Technical Specification Requirements for Antivirus

Protection

- Platform Supported: Windows 7 or later / Windows Server 2012 R2
- Centralized Management Console for multiple operating systems: Windows, Linux and virtualized platforms
- Actionable security dashboard (can perform full scan, cleanup and remediation from the console)
- Full active directory integration for automatic deployment of endpoint agents
- Centralized multiple platform updating
- Targeted remote malware and potentially unwanted applications (PUA) cleanup from console
- Targeted remote PUA/Suspicious/Buffer overflow protection authorization
- Rootkit detection and cleanup
- Detects, block and clean up known and unknown threats, included virus, spyware, adwares and PUAs.
- Monitors applications launched on the endpoints, removable devices and data that are forwarded or transmitted
- Assess computers for missing patches

Endpoint Client Firewall

- Platform supported: Windows 7 or later
- Provides stealth mode
- Prevents application hijacking and checksum-based exclusion
- Centrally Managed Firewall
- Location-aware firewall so different firewall policies can be applied when endpoint is within or outside the company network.
- Part of the endpoint protection

Application Control

- Selectively authorize or block legitimate Applications that impact network bandwidth, Systems availability, and user productivity
- Vendor-managed list to offload the administrator from monitoring new applications or versions Administrators can select and allow specific applications or specific categories of applications.
- Provides and automatically updates the list of controlled applications
- Integrated in unified detection engine

- Policy set in central management console
- Allows different policies for different groups
- Can enforce company policies as well as reduce security risks.
- Stop instant messaging, games, peer-to-peer applications who consume bandwidth.
- Prevent confidential information from being exposed via peer-to-peer exchange or transmitted via instant messaging

Device Control

- Control the use of removable storage, optical media drives and wireless networking devices and define which computers have access to specific removable devices
- Supports device instance and model exceptions
- Easy authorization of allowed devices
- Integrated in unified detection engine
- Policy set in central management console
- Allows different policies for different groups
- Block Windows from bridging two networks
- Control MTP / PTP devices.

Host Intrusion Prevention System (HIPS)

- Guarding against unknown threats by analyzing behavior before code executes
- Stop zero-day threats with built-in HIPS Behavioral Protection
- Suspicious Behavior Detection
- Buffer Overflow Protection

Runtime Protection

- Monitor and block suspicious behavior like registry or critical windows system files modification
- Protection against buffer overflow

Web Protection

- Block URLs that are hosting malware
- Live in-the-cloud lookups check database of Millions of compromised sites
- Protects users everywhere, in the office, and when not behind corporate protection, i.e. at home or over public WIFI

- Integrated into existing endpoint agent with no endpoint configuration required
- Online scanning for malware (in the cloud)
- Ability to detect and block compromised / hijacked trusted sites
- Multi-web browser support

Data Loss Prevention

- Data Loss protection
- Control the transfer of sensitive data
- Integrated into endpoint agent

Data control

- Must be fully integrated content monitoring solution
- Monitors data transferred onto data points like removable storage, optical and disk drives, and internet-enabled applications (web browser, email client, instant messaging)
- Block/allow/warn/log transfer of files based on "true" file type and/or content using regular expressions
- Control the transfer of sensitive data
- Monitor transfer of sensitive data to removable storage.

Tamper Protection

- Prevents users from uninstalling the antivirus, auto update, client firewall, remote management system and disk encryption on a windows computer
- Policy is configured within Enterprise Console
- Requires password to be set for protection and can only be configured on the endpoint if the user has administration rights or the correct password is entered.

Web Control

- Control access inappropriate website
- Create Web control policy from enterprise console and apply to the right PC group
- Add own list of URLs or IP address via exceptions tab

Enterprise Control

- Platform supported: Windows Server 012 R2
- Implementation on virtual environment
- Can deploy, update, configure and monitor your clients with centralized administration of all Endpoint Protection components on simple and complex networks.
- Centralized administration tool for all components of Sophos Endpoint Protection

Policy-based

- Role-based administration privileges
- Centralized policy covering updating schedules, Antivirus and HIPS, client firewall, application, device and data control and NAC
- Can create subgroups to create an entire tree, all subgroups inherit the policies applied to the parent group

Role-based administration

- Separate view for administrator, helpdesk, auditors, etc.
- Delegate part of the administration to a list of administrators with restricted permissions.
- Can create custom roles that will suit to needs and can be are assigned to Windows users or Windows groups.

Active directory synchronization

- Automatic computer discovery and synchronization with AD structure
- Centralized policy covering updating schedules, Antivirus and HIPS, client firewall, application, device and data control and NAC

Failsafe updating

- Multiple sources of update with automatic failover
- Bandwidth throttling support for low-speed network links
- Automatically download small frequent updates from nearest and best location to reduce computer and network impact

Dashboard and Reporting

- Integrated graphical reporting delivers instant and scheduled email report of the threat alerts and infections while the security dashboard gives an at-a-glance report for outbreak risk
- Near real-time view of the security health of the organization through the use of dashboards or similar technology
- Automated email reporting when certain alert threshold is reached
- Support report output in PDF, HTML, Excel, Word, CSV

Signature Updates

- Ability to check for updates as often as every 10 minutes
- Separate schedule for signature and software updates

SUPPORT and CERTIFICATION

a. 1 year warranty, updates and support
b. 24 x 5 available phone and e-mail technical support by Manufacturer
c. 8 x 5 Onsite support, One (4) hour response time upon receipt of call; with on-site support
d. Product security updates and software upgrades
e. Quarterly Product Health Check (Phone or On-site within Metro Manila)
f. Offered solution must be in the Gartner's leaders quadrant

Delivery

- Delivery of license key/s shall be made within 15 working days from receipt of a valid Purchase Order

Number of Users – 90

Prepared by:

Oliver Templo
IT Officer

Approved by:

Arsenio De Guzman
VP for TSD