Sl #	Specifications
1	The Solution should be Hardware appliane based
2	High Availability should be provided for Email security solution. (Active/Active or Active/Passive)
3	The solution should provide unlimited domain support
4	The solution should support split mode architecture with separate Email Scanner
5	The Email Security solution should provide flexible & scalable deployment options.
6	The solution should support high email flow supporting 2000 Users for now and should be
7	The same solution should be scalable to support 10000 users of Email Security
8	The Email Security Solution should also be able to get the updates through a Proxy Server
9	The solution should provide redundancy for both scanner and control center.
10	Should combine antimalware technology with advanced heuristics to provide real-time
11	Ability to scan messages in transit or on the mailbox to protect against email borne
12	Advanced content filtering protects sensitive information using pre-defined policies,
14	Support for Microsoft Exchange Database Availability Group.
16	Flexible real-time, scheduled, and manual scanning.
17	In-memory scanning and effective multi-threading for superior performance.
18	3 years comprehensive Onsite Warranty, Support & Subscription from the Manufacturer.
19	Device should minimum have 32 GB RAM
20	Device should minimum have 1 TB built in storage

Protection

1	It should provide Phishing Detection Technology
2	Should contain Superior Spam Blocking Techniques
3	Provide Directory Harvesting Attack Protection for emails.
4	It should protect against denial of service attacks.
5	Anti-spoofing with support for SPF, DKIM and DMARC should be available.
6	Policy Rules for Users, Groups or All Users
7	Compliance Rules and Routing Support
8	Should support Email Encryption
9	Ability to scan email attachments
10	Should provide reputation based protection against bad emails/domains.
11	Zombie Detection & Time-Zero Virus Protection.
12	Should provide more than 2 engines for Anti-virus scanning.
13	Solution should provide inbound/outbound protection for emails.
14	Provision of connection management with advanced IP reputation should be available.
15	Anti-spoofing with support for SPF, DKIM and DMARC
16	Zombie detection
17	The feature of adjusting the Spam Aggressiveness should be available.
18	Device should also support Multi engine Advanced Threat Protection and should be
19	Advance threat protection should provide 100% catch rate and should be validated by
20	Different level of Spam aggressiveness should be readily available. Ex: Medium, Strong etc.
21	Ability to perform heuristics for email traffic.
22	Should support Bayesian scanning.

complaince and Encryption

1	Robust policy management,
2	Attachment scanning
3	Approval boxes/workflow
5	Dictionaries
6	Encryption of emails should be provided as an option.
7	Searches for predefined social security numbers, bank routing numbers or credit card
8	Attachment scanning—Looks for content within document attachments, including Word,
9	Set and enforce policies for common compliance setups
10	Enable organizations handling health or financial records to monitor for HIPAA, SOX or
11	Enable the viewing of email that potentially violates compliance policies before allowing it
13	Archiving: organizations should be able to route email that matches a specific policy to an
14	Securely routes email that matches a specific policy to an integrated, seamless cloud
15	Should enables organizations to monitor and report on compliance-related email traffic.
16	Email encryption service to ensure secure exchange of confidential information

Administration

1	Configuration of the solution should be easy to configure with initial setup wizard.
2	Ease of Use
3	The solution should provide secure management through Graphical User interface via
4	Detection of appliance through ICMP should by default be disabled.
5	Quick Configuration Steps should be available directly from appliance.
6	Updates for Reputation Engine, Anti-Spam and Cloud based protection should be every 5
7	Ability to search messages
8	Auditing of emails should be readily available through the GUI
9	The email security solution should have the possibility of Integrating with LDAP
10	Per User Junk Box should be available in the solution
11	Junk Button should be provided for Outlook
12	Have the ability for Per User Anti-Spam Aggressiveness should be available.
13	Have the ability to provide Per User Allowed/Blocked Lists
14	Single Sign On should be available.
15	The solution should be compatible with all email servers
16	The MTA should provide high throughput for email processing.
17	The solution should be able to scale extensively via different form factors.
18	Provide overview and visualization of Good Vs Bad Emails
19	Record ID matching to easily search for predefined information
20	Attachment scanning to stop the release of unauthorized information
21	It should provide the options of Adding disclaimers for both inbound and outbound email.
22	Should be able to block attachments by Size.
23	Provide the option to limit the size of emails through the solution.

Reporting

1	Scheduling of Reports for Emails should be available
3	Compliance reporting should be part of the solution.
4	Should provide a dashboard for monitoring emails Good Vs Bad Emails etc.

Comply(Yes/No)	Page Number in Data sheet