YÊU CẦU KỸ THUẬT

Đối với "Mua sắm bản quyền phần mềm cho hệ thống an ninh mạng"

1. MỤC ĐÍCH VÀ PHẠM VI SỬ DỤNG

Mua sắm bản quyền phần mềm cho hệ thống An ninh mạng.

2. YÊU CẦU CHUNG:

- Bản quyền và dịch vụ phải được cung cấp trực tiếp từ nhà sản xuất hoặc đại lý ủy quyền hợp pháp tại Việt Nam.
- Nhà thầu phải cung cấp chứng từ chứng minh nguồn gốc bản quyền (thư ủy quyền, giấy xác nhận phân phối hoặc tài liệu tương đương).
- Bảo hành và hỗ trợ kỹ thuật thực hiện theo điều kiện và chính sách của nhà sản xuất.

3. YÊU CẦU VỀ KỸ THUẬT, CÔNG NGHỆ:

Phần mềm phải có các tính năng và thông số kỹ thuật tối thiểu như mô tả trong danh mục.

- **Mục số 1: Trang bị phần mềm quản lý hợp nhất thiết bị đầu cuối** nhằm phục vụ công tác quản trị, giám sát, cấu hình và bảo mật các thiết bị CNTT trong hệ thống của Liên doanh Việt – Nga Vietsovpetro.
- Phần mềm phải cho phép quản lý tập trung các máy chủ trong hệ thống, hỗ trợ tự động hóa các tác vụ quản trị CNTT, đồng thời tích hợp và vận hành đồng bộ với hệ thống quản trị CNTT hiện đang sử dụng tại Vietsovpetro.

➢ **Yêu cầu bản quyền**

- Phần mềm phải đáp ứng các yêu cầu bản quyền sau:
  - Giải pháp phần mềm quản lý hợp nhất thiết bị đầu cuối cấp doanh nghiệp (Enterprise Endpoint Management Solution).
  - Mô hình cấp phép: bản quyền vĩnh viễn (Perpetual Licensing Model).
- Phạm vi bản quyền tối thiểu: / Минимальный объем лицензирования:
  - Quản lý 250 máy chủ (servers)..
  - 01 tài khoản kỹ thuật viên quản trị hệ thống (Technician/Admin License).
- Bản quyền phải bao gồm:
  - Phí cấp phép cài đặt và sử dụng phần mềm.
  - Phí bảo trì và hỗ trợ kỹ thuật hằng năm (Annual Maintenance and Support – AMS) cho toàn bộ số lượng bản quyền, bao gồm:
    - Quyền cập nhật phiên bản phần mềm.
    - Cập nhật bản vá lỗi và bản vá bảo mật.
    - Hỗ trợ kỹ thuật từ nhà sản xuất hoặc nhà cung cấp.

- **Yêu cầu chức năng chính**

Phần mềm phải cung cấp tối thiểu các chức năng sau:

i. Quản lý thiết bị tập trung
   - Quản lý tập trung các thiết bị CNTT trên một nền tảng thống nhất.
   - Thu thập và quản lý thông tin thiết bị (phần cứng và phần mềm).
   - Theo dõi trạng thái hoạt động của các thiết bị được quản lý.
   - Hỗ trợ cơ chế triển khai tác nhân quản lý (Agent-based management) trên thiết bị nhằm thu thập thông tin và thực hiện các tác vụ quản trị từ xa.

ii. Quản lý bản vá và cập nhật hệ thống
   - Phát hiện và quản lý các bản vá của hệ điều hành.
   - Triển khai bản vá từ xa theo chính sách quản trị.
   - Theo dõi trạng thái cập nhật của các thiết bị.
   - Hỗ trợ quản lý và triển khai bản vá cho các phần mềm ứng dụng phổ biến của bên thứ ba (third-party patch management).
   - Cho phép lập lịch và tự động hóa quá trình triển khai bản vá.

iii. Kiểm kê tài sản CNTT
   - Tự động thu thập thông tin phần cứng và phần mềm của thiết bị.
   - Lập danh mục tài sản CNTT trong hệ thống.
   - Theo dõi các thay đổi cấu hình thiết bị.

iv. Triển khai và quản lý phần mềm
   - Cài đặt, cập nhật hoặc gỡ bỏ phần mềm từ xa trên các thiết bị được quản lý.
   - Triển khai phần mềm theo nhóm thiết bị hoặc theo chính sách quản trị.
   - Lập lịch triển khai phần mềm tự động.
   - Hỗ trợ kho lưu trữ phần mềm tập trung (software repository) để phục vụ triển khai và cập nhật phần mềm trong hệ thống nội bộ.

v. Điều khiển và hỗ trợ thiết bị từ xa
   - Cho phép quản trị viên truy cập và điều khiển thiết bị từ xa.
   - Hỗ trợ xử lý sự cố kỹ thuật cho người dùng.
   - Theo dõi và ghi nhận các phiên hỗ trợ kỹ thuật.

vi. Quản lý cấu hình và bảo mật
   - Thiết lập và áp dụng các chính sách cấu hình hệ thống.
   - Áp dụng các chính sách bảo mật cho thiết bị đầu cuối.
   - Kiểm soát cấu hình thiết bị theo tiêu chuẩn quản trị CNTT.

- Cho phép kiểm soát một số thiết bị ngoại vi hoặc ứng dụng theo chính sách bảo mật của tổ chức.

vii. Giám sát và cảnh báo

- Giám sát tình trạng thiết bị và trạng thái thực hiện các tác vụ quản trị..
- Phát hiện và cảnh báo các sự cố phát sinh trong quá trình quản trị hệ thống.

viii. Báo cáo và thống kê

- Cung cấp hệ thống báo cáo phục vụ công tác quản trị thiết bị.
- Báo cáo tài sản CNTT, phần mềm cài đặt và tình trạng cập nhật hệ thống.

ix. Phân quyền quản trị

- Cho phép phân quyền quản trị theo vai trò.
- Quản lý tài khoản quản trị và quyền truy cập hệ thống.

➢ **Yêu cầu tương thích và tích hợp hệ thống**

- Có khả năng tích hợp với hệ thống thư mục người dùng (Directory Services) trong hạ tầng CNTT.
- Có khả năng tích hợp và vận hành đồng bộ với hệ thống quản trị CNTT hiện đang sử dụng tại Vietsovpetro.
- Hỗ trợ API hoặc cơ chế tích hợp tiêu chuẩn phục vụ trao đổi dữ liệu giữa các hệ thống.

- **Mục số 2: Phần mềm bảo mật thư điện tử (Security for Mail Server)**

Phần mềm bảo mật thư điện tử (Security for Mail Server) được trang bị nhằm cung cấp giải pháp bảo vệ toàn diện hệ thống email chiều gửi và nhận (Inbound/Outbound Email Security). Các mục đích chính bao gồm:

- Phòng chống thư rác (Spam), mã độc (Malware), phần mềm tống tiền (Ransomware) và các hình thức tấn công có chủ đích (APT) qua email trước khi thư được chuyển vào hệ thống máy chủ thư điện tử nội bộ.
- Bảo mật email dựa trên công nghệ máy học (Machine Learning), trí tuệ nhân tạo (AI) và tích hợp môi trường cô lập (Sandbox) để phân tích chuyên sâu.
- Ngăn chặn các hình thức lừa đảo qua email (Phishing), giả mạo địa chỉ (Spoofing) và rò rỉ dữ liệu (DLP - Data Loss Prevention).

➢ **Yêu cầu bản quyền**

- Phần mềm bắt buộc phải là sản phẩm đóng gói thương mại chính thức từ hãng bảo mật, có giấy phép sử dụng rõ ràng.
- Không chấp nhận các giải pháp mã nguồn mở chưa thương mại hóa hoặc các phiên bản thử nghiệm (beta).

- Phần mềm phải thuộc nhóm các giải pháp bảo mật email uy tín toàn cầu, đáp ứng hoặc được đánh giá phù hợp với các tiêu chuẩn, tiêu chí, khuyến nghị từ các tổ chức độc lập uy tín như: Bộ quy tắc bảo mật Email toàn cầu của ITU, Rapid7, Gartner hoặc tương đương.
- Phần mềm được cung cấp dưới dạng Email Security Gateway, đặt tại lớp trung gian trước hệ thống máy chủ email của đơn vị.
- Phần mềm được cài đặt trên máy chủ ảo hóa (VMware, Hyper-V...) hoặc máy chủ vật lý, cho phép triển khai theo mô hình phù hợp với hạ tầng hiện tại (On-premise).
- Đảm bảo hệ thống có khả năng mở rộng linh hoạt trong tương lai theo nhu cầu sử dụng thực tế.
- Phạm vi bản quyền áp dụng cho 7600 hộp thư điện tử của đơn vị trong thời hạn 01 năm, bao gồm giấy phép hỗ trợ kỹ thuật và quyền cập nhật cơ sở dữ liệu nhận diện mối đe dọa liên tục.
- Bảo vệ song song cả hai chiều gửi và nhận email (Inbound + Outbound) cho các tài khoản quản trị, tài khoản người dùng và hệ thống thư điện tử nội bộ.

➢ **Yêu cầu chức năng chính**

i. Chức năng lọc thư rác và mã độc

- Phát hiện và ngăn chặn thư rác (Spam) dựa trên nhiều cơ chế phân tích nội dung, nguồn gửi và tính điểm spam theo thuật toán Bayesian nhằm giảm false positive.
- Hỗ trợ cơ chế RBL/SURBL, Greylist, xác thực người nhận (RCPT Inspection) và giới hạn tần suất nhận thư (Rate Limit) để chống tấn công flood/mail bomb.
- Kiểm tra tệp đính kèm đa lớp: đối chiếu mẫu tĩnh, luật tùy biến (YARA Rule), và phân tích động trong môi trường Sandbox (môi trường cô lập).
- Hỗ trợ trace URL đến điểm cuối (endpoint) để xác minh, phát hiện link lồng nhiều lớp và link độc hại ẩn bên trong tệp đính kèm (Word, Excel, PDF).

ii. Bảo vệ chống giả mạo và tấn công email

- Hỗ trợ kiểm tra và xác thực các cơ chế SPF, DKIM và DMARC nhằm đảm bảo tính hợp lệ của email gửi đến.
- Có khả năng tự động học (Machine Learning) về SPF và domain liên lạc hợp lệ để giảm thiểu false positive.
- Phát hiện giả mạo header email theo tối thiểu 03 dạng: giả mạo địa chỉ (Address), giả mạo ID, giả mạo tên miền (Domain).

- Hỗ trợ phát hiện tên miền giả mạo (Look-alike Domain) theo tối thiểu 04 mức độ tương tự khác nhau bao gồm cả khác biệt TLD.
- Theo dõi đường đi email theo quốc gia (Send Location Risk) và cảnh báo tuyến gửi đột biến.

iii. Kiến trúc vận hành

- Có kiến trúc phân lớp rõ ràng gồm lớp lọc thư rác (Spam Filter) và lớp chống tấn công (APT Protection) phối hợp nhịp nhàng.
- Có khả năng triển khai chạy dự phòng (High Availability) và cân bằng tải (Load Balancing).
- Tích hợp tốt với nền tảng quản lý thư mục Active Directory (AD) / LDAP để tự động đồng bộ trạng thái tài khoản.
- Giải pháp hỗ trợ cơ chế cấp tenant riêng cho đơn vị, đảm bảo dữ liệu log và cấu hình cô lập hoàn toàn.

iv. Giám sát, quản trị tự phục vụ (Self-Service) và báo cáo

- Cung cấp giao diện quản trị tập trung (Web Console) đa ngôn ngữ (bao gồm Tiếng Việt và Tiếng Anh).
- Hỗ trợ phân quyền quản trị viên dựa trên vai trò (Group Admin).
- Quản lý danh sách trắng (whitelist) và danh sách đen (blacklist) đa tầng theo tối thiểu 03 cấp (chung toàn hệ thống, theo nhóm, theo địa chỉ thư cá nhân) với phạm vi kiểm tra Subject, Body, Header, IP, Domain.
- Hỗ trợ cảnh báo qua email khi phát hiện mã độc, ransomware hoặc URL nguy hiểm mức độ cao.
- Gửi báo cáo định kỳ (Blocked Mail Report) cho từng người dùng cuối.
- Lưu trữ nhật ký thao tác quản trị viên (Audit Log) và log sự kiện tối thiểu 06 tháng phục vụ kiểm toán và truy vết. Báo cáo hỗ trợ tùy chỉnh logo, tiêu đề theo nhận diện thương hiệu.

➢ **Yêu cầu tương thích và tích hợp hệ thống**

- Áp dụng cho hệ thống email hiện hữu, bao gồm khả năng hỗ trợ tích hợp mà không làm thay đổi kiến trúc hệ thống thư điện tử đang vận hành.
- Tích hợp với hệ thống giám sát an toàn thông tin tập trung (SIEM) thông qua giao thức chuẩn.
- Hỗ trợ kiểm thử và đưa hệ thống vào vận hành chính thức.
- Cung cấp hỗ trợ kỹ thuật trong suốt thời gian cung cấp dịch vụ (01 năm).
- Đảm bảo dịch vụ hoạt động ổn định và không làm gián đoạn hệ thống thư điện tử đang khai thác.

- **Mục số 3: Tường lửa cho Cơ sở dữ liệu**

➢ **Yêu cầu bản quyền**

- Phần mềm phải nằm trong nhóm Leaders trong các báo cáo đánh giá từ năm 2025, bao gồm các giải pháp đã được đánh giá và xếp hạng bởi các tổ chức xếp hạng giải pháp bảo mật uy tín như Gartner hoặc Forrester hoặc KuppingerCole.
- Cung cấp 02 bản quyền thiết bị tường lửa cơ sở dữ liệu dạng máy ảo (Virtual Appliance), gói thuê bao nâng cao (Enhanced Subscription) trong thời hạn 01 năm.
- Tổng năng lực xử lý của 02 thiết bị tương đương 200 CPU threads.
- Bao gồm 100 bản quyền DB Agents cài đặt trên máy chủ cơ sở dữ liệu để giám sát và bảo vệ truy cập.
- Cung cấp 01 bản quyền máy chủ quản lý tập trung dạng máy ảo (Management Server Virtual Appliance), gói thuê bao trong thời hạn 01 năm.
- Bản quyền phải bao gồm:
  - Phí cấp phép cài đặt và sử dụng phần mềm.
  - Phí bảo trì và hỗ trợ kỹ thuật hằng năm (Annual Maintenance and Support – AMS) cho toàn bộ số lượng bản quyền, bao gồm:
    - Quyền cập nhật phiên bản phần mềm.
    - Cập nhật bản vá lỗi và bản vá bảo mật.
    - Hỗ trợ kỹ thuật từ nhà sản xuất hoặc nhà cung cấp.

➢ **Yêu cầu chức năng chính**

Phần mềm phải cung cấp tối thiểu các chức năng sau:

i. Kiến trúc triển khai và thu thập dữ liệu
   - Hỗ trợ cơ chế triển khai linh hoạt, không làm thay đổi kết cấu, mô hình mạng hiện hữu
   - Hỗ trợ triển khai tác nhân (DB Agent) trên máy chủ CSDL để thu thập và phân tích truy vấn.
   - Agent cài trên máy chủ CSDL thu thập các hoạt động trên Shared Memory, IPC, TCP local, BEQ,..
   - Hỗ trợ cơ chế kiểm soát Agent dựa trên mức tải hiện tại của máy chủ CSDL
   - Agent phải có cơ chế nén dữ liệu để tiết kiệm băng thông trên đường truyền.

ii. Phát hiện và ngăn chặn tấn công cơ sở dữ liệu
   - Phát hiện và ngăn chặn truy cập trái phép, tấn công SQL Injection và các hành vi bất thường đối với cơ sở dữ liệu.

- Phát hiện, cảnh báo, ngăn chặn các kết nối bất thường mà user/client chưa từng thực hiện, kết nối đến từ source IP/Application lạ bên trong hệ thống với cơ chế hồ sơ động.
- Phát hiện, cảnh báo, ngăn chặn các truy cập SQL trái quyền.
- Kiểm tra hợp lệ giao thức CSDL/SQL (SQL protocol validation, DB protocol Validation) như kiểm tra độ dài, kích thước header, giá trị tham số có hợp lệ.

iii. Cơ chế học hành vi và phân tích truy cập (Behavior Analysis)

- Cho phép tự học và xây dựng hồ sơ động (Dynamic Profile/Dynamic Profiling) về chính sách bảo vệ. Các thay đổi hợp lệ của ứng dụng và CSDL trong một thời gian được tự động nhận ra và cập nhật vào profile.

iv. Quản lý chính sách bảo mật cơ sở dữ liệu

- Cung cấp các chính sách Audit và Security được định nghĩa và áp dụng một cách độc lập với nhau.
- Áp dụng chính sách theo đối tượng DB cần bảo vệ (máy chủ/service) mà không phải áp chính sách theo DBF gateway.
- Cung cấp các chính sách bảo vệ (Security Policy) nhiều mức, gồm mức mạng (Network Security Policies), mức dịch vụ CSDL (Database Service Level Security Policies), và mức ứng dụng CSDL (DB Application Level Policies).
- Cung cấp các mẫu chính sách được định nghĩa sẵn, cho phép tùy biến chính sách.
- Hỗ trợ định nghĩa chính sách an ninh tập trung áp dụng cho toàn bộ hệ thống DB, với các loại DB khác nhau (MSSQL, Oracle, MySQL), không yêu cầu định nghĩa cùng chính sách lặp lại nhiều lần cho từng hệ thống CSDL khác nhau.

v. Cơ chế phát hiện tấn công dựa trên chữ ký (Signature-based Detection)

- Cung cấp chính sách bảo mật có sẵn xử lý các vấn đề bảo mật sau: SQL Protocol Validation, Oracle SQL Protocol Validation, SQL Correlation Policy, SQL Protocol Signatures.
- Cung cấp signature phát hiện/chống tấn công, và Signature bảo vệ điểm yếu đã biết (gắn theo mã CVE), các mẫu được cập nhật liên tục. Phát hiện tấn công xâm nhập theo mẫu tấn công (signature) và tấn công khai thác điểm yếu đã biết (áp dụng cho CSDL quan hệ).

- Cho phép người dùng tùy biến, tự viết Signature sử dụng ngôn ngữ Regular Expressions.
- Hỗ trợ cơ chế cập nhật Signature mới nhất, cho phép cấu hình để tự động cập nhật theo ngày, tuần, tháng, ….

vi. Quản lý nhật ký, kiểm toán và tuân thủ

- Hỗ trợ cơ chế cảnh báo, ghi log, lưu vết phục vụ kiểm toán và tuân thủ an toàn thông tin..
- Log hoạt động của DB phải được sinh ra từ giải pháp DBF, không sử dụng log audit native trên cơ sở dữ liệu.
- Hỗ trợ quản lý, lưu trữ dữ liệu audit: Encrypt audit archives, Data signing, FTP archive, SCP archive.
- Dữ liệu nhật ký/Audit phải được lưu trong flat file được mã hóa, không lưu trong CSDL quan hệ để đảm bảo tính bảo mật và nguyên vẹn.
- Có tính năng che dữ liệu (Masking) nhạy cảm trong log/alert.

vii. Quản lý tập trung và giám sát hệ thống

- Quản lý tập trung thông qua máy chủ quản lý chuyên dụng..
- Cung cấp quản trị tập trung cho phép cấu hình chính sách, tạo báo cáo, hiển thị log và giám sát sự kiện trong thời gian thực cho tất cả các thiết bị DB Firewall và agent trên cùng một giao diện duy nhất.
- Cung cấp báo cáo, thống kê và theo dõi trạng thái bảo mật hệ thống cơ sở dữ liệu.
- Dữ liệu báo cáo tổng hợp từ nhiều DBF gateway có thể được cấu hình lấy dữ liệu nhật ký theo phút và giờ (như là lấy dữ liệu nhật ký trong 15 phút qua, trong 1 giờ qua,..)

viii. Khả năng phát hiện và đánh giá bảo mật cơ sở dữ liệu

- Có khả năng tự động phát hiện (discover) các máy chủ CSDL. Tìm và phân loại dữ liệu nhạy cảm trong CSDL (áp dụng cho CSDL quan hệ).
- Đánh giá điểm yếu trên CSDL. Đánh giá dựa theo chuẩn DISA STIG, CIS và CVSS (Common Vulnerability Scoring System).

ix. Khả năng mở rộng và hỗ trợ hệ quản trị CSDL

- Hỗ trợ các hệ quản trị CSDL quan hệ: bao gồm Oracle, Microsoft SQL Server, MySQL, Postgres, ….
- Hỗ trợ tuỳ chọn mở rộng cho các CSDL, Big data/Non-SQL khác: MongoDB, Cassandra, ….

- Hỗ trợ tùy chọn mở rộng triển khai các gateway trong chế độ cluster N+1, cho phép chia tải giữa các thành viên trong cluster.
- Sản phẩm được đánh giá thuộc phân khúc top ở những bảng xếp hạng giải pháp bảo mật uy tín như Gartner, Forrester, KuppingerCole ….

➢ **Yêu cầu tương thích và tích hợp hệ thống**

- Có khả năng tích hợp với hệ thống cơ sở dữ liệu hiện hữu..
- Đảm bảo không làm gián đoạn hệ thống cơ sở dữ liệu đang khai thác trong quá trình triển khai.

4. YÊU CẦU VỀ THỜI GIAN VÀ ĐỊA ĐIỂM GIAO HÀNG

- Thời gian cung cấp: hoàn thành việc cung cấp và kích hoạt bản quyền trong vòng 45 ngày kể từ ngày ký hợp đồng.
- Nhà thầu phải hoàn thành cài đặt trong vòng 30 ngày kể từ ngày Vietsovpetro thông báo cài đặt.
- Thời hạn hiệu lực bản quyền: 12 tháng kể từ ngày cài đặt.
- Địa điểm bàn giao: Liên doanh Việt – Nga Vietsovpetro, 105 Lê Lợi, P. Vũng Tàu, TP. HCM..
- Hình thức bàn giao: gửi chứng nhận bản quyền điện tử (License Certificate) và xác nhận kích hoạt thành công từ nhà sản xuất.

5. HỖ TRỢ KỸ THUẬT CỦA NHÀ THẦU

- Nhà thầu bằng chi phí của mình phải chịu trách nhiệm cài đặt, tích hợp vào các hệ thống hiện có của Vietsovpetro.
- Yêu cầu về triển khai và dịch vụ kèm theo, Nhà thầu phải cung cấp đầy đủ các dịch vụ sau:
  - ➢ Cài đặt và cấu hình phần mềm theo yêu cầu kỹ thuật.
  - ➢ Tích hợp với hệ thống hiện hữu
  - ➢ Kiểm tra và nghiệm thu đầy đủ các chức năng.
  - ➢ Hướng dẫn vận hành cơ bản cho cán bộ quản trị.
  - ➢ Nhân sự phải có chứng chỉ triển khai liên quan phần mềm mà nhà thầu cung cấp như trong hồ sơ dự thầu hoặc đã có kinh nghiệm triển khai phần mềm như trong hồ sơ dự thầu.
  - ➢ Mục 3: Nhân sự tham gia triển khai phải có chứng chỉ về tường lửa cơ sở dữ liệu như là “DISC Imperva Data Security Certification Exam” hoặc tương đương.

6. YÊU CẦU VỀ TÀI LIỆU KỸ THUẬT:

- Tài liệu kỹ thuật nhà thầu cần cung cấp kèm theo chào hàng giai đoạn đấu thầu:
    - Tài liệu mô tả phần mềm.
    - Giấy chứng nhận là chủ sở hữu Phần mềm hoặc nhà phân phối và cung cấp hợp pháp được ủy quyền từ chủ sở hữu Phần mềm hoặc từ nhà phân phối chính thức trong khu vực.
    - Hồ sơ tài liệu chứng minh năng lực triển khai phần mềm mà nhà thầu cung cấp (Hợp đồng đã thực hiện, kinh nghiệm, chứng chỉ liên quan, ...)
- Cam kết bàn giao tài liệu hướng dẫn vận hành sau khi hoàn thành triển khai.

7. YÊU CẦU VỀ CHỨNG CHỈ:

- Nhà thầu được yêu cầu cam kết cung cấp các chứng chỉ sau:
    - Bản quyền phần mềm phải là chính hãng, thể hiện dưới dạng bản cứng hoặc bản điện tử (e-license) hoặc phần cứng (hardware key).
    - Giấy cam kết bảo hành cho tất cả các mục.

DANH MỤC HÀNG HÓA/ DỊCH VỤ

STT	Tên hàng hóa/ Dịch vụ	Đặc tính kỹ thuật	Đvt	Khối lượng	Ghi chú
1	Phần mềm quản lý hợp nhất thiết bị đầu cuối	Phần mềm quản lý hợp nhất thiết bị đầu cuối - Cung cấp bản quyền phần mềm quản lý tập trung thiết bị đầu cuối cấp doanh nghiệp, mô hình cấp phép vĩnh viễn (Perpetual Licensing). - Phạm vi bản quyền cho phép quản lý tối thiểu 250 máy chủ và 01 tài khoản kỹ thuật viên quản trị hệ thống. - Hỗ trợ quản lý tập trung thiết bị, triển khai bản vá hệ điều hành và ứng dụng, kiểm kê tài sản CNTT, triển khai phần mềm và hỗ trợ điều khiển từ xa. - Hỗ trợ thiết lập chính sách cấu hình và bảo mật thiết bị, giám sát trạng thái hệ thống và cung cấp báo cáo quản trị. - Bao gồm dịch vụ bảo trì và hỗ trợ kỹ thuật hằng năm (Annual Maintenance and Support – AMS) cho toàn bộ số lượng bản quyền. - Bao gồm dịch vụ cài đặt, cấu hình và bàn giao vận hành hệ thống.	Set	1	

2	Phần mềm bảo mật thư điện tử (Security for Mail Server)	Phần mềm bảo mật thư điện tử (Security for Mail Server) bảo vệ toàn diện hệ thống email chiều gửi và nhận (Inbound/Outbound Email Security). - Phạm vi bản quyền áp dụng cho 7600 hộp thư điện tử của đơn vị trong thời hạn 01 năm, bao gồm giấy phép hỗ trợ kỹ thuật và quyền cập nhật cơ sở dữ liệu nhận diện mối đe dọa liên tục. - Phòng chống thư rác (Spam), mã độc (Malware), phần mềm tống tiền (Ransomware) và các hình thức tấn công có chủ đích (APT) qua email trước khi thư được chuyển vào hệ thống máy chủ thư điện tử nội bộ. - Bảo mật email dựa trên công nghệ máy học (Machine Learning), trí tuệ nhân tạo (AI) và tích hợp môi trường cô lập (Sandbox) để phân tích chuyên sâu. - Ngăn chặn các hình thức lừa đảo qua email (Phishing), giả mạo địa chỉ (Spoofing) và rò rỉ dữ liệu (DLP - Data Loss Prevention). - Bao gồm dịch vụ cài đặt, cấu hình và bàn giao vận hành hệ thống.	Set	1	
3	Tường lửa cho Cơ sở dữ liệu	Tường lửa cho Cơ sở dữ liệu - Cung cấp 02 bản quyền thiết bị tường lửa cơ sở dữ liệu dạng máy ảo (Virtual Appliance), gói thuê bao nâng cao (Enhanced Subscription) trong thời hạn 01 năm. - Tổng năng lực xử lý tương đương 200 CPU threads. - Bao gồm 100 bản quyền DB Agents cài đặt trên máy chủ cơ sở dữ liệu để giám sát và bảo vệ truy cập. - Cung cấp 01 bản quyền máy chủ quản lý tập trung dạng máy ảo (Management Server Virtual Appliance), gói thuê bao trong thời hạn 01 năm. - Hỗ trợ giám sát, phân tích và kiểm soát truy cập cơ sở dữ liệu theo thời gian thực. - Phát hiện và ngăn chặn truy cập trái phép, tấn công SQL Injection và các hành vi bất thường đối với cơ sở dữ liệu. - Cung cấp cơ chế cảnh báo, báo cáo, lưu vết và phục vụ kiểm toán an toàn thông tin. - Bao gồm dịch vụ triển khai, cấu hình, tích hợp với hệ thống hiện hữu và bàn giao vận hành. - Đảm bảo hệ thống hoạt động ổn định, không làm gián đoạn dịch vụ cơ sở dữ liệu đang khai thác.	Set	1	