Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

- Tên dự toán mua sắm: Lựa chọn đơn vị cung cấp Bản quyền phần mềm bảo mật của Bệnh viện ĐKKV Long Khánh.

- Tên gói thầu: Lựa chọn đơn vị cung cấp Bản quyền phần mềm bảo mật của Bệnh viện ĐKKV Long Khánh.

- Chủ đầu tư: Bệnh viện đa khoa khu vực Long Khánh.

- Nguồn vốn: Quỹ phát triển hoạt động sự nghiệp.

- Thời gian thực hiện: 365 ngày kể từ ngày hợp đồng có hiệu lực.

1.2. Yêu cầu về kỹ thuật

Nhà thầu chào hàng hóa phải đáp ứng các thông số kỹ thuật như sau:

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
	Bản quyền phần mềm bảo mật dùng cho máy tính	Bản quyền	1 năm	250
1	**Chất lượng của sản phẩm Endpoint Protection**			
1.1	Sản phẩm Endpoint Protection là sản phẩm nổi tiếng, có trong danh sách đánh giá và được chứng chứng nhận bởi AV-Test, AV-Comparatives			
1.2	Phần mềm phải được sử dụng nhiều và có uy tín tại Việt Nam, đạt được sự công nhận và chứng minh bằng các giải thưởng do người tiêu dùng bình chọn			
1.3	Phải hỗ trợ cộng thêm thời gian triển khai (cộng trực tiếp vào thời gian sử dụng bản quyền)			
1.4	Có hỗ trợ phiên bản tiếng Việt dành cho bản cài đặt ở phía người dùng			
1.5	Sản phẩm có tên trong danh mục các sản phẩm phòng, chống phần mềm độc hại đáp ứng được yêu cầu kỹ thuật theo Chỉ thị số 14/CT-TTg theo kết quả đánh giá của hội đồng đánh giá tại chuyên mục tiêu chuẩn, chất lượng và đánh giá phù hợp của cổng thông tin điện tử của Bộ Thông Tin và Truyền Thông.			
2	**Sản phẩm Endpoint Protection cung cấp khả năng bảo vệ cho các hệ điều hành**			
2.1	Máy trạm: Windows, Linux, Mac			
2.2	Máy chủ: Windows, Linux			

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
2.3	Bản quyền phải bảo vệ cho thiết bị Android và iOS của nhân viên (x2 mobile không cần mua thêm)			
2.4	Hỗ trợ IPv6			
3	**Khả năng bảo vệ của sản phẩm Endpoint Protection**			
3.1	Khả năng bảo vệ Malware			
3.1.1	Bảo vệ trong thời gian thực chống lại tất cả các loại malware			
3.1.2	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			
3.1.3	Khả năng phát hiện và tiêu diệt malware lây nhiễm qua 3 con đường: file, web, mail			
3.1.4	Có 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), hỗ trợ dò quét các tập tin nén.			
3.1.5	Có thể tùy chỉnh quét sâu, quét nhanh, quét khu vực quan trọng, quét toàn bộ máy tính, quét virus trong bộ nhớ			
3.1.6	Có thể ra lệnh quét bằng tay hoặc theo lịch			
3.1.7	Tính năng phát hiện các trang web và email lừa đảo			
3.1.8	Cung cấp khả năng dò quét lưu lượng HTTPS, HTTP, FTP để tìm kiếm virus, spyware hay các loại mã độc khác.			
3.2	Khả năng bảo vệ bằng công nghệ điện toán đám mây			
3.2.1	Ngoài việc bảo vệ dựa trên cơ sỡ dữ liệu update, phần mềm phải có 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)			
3.2.2	Cơ sở dữ liệu trên đám mây phải chứa 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			
3.2.3	Đám mây phải có hệ thống phản ứng khẩn cấp để cung cấp khả năng phản ứng nhanh nhất với các tập tin và trang web độc hại nguy hiểm mới nhất			
3.3	Khả năng bảo về bằng công nghệ phân tích hành vi, phòng thủ chủ động			

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
3.3.1	Có công nghệ Phân tích hành vi "Behavioral Analysis" 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)			
3.3.2	Có công nghệ đặt biệt theo dõi hệ thống "Remediation Engine" để phục hồi các hành động của đối tượng nguy hiểm gây ra trên máy tính (đặc biệt là đối phó với các dòng virus mã hóa), nhằm phục hồi lại trạng thái ban đầu của các tập tin bị các đoạn mã độc hại can thiệp			
3.3.3	Công nghệ Anti-cryptor (chống virus mã hóa) bảo vệ cho hệ thống server			
3.3.4	Khả năng bỏ qua các đối tượng tin tưởng, có chữ kỹ số			
3.4	Khả năng bảo vệ chống hacker và tấn công mạng			
3.4.1	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,			
3.4.2	Khả năng cho phép hoặc ngăn chặn các port chỉ định			
3.4.3	Hệ thống phát hiện các cuộc tấn công (HIDS) giúp theo dõi, phát hiện và ngăn chặn các cuộc tấn công mạng			
3.4.4	Khả năng từ chối truy cập từ các máy tính bị nhiễm mã độc hoặc có các hành động tấn công mạng cùng khả năng thêm loại trừ các địa chỉ IP tin tưởng			
3.4.5	Cung cấp khả năng ngăn chặn tấn công mạng và báo cáo nguồn lây nhiễm.			
3.5	Khả năng ngăn chặn việc khai thác lỗ hổng bảo mật			
3.5.1	Khả năng quét toàn bộ hệ điều hành và các phần mềm để phát hiện lỗ hổng bảo mật			
3.5.2	Khả năng hoạt động theo thời gian thực để phát hiện lỗ hổng bảo mật khi chạy các ứng dụng			
3.5.3	Thiết lập mức độ quan trọng của các lỗ hổng bảo mật, và đưa ra khuyến cáo để vá lỗ hổng bảo mật đó.			
3.5.4	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)			
3.6.1	Quản lý thiết bị (cho phép dùng hoặc không dùng) dựa trên phân loại của thiết bị hoặc loại bus kết nối			
3.6.2	Khả năng tạo danh sách trắng dựa trên số serial			
3.6.3	Khả năng phân quyền Read/Write để quản lý thiết bị			

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
3.6.4	Tương thích với AD với khả năng áp dụng các chính sách khác nhau cho các nhóm người dùng và máy tính khác nhau			
3.6.5	Cung cấp tính năng Anti-bridging cho máy trạm Windows để năn chặn việc thiết lập trái phép kết nối vào mạng nội bô bằng cách vượt qua các công cụ phòng thủ mạng biên. Cung cấp khả năng cấm các kết nối có dây, Wi-fi và modem.			
3.6.6	Tự động dò quét thiết bị lưu trữ ngoại vi để tìm kiếm mã độc ngay khi được cắm vào máy tính.			
3.6.7	Giải pháp cung khả năng cấu hình mạng Wi-fi dựa trên tên, kiểu xác thực, kiểu mã hóa sau đó có thể sử dụng để cho phép hoặc ngăn chặn kết nối Wi-fi.			
3.7	Khả năng kiểm soát trang Web (Web Control)			
3.7.1	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			
3.7.2	Khả năng tự tạo các nhóm phân loại web theo chính sách riêng			
3.7.3	Báo cáo về tất cả các hoạt động truy cập web của người dùng trên máy tính			
3.7.4	Tương thích với AD với khả năng áp dụng các chính sách khác nhau cho các nhóm người dùng và máy tính khác nhau			
3.8	Khả năng Kiểm soát ứng dụng (Application Control)			
3.8.1	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, Chát, Media,..), theo đánh giá hạng bảo mật và uy tín của ứng dụng			
3.8.2	Có các quy tắc để kiểm tra giám sát hoạt động của các ứng dụng, khả năng đáng giá danh tiếng của ứng dụng, từ đó tự động phân loại mức độ tin tưởng của ứng dụng vào một trong bốn nhóm mặc định: Tin tưởng, giới hạn thấp, giới hạn cao, không tin tưởng			
3.8.3	Có tùy chỉnh mặc định cấm chạy tất cả ứng dụng cũng như khả năng đưa một ứng dụng vào vùng tin tưởng và loại trừ			
3.8.4	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,...)			

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
3.8.5	Tương thích với AD với khả năng áp dụng các chính sách khác nhau cho các nhóm người dùng và máy tính khác nhau			
3.8.6	Cung cấp khả năng thiết lập danh sách trắng (whitelist) các ứng dụng dựa trên chứng thư số, MD5, SHA256, metadata, đường dẫn file.			
3.8.7	Giải pháp cung cấp khả năng kiểm soát PowerShell scripts			
3.8.8	Giải pháp có chế độ "test" có cung report để kiểm tra trước khi thực hiện chặn các ứng dụng.			
3.8.9	Cloud Discovery: giám sát việc sử dụng các dịch vụ đám mây trên Windows			
4	**Khả năng quản lý tập trung của sản phẩm Endpoint Protection**			
4.1	Khả năng triển khai từ xa			
4.1.1	Công cụ quản trị tập trung được quản lý qua Console hoặc qua Web			
4.1.2	Từ công cụ 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 (trong quá trình triển khai sẽ tự động remove phần mềm antivirus không tương thích)			
4.1.3	Có khả năng tự động cài đặt từ xa chương trình antivirus đến các máy trạm mới xuất hiện (hoặc vừa cài lại hệ điều hành) trong hệ thống mạng			
4.1.4	Hỗ trợ phương pháp triển khai nhanh tại máy trạm, bằng cách tạo file cài đặt "stand-alone". Tại máy trạm, chỉ cần click 1 lần vào file cài đặt "stand-alone" thì chương trình antivirus tự động cài đặt vào máy trạm			
4.1.5	Hỗ trợ cài đặt phần mềm antivirus bảo vệ cho các thiết bị mobile từ xa (nếu có nhu cầu)			
4.2	Khả năng quản lý từ xa			
4.2.1	Phần mềm có khả năng triển khai quản lý qua Cloud hoặc On-premise			
4.2.2	Từ công cụ quản trị tập trung, có khả năng tạo các "Group" máy tính khác nhau với khả năng áp dụng các chính sách khác nhau cho từng group máy tính này			
4.2.3	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)			

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
4.2.4	"Update" cơ sỡ dữ liệu virus tập trung theo lịch từ công cụ quản trị tập trung			
4.2.5	Tạo các "Task" ra lệnh quét virus (Full Scan, Quick Scan,…) các máy trạm chỉ định (có thể đặt lịch quét định kỳ)			
4.2.6	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)			
4.2.7	Từ công cụ quản trị tập trung, người quản trị có khả năng quản lý tập trung tính năng "Endpoint Control"			
4.2.8	Từ công cụ quản trị tập trung có thể can thiệp thay đổi tùy chỉnh phần mềm antivirus cài trên một máy trạm bất kỳ (khi cần thiết)			
4.2.9	Công cụ quản trị tập trung phải tương thích với AD với khả năng áp dụng các chính sách "Endpoint Control" khác nhau cho từng nhóm người dùng khác nhau			
4.2.10	Công cụ quản trị tập trung có khả năng quản lý lỗ hổng bảo mật và bản vá lỗi tập trung cho các sản phẩm của Microsoft và các phần mềm khác được cài đặt trên tất cả các máy tính trong hệ thống mạng			
4.2.11	Công cụ 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			
4.2.12	Công cụ quản trị tập trung phải hỗ trợ khả năng quản lý theo mô hình phân cấp "Master – Slave" cho công ty có nhiều chi nhánh, với khả năng cấu hình chi tiết các quyền được quản trị cho IT các chi nhánh			
4.2.13	Đối với các phân vùng mạng không khả dụng cho mô hình quản lý phân cấp "Master - Slave", cần hỗ trợ tính năng thiết lập một hoặc một số máy trạm trong phân vùng mạng này làm trung gian để giao tiếp với máy chủ quản lý. Các máy trạm trong phân vùng mạng này không giao tiếp trực tiếp với máy chủ quản lý mà thông qua máy trạm trung gian, giúp tiết kiệm băng thông.			
4.2.14	Chỉ cần dùng một giao diện quản lý tập trung duy nhất cho phép quản lý phần mềm bảo vệ dưới các máy chủ, máy trạm và thiết bị di động.			

Stt	Danh mục thiết bị	Đvt	Thời hạn	Số lượng
4.2.15	Khả năng cung cấp tính năng phân tích điều tra nguồn gốc tấn công			
4.2.16	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			
4.2.17	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 tập trung			
4.3.1	Hiển thị thông tin báo cáo trên Dashboard.			
4.3.2	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			
4.3.3	Cho phép tạo ra các báo cáo theo mẫu chuẩn hoặc tuỳ chỉnh để tạo báo cáo với các thông tin cần thiết			
4.3.4	Tính năng "Computer Selections" để chứa đựng danh sách các máy tính có cùng một điều kiện chỉ định giống nhau			
4.3.5	Báo cáo có thể đặt lịch để gửi qua email và có thể lưu trữ dưới các định dạng HTML, XML, PDF			
4.3.6	Lưu trữ tập trung tất cả các "Event". Event phải được phân loại mức độ quan trọng			
4.3.7	Phải tích hợp được với các hệ thống SIEM (QRadar, ArcSight, Splunk, Syslog)			
4.3.7	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**			
5.1	Hãng phải có tổng đài hỗ trợ kỹ thuật từ xa tại Việt Nam với thời gian hỗ trợ tất cả các ngày trong tuần, kể cả ngày lễ (từ 8h sáng đến 10h đêm)			
5.2	Nhân viên trực tổng đài hỗ trợ kỹ thuật phải được đào tạo và có được chứng chỉ từ hãng			

1.3. Các yêu cầu khác

- Giá đã bao gồm toàn bộ chi phí vận chuyển tới địa điểm giao hàng tại Bệnh viện đa khoa khu vực Long Khánh. Địa chỉ: Số 911, đường 21/4, P. Bình Lộc, T.Đồng Nai.

Mục 2. Bản vẽ

- Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

- Các kiểm tra và thử nghiệm cần tiến hành gồm có: Kiểm tra và nghiệm thu chất lượng sản phẩm theo quy định.
- Trường hợp cơ quan chức năng có kết luận về chất lượng sản phẩm không đúng theo gói thầu cung cấp thì Chủ đầu tư hoàn trả sản phẩm và yêu cầu Nhà thầu bồi thường thiệt hại theo mức thiệt hại thực tế.