Bitdefender GravityZone Email Security

Mehrstufige cloudbasierte E-Mail-Sicherheit für Ihr Unternehmen, Erweitert alle Office 365-Installationen um eine effektive Bedrohungsabwehr.

Bitdefender GravityZone Email Security ist eine umfassende Lösung zum Schutz Ihrer E-Mails, die alle Anforderungen an die E-Mail-Sicherheit abdeckt. So erhält Ihr Unternehmen umfassende E-Mail-Sicherheit, die mehr bietet als nur den Schutz vor Malware und anderen traditionellen Bedrohungen wie Spam, groß angelegten Phishing-Angriffen und schädlichen URLs. Auch gezielte und komplexe E-Mail-Angriffe wie Business E-Mail Compromise (BEC) und CEO-Betrug werden zuverlässig abgewehrt.

Beispielloser Bedrohungsschutz

Umfassender Technologie-Stack für zuverlässigen Schutz vor bekannten, unbekannten und aufkommenden E-Mail-Bedrohungen

Schutz vor CEO-Fraud-Angriffen

Erkennt Bedrohungen, auch wenn keine Malware vorliegt, so zum Beispiel im Falle von Credential Phishing und Hochstapler-E-Mails

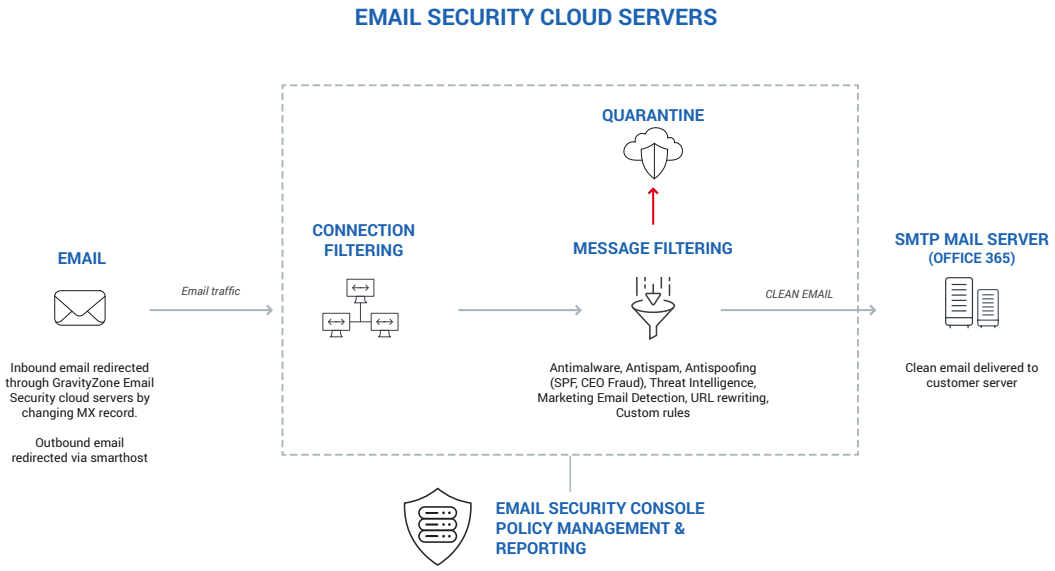
Gleich mehrere Scan-Engines

Kombiniert herkömmliche signaturbasierte und verhaltensbasierte AV-Engines zum automatischen Schutz vor neuen Verfahren zum Verbergen von Malware

Und so funktioniert es

- Herkömmliche Abgleiche von Mustern, Nachrichtenattributen und Merkmalen werden durch algorithmische Analysen ergänzt, um eine **optimale Bedrohungserkennung ohne Beeinträchtigung der Genauigkeit zu gewährleisten.**.
- **Die Kombination verschiedener signatur- und verhaltensbasierter AV-Engines** bietet Schutz vor allen Formen von Malware, einschließlich Zero-Day-Varianten:
- **Die Verhaltensanalyse** umfasst mehr als 10.000 Algorithmen, die mehr als 130 Variablen in jeder E-Mail analysieren.
- **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, unternehmensweite Quarantäne, 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 umfassende 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.

GravityZone Email Security: Architektur



GravityZone Email Security: Funktionen

SCHUTZFUNKTIONEN

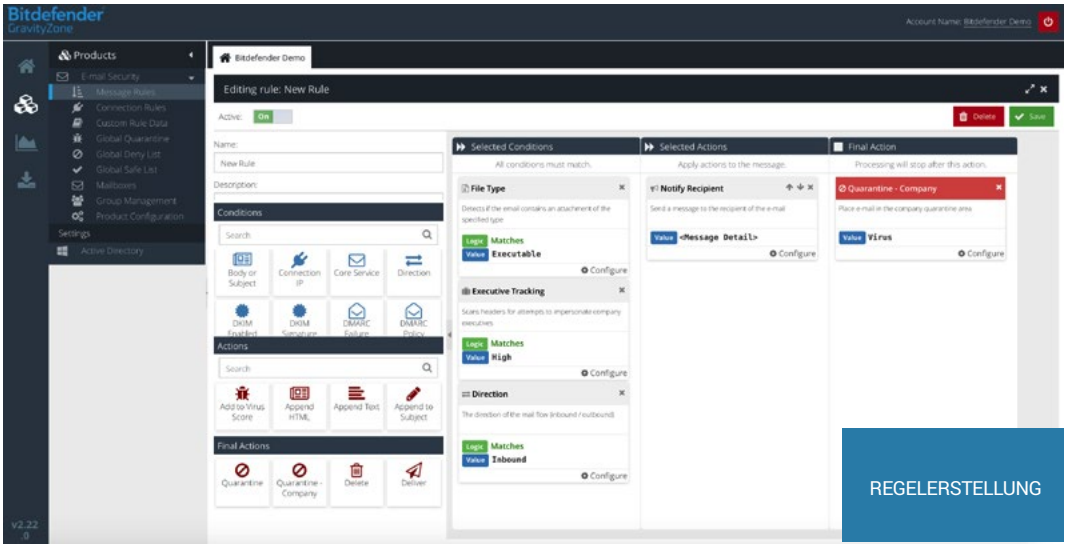
- Spam-Schutz: Gleich mehrere Engines kombinieren verschiedene Technologien, um sowohl Spam als auch komplexere gezielte Phishing-Versuche und Angriffe mit falschen Identitäten zu erkennen.
- Malware-Schutz: Verschiedene herkömmliche signatur- und verhaltensbasierte AV-Engines zur Erkennung von Malware.
- "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: Erstellung von unternehmensweiten und benutzerspezifischen Safe- & 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: Unterstützt 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:
  - Fügt 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 von Listen mit beliebig vielen Stichwörtern. 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.

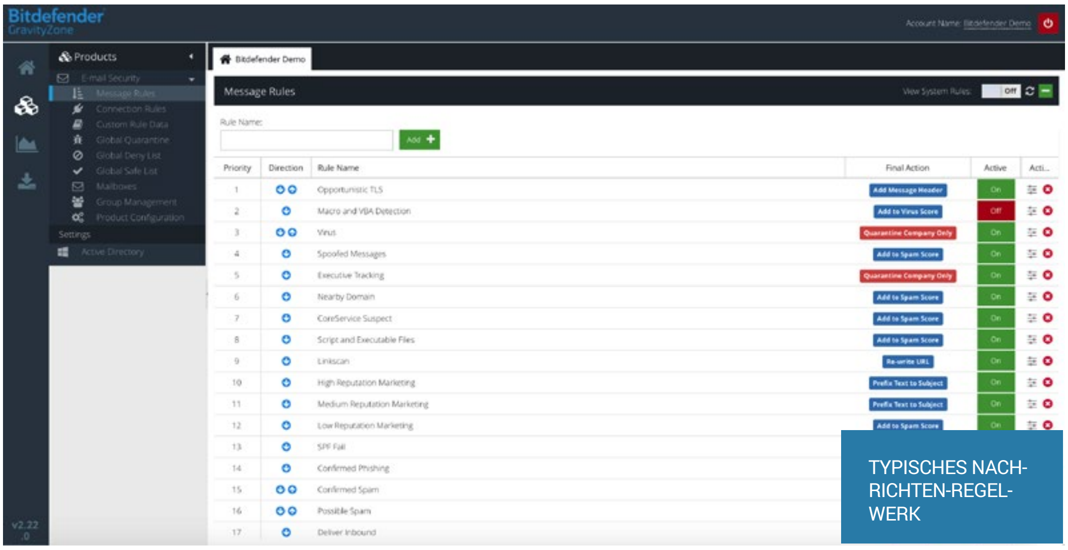
VERWALTUNGSFUNKTIONEN

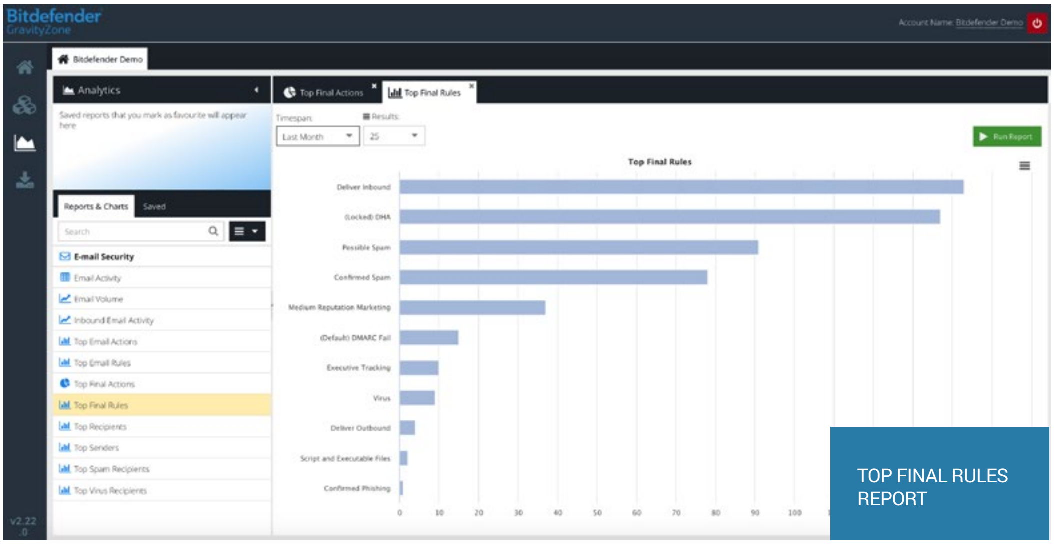
- Richtlinien-Engine: Über 20 bedingte Auslöser zur Steuerung der E-Mail-Zustellung und zur Filterung von Nachrichten basierend auf Größe, Stichwörtern, Spam-Score, Zeit, Quelle, Ziel, Größe des Anhangs, Header, AD-Attributen und mehr.
- Benutzersynchronisierung: Der Active Directory-Synchronisierungsdienst stellt sicher, dass Änderungen repliziert werden. Bei Bedarf Anwendung von Regeln anhand der AD-Gruppenzugehörigkeit.
- Web-Oberfläche: Vollständig über die GravityZone Email Security-Konsole bereitgestellt und verwaltet.
- Delegierte Administration: Ermöglicht die Erstellung mehrerer Administratoren mit unterschiedlichen Zugriffsebenen.
- 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- & Deny-Listen verwalten. Benutzer können die Häufigkeit und die Tage für den Versand von Digest-E-Mails festlegen.
- Disclaimer: Allen ausgehenden E-Mails können HTML- und/oder Nur-Text-Disclaimer hinzugefügt werden. 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 anhand von 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.







BEREITSTELLUNG

- 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.
- Ändern Sie MX-Einträge, um eingehende E-Mails über die Cloud Email Security-Server umzuleiten.
- Konfigurieren Sie Smarthosts, um ausgehende E-Mails über die Cloud Email Security-Server umzuleiten.

Weitere Informationen finden Sie unter: https://www.bitdefender.com/business/gravityzone-addons/email-security.html

Oder wenden Sie sich direkt an Ihren Bitdefender-Partner vor Ort.

Bitdefender

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 umfassende Forschungen und Entwicklungen. Weitere Informationen sind unter www.bitdefender.de verfügbar.

BD-NGZ-Nov.14.2019-Tk#: crea3183
Bitdefender-NGZ-EmailSecurity-Datasheet-CREAT4014-A4-de_DE