BUDGETARY OFFER INVITES

FOR

PROCUREMENT OF COMPREHENSIVE ANTIVIRUS SECURITY SOLUTION FOR DESKTOP COMPUTERS

LAST DATE FOR SUBMISSION OF BUDGETARY OFFER: 18.03.2014

Director (IT)

Room No 7008, 7th floor, IT Department,

NDMC, Palika Kendra, Sansad Marg, New Delhi -110001

Email: director.it@ndmcmail.gov.in

Phone: 41501383(D), 41501353-60 Extn.: 2701

1. SCOPE OF THE PROJECT

S.No.	Description
1.	An Enterprise antivirus solution for 2000 Desktops (Approx), controllable with a centralized Antivirus Server.
2.	Solution should able to Detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and RootKit.
3.	Endpoint solution technology should include a behavioral based technology apart from providing the signatures for known threats, vulnerability ad-heuristic based approach. It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.
4.	Solution firewall engine should have option to allow or block support of network protocols, including Ethernet, Token Ring, IPX/SPX, AppleTalk, and NetBEUI. Can block protocol drivers (example: VMware, WinPcap) and should have Adapter specific rules – e.g. Ethernet , Wireless, VPN
5.	Proposed IPS solution should allow customer to edit and create the IPS signature using snort/custom based format if required
6.	Solution should able to **block devices** based on Windows Class ID and should include USB, Infrared, Bluetooth, Serial, Parallel, fire wire, SCSI and PCMCIA. Solution should also be able to block and give read/write/execute permission for mentioned devices
7.	Solution should provide application analysis, process control, file and registry access control, module and DLL control.
8.	Proposed Solution should be able to deploy flexible and different security policies depending upon the relationship of following network triggers –

	- IP address (range or mask) - DNS Server - DHCP Server - WINS Server - Gateway Address - TMP Token Exists (hardware token) - DNS Name Resolves to IP - Policy Manager Connected - Network Connection (wireless, VPN, Ethernet, dialup)
9.	Proposed IPS solution should combines NIPS (network) and HIPS (host) both with Generic Exploit Blocking (GEB) for one signature to proactively protect against all variants, Granular application access control and behavior based technology mentioned above.
10.	Proposed solution should be able provide superior root kit detection and removal. This should have access below the operating system to allow thorough analysis and repair.
11.	**Denial of service detection and** protection - Should Protects the system from multiple forms of anomalous network behavior that is designed to disrupt system availability and/or stability.
12.	**Denial of service detection and** protection - Should Protects the system from multiple forms of anomalous network behavior that is designed to disrupt system availability and/or stability.
13.	**Anti-spoofing** - Should Protects the transmission of data from being sent to a hacker system who has spoofed their IP or Mac Address
14.	Agent has the ability to detect and block process execution chains. It is able to detect when a malicious application tries to execute a trusted application, and then use the trust privileges of that application to access the network.
15.	**Anti-application hijacking** - Should prevent hackers and web sites

	from identifying the operating system and browser of individual computers.
16.	**Code insertion attack prevention** - Prevent malicious applications from inserting code into trusted application to bypass outbound application fire walling.
17.	**Protocol adapter attack prevention** - Prevent malicious applications from using their own protocol adapter to bypass outbound fire walling.
18.	Antivirus and Antispyware policy can have options by default to choose High Security and High performance to have a right balance while deployment in the production network.
19.	Antivirus schedules scans should get delayed/rescheduled while laptops are running on batteries.
20.	Antivirus should have behavior based technology to scan for Trojans, worms and key stroke loggers to protect from zero day threats. Sensitivity level of this should get adjusted with customized scanning frequency.
21.	Antivirus Solution should have internet browser protection and homepage should be configurable if security risk changes that.
22.	Antivirus solution should be able to Scan POP3 email traffic including email clients Microsoft outlook, lotus notes and outlook express.
23.	Desktop Firewall rules should be configurable depending upon the adapters including Ethernet, wireless, Dialup, VPN (Microsoft PPTP, Nortel, Cisco).
24.	Desktop Firewall rules should be configurable depending upon the state of screen saver "ON" & "Off".
25.	Desktop Firewall Policies should be configurable depending upon the time and day.
26.	The solution must have readymade policies including – - To Make all removable drives read only , - To block program from running from removable drives , - Protect clients files and registry keys ,

	- Log files written to USB drives , - Block modifications to host files
27.	Solution must be able to display and customize warning messages on infected computers. For example, if users have a spyware program installed on their computers, you can notify them that they have violated your corporate policy.
28.	Management server should have the capabilities to add multiple domains if required for the different locations to assign the different administrators for other locations. Each domain should shares the same management server and database & This separation prevents administrators in one domain from viewing data in other domains. These administrators can view and manage the contents of their own domain, but they cannot view and manage the content of other domains.
29.	Solution must provide a group updater for remote site and must have bandwidth throttling option to streamline updates and thereby reducing load on the bandwidth
30.	To conserve the network bandwidth clients should be configurable to upload the maximum records of logs to the management server.
31.	**The Host-based, self-enforcement** - It should use a desktop firewall (built into the agent) to permit or deny managed endpoints access to the network. This method should offer the fastest and easiest implementation as it requires: No infrastructure changes and No additional deployment efforts.
32.	Solution should have the integration with various client management & patch management solution
33.	It must have compliance check policy templates for client management agent to ensure that agent is always installed, running and updated.
34.	Solution must have the ability to validate the users connecting to the

	Enterprise network by determining the following: - Their host-firewall policy matches the policy defined on the management server - Host-IPS is running. And HIPS signature files are up to date - Anti-Virus is running and Anti-Virus definitions/.DAT files are up-to-date according to enterprise security policy - Custom or third-party security applications are running. - The patch level of the operating system meets enterprise security policy. - The patch level of applications meets enterprise security policy. - Registry values are present. - The password strength meets minimum requirements - Windows Update tool is enabled and running. - They are permitted to alter their network configuration settings. - Minimum service pack requirements are met. - Anti-Spyware is running. - The agent is a valid agent - Determine if a custom or third-party files are present. - Add/Remove Programs is enabled for the user. - Enforce the presence and update status of Anti-Spyware products
35.	Solution should have following policies templates to check & enforce the security of workstations – - Minimum password age, password length, complexity and history - To Disable Guest account, registry editing, add or remove program, remote desktop, IP change, windows CD and windows auto play.
36.	Host Integrity rule priorities and conditions enable administrators to create interdependencies between rules such as "if/then/else" conditions and determine the order in which rule are executed. For Example, rule conditions allow administrator to create

	policies such as "the host must be running either anti-virus 1 or anti-virus 2." Rule priorities ensure the Host Integrity rules are run in the correct order. For example, Agent could download and install a required operating system patch before initiating the update of a hot fix.
37.	If the host is non-compliant with security policies, Agent can automatically initiate a restoration action, which can include running command line, downloading and executing/inserting a file, rechecking the host for compliance, and ultimately granting access for the compliant host to the network.
38.	Solution must be scalable to incorporate the following with no installation of component on clients should need be in future:
39.	It should support conversion to and from virtual environments like VMware, Microsoft Hyper & Microsoft Virtual Server
40.	It should support scheduling of recovery points
41.	It should auto-detect hardware and install appropriate drivers while recovering a system from complete crash situation.
42.	Solution should support saving of recovery points at FTP locations, DAS, NAS, USB Drive, DVD drives
43.	The solution must be able to initiate automatic threat con driven backups as soon as the threat landscape increases.
44.	The solution should provide a complimentary disaster recovery for critical servers and clients.
45.	The solution must provide bare metal recovery to the existing or dissimilar hardware possible in minutes
46.	System Recovery solution should support for Dissimilar Hardware recovery in case of a complete system crash
47.	The solution must provide physical to virtual and virtual to physical conversion. With this functionality, administrators can have can follow best-practices, such as testing deployments in virtual environments or using virtual environment as an immediate disaster recovery site.

48.	An optional Granular Restore should also be part of solution.
49.	Should support for 32 bit & 64 bit Windows (incl. XP, Vista, 7, 8)
50.	The software should not affect the system resources with less consumption of system resources which include RAM, CPU and H.D Space utilization.
51.	Must scan and block threats originating from Floppy disks, CD ROMs, USBs and Network Drives automatically in real-time when accessed
52.	Detect and remove infected files on the fly in real time.
53.	Should not have file size restriction in real time and On Demand Scanning.
54.	Allow / prevent the concerned I.T Personnel to change the settings of antivirus by password protecting the software
55.	Incremental Updates to be available online
56.	Support for Compressed File scanning & repair.
57.	Proactive protection against zero day/zero hour threats.
58.	Should support exclusion list by File Extensions
59.	Should be IPV6 ready.
60.	Should have ICSA Certification.

2. ELIGIBILITY CRITERIA

1. The Bidder can be a company/Corporation/Firm, registered in India. The company should be in existence at least for the last 5 years from the date of Tender notification.

2. The bidder should be a developer, manufacturer or the OEM authorized representative of respective products / items and should be in business of manufacture, and or supply and maintenance of the offered items for a minimum period of one year in Delhi.

3. One service centre at Delhi with five support engineers.

4. The bidder should have minimum annual turnover for the items/product mentioned (irrespective of brand/model) in Procurement Schedules and for the brand offered, during 2008-2013.

5. The bidder should have an annual turnover of at least Rs. 1.00 Crore (hundred Lakhs rupees) in each of the last 3 financial years i.e. 2010-11, 2011-12 and 2012-13.

6. The bidder should furnish the information on major past supplies under the relevant product/services and satisfactory performance for the last one financial year.