SỞ Y TẾ THÀNH PHỐ ĐỒNG NAI
BỆNH VIỆN ĐA KHOA ĐỒNG NAI

Số: 123 /TM-BVĐKĐN

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

Đồng Nai, ngày 05 tháng 5 năm 2026

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

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 08 tháng 05 năm 2026

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 Tam Hiệp, Thành phố Đồng Nai.

Người liên hệ: Hồ Huy Bình Chức vụ: Phó Trưởng Phòng CNTT

SĐT: 0933 350 273. Email: cntt.bvdkdn@gmail.com

Rất mong được sự quan tâm của các nhà thầu.

Trân trọng.

GIÁM ĐỐC

SỞ Y TẾ THÀNH PHỐ ĐỒNG NAI
BỆNH VIỆN ĐA KHOA ĐỒNG NAI

Ngô Đức Tuấn

Nơi nhận:
- Quý nhà thầu quan tâm;
- Lưu: VT, CNTT.
(Xoanglt)

PHỤ LỤC

(kèm theo Thư mời số: 123 /TM-BVĐKĐN ngày 05 tháng 5 năm 2026)

1. *Nội dung công việc:*

STT	MÔ TẢ
I	**YÊU CẦU TÍNH NĂNG ĐỐI VỚI MÁY CHỦ:**
1	**Chất lượng của phần mềm:**
	Có chức năng kết nối, chia sẻ thông tin từ hệ thống quản lý tập trung với hệ thống kỹ thuật của cơ quan chức năng theo tiêu chuẩn, quy chuẩn quốc gia và yêu cầu kỹ thuật tại Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.
	Ngôn ngữ phần mềm: hỗ trợ tiếng Việt hoặc/và tiếng Anh
2	**Phần mềm bảo vệ cho các hệ điều hành:**
	Máy trạm và máy chủ: Windows, Linux, MacOS…
	Bản quyền phải bảo vệ cho thiết bị Android và iOS của nhân viên (không mua thêm)
	Bản quyền phải bảo vệ cho Microsoft Office 365, tích hợp bảo vệ Microsoft Office 365 (không mua thêm)
3	**Khả năng bảo vệ của phần mềm:**
3.1	**Khả năng bảo vệ chống Malware**
	Bảo vệ trong thời gian thực chống lại các loại malware
	Khả năng tự bảo vệ: Không cho phần mềm độc hại vô hiệu hóa; đặt mật khẩu để bảo vệ chương trình; ngăn chặn quá trình điều khiển phần mềm antivirus từ máy tính điều khiển từ xa
	Công nghệ quét thông minh loại trừ các tập tin đã quét (chỉ quét những files mới và những files có sự thay đổi so với lần quét virus gần nhất)
	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
	Có thể ra lệnh quét bằng tay hoặc theo lịch
	Công nghệ phát hiện các trang web và email lừa đảo
3.2	**Khả năng bảo vệ chống Ransomware**
	Công nghệ khắc phục hậu quả, phục hồi (rolling back) trong thời gian thực, nhằm phục hồi (restore) tự động ngay lập tức trạng thái ban đầu của các tập tin bị phần mềm độc hại can thiệp mã hóa
	Công nghê chống ransomware bảo vệ riêng cho hệ điều hành Windows Server
	Công nghệ bảo vệ các thư mục chia sẻ khỏi ransomware

	Có công nghệ bảo vệ các đuôi file chỉ định, chỉ cho phép các chương trình tin tưởng mới được phép can thiệp chỉnh sửa các loại file được bảo vệ, nhằm bảo vệ dữ liệu của doanh nghiệp khỏi ransomware
3.3	**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
	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.
3.4	**Khả năng bảo vệ chống hacker và tấn công mạng**
	Cho phép giám sát trong thời gian thực toàn bộ giao tiếp vào và ra máy tính thông qua các Port, địa chỉ IP, ứng dụng
	Khả năng cho phép hoặc ngăn chặn các port chỉ định
	Hệ thống phát hiện các cuộc tấn công, giúp theo dõi, phát hiện và ngăn chặn các cuộc tấn công mạng, có các báo cáo chi tiết
3.5	**Khả năng quét và ngăn cản việc khai thác lỗ hổng bảo mật**
	Khả năng quét toàn bộ hệ điều hành và các phần mềm để phát hiện lỗ hổng bảo mật
	Khả năng hoạt động theo thời gian thực để phát hiện lỗ hổng bảo mật khi chạy các ứng dụng
	Thiết lập mức độ quan trọng của các lỗ hổng bảo mật, và đưa ra khuyến cáo để vá lỗ hổng bảo mật đó.

	Có khả năng ngăn chặn hacker và các phần mềm độc hại khai thác lỗ hổng bảo mật của hệ điều hành và các phần mềm, mặc dù các lỗ hổng chưa được vá lỗi
3.6	**Khả năng Kiểm soát thiết bị (Device Control)**
	Quản lý thiết bị (cho phép dùng hoặc không dùng) dựa trên phân loại của thiết bị hoặc loại bus kết nối
	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
3.7	**Khả năng kiểm soát trang Web (Web Control)**
	Chính sách ngăn web theo địa chỉ chỉ định, theo phân loại sẵn có (game, tin tức, mạng xã hội, web mail,...), theo loại dữ liệu (Video, Sound,..) hoặc theo mức hạng đánh giá
	Khả năng tự tạo các nhóm phân loại web theo chính sách riêng
	Báo cáo về tất cả các hoạt động truy cập web của người dùng trên máy tính
3.8	**Khả năng Kiểm soát ứng dụng (Application Control)**
	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
	Tạo danh sách trắng (cho phép chạy) hoặc danh sách đen (không cho phép chạy) theo từng ứng dụng chỉ định, theo nhóm các ứng dụng chỉ định, theo nhóm phân loại ứng dụng sẵn có (Office, Chat, Media,..), theo đánh giá hạng bảo mật và uy tín của ứng dụng
	Có khả năng đưa một ứng dụng vào vùng tin tưởng và loại trừ
	Khả năng hạn chế một số hành động cụ thể của các ứng dụng được chỉ định (truy cập thiết bị, truy cập registry, tự sao chép, nhân đôi tiến trình,...)
	Cloud Discovery, giám sát việc sử dụng các dịch vụ đám mây trên Windows
	Cloud Blocking, chặn truy cập đến các dịch vụ đám mây trên Windows
	Data discovery bảo vệ dữ liệu nhạy cảm trên Microsoft sharepoint, Onedrive, Teams
3.9	**Khả năng mã hóa dữ liệu (Data Encryption)**
	Mã hóa mức File, Folder, Full Disk, ổ đĩa di động (hỗ trợ chế độ Portable File Manager để có thể mở dữ liệu trong ổ đĩa di động bị mã hóa ở các máy tính chưa cài đặt Endpoint)
	Chế độ END USER TRANSPARENCY, hoạt động trong suốt, người dùng cuối có thể không nhận thức được công nghệ mã hóa đang chạy.

	Chế độ PRE-BOOT AUTHENTICATION trong mã hóa Full Disk, đăng nhập một lớp trước khi hệ điều hành khởi động
	Source cài đặt tích hợp vào phân mềm antivirus, không cần một phần mềm mã hóa riêng biệt và được quản lý qua công cụ quản trị tập trung duy nhất
3.10	**Khả năng cung cấp các tính năng quản trị hệ thống (System Management)**
	Hỗ trợ cài đặt triển khai hệ điều hành và các phần mềm của hãng thứ 3 từ xa
	Quản lý, cài đặt lỗ hổng bảo mật và bản vá lỗi tập trung của các phần mềm và hệ điều hành
	Quản lý phần mềm, phần cứng: tự động discovery, inventory, notification và tracking tất cả các phần mềm và phần cứng
	Tương thích với các hệ thống SIEM (QRadar, ArcSight, Splunk, Syslog)
3.11	**Khả năng cung cấp tính năng phân tích điều tra nguồn gốc tấn công**
	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
3.12	**Khả năng cung cấp tính năng quét dựa trên chỉ dấu xâm nhập (IOC Scan)**
	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.
3.14	**Khả năng phản ứng nhanh chóng để tránh thiệt hại thêm**
	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
	Cybersecurity fo IT Online Training : khóa học nâng cao khả năng phát hiện và xử lý sự cố cho online IT.
4	**Khả năng quản lý tập trung của phần mềm :**
4.1	**Khả năng triển khai từ xa**
	Phần mềm quản lý tập trung có thể cài trên máy tính Windows hoặc Linux đặt tại hệ thống của khách hàng
	Phần mềm quản trị tập trung được quản lý qua On-premises console hoặc qua Web Console
	Từ phần mềm quản trị tập trung, có thể triển khai cài đặt từ xa chương trình antivirus đến tất cả các máy tính trong hệ thống mạng
	Có tính năng tự động remove phần mềm antivirus không tương thích trong quá trình triển khai
	Hỗ trợ phương pháp cho nhân viên tham gia vào quá trình triển khai. Chỉ cần click 1 lần vào file cài đặt tự động, thì chương trình antivirus tự động cài đặt vào máy trạm và kết nối về công cụ quản trị tập trung
	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
4.2	**Khả năng quản lý tập trung**
	Quản lý tập trung tình hình virus trên tất cả các máy trạm và máy chủ trong toàn bộ hệ thống
	Thiết lập tập trung cấu hình của phần mềm antivirus theo chính sách của tổ chức. Chính sách sẽ áp dụng theo từng group máy tính chỉ định. Người dùng không có quyền thay đổi các thiết lập (ngoài trừ trường hợp được cấp quyền)
	Cập nhật cơ sở dữ liệu virus tập trung, theo lịch
	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
	Phần mềm quản trị tập trung có khả năng quản lý tập trung tất cả các tập tin chứa mã độc (hoặc nghi ngờ chứa mã độc) đã bị xử lý bởi chương trình antivirus được cài đặt trên tất cả các máy tính trong hệ thống mạng. Tập tin được lưu trữ với định dạng an toàn, giúp tránh trường hợp mất mát dữ liệu do nhận dạng lầm

	Phần mềm quản trị tập trung cho phép người quản trị có thể đặt lịch quét định kỳ, cũng như ra lệnh quét tại một thời điểm bất kỳ, cho các máy trạm tham gia hệ thống. Việc này có thể được thực hiện theo từng nhóm máy tính khác nhau.
	Khả năng quản lý tập trung theo mô hình phân cấp master - slave
	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
	Phần mềm quản trị tập trung phải có khả năng cho phép ra lệnh xóa dữ liệu chỉ định từ xa khỏi máy tính của người dùng.
4.3	**Khả năng quản lý báo cáo và sự kiện**
	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 tạo ra các báo cáo theo mẫu chuẩn hoặc tuỳ chỉnh để tạo báo cáo với các thông tin cần thiết
	Có tính năng thống kê danh sách các máy tính có cùng một điều kiện chỉ định giống nhau
	Báo cáo có thể đặt lịch để gửi qua email và có thể lưu trữ dưới các định dạng HTML, XML, PDF
	Lưu trữ tập trung tất cả các sự kiện. Event phải được phân loại mức độ quan trọng
	Phải tích hợp được với các hệ thống SIEM
	Hỗ trợ thiết lập gửi thông báo tức thời các sự kiện nghiêm trọng (qua Email, SNMP, SMS, chạy Script)
5	**Hỗ trợ kỹ thuật**
	Đơn vị cung cấp phần mềm phải có tổng đài hỗ trợ kỹ thuật từ xa tại Việt Nam với thời gian hỗ trợ tất cả các ngày trong tuần.
	Nhân viên trực tổng đài hỗ trợ kỹ thuật phải được đào tạo và có được chứng chỉ từ hãng
II	**YÊU CẦU TÍNH NĂNG ĐỐI VỚI MÁY TRẠM:**
1	Chất lượng của phần mềm:
	Có chức năng kết nối, chia sẻ thông tin từ hệ thống quản lý tập trung với hệ thống kỹ thuật của cơ quan chức năng theo tiêu chuẩn, quy chuẩn quốc gia và yêu cầu kỹ thuật tại Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018.

	Ngôn ngữ phần mềm: hỗ trợ tiếng Việt hoặc/và tiếng Anh
2	Phần mềm bảo vệ cho các hệ điều hành
	Máy trạm và máy chủ: Windows, Linux, MacOS…
	Bản quyền phải bảo vệ cho thiết bị Android và iOS của nhân viên (không mua thêm)
3	Khả năng bảo vệ của phần mềm:
3.1	Khả năng bảo vệ chống Malware
	Bảo vệ trong thời gian thực chống lại các loại malware
	Khả năng tự bảo vệ: Không cho phần mềm độc hại vô hiệu hóa; đặt mật khẩu để bảo vệ chương trình; ngăn chặn quá trình điều khiển phần mềm antivirus từ máy tính điều khiển từ xa
	Công nghệ quét thông minh loại trừ các tập tin đã quét (chỉ quét những files mới và những files có sự thay đổi so với lần quét virus gần nhất)
	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
	Có thể ra lệnh quét bằng tay hoặc theo lịch
	Công nghệ phát hiện các trang web và email lừa đảo
3.2	Khả năng bảo vệ chống Ransomware
	Công nghệ khắc phục hậu quả, phục hồi (rolling back) trong thời gian thực, nhằm phục hồi (restore) tự động ngay lập tức trạng thái ban đầu của các tập tin bị phần mềm độc hại can thiệp mã hóa
	Công nghê chống ransomware bảo vệ riêng cho hệ điều hành Windows Server
	Công nghệ bảo vệ các thư mục chia sẻ khỏi ransomware
	Có công nghệ bảo vệ các đuôi file chỉ định, chỉ cho phép các chương trình tin tưởng mới được phép can thiệp chỉnh sửa các loại file được bảo vệ, nhằm bảo vệ dữ liệu của doanh nghiệp khỏi ransomware
3.3	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
	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.
3.4	Khả năng bảo vệ chống hacker và tấn công mạng
	Cho phép giám sát trong thời gian thực toàn bộ giao tiếp vào và ra máy tính thông qua các Port, địa chỉ IP, ứng dụng
	Khả năng cho phép hoặc ngăn chặn các port chỉ định
	Hệ thống phát hiện các cuộc tấn công, giúp theo dõi, phát hiện và ngăn chặn các cuộc tấn công mạng, có các báo cáo chi tiết
3.5	Khả năng quét và ngăn cản việc khai thác lỗ hổng bảo mật
	Khả năng quét toàn bộ hệ điều hành và các phần mềm để phát hiện lỗ hổng bảo mật
	Khả năng hoạt động theo thời gian thực để phát hiện lỗ hổng bảo mật khi chạy các ứng dụng
	Thiết lập mức độ quan trọng của các lỗ hổng bảo mật, và đưa ra khuyến cáo để vá lỗ hổng bảo mật đó.
	Có khả năng ngăn chặn hacker và các phần mềm độc hại khai thác lỗ hổng bảo mật của hệ điều hành và các phần mềm, mặc dù các lỗ hổng chưa được vá lỗi
3.6	Khả năng Kiểm soát thiết bị (Device Control)
	Quản lý thiết bị (cho phép dùng hoặc không dùng) dựa trên phân loại của thiết bị hoặc loại bus kết nối
	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
3.7	Khả năng kiểm soát trang Web (Web Control)

	Chính sách ngăn web theo địa chỉ chỉ định, theo phân loại sẵn có (game, tin tức, mạng xã hội, web mail,...), theo loại dữ liệu (Video, Sound,..) hoặc theo mức hạng đánh giá
	Khả năng tự tạo các nhóm phân loại web theo chính sách riêng
	Báo cáo về tất cả các hoạt động truy cập web của người dùng trên máy tính
3.8	Khả năng Kiểm soát ứng dụng (Application Control)
	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
	Tạo danh sách trắng (cho phép chạy) hoặc danh sách đen (không cho phép chạy) theo từng ứng dụng chỉ định, theo nhóm các ứng dụng chỉ định, theo nhóm phân loại ứng dụng sẵn có (Office, Chat, Media,..), theo đánh giá hạng bảo mật và uy tín của ứng dụng
	Có khả năng đưa một ứng dụng vào vùng tin tưởng và loại trừ
	Khả năng hạn chế một số hành động cụ thể của các ứng dụng được chỉ định (truy cập thiết bị, truy cập registry, tự sao chép, nhân đôi tiến trình,...)
	Cloud Discovery, giám sát việc sử dụng các dịch vụ đám mây trên Windows
3.9	Khả năng cung cấp các tính năng quản trị hệ thống (System Management)
	Quản lý phần mềm, phần cứng: tự động discovery, inventory, notification và tracking tất cả các phần mềm và phần cứng
	Tương thích với các hệ thống SIEM (QRadar, ArcSight, Splunk, Syslog)
3.10	Khả năng cung cấp tính năng phân tích điều tra nguồn gốc tấn công
	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
4	Khả năng quản lý tập trung của phần mềm:
4.1	Khả năng triển khai từ xa
	Phần mềm quản lý tập trung có thể cài trên máy tính Windows hoặc Linux đặt tại hệ thống của khách hàng

	Phần mềm quản trị tập trung được quản lý qua On-premises console hoặc qua Web Console
	Từ phần mềm quản trị tập trung, có thể triển khai cài đặt từ xa chương trình antivirus đến tất cả các máy tính trong hệ thống mạng
	Có tính năng tự động remove phần mềm antivirus không tương thích trong quá trình triển khai
	Hỗ trợ phương pháp cho nhân viên tham gia vào quá trình triển khai. Chỉ cần click 1 lần vào file cài đặt tự động, thì chương trình antivirus tự động cài đặt vào máy trạm và kết nối về công cụ quản trị tập trung
	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
4.2	Khả năng quản lý tập trung
	Quản lý tập trung tình hình virus trên tất cả các máy trạm và máy chủ trong toàn bộ hệ thống
	Thiết lập tập trung cấu hình của phần mềm antivirus theo chính sách của tổ chức. Chính sách sẽ áp dụng theo từng group máy tính chỉ định. Người dùng không có quyền thay đổi các thiết lập (ngoài trừ trường hợp được cấp quyền)
	Cập nhật cơ sở dữ liệu virus tập trung, theo lịch
	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
	Phần mềm quản trị tập trung có khả năng quản lý tập trung tất cả các tập tin chứa mã độc (hoặc nghi ngờ chứa mã độc) đã bị xử lý bởi chương trình antivirus được cài đặt trên tất cả các máy tính trong hệ thống mạng. Tập tin được lưu trữ với định dạng an toàn, giúp tránh trường hợp mất mát dữ liệu do nhận dạng lầm
	Phần mềm quản trị tập trung cho phép người quản trị có thể đặt lịch quét định kỳ, cũng như ra lệnh quét tại một thời điểm bất kỳ, cho các máy trạm tham gia hệ thống. Việc này có thể được thực hiện theo từng nhóm máy tính khác nhau.
	Khả năng quản lý tập trung theo mô hình phân cấp master - slave
	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
	Phần mềm quản trị tập trung phải có khả năng cho phép ra lệnh xóa dữ liệu chỉ định từ xa khỏi máy tính của người dùng.
4.3	Khả năng quản lý báo cáo và sự kiện
	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 tạo ra các báo cáo theo mẫu chuẩn hoặc tuỳ chỉnh để tạo báo cáo với các thông tin cần thiết
	Có tính năng thống kê danh sách các máy tính có cùng một điều kiện chỉ định giống nhau
	Báo cáo có thể đặt lịch để gửi qua email và có thể lưu trữ dưới các định dạng HTML, XML, PDF..
	Lưu trữ tập trung tất cả các sự kiện. Event phải được phân loại mức độ quan trọng
	Phải tích hợp được với các hệ thống SIEM
	Hỗ trợ thiết lập gửi thông báo tức thời các sự kiện nghiêm trọng (qua Email, SNMP, SMS, chạy Script)
5	Hỗ trợ kỹ thuật
	Đơn vị cung cấp phần mềm phải có tổng đài hỗ trợ kỹ thuật từ xa tại Việt Nam với thời gian hỗ trợ tất cả các ngày trong tuần.
	Nhân viên trực tổng đài hỗ trợ kỹ thuật phải được đào tạo và có được chứng chỉ từ hãng

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.
- 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	300		
	Tổng cộng (Bao Gồm VAT và các chi phí theo quy định)				