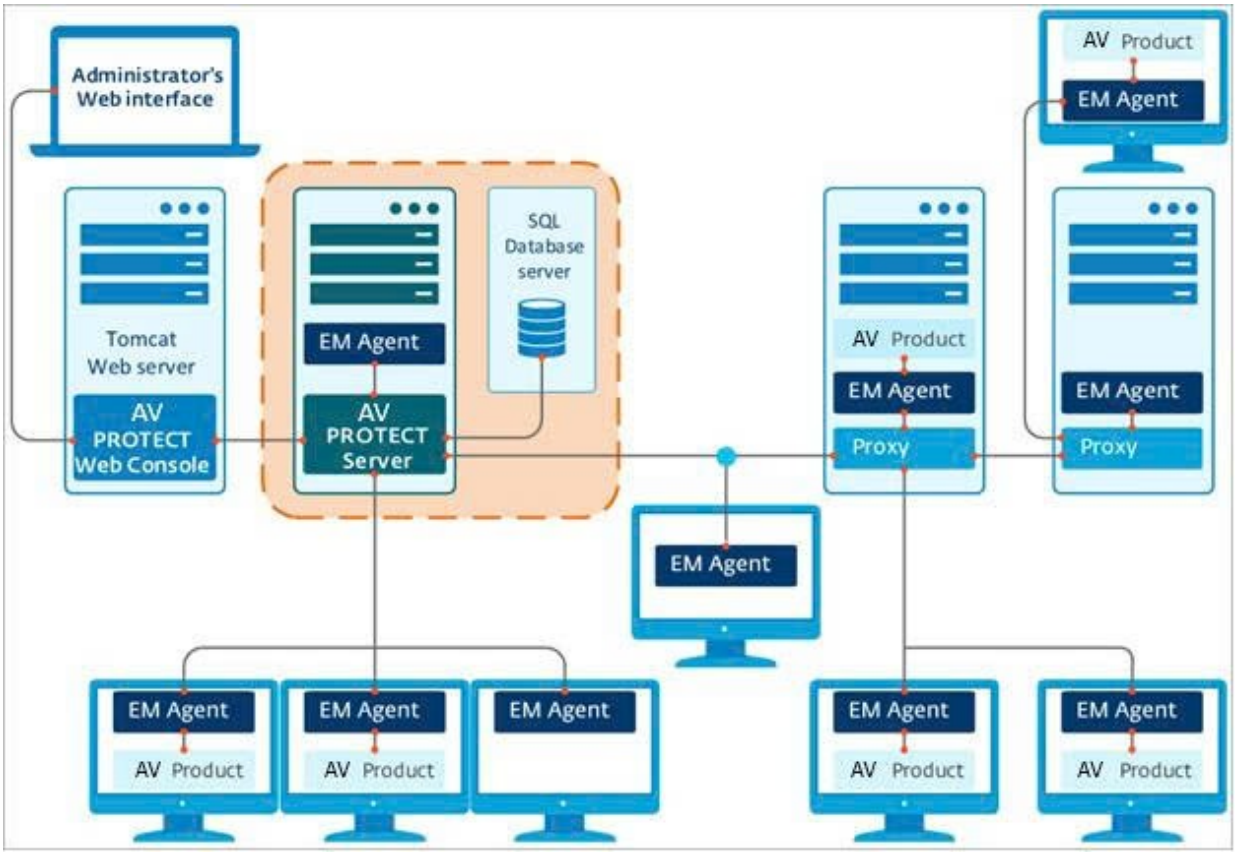
Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

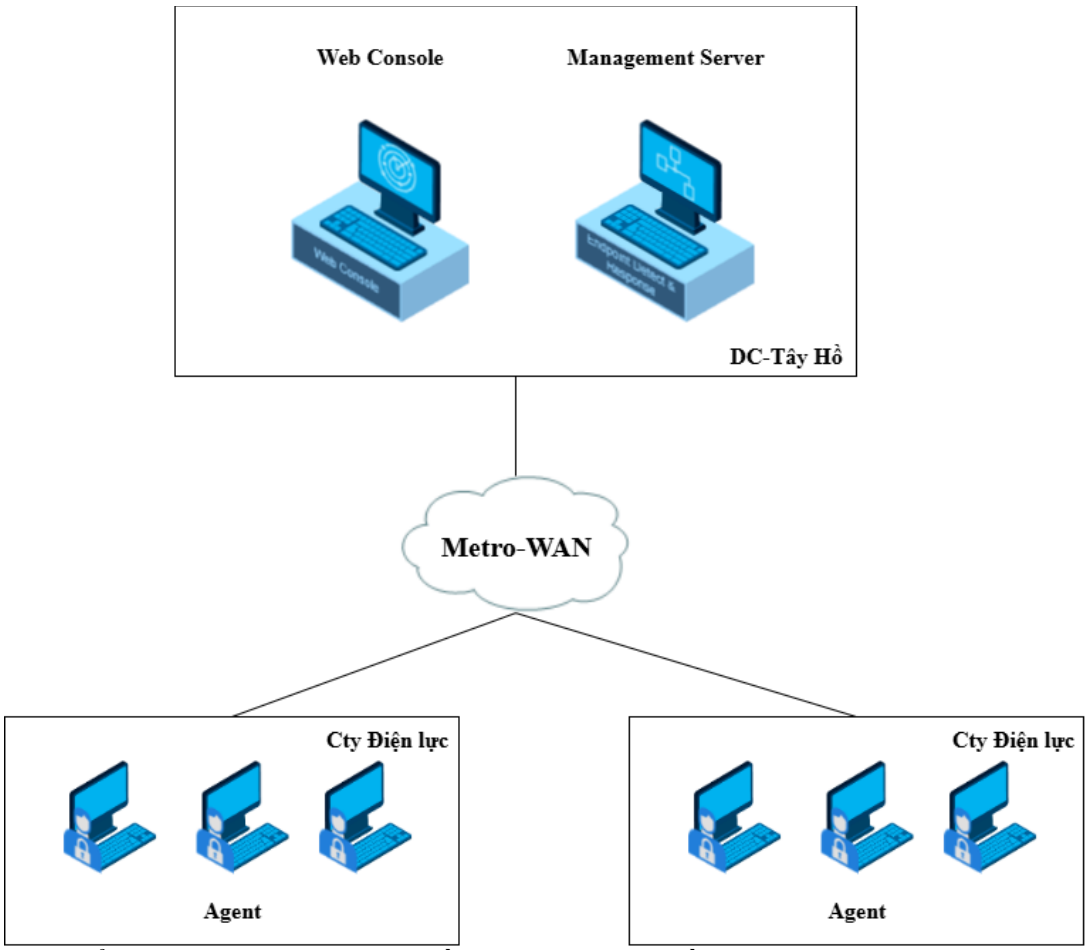
1.1.1 Mô hình kiến trúc



STT	Hạng mục	Mô tả	Các dịch vụ hệ thống
1	Máy chủ quản trị Web Console	Cung cấp giao diện quản trị Web cho thành phần quản trị tập trung Management Server.	- Dịch vụ Web Tomcat. - Dịch vụ Web Console.
2	Máy chủ quản trị Management Server	Đóng vai trò xử lý dữ liệu kết nối với các Agent được cài đặt trên máy chủ/máy trạm.	- Dịch vụ Database SQL Server. - Dịch vụ Management Server.
3	Máy trạm Agent	Được cài đặt ở các máy chủ/máy trạm cần được bảo vệ khỏi mã độc.	- Dịch vụ Agent. - Dịch vụ Endpoint Products.

1.1.2 Mô hình triển khai áp dụng

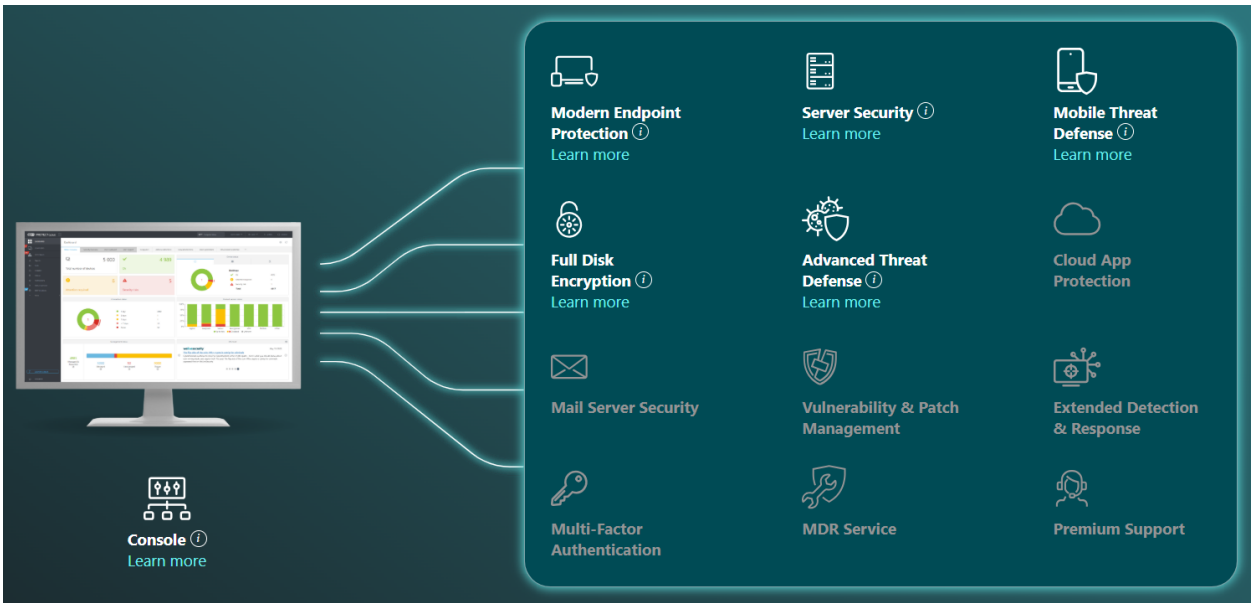
Mô hình triển khai



Mô hình triển khai giải pháp bao gồm các thành phần:

- Tại TTDL (DC-Tây Hồ): sẽ là các máy chủ quản trị tập trung, các luồng dữ liệu sẽ bao gồm Luồng dữ liệu kết nối Internet để cập nhật mẫu phát hiện tấn công, và các truy vấn theo thời gian thực. Và luồng dữ liệu quản trị và cập nhật dữ liệu đến các Agent.
- Tại Công ty Điện lực: sẽ cài đặt Agent trên các máy tính người dùng để bảo vệ máy trạm, các Agent sẽ kết nối về TTDL thông qua đường Metro-WAN.

Mô tả các chức năng giải pháp



- Console: Cung cấp giao diện quản trị tập trung cho hệ thống phòng chống mã độc trên máy trạm điểm cuối.
- Modern Endpoint Protection: Cung cấp khả năng bảo vệ máy trạm với các công nghệ Next-Genration AV, Device Control, Anti-Phishing, Ransomware Remediation.
- Server Security: Cung cấp khả năng bảo vệ máy chủ.
- Mobile Threat Defense: Cung cấp khả năng phòng chống mã độc trên các thiết bị di động Android, iOS.
- Full Disk Encryption: Cung cấp khả năng mã hóa ổ cứng máy trạm.
- Advanced Threat Defense: Cung cấp khả năng phòng chống các mã độc nâng cao.

1.1.3 Các tính năng

STT	Tính năng	Mô tả
a) Console: Cung cấp giao diện quản trị tập trung cho hệ thống phòng chống mã độc trên máy trạm điểm cuối.		
1	**Phân quyền & người dùng (RBAC)**	Hỗ trợ tạo nhiều người dùng và nhóm quyền, giới hạn truy cập theo khu vực chức năng của console; cho phép phân tách nhiệm vụ trong môi trường doanh nghiệp lớn.
2	**Xác thực đa yếu tố (MFA)**	Bảo vệ truy cập console bằng xác thực nhiều lớp; tăng cường an toàn quản trị.

STT	Tính năng	Mô tả
3	**Nhóm động (Dynamic Groups)**	Tự động phân loại thiết bị dựa trên trạng thái hiện tại hoặc tiêu chí do quản trị viên định nghĩa.
4	**Chính sách & quyền kế thừa (Policy Management)**	Cho phép thiết lập nhiều chính sách cho cùng nhóm hoặc thiết bị; hỗ trợ kế thừa và khóa cấu hình người dùng.
5	**Hệ thống báo cáo nâng cao**	Cung cấp báo cáo mẫu và tùy chỉnh báo cáo theo yêu cầu quản trị.
6	**Tích hợp SIEM / SOC**	Xuất log theo định dạng **JSON** hoặc **LEEF**, dễ dàng tích hợp với hệ thống SIEM và trung tâm điều hành an ninh (SOC).
7	**Tương thích nền tảng quản lý di động (MDM)**	Hỗ trợ quản lý Android và iOS/iPadOS qua **Microsoft Intune, Entra ID, Apple Business Manager (ABM)** và **VMware Workspace ONE**.
8	**Phân tích mối đe dọa nâng cao (Advanced Threat Defense)**	Nâng cao khả năng phát hiện tấn công zero-day và ransomware thông qua sandbox đám mây mạnh mẽ của antivirus.
9	**Quản lý tài sản CNTT (IT Asset Visibility)**	Báo cáo chi tiết toàn bộ ứng dụng và phần cứng được cài đặt trong tổ chức; hỗ trợ kiểm kê và giám sát tài sản.
b) Modern Endpoint Protection: Cung cấp khả năng bảo vệ máy trạm với các công nghệ hiện đại.		
1	**Cập nhật dựa trên đám mây**	Tự động cập nhật định nghĩa và phản ứng nhanh với mối đe dọa mới mà không cần chờ bản cập nhật định kỳ.
2	**Phòng vệ đa lớp**	Phát hiện và ngăn chặn mã độc ở các giai đoạn trước, trong và sau khi thực thi, tối ưu cho nhiều môi trường hoạt động.
3	**Phát hiện ứng dụng lỗi định dạng / bị chiếm quyền**	Bảo vệ chống tấn công không file (fileless attack); liên tục quét bộ nhớ để phát hiện hành vi bất thường.
4	**Máy học (Machine Learning)**	Ứng dụng AI và mạng nơ-ron từ năm 1997; hỗ trợ chế độ học máy chuyên sâu, hoạt động cả khi không có kết nối Internet.
5	**Sandbox tích hợp sẵn (In-product Sandbox)**	Phân tích hành vi thực tế của mã độc bị làm rối (obfuscated malware) trong môi trường cách ly an toàn.

STT	Tính năng	Mô tả
6	**Bảo vệ tấn công mạng**	Phát hiện và ngăn chặn các lỗ hổng và tấn công khai thác trên tầng mạng.
7	**Phòng chống botnet**	Giám sát và chặn liên lạc độc hại từ botnet; xác định tiến trình phát sinh liên lạc và cảnh báo cho người dùng.
8	**Hệ thống phòng thủ xâm nhập HIPS**	Theo dõi hành vi hệ thống, áp dụng tập luật để ngăn hoạt động đáng ngờ và can thiệp trái phép.
9	**Quét UEFI**	Bảo vệ tầng khởi động hệ thống; giám sát và xác minh tính toàn vẹn firmware UEFI, cảnh báo khi bị sửa đổi.
10	**Bảo vệ trình duyệt**	Lớp bảo mật dành riêng cho trình duyệt – bảo vệ bộ nhớ, bàn phím, và cho phép định danh URL được bảo vệ.
11	**Quét bộ nhớ nâng cao**	Phát hiện mã độc hoạt động trong bộ nhớ (fileless malware); quét tiến trình khi hành vi độc hại được kích hoạt.
12	**Ngăn chặn khai thác lỗ hổng**	Giám sát ứng dụng dễ bị khai thác (trình duyệt, PDF reader, email, Java, Flash...), chặn kỹ thuật khai thác thay vì chỉ dựa trên CVE.
13	**Ngăn chặn rasomware**	Phân tích hành vi và danh tiếng ứng dụng; phát hiện và ngăn chặn tiến trình có đặc điểm ransomware.
14	**Tự động khôi phục**	Tự động khôi phục tệp từ bản sao lưu an toàn; giảm thiểu gián đoạn và thiệt hại do tấn công mã hóa dữ liệu.
c) Server Security: Khả năng bảo vệ máy chủ.		
1	**Kiểm soát truy cập web**	Kiểm soát truy cập web; chặn các trang web không phù hợp, độc hại hoặc làm giảm năng suất; đảm bảo chính sách thống nhất trên toàn bộ máy trạm và máy chủ.
2	**Firewall cho máy chủ**	Kiểm soát toàn bộ lưu lượng mạng của Windows Server thông qua tường lửa tối ưu cho môi trường máy chủ.
3	**Phòng chống ransomware**	Lớp bảo vệ bổ sung chống ransomware; giám sát hành vi và danh tiếng ứng dụng, phát hiện và chặn tiến trình có đặc điểm mã hóa tống tiền.

STT	Tính năng	Mô tả
4	**Phòng chống tấn công mạng**	Phát hiện và ngăn chặn tấn công khai thác lỗ hổng trên tầng mạng, kể cả các lỗ hổng chưa được vá hoặc triển khai bản vá.
5	**Hỗ trợ hệ điều hành Like Unix**	Cung cấp bộ cài cho các bản phân phối phổ biến của Unix_based (RedHat, SuSE, v.v.) tuân thủ chuẩn FHS; không yêu cầu thư viện ngoài trừ LIBC.
6	**Phòng chống xâm nhập trái phép trên máy chủ**	Giám sát hoạt động hệ thống theo tập luật xác định sẵn; nhận diện và chặn hành vi bất thường hoặc xâm nhập trái phép.
7	**Quét bộ nhớ nâng cao**	Phát hiện mã độc ẩn (fileless malware) bằng cách giám sát hành vi tiến trình và quét khi mã độc hoạt động trong bộ nhớ.
8	**Phòng chống botnet**	Phát hiện và ngăn chặn liên lạc với botnet; xác định tiến trình gây ra liên lạc độc hại và cảnh báo cho người dùng.
9	**Phân tích hành vi bằng sandbox trên cloud**	Phân tích tệp khả nghi trong môi trường sandbox trên đám mây để phát hiện các mẫu mã độc mới, chưa từng xuất hiện.
10	**Ngăn chặn khai thác lỗ hổng**	Giám sát ứng dụng dễ bị khai thác (trình duyệt, trình đọc tài liệu, email client, Flash, Java...); chặn kỹ thuật khai thác ngay khi kích hoạt.
11	**Tích hợp sandbox**	Phân tích hành vi thực tế của mã độc bị làm rối (obfuscated malware) trong môi trường an toàn nội bộ.
d) Mobile Threat Defense: Phòng chống mã độc trên các thiết bị di động Android, iOS.		
1	**Quản lý tập trung:**	*Điều khiển toàn bộ thiết bị đầu cuối và di động từ bảng điều khiển . (Hỗ trợ Android, iOS, iPadOS)*
2	**Phòng vệ đa lớp:**	*Phát hiện và ngăn chặn mã độc trước, trong và sau khi thực thi; tối ưu cho hiệu năng thiết bị di động. (Hỗ trợ Android)*
3	**Bảo vệ chống lừa đảo:**	*Ngăn chặn truy cập vào các website giả mạo thu thập mật khẩu, dữ liệu ngân hàng hoặc thông tin nhạy cảm. (Hỗ trợ Android)*
4	**Giám sát truy cập dữ liệu:**	*Theo dõi quyền truy cập ứng dụng tới dữ liệu cá nhân/doanh nghiệp, phân loại theo nhóm để kiểm soát linh hoạt. (Hỗ trợ Android)*

STT	Tính năng	Mô tả
5	**Lọc nội dung web:**	*Giới hạn hoặc chặn truy cập website không phù hợp hoặc ảnh hưởng năng suất; hỗ trợ mẫu báo cáo mặc định và tùy chỉnh. (Hỗ trợ Android)*
6	**Hỗ trợ hệ điều hành:**	*Android:;iOS / iPadOS:*
e) Full Disk Encryption: Khả năng mã hóa ổ cứng máy trạm.		
1	**Quản lý Tập trung**	Tích hợp trực tiếp trong **console**, cho phép quản trị viên quản lý mã hóa từ giao diện quen thuộc, tiết kiệm thời gian.
2	**Mã hóa Tăng tốc bằng Phần cứng**	Sử dụng **AES-NI** để thực hiện mã hóa AES 256-bit với hiệu suất cao, giảm thiểu tác động đến hệ thống.
3	**Mã hóa Ổ đĩa Toàn diện**	Mã hóa toàn bộ ổ đĩa hệ thống, phân vùng và thiết bị lưu trữ, bảo vệ dữ liệu khỏi mất mát hoặc đánh cắp.
4	**Quản lý Đa nền tảng**	Quản lý mã hóa ổ đĩa trên **Windows** và mã hóa gốc **macOS (FileVault)** từ cùng một bảng điều khiển.
5	**Triển khai với cấu hình định sẵn**	Hỗ trợ triển khai Full Disk Encryption với **mật khẩu được định sẵn**, giúp đơn giản hóa quá trình cài đặt cho quản trị viên.
6	**Kiểm soát chính sách mật khẩu**	Quản trị viên có thể đặt yêu cầu mật khẩu (độ phức tạp, số lần nhập sai, thời hạn), và cho phép người dùng thay đổi mật khẩu khi cần.
7	**Bảo vệ 2 lớp**	Cung cấp lớp bảo vệ kép, giảm rủi ro vi phạm, đáp ứng yêu cầu tuân thủ bảo mật dữ liệu.
8	**Mã hóa có chọn lọc**	Cho phép mã hóa **chỉ vùng dữ liệu đã sử dụng** trên hệ thống mới hoặc ổ đã xóa sạch, giúp tiết kiệm thời gian và tài nguyên khi triển khai.
f) Advanced Threat Defense: Phòng chống các mã độc nâng cao.		
1	**Phát hiện đa tầng**	Sử dụng **4 lớp phân tích độc lập** nhằm tối đa hóa khả năng phát hiện: (1) Phân tích tĩnh & giải nén, (2) Phân tích tĩnh + động với **Machine Learning & Deep Learning**, (3) Kiểm tra hành vi trong **sandbox mô phỏng cao cấp**, (4) Phân tích hành vi sâu để phát hiện mẫu độc hại.

STT	Tính năng	Mô tả
2	**Xử lý Mối đe dọa Tự động**	Endpoint hoặc Server tự động xác định mẫu là "tốt / xấu / không rõ". Mẫu không rõ được gửi đến **console** để phân tích và đồng bộ kết quả đến toàn bộ endpoint trong vài phút.
3	**Khả năng Hiển thị/Quan sát Tập trung**	Mọi trạng thái phân tích mẫu hiển thị trong bảng điều khiển. Có thể yêu cầu xóa mẫu sau phân tích để đảm bảo quyền riêng tư.
4	**Bảo vệ Người dùng Từ xa**	Phân tích file và hành vi **kể cả khi người dùng làm việc ngoài mạng nội bộ**, đảm bảo bảo vệ liên tục.
5	**Chặn Thời gian Thực**	Khi phát hiện mẫu nghi ngờ, tiến trình bị **chặn thực thi** cho đến khi có kết quả phân tích; toàn bộ hệ thống mạng được cập nhật kết quả trong vài phút.
6	**Kiểm soát Chính sách Chi tiết/Từng phần**	Cho phép **cấu hình chính sách chi tiết theo từng máy**, kiểm soát nội dung gửi đi và hành động tương ứng với kết quả phân tích.
7	**Gửi Mẫu Thủ công**	Người dùng hoặc quản trị viên có thể **gửi mẫu thủ công** từ sản phẩm antivirus để phân tích; kết quả hiển thị trực tiếp trên **console** kèm thông tin người gửi.
g) Các yêu cầu kỹ thuật khác		
1	**Yêu cầu tối thiểu tài nguyên máy trạm**	RAM =< 1GB Dung lượng ổ cứng còn trống tối thiểu: 1GB Phần mềm cài đặt trên máy trạm không làm ảnh hưởng đến hoạt động của máy trạm
2	**Có khả năng kết nối, chia sẻ thông tin**	Cho phép kết nối, chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng Quốc gia theo hướng dẫn tại công văn số 2290/BTTTT-CATTT ngày 17/7/2018 của Bộ Thông tin và Truyền thông.
3	Chỉ cài đặt 1 phần mềm duy nhất đáp ứng tất cả các yêu cầu tính năng trên	

1.1.4. Số lượng và thời hạn bản quyền:

Vật tư, thiết bị chính	Chủng loại/Quy cách	Đơn vị tính	Số lượng
Bản quyền phần mềm diệt Virus. Thời hạn bản quyền 01 năm	Bao gồm cài đặt và hỗ trợ dịch vụ 01 năm	License	4000

1.1.5 Yêu cầu về triển khai và đào tạo:

Yêu cầu nhà thầu kết hợp với Công ty Công nghệ thông tin điện lực Thành Phố Hà Nội:

- Triển khai cài đặt tích hợp phần mềm; kiểm tra, hiệu chỉnh phần mềm.
- Thực hiện đào tạo và chuyển giao vận hành hệ thống.