ĐẠI HỌC Y DƯỢC TPHCM
BỆNH VIỆN ĐẠI HỌC Y DƯỢC

Số: 60./BVĐHYD-CNTT
V/v mời chào giá

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

Thành phố Hồ Chí Minh, ngày 09 tháng 01 năm 2021

Kính gửi: Quý nhà cung cấp

Bệnh viện Đại học Y Dược TP. Hồ Chí Minh mời Quý nhà cung cấp có quan tâm, có khả năng cung cấp bản quyền phần mềm phòng chống mã độc cho các thiết bị đầu cuối của Bệnh viện Đại học Y Dược TP. Hồ Chí Minh, báo giá theo phụ lục đính kèm.

Đề nghị Quý nhà cung cấp có quan tâm gửi file word/excel và bản scan báo giá có đóng dấu theo mẫu đính kèm đến email moichaogia@umc.edu.vn và email congnghethongtin@umc.edu.vn và gửi bản giấy có đóng dấu về Phòng Công nghệ thông tin, Bệnh viện Đại học Y Dược TP. Hồ Chí Minh, địa chỉ số 215 Hồng Bàng, Phường 11, Quận 5, TP. Hồ Chí Minh.

- Hồ sơ gửi kèm theo báo giá bao gồm các tài liệu: catalogue sản phẩm và các tài liệu kỹ thuật liên quan khác.
- Thời gian nhận báo giá: đến hết ngày 16./.01../2021.
- Điện thoại liên hệ: 028.39525391 (Chị Huỳnh Thụy Cẩm Thương - Phòng CNTT)

Trân trọng./.

Nơi nhận:
- Như trên;
- Đơn vị Quản lý đấu thầu (để đăng tin);
- Lưu: VT, CNTT (K08-047-htcthuong)(2).

KT. GIÁM ĐỐC

BỘ Y TẾ * ĐẠI HỌC Y DƯỢC TP. HỒ CHÍ MINH * BỆNH VIỆN ĐẠI HỌC Y DƯỢC TP. HỒ CHÍ MINH

Trương Quang Bình
Phó Giám đốc

PHỤ LỤC
DANH MỤC HÀNG HÓA MỜI CHÀO GIÁ

(Kèm theo công văn số ..60../BVĐHYD-CNTT ngày 09./..01./2021)

Stt	Tên hàng hóa	Yêu cầu kỹ thuật	Đơn vị tính	Số lượng	Ghi chú
1	Bản quyền phần mềm phòng chống mã độc cho các thiết bị đầu cuối - Thời hạn sử dụng bản quyền: 12 tháng	Theo yêu cầu kỹ thuật chi tiết bên dưới	Bản quyền	2.031	

Yêu cầu kỹ thuật chi tiết

Stt	Nội dung yêu cầu	Mô tả
I	**Yêu cầu kỹ thuật, tính năng của phần mềm**	
1.	Bản quyền phần mềm	Bản quyền mua mới
2.	Máy chủ quản trị tập trung (Centralized Management)	- Giao diện bảng điều khiển, báo cáo, cảnh báo tập trung. - Giao diện duy nhất cho tất cả các tính năng vấn đề về bảo mật. - Thiết lập chính sách tập trung. - Cập nhật các Pattern, Engine cho toàn bộ hệ thống tập trung. - Trung tâm chia sẻ các thông tin về file, hash, IP, URL, domain nguy hiểm. - Thu thập log tập trung, có thể chia sẻ cho hệ thống giám sát an toàn thông tin SIEM (Security Information and Event Management) - Mở rộng sự trực quan xuyên suốt cho các mô hình triển khai như on-premise (máy chủ đặt tại trung tâm dữ liệu Bệnh viện Đại học Y Dược TP. Hồ Chí Minh), Cloud (đám mây), Hybrid (cả hai). - Báo cáo: hỗ trợ báo cáo theo các định dạng PDF, DOCX, XLSX, HTML, XML, CSV. Hỗ trợ các mẫu báo cáo có sẵn hoặc có thể tùy biến. Chẳng hạn như mẫu báo cáo theo mã độc, theo người dùng phát hiện, theo máy trạm phát hiện, nhóm, theo kiểu mối đe dọa ransomware/ spyware/ grayware/ viruses. Hỗ trợ theo từng cấp độ như chi tiết hoặc tóm tắt. Báo cáo hỗ trợ tùy biến mẫu (custom template) cho phép quản trị tự định nghĩa mẫu theo nhu cầu. - Có thể tích hợp với máy chủ Active Directory dùng để xác thực cho quản trị.

Stt	Nội dung yêu cầu	Mô tả
3.	Hỗ trợ các tính năng chính để bảo vệ máy tính	- Sử dụng kết hợp nhiều công nghệ bảo vệ mã độc cao cấp để bảo vệ an toàn thông tin trên máy đầu cuối cũng như người dùng. Giải pháp có thể học, tương thích, tự động chia sẻ các mối đe dọa trong xuyên suốt môi trường mạng Bệnh viện. - Tự động phát hiện và đáp ứng sự tăng trưởng nhanh chóng của các biến thể mã độc gây nên mối đe dọa cho hệ thống, bao gồm cả fileless và ransomware. - Cung cấp sự trực quan về khả năng điều tra và kiểm soát trên toàn bộ hệ thống bằng cách hỗ trợ sử dụng bộ công cụ EDR, hỗ trợ tích hợp mạnh mẽ với SIEM và bộ mã API được công bố rộng rãi mà không cần cài đặt thêm agent. - Hỗ trợ mô hình quản trị agent tất cả trong một (All-in-one) triển khai cho On-premise. Các tính năng tối thiểu gồm có anti-malware, kiểm soát ứng dụng, phòng chống xâm nhập IPS, kiểm soát thiết bị ngoại vi, phòng chống thất thoát dữ liệu DLP - Hỗ trợ bảo vệ toàn bộ người dùng/ thiết bị đầu cuối trong Bệnh viện (hoặc các máy của Bệnh viện hoạt động bên ngoài Bệnh viện) khỏi mã độc như Trojans, worms, spyware, ransomware, có khả năng tự thích nghi để phát hiện các biến thể mới chưa biết và các mối đe dọa mới như mã độc mã hóa, mã độc fileless - Cung cấp khả năng phát hiện và phản ứng lại với phát hiện ngay trong một tập giải pháp. - Hỗ trợ vá ảo các lỗ hổng bảo mật đã biết và chưa biết cho thiết bị đầu cuối. Có thể bảo vệ người dùng ngay cả khi bản vá chính thức chưa phát hành hoặc triển khai. - Phải trực quan và kiểm soát tập trung: nhiều tính năng có thể được quản trị thông qua một giao diện kiểm soát console duy nhất để cung cấp sự trực quan tập trung và kiểm soát tất cả tính năng. - Có thể cài đặt trên máy chủ đặt tại trung tâm dữ liệu tại cơ sở của Bệnh viện Đại học Y Dược TP. Hồ Chí Minh (triển khai on-premise). - Chỉ một giải pháp có thể bảo vệ các mối đe dọa đã biết và chưa biết cho endpoints Windows, MAC và cả VDI. - Giải pháp hỗ trợ công nghệ máy học với độ tin cậy cao (high-fidelity machine learning) với nhiều công nghệ phát hiện khác nhau để đảm bảo khả năng phát hiện tốt nhất các ransomware cũng như tấn công tinh vi.

Stt	Nội dung yêu cầu	Mô tả
		- Hỗ trợ nhiều công nghệ không dấu vết (signature-less techniques), bao gồm tối thiểu các công nghệ như máy học độ tin cậy cao (high-fidelity machine learning), phân tích hành vi, ngăn ngừa các biến thể (variant protection), kiểm tra độ tin cậy của mẫu (census check), kiểm soát ứng dụng, ngăn chặn khai thác trong tài liệu (exploit prevention), độ nổi tiếng trên web (web reputation), chặn kết nối đến máy chủ điều khiển và kiểm soát (máy chủ C&C) - Kết hợp công nghệ giảm thiểu phát hiện sai (Noise cancellation) như kiểm tra độ tin cậy (census check) và kiểm tra whitelist ở các lưới bảo vệ không dựa trên dấu vết (signature-less) - Có thể ngay lập tức chia sẻ các thông tin về hành vi mạng bất thường và file với các lưới bảo vệ khác để chặn các tấn công kèm theo. - Cung cấp ngăn chặn các Ransomware tinh vi mã hóa tập tin (file) ở thiết bị đầu cuối, có thể ngắt các hành vi nguy hiểm, và có thể phục hồi các tập tin (file) đã bị mã hóa nếu cần thiết. - Cho phép chia sẻ các phát hiện mối đe dọa tinh vi trên phạm vi toàn tổ chức (sharing threat intelligent) - Cho phép tùy biến giao diện bảng điều khiển (dashboard) phù hợp với nhiều vai trò quản trị khác nhau. - Hỗ trợ bảo vệ đa nền tảng như: Windows 7, Windows 8.1, Windows 10, MAC OS. - Hỗ trợ khả năng kết nối với các sandbox on-premise hoặc dạng dịch vụ Sandbox SaaS. Tính năng để mở rộng trong tương lai mà không cần cài thêm agent.
4.	Có đầy đủ các tính năng bảo mật nâng cao cung cấp sẵn trong phần mềm (Threat Detection Capabilities)	- Tính năng phát hiện mã độc sử dụng công nghệ máy học với độ tin cậy cao ở cả hai mức độ trước thực thi (pre-execution) và thực thi (runtime) - Tính năng phân tích hành vi, dùng để ngăn chặn dạng tấn công sau: sử dụng script khai thác, Ransomware, Memory inspection, Browser exploit protection - Tính năng kiểm tra độ nổi tiếng của file (File reputation), độ nổi tiếng của web (web reputation), bảo vệ phát hiện các biến thể mã độc mới, kiểm tra độ an toàn theo thống kê (Census check) - Tính năng ngăn chặn tấn công khai thác (host firewall, exploit protection)

Stt	Nội dung yêu cầu	Mô tả
		- Kiểm soát thiết bị ngoại vi (device control), nhận biết vị trí (location awareness): theo vị trí của máy trạm, áp dụng tới từng người dùng, nhóm người dùng, có thể kết nối với máy chủ Active Directory, khóa tập tin autorun, hỗ trợ cả thiết bị di động, CD/DVD, Đĩa mềm, ổ đĩa mạng, USB và các đĩa lưu trữ, sinh trắc học, thiết bị giao tiếp hồng ngoại, bluetooth. - Chính sách cho device control hỗ trợ nhiều action như: Toàn quyền truy cập (Full access), Custom (tùy chỉnh), Đọc và thực thi (Read and execute), Chỉ đọc (Read only), Chỉ liệt kê nội dung thiết bị (List device content only), Chặn thiết bị (Block) - Hỗ trợ tính năng iDLP tích hợp trên endpoint: Khả năng xác định nội dung trong các tài liệu theo từ khóa hoặc template. Dò quét trên tất cả các kênh truyền dữ liệu như email, webmail, cloud, FTP, USB, Instance Messenger, network share, print screen, DVD…Cho phép thực thi mã hóa khi copy dữ liệu sang USB bên ngoài hoặc upload lên nới lưu trữ đám mây (Cloud Storage) - Hỗ trợ DLP với các template định nghĩa sẵn giúp tổ chức có thể nhanh chóng tuân thủ với các bộ nguyên tắc như GDPR, PCI/DSS, HIPAA, GLBA … - Ngăn chặn Command and control (C&C) - Tính năng Update Agent: cho phép lựa chọn một số agent làm thành phần cache các thông tin cập nhật như pattern, engine. Các agent chỉ cần cập nhật từ máy này giúp giảm lưu lượng cập nhật trực tiếp từ máy chủ - Có khả năng tùy biến dashboard quản trị, tùy biến theo các nhu cầu của quản trị viên như xem theo mục security, xem theo DLP, xem theo phát hiện ransomware, xem theo phát hiện application control, xem thống kê cập nhật của máy trạm…
5.	Có tính năng vá ảo các lỗ hổng Bảo mật cho máy trạm (Vulnerability Protection)	- Hỗ trợ nhanh chóng các bản vá ảo lỗ hổng bảo mật cho máy trạm, bao gồm cả thiết bị IoT. - Ngăn chặn các khai thác lỗ hổng zero-day cho máy trạm vật lý, máy laptop, VDI trong mạng hoặc ngoài mạng của bệnh viện. - Ngăn chặn khai thác lỗ hổng đã biết/chưa biết trước khi bản vá được triển khai, hoặc bản vá có thể không bao giờ được cung cấp.

Stt	Nội dung yêu cầu	Mô tả
		- Bảo vệ máy trạm với tối thiểu tác động đến hiệu năng máy trạm, trải nghiệm của người dùng. - Có khả năng kiểm tra sâu gói tin (DPI) để nhận dạng nội dung gói tin có thể gây nguy hại cho lớp ứng dụng - Bộ lọc cho phép lọc các lưu lượng mạng và đảm bảo phải được cho phép thông qua lưới lọc tường lửa có trạng thái (stateful inspection) - Ngăn chặn mã độc backdoor - Đơn giản hóa triển khai và quản trị bằng một agent duy nhất (chung với tính năng ngăn chặn antimalware), quản trị và giám sát tập trung các patch, giảm thiểu tối đa việc phải khởi động lại hệ thống.
6.	Có tính năng giám sát Ứng dụng máy trạm (Application Control)	- Cho phép nâng cao khả năng phòng thủ chống lại mã độc và APT bằng cách ngăn chặn các ứng dụng không biết/không mong muốn thực thi trên máy trạm bằng sử dụng chính sách động kết hợp danh sách trắng (whitelist) và danh sách đen (blacklist) - Ngăn chặn các ảnh hưởng tiềm tàng từ các ứng dụng không mong muốn/không biết như file thực thi, file DLL, ứng dụng window app store, các device drivers và các file dạng Portable Executable (PE) - Kết hợp với các lưới bảo vệ khác của tập giải pháp nhằm cung cấp khả năng tương quan các dữ liệu về mối đe dọa và ngăn chặn các mối đe dọa xảy ra hiệu quả hơn - Cơ sở dữ liệu đám mây về dữ liệu ứng dụng được phân tích và tương quan hỗ trợ trên 1 triệu file record - Hỗ trợ cấu hình chính sách App control chi tiết tới mức người dùng - Hỗ trợ chính sách động cho phép người dùng cài đặt các ứng dụng cho phép dựa trên các tiêu chí về mức độ nổi tiếng (reputation-based) như prevalence, mức độ trưởng thành của ứng dụng (maturity of the application). - Hỗ trợ thiết lập chính sách app control dựa trên tên ứng dụng, đường dẫn, regular expression, hoặc certificate cho cả whitelist và blacklist. - Cho phép lệnh đóng cửa (lockdown) hệ thống để khóa người dùng không cho phép thực thi các ứng dụng mới.
7.	Có khả năng hỗ trợ bảo mật dành cho máy	- Cung cấp các tính năng bảo mật cho máy Apple MAC, khả năng phát hiện mã độc tinh vi dùng máy học (Machine Learning)

Stt	Nội dung yêu cầu	Mô tả
	hệ điều hành Mac (Security for MAC)	- Tùy chọn hỗ trợ EDR cho máy MAC mà không cần cài đặt thêm agent - Không ảnh hưởng tới trải nghiệm người dùng MAC - Quản trị tập trung trên toàn bộ trên máy chủ với 1 giao diện, kể cả máy Windows và MAC, trên cả hai môi trường Cloud và On-premise hoặc hybrid
8.	Có tính năng mã hoá Dữ Liệu trên máy trạm (Endpoint Encryption)	- Đảm bảo bảo vệ dữ liệu bằng cách mã hóa dữ liệu trên endpoint - Hỗ trợ mã hóa ổ đĩa, mã hóa thư mục và tập tin, mã hóa thiết bị di động - Hỗ trợ quản trị Microsoft BitLokcer và Apple FileVault
9.	Có thể bảo mật cho Thiết bị di động (Mobile Security)	- Khả năng thực thi các chính sách về mobile, thiết bị, ứng dụng và bảo mật trên các nền tảng iOS và Android - Antimalware, mã hóa dữ liệu (Data Encryption), thực thi mật khẩu (password enforcement), (khóa từ xa) remote lock, quản trị ứng dụng, quản trị thiết bị cho thiết bị iOS và Android - Quản trị tập trung, cung cấp giao diện single view cho tổ chức quản trị từ desktop cho đến thiết bị di động.
II	**Triển khai giải pháp bảo mật thiết bị đầu cuối (Endpoint)**	
1.	Cài đặt, triển khai phần mềm phòng chống mã độc cho các thiết bị đầu cuối (máy chủ và máy trạm)	Cài đặt, triển khai phần mềm phòng chống mã độc cho các thiết bị đầu cuối (máy chủ và máy tính) tại cơ sở của Bệnh viện Đại học Y Dược TP. Hồ Chí Minh gồm: • Cơ sở 1: 215 Hồng Bàng, Phường 11, Quận 5, TPHCM. • Cơ sở 2: 201 Nguyễn Chí Thanh, Phường 12, Quận 5, TPHCM.
		Phần mềm Endpoint security cài đặt phải có bản quyền hợp pháp của hãng sản xuất
2.	Cài đặt, triển khai công cụ quản trị tập trung để quản lý các thiết bị đầu cuối	Cài đặt, triển khai công cụ quản trị tập trung để quản lý các thiết bị đầu cuối cho máy chủ tại cơ sở của Bệnh viện Đại học Y Dược TP. Hồ Chí Minh gồm: • Cơ sở 1: 215 Hồng Bàng, Phường 11, Quận 5, TPHCM. • Cơ sở 2: 201 Nguyễn Chí Thanh, Phường 12, Quận 5, TPHCM.

Stt	Nội dung yêu cầu	Mô tả
3.	Đào tạo và hướng dẫn cho nhân sự quản trị hệ thống	Nhân sự tham gia đào tạo do Bệnh viện Đại học Y Dược TP. Hồ Chí Minh chỉ định (tối thiểu 05 người)
4.	Thời gian triển khai	Không quá 2 tuần (thời gian này không được tính vào thời gian có hiệu lực của bản quyền phần mềm phòng chống mã độc cho thiết bị đầu cuối)
III.	**Yêu cầu khác**	
1.	Thời gian sử dụng	- Bản quyền hỗ trợ kỹ thuật từ hãng sản xuất trong 12 tháng, bản quyền phải được gắn liền với tài khoản email bảo mật của Bệnh viện. - Mở kênh hỗ trợ kỹ thuật trực tiếp đến các kỹ sư của hãng sản xuất phần mềm. - Miễn phí cập nhật và nâng cấp sản phẩm phần mềm phòng chống mã độc trong 12 tháng.
2.	Yêu cầu về dịch vụ	- Hỗ trợ qua điện thoại và các kênh hỗ trợ như: thư điện tử và trên web trong vòng 12 tháng theo gói dịch vụ 24/7 (24 giờ/ ngày, 7 ngày/ tuần bao gồm cả ngày nghỉ).