B

Bitdefender Gravityzone Email Security

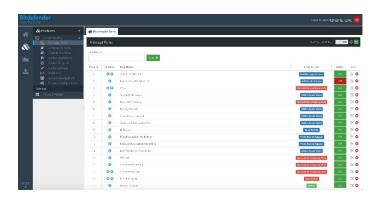## Leading cloud-based email security, part of Bitdefender GravityZone Cloud MSP Security

Bitdefender GravityZone Email Security helps MSPs protect customers' emails from spam, phishing, malware as well as sophisticated and targeted attacks. It prevents impersonation and fraud, leveraging multiple leading security engines and behavioural technologies to analyse incoming and outgoing email content, URLs, and attachments.
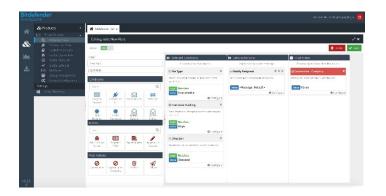
Traditional pattern, message attribute and characteristic matching are complemented by algorithmic analysis for **ultimate threat detection without impacting accuracy**.

10,000 algorithms analyzing more than 130 variables extracted from each email message.

A sophisticated policy engine allows IT administrators to customize exactly how email flows in and out of the organization. The engine can inspect all aspects of email, including size, content, attachments, headers, sender and recipients, and take appropriate actions to deliver, quarantine, company quarantine, re-route, notify or reject the message.

Compatible with all email service providers and fully supports hybrid environments using Exchange on-premises with Microsoft 365 Exchange Online or Gmail. Deliver email to different providers based on user AD Group membership.

Get email security designed for efficiency and ultimate protection

Gain Unparalleled Protection with Multiple Scanning Engines
Multiple scanning engines and behavioral technologies protect your customers against spam, viruses, phishing attacks, ransomware, malware, and other email-borne threats.

Stop CEO Fraud and Business Email Compromise
Detects threats that don't involve malware, such as credential phishing and imposter emails.

Protect Microsoft 365 Customers
Seamless integration with Microsoft 365 via an Azure connector and an OnPrem Active Directory Connector simplifies deployment and management of Microsoft 365 mailboxes and helps you keep your customers safe from email attacks aimed at Microsoft 365 users.

Simplify your MSP Security Suite
Streamline tasks with multitenancy, consolidated user management and monthly licensing for endpoint and email security.

Key Features

PROTECTION

Multiple Signature and Behavior-based Antivirus Engines	Protection from all forms of malware, including zero-day variants.
Anti-spam	Multiple engines use a combination of technologies to detect spam and more sophisticated targeted phishing and impersonation attacks.
LinkScan: On-demand URL Protection	Provides time of click protection from malicious URLs in emails with the option to scan links at time of delivery.
TLS Encryption	Option to enforce TLS encryption and restrict communication with other email servers that do not support the TLS protocol.
Secure Email	A simple email encryption solution to protect sensitive data in transit.
Sending Limit Monitoring	Protects against attempts to send large volumes of outbound messages to help prevent domain & IP blacklisting.
Support for SPF, DKIM and DMARC	Helps protect against impersonation attacks.
Executive Tracking	Details synced from Active Directory automatically detect users' real names within header and envelope address fields to protect against impersonation attacks and CEO fraud.
Nearby (cousin)	Compares sender domain to legitimate domain names to identify nearby domains (that vary from the actual domain name by one or two characters).
File Attachment Blocking	MIME checking of file attachments and the ability to detect password protected archives.
Directory Harvest Attack (DHA) Prevention	Blocks directory harvesting attacks by closing off the connection from a recipient once the fake email address threshold is reached.
Recurrent Pattern Matching	Combined with algorithmic analysis, connection-level analysis, sender/server validation and threat intelligence add a powerful additional layer of security to protect Microsoft 365 users against threats.

MANAGEMENT

Multitenant Email Security Platform	Designed to streamline and automate user management, provisioning, and monthly usage-based licensing by consolidating tasks for both endpoint and email protection within the same console.
Delegated Administration	Allows creation of multiple administrators with different levels of access.
Fully Featured Company and Personal Quarantines	For greater control over message management.
Quarantine Digest Emails	List all messages within the user's quarantine and gives users the option to view, release or block messages.
Safe & Deny lists	Create companywide or individual lists.
Detailed Message Tracking	Quickly view why an email was delivered or rejected, including the ability to view email headers and messages.
Deep Message Categorization	Enables flexible policies to detail how different types of messages are processed and tagged.
Policy Engine	Over 20 conditional triggers to control email delivery and filter messages based on size, keywords, spam score, time, source, destination, attachment size, headers, AD attributes and more.
Signature Management	Append the HTML and/or plain text disclaimers for all outbound email, including the ability to set disclaimers for different domains for brand, signature, and disclaimer consistency.
Active Directory Synchronization	Auto-sync Microsoft 365 shared mailboxes and Active Directory objects (users, groups, and OUs) across cloud, local and Exchange on-premises environments via either an Azure Connector or OnPrem Active Directory Connector.

REPORTING	
Real-time Visibility	Charts provide real-time, detailed visibility into inbound and outbound email flow, as well as rules triggered, and actions taken.
Report Builder	Reports can be defined based on available file names and criteria, exported, and saved. Audit reports can be searched based on time, user, sender address, subject, sender IP, recipient, direction, final action, rule name.
Top Trend Reports	A selection of pre-defined trend reports with chart and table data can be exported to PDF and emailed to recipient for increased visibility.
Detailed Audit (Message Tracking)	Provides a detailed analysis of individual messages and the reason an email was delivered or rejected. This includes email headers and full conversation with the remote email server to ease investigations.
Log Retention and Auto-archiving	Log data is archived automatically after 90 days and available to download from the console for a further period of 12 months.

Deployment

- Quick and easy deployment: Simply redirect domain MX records to the GravityZone Email Security Cloud.

- Configure smart hosts to re-route outbound email through GravityZone Email Security Cloud.

Help prevent email threats and boost your customers' security posture with GravityZone Email Security

Optional Add-on Services

MANAGED DETECTION AND RESPONSE

Optional Add-on Products

SECURITY
FOR VIRTUALIZED ENVIROMENTS

Included Security Modules

EMAIL
SECURITY

PATCH
MANAGEMENT

LOCAL AND CLOUD MACHINE LEARNING AV & ANTIMALWARE

Ransomware
Mitigation

Anti-
exploit

Web
Protection

Risk
Analytics

**SINGLE CONSOLE
SINGLE AGENT**

Firewall
and
Network
Attack
Defense

FULL DISK
ENCRYPTION

ADVANCED THREAT SECURITY
(HYPERDETECT + SANDBOX ANALYZER)

Content and
Device Control

Behavior
Monitoring

ENDPOINT DETECTION
AND RESPONSE