



## Atizlan Mail-Guardian appliance offers a comprehensive email security solution

**The war against spammers is not a simple one and requires spam fighters to be dynamic, sophisticated and creative.**

Mail-Guardian series is a leading email security appliance that protects organizations of up to 10000 users, from both targeted and non-targeted email-related threats. Mail-Guardian provides a buffer between the Internet and the organization's email systems, using a full pack of perimeter security layers.

### Virus Protection

Mail-Guardian inspects all email traffic and protects the organization's network from known and emerging threats, such as Viruses & new-age Virus outbreaks, Worms and Trojan-horses. This is done by using a five layer Anti-Virus system composed of Atizlan's proprietary Email-Worm detector, a triple F-SeCure Anti-Virus engine and a Zero-Hour™ Outbreak detection engine.

### Spam and Phishing Prevention

Fighting spammers has become a challenge as spammers are constantly improving their technologies to bypass Anti-Spam systems.

Mail-Guardian has an advanced eleven-layer Anti-Spam engine, enhanced by proven technology that prevents all known Spam, including **Imagebased Spam**. All incoming mail undergoes an in-depth analysis by the different Anti-Spam layers. Mail-Guardian identifies 98.5% of incoming Spam and immediately blocks or tags it as Spam in accordance with the organization's policy. By combining Anti-Spam technologies with advanced policy management, Atizlan has reduced the false positive ratio to almost zero.

### Advanced Management

Mail-Guardian's innovative policy management mechanism enables administrators to define rules for the entire organization. This enables the System Administrators to enforce the organization's policy for both incoming and outgoing mail flow. Mail-Guardian smoothly interconnects with existing directory services using the LDAP protocol.

Users can manage their own quarantine and Black & White lists. Furthermore, users receive daily reports, from which they can manage their mail flow and release quarantined mail.

### Easy installation

With no need for software installation, Mail-Guardian integrates into any network topology as an SMTP relay. In most cases, Mail-Guardian's default settings are sufficient for most organizations, thus making the installation and configuration easy and simple.

### Benefits

- ✓ Complete email protection suite
- ✓ Provides enterprise-level solution for small organizations
- ✓ One-stop-shop, no additional licensing costs
- ✓ Real-time technology implementation against new emerging threats
- ✓ Reduces bandwidth using perimeter-level protection layers
- ✓ Reputation filters keep potential threats away from your network
- ✓ Outbreak detection engine keeps your network clean from new-age email Viruses
- ✓ Proven technology against Image-based Spam
- ✓ Anti-Phishing prevention, protects users from fraudulent mail
- ✓ Auto-updated self-maintained system
- ✓ Significantly fast ROI

## Specification and Features

Number of mail users	100-10000 (as per requirement)
Domains	Unlimited
Ethernet	1xGbE & 1x10/100Mbps
Storage size	80 GB
Input Power	100/230VAC 50/60Hz
Dimensions (WxDxH)	31x35.8x8.75 cm (12.2x14.1x3.4 inch)
Warranty	1 year limited warranty
Licensing	100-10000 (as per requirement)
Certifications	FCC, CE, UL, CUL, CB, RoHS

### Anti-Spam Engines

#### Perimeter Engines

Zombie detection & IP Reputation system External and Internal RBL lookups NextGen Greylisting

#### Recurrent Pattern

#### Detection (RPD™) Deep

#### Inspection Engines

Image Analysis engine  
Bayesian statistical engine  
Heuristic engine with over 2,500 rules URL, Telephone & Email Database Domain to IP conversion (SURBL)  
Honey pots with real-time database update SPF and DomainKeys support

### Anti-Virus Engines

Atizlan Proprietary heuristic Worm detection engine F-Secure® Orion - heuristic-based  
F-Secure® Libra - signature-based  
Kaspersky® AVP - heuristic and signature based **Zero-Hour™** outbreak detection

### Anti-Phishing Engines

Internal updated databases External databases

### Advanced Policy Management

Support LDAP: Pre-defined & Open LDAP Management credentials  
Separate rules for Incoming and Outgoing mail Spam thresholds  
Spam quarantine and/or tagging  
Footnote rules Notification rules  
Attachment rules  
Black and White lists (global/personal)

### End-user interface

Personal Black and White lists  
Personal quarantine management  
HTTP and/or email-based interface

### Perimeter-level protection package

DoES (Denial of Email Service) resilience Mail-bombing protection  
Syntax verifications  
Zombie detection & IP Reputation system Harvest prevention  
IP Rate limit  
Spoofing prevention for incoming mail  
Spoofing prevention for outbound mail (Anti-Zombie)  
Validation of sender's domain  
SMTP Authentication:  
Local/LDAP/Forward  
Brute-force prevention

### Reporting

Mail traffic management  
Administrative daily report  
Detailed statistics and reports  
SNMP Active monitoring  
End-user mail traffic reports

### Mail-Server (optional)

POP3/S and IMAP/S  
Virtual domains support Disk quota management Automatic mailbox backup Secure Web-Access

### More Features

Backscatter prevention  
POP3 Retriever  
POP3 Transparent proxy