BỆNH VIỆN HỮU NGHỊ
VIỆT NAM-CU BA
**PHÒNG KẾ HOẠCH TỔNG HỢP**

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
**Độc lập - Tự do - Hạnh phúc**

V/v: Mời chào giá thẩm định giá gói thầu phần mềm diệt virus năm 2023

*Hà Nội, ngày 21 tháng 10 năm 2022*

# Thư mời chào tham gia thẩm định giá

Kính gửi: Quý đơn vị thẩm định

Thực hiện kế hoạch đấu thầu Mua sắm phần mềm diệt virus cho Bệnh viện hữu nghị Việt Nam Cu Ba năm 2023, Bệnh viện có nhu cầu thẩm định giá nội dung:

| STT | Nội dung | Đơn vị | Số lượng |
|---|---|---|---|
| 1 | Bản quyền phần mềm diệt virus dùng cho máy tính (máy chủ và máy trạm)<br>Thông số kỹ thuật (*Chi tiết kèm theo*)<br>Thời hạn: 1 năm | License | 120 |

Bệnh viện kính mời các đơn vị quan tâm, có đủ điều kiện về năng lực thẩm định giá gửi báo giá thẩm định về phòng Kế hoạch tổng hợp; Bệnh viện Hữu nghị Việt Nam - Cu Ba địa chỉ: 37 Hai Bà Trưng - Hoàn Kiếm - Hà Nội;

Trước 9h00 ngày 26 tháng 10 năm 2022.

Đầu mối tiếp nhận: Ông Phạm Minh Thành - Tổ công nghệ thông tin

Điện thoại: 0852799473

Xin trân trọng cảm ơn sự hợp tác của quý đơn vị./.

**Nơi nhận:**
- Như trên
- Lưu, KHTH

**TRƯỞNG PHÒNG**

**Lò Thị Hà**

# THÔNG SỐ KỸ THUẬT SẢN PHẨM

| TT | Nội dung |
|---|---|
| **I** | **Phần mềm diệt virus cho máy chủ, máy trạm** |
| **1.** | **Hỗ trợ các hệ điều hành:** |
| 1 | Hệ điều hành Microsoft Windows 7, 8, 10 |
| 2 | Hệ điều hành Microsoft Windows Server 2008, 2012, 2016, 2019 |
| 3 | Hệ điều hành Mobile: iOS, Android |
| 4 | Hỗ trợ hệ điều hành Linux: Ubuntu, Debian, Red Hat, CentOS, SuSe |
| 5 | Hỗ trợ hệ điều hành MAC: từ MAC OS X 10.14 hoặc phiên bản mới hơn |
| **2.** | **Chức năng Anti-Virus** |
| 1 | Giải pháp hỗ trợ Auto-Protect quét thời gian thực. |
| 2 | Có khả năng phát hiện và diệt viruses, spyware, worm, trojan rootkit, Keyloger Macro,… |
| 3 | Cho phép lựa chọn quét nhanh, quét full, quét tức thời, quét theo lịch trình và hỗ trợ quét từ xa qua giao diện quản lý tập trung. |
| 4 | Có khả năng chỉ quét những files mới và những files có sự thay đổi so với lần quét virus gần nhất giúp tăng tốc độ quét virus. |
| 5 | Phải quét bộ nhớ hệ thống để phải hiện các rootkit, tiến trình ẩn, và các hành vi khác cho thấy mã độc hại đang cố gắng ẩn giấu. |
| 6 | Có chức năng Quanrantine đối tượng bị nghi lây nhiễm trước khi thực hiện Repair/Delete, khi cần có thể Restore lại từ các file này. |
| 7 | Có chức năng thông báo cho người sử dụng và quản trị hệ thống về việc phát hiện đối tượng bị nhiễm mã độc qua hộp thoại cảnh báo cho người sử dụng; email và/hoặc system log message cho người quản trị. Thông tin cảnh báo bao gồm: Tên thiết bị, định danh người dùng, tên và đường dẫn đối tượng bị lây nhiễm, tên loại mã độc, hành động mà chương trình đã thực hiện với đối tượng. |
| 8 | Cho phép người quản trị có thể thiết lập mặc định các hành động sẽ thực hiện khi chương trình phát hiện mã độc: Alert/ Notify, Clean, Delete/ Remove, Move/ Quarantine, Promt for Action. |
| 9 | Hỗ trợ các tính năng mà nhờ đó người quản trị có thể lập kế hoạch ngăn chặn việc bùng nổ lây lan virus trong hệ thống. |
| 10 | Có chức năng Web Anti-virus, đáp ứng quét cho traffic web, email, file theo cơ chế proactive. |
| 11 | Bảo vệ các nguy cơ từ Email bằng việc quét toàn bộ các Email vào/ra để phát hiện và ngăn chặn các nguy cơ từ Email. Hỗ trợ các giao thức: POP3, SMTP, IMAP |
| **3.** | **Chức năng giám sát mạng và giám sát hệ thống** |
| 1 | Cho phép xem toàn bộ các kết nối mạng trên máy tính theo thời gian thực. |
| 2 | Cho phép ghi lại hoạt động của các ứng dụng trên máy tính, cung cấp |

| | |
|---|---|
| | thông tin này để nâng cao tính bảo mật. |
| **4.** | **Chức năng HIPS (Host IPS)** |
| 1 | Phải có khả năng phát hiện và ngăn chặn việc quét cổng, tấn công từ chối dịch vụ, tấn công vào lỗ hổng bảo mật của các hệ điều hành và các ứng dụng… |
| 2 | Có chức năng tự động ngăn chặn lưu lượng truy cập gây hại đến máy tính từ một máy tính có chứa mã độc hoặc nhiễm độc. |
| **5.** | **Chức năng Desktop Firewall** |
| 1 | Phải có chức năng hỗ trợ kiểm soát traffic vào/ra. |
| 2 | Cho phép thao tác kiểm soát Firewall Client từ xa như: Disable, Enable từ xa. |
| 3 | Giải pháp phải có khả năng cảnh báo, giám sát các ứng dụng đang chạy. |
| 4 | Cho phép tạo ra tập luật (rule) dựa trên ứng dụng hoặc mạng (application network, network packet rule). Hỗ trợ các dạng protocol: TCP, UDP, ICMP, ICMPv6, IGMP, và GRE. |
| **6.** | **Chức năng Device control** |
| 1 | Phải có khả năng xác định thiết bị nào có thể hoặc không thể sử dụng trên Windows. |
| 2 | Phải có khả năng ngăn cấm các ứng dụng chạy từ thiết bị lưu trữ ngoài. |
| 3 | Phải có khả năng thiết lập lịch được sử dụng thiết bị cắm ngoài qua giao tiếp USB. |
| 4 | Cho phép thiết lập danh sách các thiết bị cắm ngoài được sử dụng (Trusted Device). |
| **7** | **Chức năng Web Control** |
| 1 | Lọc Web theo URL, Category, Data, Content. |
| 2 | Giới hạn truy cập Web theo lịch |
| 3 | - Cho phép quét toàn bộ giao tiếp thông qua giao thức FTP, HTTP, kiểm tra toàn bộ URL xem có trong danh sách các website chứa mã độc hay website lừa đảo hay không.<br>- Cho phép tạo ra các luật để hạn chế hay cấm người dùng truy cập vào những nội dung không cho phép. Các luật này cho phép kết hợp với Active Directory để tạo các luật liên quan tới người dùng hay nhóm người dùng trong Active Directory.<br>- Khả năng lọc bảo vệ web có thể qua: Lọc nội dung, sử dụng địa chỉ tài nguyên, tên của user/group.<br>- Tập luật có thể thực hiện theo lịch, cho phép các luật thực hiện theo thời gian cụ thể. |
| **8.** | **Chức năng Application Control** |
| 1 | Cho phép thiết lập danh sách trắng bằng việc phân loại các ứng dụng theo đánh giá của nhà sản xuất, hoặc sử dụng công nghệ điện toán đám mây. |
| 2 | Cho phép tạo ra danh sách trắng các ứng dụng theo nhóm người sử dụng |

| | |
|---|---|
| | bằng việc kết hợp với AD/LDAP. |
| 3 | Khả năng thiết lập danh sách đen các ứng dụng theo nhóm, theo sự phân loại của nhà sản xuất hoặc theo cơ chế bảo mật của mỗi đơn vị sử dụng. |
| **9.** | **Chức năng Virus Update** |
| 1 | Hỗ trợ update bằng tay tại Client từ Server quản lý. |
| 2 | Hỗ trợ Update cho nhiều Client từ Server quản lý. |
| 3 | Hỗ trợ lập lịch tự động download update. |
| 4 | Server quản lý trung gian: Có thể tải Update từ nhiều nguồn khác nhau (từ server quản lý cấp trên, từ nhà cung cấp qua Internet), có thể thiết lập mềm dẻo việc lựa chọn nguồn update. |
| 5 | Giao thức dùng để update virus từ nhà cung cấp, từ máy chủ là giao thức chuẩn: HTTP hoặc FTP và có thể hoạt động thông qua Proxy. |
| **10.** | **Chức năng quét lỗ hổng bảo mật** |
| 1 | Có khả năng quét lỗ hổng bảo mật các sản phẩm của Microsoft và các hãng khác. |
| 2 | Bảo vệ thiết bị khỏi ransomware bao gồm cả các thư mục chia sẻ trên máy chủ ( ransomware including protection for server share folders) |
| 3 | Phục hồi dữ liệu bị nhiễm mã độc ( Malicious action rollback) |
| **11.** | **Một số chức năng bảo vệ khác** |
| 1 | Cho phép quét toàn bộ các giao tiếp sử dụng các phần mềm IM: IRC, Mail, AIM, ICQ, MSN |
| 2 | **Khả năng tự bảo vệ:**<br>- Phần mềm diệt virus phải có khả năng tự bảo vệ trước các mối nguy cơ từ mã độc, như việc mã độc muốn xóa chương trình diệt virus ra khỏi máy tính. Việc bảo vệ được thực hiện trên file của trương trình trên ổ đĩa, trên RAM và trong Registry.<br>- Ngăn chặn tất cả quá trình điều khiển chương trình diệt virus qua máy tính điều khiển từ xa.<br>- Thiết lập Password để bảo vệ chương trình khi muốn truy cập hay thực hiện các tác vụ cụ thể. |
| **12.** | **Chức năng Report** |
| 1 | Hỗ trợ report các thông tin ngay tại máy trạm: Virus quét được; vị trí file nhiễm virus; vị trí file backup; file được backup; trạng thái Start-stop của service theo từng ngày. |
| 2 | Hỗ trợ thống kê, báo cáo tình hình virus trên toàn mạng. |
| 3 | Hỗ trợ thống kê, báo cáo theo lịch trình tự thiết lập. |
| 4 | Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn mạng |
| 5 | Hỗ trợ xuất báo cáo qua nhiều dạng khác nhau" PDF, XLS,… |
| 6 | - Các báo cáo phải được phân loại theo mức độ quan trọng.<br>- Các thông báo hệ thống được thực hiện dưới dạng Pop-up trên thanh |

| | |
|---|---|
| | Taskbar. Các báo cáo có thể thực hiện qua Email.<br>- Hiển thị nhiều thông tin trên Drashboard.<br>- Các cảnh báo có thể thực hiện qua: Email, Net Send hoặc thực thi một file nào đó. |
| **13.** | **Quản lý tập trung** |
| 1 | Phần mềm quản trị tập trung hỗ trợ cài đặt trên các hệ điều hành: Microsoft Windows 7, 8, Server 2008, Server 2012 |
| 2 | Phần mềm quản trị tập trung cho phép triển khai phân cấp theo cơ chế Master/ Slave để phù hợp với các tổ chức lớn. Giao diện phần mềm quản trị: Hỗ trợ giao diện theo chuẩn MMC của Microsoft và giao diện Web. |
| 3 | Hỗ trợ tạo Image cài đặt của hệ điều hành và ứng dụng. Hỗ trợ cài đặt từ xa hệ điều hành và các ứng dụng. Cho phép cài đặt Windows Automatic Installation Kit (WAIK) trên máy quản trị. |
| 4 | Hỗ trợ gỡ bỏ các phần mềm từ xa trên các máy Client. |
| 5 | Quản lý phần cứng dựa trên các thông tin trên Registry. |
| 6 | Hỗ trợ cài đặt từ xa các update cho hệ điều hành. Cho phép tìm kiếm và vá các lỗ hổng bảo mật |
| 7 | Điều khiển các truy cập của các thiết bị truy cập vào hệ thống mạng dựa trên các tập luật hay danh sách trắng (Network Access Control). |
| 8 | Có tính năng Exchange ActiveSyn Mobile. |
| 9 | Hỗ trợ tính năng quản lý iOS. |
| 10 | Hỗ trợ tính năng gửi tin nhắn SMS tới các thiết bị di động đã được triển khai phần mềm client. |
| 11 | Giải pháp chỉ cần một Agent chạy duy nhất quản lý cho các module của chương trình. |
| 12 | Giải pháp phải có khả năng tập trung hóa quy trình quản lý, triển khai, báo cáo. |
| 13 | Khả năng phân chia nhóm quản lý và thiết lập các chính sách quản lý khác nhau. |
| 14 | Giải pháp có khả năng cho phép người quản trị kiểm soát ngăn ngừa việc sử dụng License phần mềm Antivirus một cách trái phép. |
| 15 | Khả năng thiết lập cấu hình Anti-virus, Firewall tới từng máy trạm từ xa và không cho phép người sử dụng bình thường thay đổi các thiết lập này. |
| 16 | Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn hệ thống. |
| 17 | Chức năng quản lý, áp dụng chính sách không phụ thuộc vào Active Directory. |
| 18 | Chức năng xóa dữ liệu từ KSC không thể khôi phục được dữ liệu đã xóa. |
| **14** | **Đáp ứng chỉ thị 14/CT-TTG của Thủ tướng chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam** |