		Kiểm soát quyền của ứng dụng được phép truy cập vào hệ thống, giám sát và phân loại ứng dụng
	Kiểm soát thiết bị ngoại vi (Device Control)	Kiểm soát theo công nghệ truyền dữ liệu (ổ cứng, thiết bị lưu trữ gắn ngoài, máy in, ổ đĩa CD/DVD, …)
		Có chế độ chặn thiết bị kết nối vào máy tính theo lịch hoặc tùy chọn
		Tự động dò quét thiết bị lưu trữ ngoại vi để tìm kiếm mã độc ngay khi được cắm vào máy tính
		Khả năng tạo danh sách trắng dựa trên số serial
	Kiểm soát truy cập web (Web Control)	Thiết lập chính sách hạn chế truy cập web, ngăn chặn việc truy cập các trang web không mong muốn, website độc hại hoặc lừa đảo, kiểm soát việc truy cập theo danh mục website, theo loại dữ liệu hoặc địa chỉ web chỉ định; Báo cáo về tất cả các hoạt động truy cập web của người dùng trên máy tính

2. Yêu cầu chung đối với các nhà thầu:

* Triển khai và hỗ trợ bảo trì

- Triển khai giải pháp, cài đặt, cấu hình tối ưu sản phẩm trên hệ thống máy trạm, máy chủ thực hiện ngoài giờ hành chánh 8 giờ đến 16 giờ.
- Bảo trì, hỗ trợ 12 tháng thời gian 24/7.

3.Nội dung cần báo giá:

STT	Mặt hàng	Đvt	Số lượng	Đơn giá	Thành tiền
1	Bản quyền chương trình diệt virus cho máy chủ Sever – thời hạn 1 năm	License	20		
2	Bản quyền chương trình diệt virus cho máy trạm – thời hạn 1 năm	License	270		
	Tổng cộng (Bao Gồm VAT và các chi phí theo quy định)				

		phần mềm antivirus từ xa ngoại trừ các máy chủ quản trị;
		Quét các tệp tin khi người dùng truy cập ứng dụng, khi tải xuống từ internet hoặc trong quá trình sửa đổi tệp. Công nghệ quét tối ưu, chỉ quét các file mới và các file đã thay đổi so với lần quét trước Cập nhật các dấu hiệu nhận diện mã độc (Domain, IP, hash,…) trên hệ thống quản trị Có thể tùy chỉnh quét sâu, quét nhanh, quét khu vực quan trọng, quét toàn bộ máy tính, quét system memory, quét boot sector, quét đối tượng được tải khi khởi động OS, quét OS backup Công nghệ phát hiện các trang web và email lừa đảo
		Có khả năng phục hồi (restore) trạng thái ban đầu của các tập tin bị phần mềm độc hại can thiệp mã hóa
		Công nghệ bảo vệ các thư mục chia sẻ khỏi ransomware
	Khả năng bảo vệ nâng cao bằng công nghệ phân tích hành vi và điện toán đám mây	Có công nghệ phân tích hành vi với khả năng nhận diện virus dựa trên việc phân tích hành vi của đối tượng (thay vì chỉ dựa vào cơ sỡ dữ liệu update)
		Có công nghệ kiểm soát sự bất thường, giám sát và chặn các hành động đáng ngờ không phải là điển hình của các máy tính trong mạng của công ty, sử dụng một tập hợp các quy tắc để theo dõi hành vi bất thường. Công nghệ phải có khả năng hoạt động ở chế độ training mode hoặc real time
		Ngoài việc bảo vệ dựa trên cơ sỡ dữ liệu update, phần mềm phải có công nghệ bảo mật đám mây với khả năng kết nối thường xuyên với cơ sỡ dữ liệu điện toán đám mây của hãng để cập nhật các mối đe dọa nguy hiểm mới nhất (mặc dù chương trình chưa kịp kết nối máy chủ để update)
		Công nghệ bảo mật đám mây phải có khả năng xử lý các mối nguy hiểm mới nhất và đang bùng phát, được tạo thành từ hàng triệu người dùng phần mềm antivirus trên toàn thế giới để đảm bảo tính toàn cầu và phổ biến
	Kiểm soát ứng dụng (Application Control)	Quản lý ứng dụng được khởi chạy, ngăn chặn các ứng dụng không mong muốn
		Tự động phân loại các ứng dụng cài đặt trên máy tính vào các nhóm: Tin tưởng, Hạn chế thấp, hạn chế cao, không tin tưởng. Mỗi nhóm có quyền truy cập vào hệ thống khác nhau

		Hỗ trợ xác thực 2 yếu tố (Two-factor Authentication) để tăng cường bảo mật
		Quản lý thông tin trên máy chủ/máy trạm/thiết bị thông minh bao gồm các thông tin sau: - Địa chỉ IP, MAC, Tên máy, Hệ điều hành, Thời gian cập nhật gần nhất của Hệ điều hành trên máy chủ/máy trạm; - Trạng thái kết nối đến máy chủ quản trị; - Thông tin bản vá trên máy chủ/máy trạm; - Trạng thái cập nhật thông tin từ máy chủ quản trị; - Chính sách được thiết lập và các vi phạm trên agent.
		Có khả năng điều khiển agent tối thiểu bao gồm các chức năng sau: - Cho phép phân tích, xóa, sửa tệp tin lây nhiễm mã độc trên máy chủ/máy trạm/thiết bị thông minh; - Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent;
		Tính năng báo cáo, thống kê: - Hiển thị thông tin báo cáo trên Dashboard - Báo cáo về quá trình hoạt động của tất cả các thành phần bảo vệ và phải được phân loại theo mức độ quan trọng - Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo; - Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: EXCEL, PDF, HTML,...;
		Phần mềm quản trị tập trung phải có chính sách bảo vệ linh hoạt khi có sự bùng phát của phần mềm độc hại, tự động thay đổi policy để nâng mức độ bảo vệ cao hơn khi phát hiện số lượng virus bùng phát trong một khoảng thời gian chỉ định cụ thể
		Khả năng tự động move các máy tính mới vào group theo các điều kiện đặt ra và tự động deploy phần mềm antivirus đến các máy tính mới trong group
		Tương thích với các hệ thống SIEM Syslog
2	**Tính năng bảo vệ cho máy trạm:**	
	Phần mềm có khả năng bảo vệ cho các hệ điều hành	Hỗ trợ bảo vệ máy trạm trên các nền tảng hệ điều hành: Windows 7 SP1, 8, 10, 11, Mac, Mobile
	Tính năng phòng chống mã độc	Công nghệ Real-time protection, bảo vệ theo thời gian thực
		Không cho phần mềm độc hại vô hiệu hóa antivirus; đặt mật khẩu để bảo vệ chương trình; không cho phép bất kỳ thiết bị nào khác điều khiển

		Có chế độ chặn thiết bị kết nối vào máy tính theo lịch hoặc tùy chọn
		Tự động dò quét thiết bị lưu trữ ngoại vi để tìm kiếm mã độc ngay khi được cắm vào máy tính.
		Khả năng tạo danh sách trắng dựa trên số serial
	Kiểm soát truy cập web (Web Control)	Thiết lập chính sách hạn chế truy cập web, ngăn chặn việc truy cập các trang web không mong muốn, website độc hại hoặc lừa đảo, kiểm soát việc truy cập theo danh mục website, theo loại dữ liệu hoặc địa chỉ web chỉ định. Báo cáo về tất cả các hoạt động truy cập web của người dùng trên máy tính
	Cập nhật bản vá	Quản lý, cài đặt lỗ hổng bảo mật và bản vá lỗi tập trung của các phần mềm và hệ điều hành Tự động discovery, inventory, notification và tracking tất cả các phần mềm và phần cứng.
	Mã mã hóa dữ liệu	Quản lý mã hóa ổ đĩa BitLocker
		Source cài đặt tích hợp vào phần mềm antivirus, không cần một phần mềm mã hóa riêng biệt và được quản lý qua công cụ quản trị tập trung duy nhất.
II.	**YÊU CẦU TÍNH NĂNG CHO MÁY TRẠM**	
1	**Tính năng quản lý tập trung**	Phần mềm quản trị được cài đặt trên máy chủ quản trị tại doanh nghiệp (on premise);
		Hỗ trợ cài đặt phần mềm quản trị (Security Center) trên các nền tảng hệ điều hành: - Windows: Windows Server 2016, 2019, 2022,… - Hệ điều hành Linux;
		Phân quyền quản trị endpoint theo đơn vị; Endpoint tại đơn vị sẽ giao tiếp với máy chủ đặt tại đơn vị để nhận chính sách, Tác vụ, ... Tùy chỉnh tập trung "Policy" theo chính sách của doanh nghiệp. Policy sẽ áp dụng theo từng Group máy tính chỉ định và có tác dụng ngay lập tức đến từng máy trạm nằm trong Group . Người dùng không có quyền thay đổi các thiết lập (ngoài trừ trường hợp được cấp quyền) Hỗ trợ tạo "Out-of-office policy" để áp dụng 2 chính sách khác nhau dành cho một máy tính (khi nhân viên ở văn phòng và khi nhân viên ở ngoài văn phòng)
		Phần mềm quản trị tập trung có khả năng phát hiện các lỗ hổng bảo mật của hệ điều hành và các phần mềm cài đặt trong hệ thống Quản lý phần mềm, phần cứng: tự động discovery, inventory, notification và tracking tất cả các phần mềm và phần cứng

		Cung cấp khả năng hiển thị rõ ràng hơn về các đối tượng độc hại bằng "thẻ sự cố", mô tả chi tiết quá trình lây nhiễm, với đường lây lan của đối tượng, liệt kê các dữ liệu được thu thập trong thẻ sự cố như: registry, file drop, network Xem toàn bộ phạm vi của bất kỳ mối đe dọa nào. Hiểu nguyên nhân gốc rễ của mối đe dọa và cách nó thực sự xảy ra. Tìm ra đợt tấn công bắt đầu từ đâu? khi nào? mối đe dọa này có còn đang ẩn nấp ở đâu? để loại bỏ các gốc rễ của cuộc tấn công đó Hỗ trợ khả năng truy vấn thông tin mở rộng về đối tượng nguy hiểm trên Threat Intelligence Portal của hãng
		- Phản hồi với thiết bị đầu cuối khi phát hiện mã độc tấn công: - Đưa ra các phản ứng nhanh với các mối đe dọa phức tạp, tinh vi, đang ẩn nấp trước khi chúng gây ra các thiệt hại; - Cô lập các thiết bị đầu cuối bị nhiễm mã độc ra khỏi mạng; - Tự động cách ly các tập tin độc hại đang ẩn nấp, lây lan khắp hệ thống mạng;. Có khả năng tạo chỉ dấu xâm nhập IOC từ các dữ liệu thu thập được Có khả năng quét chỉ dấu IOC trong toàn bộ hệ thống, chọn các hành động sẽ được thực hiện khi quét IOC phát hiện ra đối tượng nguy hiểm: cô lập máy tính khỏi mạng, chạy quét các khu vực quan trọng trên máy tính, tạo bản sao đến vùng cách ly và xóa đối tượng. Có khả năng đưa ra các phản ứng nhanh với các mối đe dọa phức tạp, tinh vi, đang ẩn nấp trước khi chúng gây ra các thiệt hại khác (sau khi đã điều tra): prevent, isolate, Move to Quarantine… Ngăn không cho tập tin độc hại chạy và lây lan khắp mạng trong hoặc sau quá trình điều tra Tự động cách ly các tập tin liên quan đến các mối đe dọa tinh vi đang ẩn nấp trên tất cả các điểm cuối Khả năng ra lệnh cô lập các máy bị nhiễm ra khỏi mạng. Hoặc tạo thao tác quét và cô lập các máy bị nhiễm nếu chúng có các chỉ dấu xâm nhập IoC chỉ định
	Kiểm soát ứng dụng (Application Control)	Quản lý ứng dụng được khởi chạy, ngăn chặn các ứng dụng không mong muốn
		Tự động phân loại các ứng dụng cài đặt trên máy tính vào các nhóm: Tin tưởng, Hạn chế thấp, hạn chế cao, không tin tưởng. Mỗi nhóm có quyền truy cập vào hệ thống khác nhau
		Kiểm soát quyền của ứng dụng được phép truy cập vào hệ thống, giám sát và phân loại ứng dụng.
	Kiểm soát thiết bị ngoại vi (Device Control)	Kiểm soát theo công nghệ truyền dữ liệu (ổ cứng, thiết bị lưu trữ gắn ngoài, máy in, ổ đĩa CD/DVD, …)

		Cập nhật các dấu hiệu nhận diện mã độc (Domain, IP, hash,…) trên hệ thống quản trị Có thể tùy chỉnh quét sâu, quét nhanh, quét khu vực quan trọng, quét toàn bộ máy tính, quét system memory, quét boot sector, quét đối tượng được tải khi khởi động OS, quét OS backup
		Công nghệ phát hiện các trang web và email lừa đảo
		Có khả năng phục hồi (restore) trạng thái ban đầu của các tập tin bị phần mềm độc hại can thiệp mã hóa
		Công nghệ bảo vệ các thư mục chia sẻ khỏi ransomware
	Khả năng bảo vệ nâng cao bằng công nghệ phân tích hành vi và điện toán đám mây	Có công nghệ phân tích hành vi với khả năng nhận diện virus dựa trên việc phân tích hành vi của đối tượng (thay vì chỉ dựa vào cơ sở dữ liệu update)
		Có công nghệ kiểm soát sự bất thường, giám sát và chặn các hành động đáng ngờ không phải là điển hình của các máy tính trong mạng của công ty, sử dụng một tập hợp các quy tắc để theo dõi hành vi bất thường. Công nghệ phải có khả năng hoạt động ở chế độ training mode hoặc real time
		Ngoài việc bảo vệ dựa trên cơ sở dữ liệu update, phần mềm phải có công nghệ bảo mật đám mây với khả năng kết nối thường xuyên với cơ sở dữ liệu điện toán đám mây của hãng để cập nhật các mối đe dọa nguy hiểm mới nhất (mặc dù chương trình chưa kịp kết nối máy chủ để update)
		Công nghệ bảo mật đám mây phải có khả năng xử lý các mối nguy hiểm mới nhất và đang bùng phát, được tạo thành từ hàng triệu người dùng phần mềm antivirus trên toàn thế giới để đảm bảo tính toàn cầu và phổ biến
		Hỗ trợ Cloud Sandbox, cho phép phát hiện các mối đe dọa nâng cao trên máy tính. Cloud Sandbox chạy các tập tin trong một môi trường cloud biệt lập để xác định hành động độc hại nếu có. Nếu Cloud Sandbox phát hiện thấy mối nguy hại, phần mềm endpoint sẽ thực hiện hành động thích hợp để loại bỏ mối đe dọa này trên tất cả các máy tính mà tập tin nguy hiểm được phát hiện.
	Tính năng phát hiện và phản hồi thiết bị đầu cuối (EDR)	Phát hiện sớm các nguy cơ : - Phát hiện tấn công của mã độc dựa theo thông tin: Domain, IP, hash,…; - Giám sát thời gian thực toàn bộ giao tiếp vào và ra máy tính thông qua các Port, địa chỉ IP, ứng dụng,..; Phân tích các hành vi, hoạt động của mã độc trong hệ điều hành để điều tra, xác định nguồn gốc của sự lây nhiễm;

		- Chính sách được thiết lập và các vi phạm trên agent.
		Có khả năng điều khiển agent tối thiểu bao gồm các chức năng sau: - Cho phép phân tích, xóa, sửa tệp tin lây nhiễm mã độc trên máy chủ/máy trạm/thiết bị thông minh; - Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent;
		Tính năng báo cáo, thống kê: - Hiển thị thông tin báo cáo trên Dashboard - Báo cáo về quá trình hoạt động của tất cả các thành phần bảo vệ và phải được phân loại theo mức độ quan trọng - Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo; - Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: EXCEL, PDF, HTML,…;
		Phần mềm quản trị tập trung phải có chính sách bảo vệ linh hoạt khi có sự bùng phát của phần mềm độc hại, tự động thay đổi policy để nâng mức độ bảo vệ cao hơn khi phát hiện số lượng virus bùng phát trong một khoảng thời gian chỉ định cụ thể
		Khả năng tự động move các máy tính mới vào group theo các điều kiện đặt ra và tự động deploy phần mềm antivirus đến các máy tính mới trong group
		Tương thích với các hệ thống SIEM (QRadar, ArcSight, Splunk, Syslog)
		Cybersecurity for IT Online Training : khóa học nâng cao khả năng phát hiện và xử lý sự cố cho IT online.
2	**Tính năng bảo vệ cho Server:**	
	Phần mềm có khả năng bảo vệ cho các hệ điều hành	Hỗ trợ bảo vệ máy chủ trên các nền tảng hệ điều hành: Windows Server 2008 R2 SP1,2012, 2016, 2019, 2022,... và Linux
	Tính năng phòng chống mã độc	Công nghệ Real-time protection, bảo vệ máy chủ theo thời gian thực
		Không cho phần mềm độc hại vô hiệu hóa antivirus; đặt mật khẩu để bảo vệ chương trình; không cho phép bất kỳ thiết bị nào khác điều khiển phần mềm antivirus từ xa ngoại trừ các máy chủ quản trị;
		Quét các tệp tin khi người dùng truy cập ứng dụng, khi tải xuống từ internet hoặc trong quá trình sửa đổi tệp. Công nghệ quét tối ưu, chỉ quét các file mới và các file đã thay đổi so với lần quét trước

PHỤ LỤC

(Kèm theo Thư mời số: 498/TM-BVĐKĐN ngày 26 tháng 4 năm 2025)

1. Nội dung công việc:

STT	MÔ TẢ	
I.	**YÊU CẦU TÍNH NĂNG CHO SERVER**	
1	**Tính năng quản lý tập trung**	Phần mềm quản trị được cài đặt trên máy chủ quản trị tại doanh nghiệp (on premise);
		Hỗ trợ cài đặt phần mềm quản trị (Security Center) trên các nền tảng hệ điều hành: - Windows: Windows Server 2016, 2019, 2022,… - Hệ điều hành Linux;
		Phân quyền quản trị endpoint theo đơn vị; Endpoint tại đơn vị sẽ giao tiếp với máy chủ đặt tại đơn vị để nhận chính sách, cập nhật bản vá, ... Tùy chỉnh tập trung "Policy" theo chính sách của doanh nghiệp. Policy sẽ áp dụng theo từng Group máy tính chỉ định và có tác dụng ngay lập tức đến từng máy trạm nằm trong Group . Người dùng không có quyền thay đổi các thiết lập (ngoài trừ trường hợp được cấp quyền) Hỗ trợ tạo "Out-of-office policy" để áp dụng 2 chính sách khác nhau dành cho một máy tính (khi nhân viên ở văn phòng và khi nhân viên ở ngoài văn phòng)
		Hỗ trợ quản lý, cài đặt từ xa phần mềm của hãng khác trên công cụ quản trị;
		Phần mềm quản trị tập trung có khả năng phát hiện các lỗ hổng bảo mật của hệ điều hành và các phần mềm cài đặt trong hệ thống Quản lý, cài đặt, cập nhật các lỗ hổng bảo mật và các bản vá lỗi tập trung hệ điều hành và các phần mềm của thiết bị đầu cuối Quản lý phần mềm, phần cứng: tự động discovery, inventory, notification và tracking tất cả các phần mềm và phần cứng
		Hỗ trợ quản lý, truy cập các thiết bị đầu cuối, cài đặt từ xa phần mềm của hãng khác trên thiết bị đầu cuối thông qua công cụ quản trị
		Hỗ trợ xác thực 2 yếu tố (Two-factor Authentication) để tăng cường bảo mật
		Quản lý thông tin trên máy chủ/máy trạm/thiết bị thông minh bao gồm các thông tin sau: - Địa chỉ IP, MAC, Tên máy, Hệ điều hành, Thời gian cập nhật gần nhất của Hệ điều hành trên máy chủ/máy trạm; - Trạng thái kết nối đến máy chủ quản trị; - Thông tin bản vá trên máy chủ/máy trạm; - Trạng thái cập nhật thông tin từ máy chủ quản trị;

SỞ Y TẾ ĐỒNG NAI
BỆNH VIỆN ĐA KHOA ĐỒNG NAI

Số: 498 /TM-BVĐKĐN

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

Đồng Nai, ngày 26 tháng 4 năm 2025

THƯ MỜI
V/v chào bảng giá phần mềm diệt virus cho Bệnh viện Đa khoa Đồng Nai.

Kính gửi: Quý nhà thầu quan tâm.

Bệnh viện Đa khoa Đồng Nai có kế hoạch tìm kiếm đơn vị có năng lực phù hợp nhằm thực hiện gói phần mềm diệt virus cho Bệnh viện. Để có cơ sở lập danh mục và xây dựng kế hoạch lựa chọn nhà thầu, Bệnh viện kính mời các nhà thầu quan tâm chào giá các dịch vụ theo danh mục như sau:

(chi tiết theo phụ lục kèm theo)

Yêu cầu chung đối với các nhà thầu:

- Đảm bảo tuân thủ các quy định của Pháp luật hiện hành.
- Có hồ sơ năng lực đầy đủ theo quy định.

Thời hạn nộp báo giá: Từ ngày ra Thư mời đến 16 giờ 30 phút ngày 12 tháng 05 năm 2025

Địa chỉ nhận báo giá: Phòng Công nghệ thông tin (P. 324, lầu 3), bệnh viện Đa khoa Đồng Nai.

Địa chỉ: Số 02 đường Đồng Khởi, phường Bình Đa, thành phố Biên Hòa, tỉnh Đồng Nai

Người liên hệ: Lê Thị Xoang SĐT: 0986712730.

Rất mong được sự quan tâm của các nhà thầu.

Trân trọng.

Nơi nhận:
- Như trên;
- Lưu: VT, CNTT.

GIÁM ĐỐC

SỞ Y TẾ TỈNH ĐỒNG NAI
BỆNH VIỆN ĐA KHOA ĐỒNG NAI

Ngô Đức Tuấn