 4023-A4-de-DE