|  |  |
| --- | --- |
| SỞ Y TẾ BẮC NINH  **BỆNH VIỆN ĐA KHOA TỈNH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc**  *Bắc Ninh, ngày 19 tháng 11 năm 2021* |

**THƯ MỜI BÁO GIÁ**

**Gói thầu Mua sắm phần mềm diệt virus dùng cho hệ thống máy chủ, máy trạm**

***Kính gửi:* Các Quý công ty**

*Căn cứ Luật đấu thầu số 43/2013/QH13 ngày 26/11/2013;*

*Căn cứ Nghị định số 63/2014/NĐ-CP ngày 26/6/2014 của Chính phủ quy định chi tiết thi hành một số điều của Luật đấu thầu về lựa chọn nhà thầu;*

*Căn cứ Luật Đầu tư công số 39/2019/QH14 ngày 13/6/2019;*

*Căn cứ Nghị định số 40/2020/NĐ-CP ngày 06/04/2020 của Chính phủ Quy định chi tiết thi hành một số điều của Luật Đầu tư công;*

*Căn cứ Quyết định số 11/2021/QĐ-UBND ngày 19/05/2021 của UBND tỉnh Bắc Ninh ban hành Quy định quản lý đầu tư đầu công trên địa bàn tỉnh Bắc Ninh;*

*Căn cứ Quyết định số 5907/QĐ-BVT ngày 16/9/2021 của Giám đốc Bệnh viện đa khoa tỉnh Bắc Ninh về việc phê duyệt dự án số 4a: Đầu tư trang thiết bị y tế, hành chính, công nghệ thông tin khác thuộc Dự án: cải tạo, nâng cấp cơ sở vật chất; xây dựng mới khu khám và điều trị theo yêu cầu và mua sắm trang thiết bị*

Bệnh viện đa khoa tỉnh Bắc Ninh đề nghị **các Quý công ty** gửi báo giá danh mục, số lượng, yêu cầu kỹ thuật gói thầu “Mua sắm phần mềm diệt virus dùng cho hệ thống máy chủ, máy trạm” theo phụ lục chi tiết đính kèm.

Mục đích báo giá: Làm cơ sở xây dựng dự toán kinh phí

Thời điểm gửi báo giá: Trước 10h00 ngày 23 tháng 11 năm 2021

Yêu cầu báo giá: 01 bản chính bằng tiếng Việt

Địa điểm nhận báo giá: Phòng HCQT – BVĐK tỉnh Bắc Ninh

Địa chỉ: Đường Nguyễn Quyền – Phường Võ Cường – TP Bắc Ninh

Điện thoại: 02223.821.242

*Chân thành cảm ơn./.*

|  |  |
| --- | --- |
| ***Nơi nhận****:*  - Như Kính gửi;  - Lưu TCKT. | **GIÁM ĐỐC** |
|  | **Hạ Bá Chân** |

**PHỤ LỤC CHI TIẾT**

*(Kèm theo Thư mời Báo giá ngày 19/11/2021 của Giám đốc bệnh viện)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stt** | **Sản Phẩm** | **Mô Tả Sản Phẩm** | **Đvt** | **Slg** |
| 1 | Phần mềm bảo vệ hạ tầng máy trạm | Smart Protection for Endpoints CTOTMMM1ELCZZZ  Hãng sản xuất: Trend Micro  Xuất xứ: Japan | Bản | 350 |
| 2 | Phần mềm bảo vệ hạ tầng máy chủ | Cloud One - Workload Security (Enterprise) - antimalware, network & system + XDR - annual subscription per server/VM/instance: CXC2ZZMENLCZZZ  Hãng sản xuất: Trend Micro  Xuất xứ: Japan | Bản | 06 |
| 3 | Dịch vụ triển khai, cài đặt | Dịch vụ triển khai, cài đặt | Gói | 01 |

|  |  |  |
| --- | --- | --- |
| **Stt** | **Sản phẩm** | **Tính năng/Yêu cầu chi tiết** |
| **1** | **Phần mềm bảo vệ hạ tầng máy trạm** | |
|  | **Bản quyền** | |
| Bản quyền | Đảm bảo an toàn bảo mật, hệ thống thông tin, kết nối tối đa cho 350 key (350 máy tính) |
| Thời hạn sử dụng | 03 năm |
| **Yêu cầu chung** | |
| Malware protection (Bảo vệ khỏi các phần mềm độc hại) | Hỗ trợ bảo vệ toàn bộ người dùng/máy đầu cuối trong công ty hoặc ngoài công ty 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 |
| Ngăn chặn các ransomware tinh vi mã hóa file ở máy đầu cuối, có thể ngắt các hành vi nguy hiểm, và có thể phục hồi các file đã bị mã hóa nếu cần thiết |
| Hỗ trợ các Signature-less Techniques | Bao gồm: - High-fidelity machine learning - Behavioral analysis - Variant protection - Census check - Application control - Exploit prevention - Goodfile check with other techniques like file reputation - Web reputation - Command and control (C&C) blocking |
| Hỗ trợ các tính năng | Các tính năng: - Antimalware - Vulnerability Protection - Application Control - Endpoint Detection and Response - Data Loss Prevention  - Device Control… Có thể tích hợp trong 1 agent endpoint duy nhất |
| Hỗ trợ khả năng mở rộng | Tính năng phát hiện và phản hồi EDR (Endpoint Detection and Response) là tùy chọn và được kích hoạt bằng license sử dụng trong tương lai mà không cần cài đặt thêm agent. |
| Detection and response capabilities (Khả năng phát hiện và phản ứng) | Cung cấp khả năng phát hiện và phản ứng lại với phát hiện ngay trong 1 tập giải pháp |
| Vulnerability Protection (Vá ảo các lỗ hổng bảo mật) | Hỗ trợ vá ảo các lổ hổng bảo mật đã biết và chưa biết cho máy đầu cuối. Có thể bảo vệ người dùng ngay cả khi bản vá chính thức chưa phát hành hoặc triển khai. |
| Centralized visibility and control (Khả năng hiển thị và kiểm soát tập trung) | 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. |
| Hỗ trợ High-Fidelity Machine Learning (Máy học với độ tin cậy cao) | Hỗ trợ công nghệ máy học với độ tin cậy cao với nhiều công nghệ phát hiện khác nhau đề đảm bảo khả năng phát hiện tốt nhất các ransomware cũng như tấn công tinh vi. |
| Sharing threat intelligent (Chia sẻ thông tin về mối đe dọa) | Cho phép chia sẻ các phát hiện mối đe dọa tinh vi trên phạm vi toàn tổ chức (sharing threat intelligent) |
| Hỗ trợ mã hóa dữ liệu | Đảm bảo bảo vệ dữ liệu bằng cách mã hóa dữ liệu trên endpoint |
| **Tính năng bảo vệ nâng cao** | |
| Machine Learning (Khả năng máy học) | Tính năng phát hiện mã độc sử dụng công nghệ Machine Learning với độ tin cậy cao ở cả hai mức độ tiền thực thi (pre execution) và thực thi (runtime) - Pre execution machine learning - Runtime machine learning |
| Behavioral analysis (Khả năng phân tích hành vi) | 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 ngăn chặn tấn công khai thác | - Host firewall - Exploit protection |
| Application Control (Kiểm soát ứng dụng) | Cho phép tổ chức 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 whitelist và 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 Executeable (PE) |
| Hỗ trợ chính sách động cho phép người dùng cài đặt các ứng dụng cho phép dựa trên các tiêu chí về mức độ uy tín (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 lockdown hệ thống để khóa người dùng không cho phép thực thi các ứng dụng mới. |
| Kiểm soát thiết bị ngoại vi | Device control: - Location awareness: theo vị trí của máy trạm - Áp dụng tới từng người dùng, nhóm người dùng, có thể kết nối với Active Directory - Block autorun - Hỗ trợ các mobile device, CD/DVD, Floppy disk, network drives, USB storage devices, biometric, thiết bị giao tiếp hồng ngoại, bluetooth |
| Mã hóa dữ liệu | Đảm bảo bảo vệ dữ liệu bằng cách mã hóa dữ liệu trên endpoint |
| Hỗ trợ mã hóa ổ đĩa, mã hóa folder và file, mã hóa thiết bị di động |
| Hỗ trợ quản trị Microsoft BitLokcer và Apple FileVault |
| Chính sách cho device control | - Full access - Custom - Read and execute - Read only - List device content only - Block |
| Data Loss Prevention (DLP) (Chống thất thoát dữ liệu) | - 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 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 … |
| Tính năng khác | Ngăn chặn các khai thác lổ hổng zero-day cho máy trạm vật lý, máy laptop, VDI trong mạng hoặc ngoài mạng của tổ chức |
| Ngăn chặn khai thác lổ hổng đã biết/chưa biết trước khi bản vá được triển khai, hoặc bản vá có thể không bao giờ được cung cấp. |
| Tự động điều chỉnh cấu hình bảo mật dựa trên vị trí của máy trạm. |
| Bảo vệ máy trạm với tối thiểu tác động đến hiệu năng máy trạm, trải nghiệm của người dùng. |
| Có thể phát hiện các traffic nguy hiểm ẩn dưới các giao thức phổ biến nhưng chạy qua port không chuẩn |
| Ngăn chặn backdoor |
| **Triển khai và khả năng hỗ trợ** | |
| Khả năng hỗ trợ đa nền tảng | Hỗ trợ bảo vệ đa nên tảng như: Windows 7 , Windows 8.1 , Windows 10, Windows Server 2008 R2 ,Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 |
| Cung cấp các tính năng bảo mật cho máy Apple MAC, khả năng phát hiện mã độc tinh vi dùng Machine Learning |
| Tùy chọn triển khai | Có thể được triển khai dưới dạng on-premise hoặc có sẵn ở dạng dịch vụ (SaaS) với đầy đủ tính năng và không có sự khác biệt giữa hai tùy chọn triển khai |
| Khả năng kết nối | Hỗ trợ khả năng kết nối với sandbox on-premise hoặc dạng dịch vụ Sandbox Software as a Service |
| Khả năng tích hợp | Hỗ trợ tích hợp log với SIEM |
| 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 |
| **Khả năng về quản trị** | |
| Tính năng quản trị | Quản trị tập trung trên toàn bộ tổ chức kể cả máy Windows và MAC, trên cả hai môi trường Cloud và On-premise hoặc hybrid |
| Đơn giản hóa triển khai và quản trị bằng agent đơn lẻ, quản trị và giám sát tập trung các patch, giảm thiểu tối đa việc phải reboot hệ thống. |
| Giao diện dashboard, report cảnh báo tập trung |
| Cho phép tùy biến dashboard phù hợp với nhiều vai trò quản trị khác nhau. |
| Giao diện duy nhất cho tất cả các vấn đề về security |
| Thiết lập policy 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. |
| 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… |
| Thu thập log tập trung, có thể chia sẻ cho SIEM |
| Có thể tích hợp với Active Directory dùng để xác thực cho quản trị |
| **Khả năng về báo cáo** | |
| Tính năng báo cáo (Report) | Hỗ trợ report theo các format PDF, DOCX, XLSX, HTML, XML, CSV |
| Hỗ trợ sẵn các template hoặc tùy biến.  - Template theo malware, theo người dùng phát hiện, theo máy trạm phát hiện, nhóm theo kiểu threat ransomware / spyware / grayware / viruses. - Report hỗ trợ theo từng cấp độ như chi tiết hoặc tóm tắt - Report hỗ trợ tùy biến template (custom template) cho phép quản trị tự định nghĩa template theo nhu cầu |
| **2** | **Phần mềm bảo vệ hạ tầng máy chủ** | |
|  | **Bản quyền** | |
| Bản quyền | Đảm bảo an toàn bảo mật, hệ thống thông tin, kết nối tối đa cho 06 máy chủ |
| Thời hạn sử dụng | 03 năm |
| **Tính năng chung** | |
| Bảo mật bao gồm nhiều module trên một agent duy nhất | Hỗ trợ các tính năng: - Anti Malware - Firewall - Web reputation - Vulnerability scanning - File integrity monitoring - Application control - Log inspection - Host-based intrusion prevention |
| Malware protection  (Bảo vệ khỏi các phần mềm độc hại) | Có khả năng phát hiện và ngăn chặn mã độc mới với công nghệ mới như Behavior analysis và Machine Learning |
| Ransomware protection (Bảo vệ khỏi các Ransomware) | Có khả năng chống thao tác mã hóa dữ liệu trái phép |
| Vulnerability Protection (Vá ảo các lỗ hổng bảo mật) | Vá ảo lổ hổng bảo mật đã biết và chưa biết đối với web, ứng dụng doanh nghiệp, hệ điều hành thông qua IPS |
| Intrusion prevention (Phòng chống xâm nhập) | Hỗ trợ tính năng chống xâm nhập giúp bảo vệ khỏi những cuộc tấn công SQL injection, cross-site scripting, và các web application vulnerabilities |
| Host Firewall (Tính năng tường lửa) | Hỗ trợ nhận dạng và cảnh báo các thay đổi không được biết, hoặc các tấn công mã độc tinh vi, bao gồm các ransomware ngay khi nó xảy ra trên hệ thống. |
| Applicaion control (Kiểm soát ứng dụng) | Hỗ trợ tính năng tường lửa có khả năng ngăn chặn các cuộc tấn công từ chối dịch vụ và phát hiện các hành vi dò quét như: - Computer OS Fingerprint Probe - Network or Port Scan - TCP Null Scan - TCP SYNFIN Scan - TCP Xmas Scan |
| File Integrity Monitoring (Giám sát tính toàn vẹn của tệp) | Ngăn chặn việc thực thi/cài đặt các file thực thi, các file script khi chưa được cấp phép |
| Process Memory Scanning (Quét bộ nhớ xử lý) | Giám sát sự thay đổi các files, thư viện, và dịch vụ … Lúc có một sự thay đổi từ các file, thư viện, dịch vụ … hệ thống sẽ log và cảnh báo tới nhà quản trị |
| Malware protection  (Bảo vệ khỏi các phần mềm độc hại) | Hỗ trợ Process Memory Scanning quét các process đang chạy trên RAM |
| **Khả năng triển khai và hỗ trợ** | |
| Hỗ trợ đa nền tảng hệ điều hành | Windows, Linux, Redhat, SuSE, CentOS, Ubuntu, Oracle linux, Amazon Linux |
| Hỗ trợ tích hợp với các nền tảng ảo hóa trên cloud | VMWare Cloud, Microsoft Azure, Amazon AWS |
| Đồng bộ dữ liệu với Amazon AWS, Microsoft Azure, Google Cloud Platform | Có thể đồng bộ danh sách các máy tính để triển khai bảo vệ từ cloud của Amazon AWS, Microsoft Azure, Google Cloud Platform |
| Hỗ trợ nhiều cơ chế triển khai agent | Chef, Puppet, Ansible, AWS OpsWorks, |
| Firewall hỗ trợ đầy đủ các IP-based frame (Tính năng tường lửa hỗ trợ đầy đủ các khung truyền IP-based) | • ICMP • ICMPV6 • IGMP • GGP • TCP • PUP • UDP • IDP • ND • RAW • TCP+UDP |
| Hỗ trợ vá nhanh các lỗ hổng | Hỗ trợ kiểm soát packet vào/ra hệ thống để phát hiện và ngăn chặn các hành vi khai thác lổ hổng bảo mật. Hỗ trợ tự động cập nhật các rule mới và tự động vá ngay lập tức vào hệ thống |
| Hỗ trợ tăng tốc đáp ứng các tuân thủ bảo mật | Hỗ trợ đáp ứng nhiều yêu cầu tuân thủ bao gồm GDPR, PCI DSS, HIPAA, NIST … |
| SSL Inspection (Kiểm tra kết nối SSL) | Hỗ trợ SSL Inspection giúp phân tích các traffic SSL |
| Khả năng phát hiện botnet, C&C | Phát hiện và ngăn chặn các botnet, các kết nối C&C |
| Hỗ trợ bảo vệ cho docker và container. | Hỗ trợ bảo vệ cho docker và container như vá ảo, realtime malware protection, có khả năng giám sát traffic giữa các container đang chạy |
| Hỗ trợ REST Web Services API | Hỗ trợ REST (REpresentational State Transfer) Web Services API để tích hợp với các sản phẩm khác |
| **Khả năng báo cáo và quản trị** | |
| Hỗ trợ tạo Schedule scan | Rà soát có thể được lập lịch và tự động áp đặt rule vá khi có thể nhằm loại bỏ rủi ro |
| Khả năng báo cáo (Report) | Báo cáo có thể được trích xuất dưới dạng file PDF hoặc RTF, và phải bao gồm các loại report như sau: - Attack Report (Báo cáo tấn công) - Anti-malware report (Báo cáo chống phần mềm độc hại) - Firewall Report (Báo cáo tường lửa) - Integrity Monitoring Report (Báo cáo giám sát tính toàn vẹn)  - Instrusion Prevention report (Báo cáo Phòng chống xâm nhập) |
| Khả năng quản trị tập trung | Tất cả các đối tượng được bảo vệ đều có thể được quản trị trên một màn hình quản trị duy nhất, bất kể đối tượng được bảo vệ đó là máy ảo, máy vật lý hay trên đám mây |
| Khả năng quản trị trên đám mây (dạng SaaS) | Doanh nghiệp không cần cài đặt thành phần quản trị trong DC. |
| Hỗ trợ tính năng gửi sự kiện đến Amazon SNS | Hỗ trợ gửi event tới Amazon SNS để chuyển tiếp sự kiện |
| Phân quyền tài khoản quản trị | Phân quyền cho các account quản trị tùy theo chức năng và phạm vi của từng vị trí |
| Phân quyền theo nhóm | Có thể phân quyền cho từng nhóm máy tính cần bảo vệ |
| Quản lý event theo tag (thẻ) | Có cơ chế quản lý các sự kiện liên quan đến bảo mật hệ thống thông qua các thẻ (tag) nhằm đơn giản hóa công tác phân tích |
| Automatic tag event (Tự động gắn thẻ sự kiện) | Có thể thực hiện gắn thẻ tự động cho các sự kiện bảo mật |
| Filter theo tag  (Lọc sự kiện theo thẻ) | Có cơ chế áp dụng lọc theo thẻ thông tin khi tạo báo cáo giúp thông tin được chuẩn xác hơn |
| Đáp ứng các chứng chỉ bảo mật | Tối thiểu các chứng chỉ sau: Common Criteria EAL2+, FIPS 140-2, PCI DSS, ISO 27001 |
| **3** | **Dịch vụ triển khai, cài đặt** | |
|  | Triển khai toàn bộ phần mềm cung cấp | Phần mềm bảo vệ hạ tầng máy trạm |
| Phần mềm bảo vệ hạ tầng máy chủ |
| Hỗ trợ cài đặt trên cloud của hãng sản xuất |