



The Guardian appliance offers a complete all-in-one security solution for small organizations

Guardian combines the best of Atizlan Guardian products with a powerful Firewall and Internet surfing filtering mechanism. Guardian allows organizations of up to 100 users to be protected in all aspects, such as electronic mail and Internet browsing, using a self-managed solution.

Email Components

Anti-Spam Engines – Guardian has an advanced eleven-layer Anti-Spam engine enhanced by Recurrent Pattern Detection (RPD™) technology. Guardian identifies 98.5% of incoming Spam.

Anti-Virus Engines – Guardian incorporates five Anti-Virus engines that provide full protection against known and unknown security threats. PineApp has also added the Zero-Hour™ outbreak detection engine to identify and block new-age Viruses and Worm outbreaks within minutes.

Policy-Management – Guardian's innovative Policy Management mechanism enables administrators to define rules for incoming and outgoing mail traffic. Guardian can smoothly interconnect with existing directory services using the LDAP protocol.

Mail Server (optional) – Guardian has an optional mail server module in which mailboxes can be created and managed using a simple friendly web interface.

Web enhancements

Firewall and VPN – Guardian features a powerful yet easy to use, stateful packet inspection Firewall. The system includes a VPN server (PPTP-based) with encryption support, which enables employees to connect to the organization from a remote location in a safe manner.

Web-Filtering (HTTP & FTP) – Guardian provides full protection against Viruses, Worms and Malicious-code while browsing or downloading files from the Internet. The same Anti-Virus engines that effectively block email-based Viruses are deployed against all Web-based threats.

Controlled Surfing – Guardian provides over 40 classified website (URL) categories to prevent employees from accessing nonproductive (gambling, entertainment etc.) or inappropriate (pornography, drugs, etc.) content.

Benefits

- ✓ Complete all-in-one security protection suite
- ✓ Provides enterprise-level security 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
- ✓ Automatic updates
- ✓ Easy to manage
- ✓ Significantly fast ROI
- ✓ Affordable

Specification and Features

Number of mail users	Upto 100
Domains	Limited to 5
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	25, 50, 75 & 100 users
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

Web filtering

Over 40 different categories
4 Anti-Virus engines
Dynamic URL databases
File type blocking
Content filtering

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

Firewall

Stateful packet inspection
Encrypted VPN Server
Easy configuration
Logs and reports

Supported Protocols

Inspected protocols: SMTP, POP3, HTTP and FTP
Dial-Up protocols: PPTP, PPPoE, L2TP and DHCP
VPN Tunneling: PPTP: MPPE64 and MPPE12