PHƯƠNG NAM EDU

DỊCH VỤ AN TOÀN THÔNG TIN



CÔNG TY CỔ PHẦN HỌC LIỆU VÀ THIẾT BỊ PHƯƠNG NAM

Hotline: 0903 780 668 | phuongnam.group

Tài liệu giới thiệu PNE – thông tin năng lực, hạ tầng và khách hàng tham chiếu từ tài liệu đối tác; cần xác nhận trước khi sử dụng.

PNE

PNE CYBER SECURITY SERVICES PORTFOLIO

Tư vấn chiến lược & kiến trúc ATTT

Bao gồm đánh giá rủi ro, xây dựng chiến lược ATTT, tư vấn kiến trúc bảo mật hệ thống CNTT theo cấp độ từ 1 đến 5.

Dịch vụ đánh giá & kiểm thử

Security Audit, Vulnerability Assessment, Penetration Testing và Red Team giúp nhận diện, đánh giá và xử lý các điểm yếu bảo mật.

Dịch vụ quản lý & giám sát ATTT

Managed SOC, Threat Hunting, Incident Response, DDoS Protection, SD-WAN,... bảo vệ liên tục và phản ứng tức thời 24/7.

Giải pháp bảo mật

Cloud Firewall, EDR, WAF, MFA, DLP... hỗ trợ bảo mật toàn diện cho hệ thống Cloud và mô hình Zero Trust Architecture.



PHƯƠNG NAM EDU

GIẢI PHÁP

ĐÁNH GIÁ CẤP ĐỘ AN NINH MẠNG







ĐƠN VỊ CUNG CẤP

PHƯƠNG NAM EDU

CYBER SECURITY SERVICES CENTER

NGƯỜI TRÌNH BÀY

Tư vấn giải pháp ATTT

Tài liệu giới thiệu PNE – thông tin năng lực, hạ tầng và khách hàng tham chiếu từ tài liệu đối tác; cần xác nhận trước khi sử dụng.

PNE

PNE CYBER SECURITY SERVICES PORTFOLIO

Tư vấn chiến lược & kiến trúc ATTT

Bao gồm đánh giá rủi ro, xây dựng chiến lược ATTT, tư vấn kiến trúc bảo mật hệ thống CNTT theo cấp độ từ 1 đến 5.

Dịch vụ đánh giá & kiểm thử

Security Audit, Vulnerability Assessment, Penetration Testing và Red Team giúp nhận diện, đánh giá và xử lý các điểm yếu bảo mật.

Dịch vụ quản lý & giám sát ATTT

Managed SOC, Threat Hunting, Incident Response, DDoS Protection, SD-WAN,... bảo vệ liên tục và phản ứng tức thời 24/7.

Giải pháp bảo mật

Cloud Firewall, EDR, WAF, MFA, DLP... hỗ trợ bảo mật toàn diện cho hệ thống Cloud và mô hình Zero Trust Architecture.



PNE

CẬP NHẬT KHUNG PHÁP LÝ CẤP ĐỘ AN NINH MẠNG 2026

Cơ sở pháp lý mới nhất về phân loại cấp độ, bảo vệ hệ thống thông tin và bảo vệ dữ liệu cá nhân

01 LUẬT

- **Luật An ninh mạng 116/2025/QH15**
  Hiệu lực: 01/07/2026
- **Luật Bảo vệ dữ liệu cá nhân 91/2025/QH15**
  Hiệu lực: 01/01/2026

Nền tảng pháp lý cao nhất cho an ninh mạng và bảo vệ dữ liệu cá nhân.

02 NGHỊ ĐỊNH VỀ CẤP ĐỘ

Nghị định 331/2026/NĐ-CP

Ban hành: 19/08/2026
Hiệu lực: 19/08/2026

- Bảo vệ hệ thống thông tin.
- Phân loại hệ thống thông tin theo cấp độ (Cấp 1–5).
- Hồ sơ đề xuất cấp độ.
- Thẩm định, phê duyệt cấp độ.
- Kế hoạch bảo đảm an ninh mạng theo cấp độ.

Quy định chi tiết về phân loại, đánh giá và bảo đảm an ninh mạng theo cấp độ.

03 NGHỊ ĐỊNH BIỆN PHÁP THI HÀNH

Nghị định 333/2026/NĐ-CP

- Quy định chi tiết thi hành một số điều của Luật An ninh mạng.
- Hướng dẫn tổ chức thực hiện, trách nhiệm của cơ quan, tổ chức và cá nhân.
- Chi tiết về kỹ thuật, quản lý nhà nước, kiểm tra, giám sát.

Nghị định 356/2025/NĐ-CP

- Quy định chi tiết thi hành một số điều của Luật Bảo vệ dữ liệu cá nhân.
- Hướng dẫn xử lý dữ liệu cá nhân, quyền và nghĩa vụ của chủ thể dữ liệu.
- Đánh giá tác động, chuyển dữ liệu, bảo mật dữ liệu cá nhân.

Hướng dẫn thực thi Luật An ninh mạng và Luật Bảo vệ dữ liệu cá nhân.

04 NGHỊ ĐỊNH XỬ PHẠT

Nghị định 330/2026/NĐ-CP

Ban hành: 19/08/2026
Hiệu lực: 19/08/2026

- Quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng.
- Quy định xử phạt vi phạm hành chính trong lĩnh vực bảo vệ dữ liệu cá nhân.
- Áp dụng cho tổ chức, cá nhân vi phạm các quy định của Luật và Nghị định liên quan.

Khung xử phạt và quản trị rủi ro pháp lý khi vi phạm.

05 TIÊU CHUẨN KỸ THUẬT

- **TCVN 14423:2026**
  An ninh mạng – Hệ thống thông tin – Yêu cầu cơ bản.
- **TCVN 14620:2026**
  An ninh mạng – Tường lửa – Yêu cầu kỹ thuật chung.

Hướng dẫn kỹ thuật áp dụng để triển khai, đánh giá và bảo đảm an ninh mạng.

MỐI LIÊN HỆ GIỮA CÁC VĂN BẢN PHÁP LÝ

NỀN TẢNG PHÁP LÝ
Luật An ninh mạng 116/2025/QH15
+
Luật Bảo vệ dữ liệu cá nhân 91/2025/QH15

→

PHÂN LOẠI & THỰC THI AN NINH MẠNG
NĐ 331/2026/NĐ-CP: Quy định phân loại cấp độ, đánh giá và bảo đảm an ninh mạng.
→
NĐ 333/2026/NĐ-CP: Hướng dẫn thi hành Luật An ninh mạng, chi tiết kỹ thuật và tổ chức thực hiện.

→

THỰC THI BẢO VỆ DỮ LIỆU CÁ NHÂN
NĐ 356/2025/NĐ-CP: Hướng dẫn thi hành Luật Bảo vệ dữ liệu cá nhân, bảo đảm quyền và nghĩa vụ liên quan đến dữ liệu cá nhân.

→

XỬ PHẠT & QUẢN TRỊ RỦI RO
NĐ 330/2026/NĐ-CP: Quy định xử phạt hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân.

→

HƯỚNG DẪN KỸ THUẬT
TCVN, QCVN: Hướng dẫn kỹ thuật, tiêu chuẩn áp dụng để triển khai, đánh giá và duy trì tuân thủ.

LƯU Ý QUAN TRỌNG CHO DOANH NGHIỆP

Xác định đúng cấp độ
Đánh giá, phân loại chính xác để áp dụng đúng yêu cầu bảo đảm an ninh mạng theo quy định.

Tuân thủ quy trình
Thực hiện đầy đủ: hồ sơ đề xuất – thẩm định – phê duyệt – kế hoạch bảo đảm an ninh mạng theo cấp độ.

Triển khai biện pháp bảo đảm
Áp dụng các biện pháp kỹ thuật, quản lý theo TCVN, QCVN để bảo vệ hệ thống thông tin và dữ liệu cá nhân.

Giảm thiểu rủi ro pháp lý
Tuân thủ pháp luật giúp giảm thiểu rủi ro, tránh xử phạt và nâng cao uy tín, niềm tin với khách hàng, đối tác.

HIỆU LỰC TẤT CẢ CÁC VĂN BẢN
Các văn bản nêu trên có hiệu lực (từ ngày hiệu lực tương ứng) và được áp dụng thống nhất từ năm 2026 trở đi.

Nguồn tham chiếu: Luật ANM 116/2025/QH15; Luật BVDLCN 91/2025/QH15; NĐ 331/2026/NĐ-CP; NĐ 333/2026/NĐ-CP; NĐ 356/2025/NĐ-CP; NĐ 330/2026/NĐ-CP; TCVN 14423:2026; TCVN 14620:2026.

PNE

THẨM QUYỀN, TRÌNH TỰ, THỦ TỤC XÁC ĐỊNH CẤP ĐỘ

Cập nhật theo Nghị định 331/2026/NĐ-CP về bảo vệ an ninh mạng đối với hệ thống thông tin.

1. Đối với dự án đầu tư xây mới hoặc mở rộng, nâng cấp

- Xác định cấp độ và yêu cầu bảo vệ an ninh mạng phải được xem xét ngay trong giai đoạn chuẩn bị đầu tư, thiết kế, xây dựng.
- Hồ sơ phải kèm căn cứ xác định cấp độ, kết quả đánh giá rủi ro an ninh mạng và phương án bảo đảm an ninh mạng theo cấp độ đề xuất.

2. Đối với hệ thống thông tin đang vận hành

STT	Trình tự, thủ tục	Cấp độ 1–2	Cấp độ 3	Cấp độ 4	Cấp độ 5
1	Xác định cấp độ và lập hồ sơ	Đơn vị vận hành / Chủ quản HTTT	Đơn vị vận hành / Chủ quản HTTT	Đơn vị vận hành / Chủ quản HTTT	Đơn vị vận hành / Chủ quản HTTT
2	Đánh giá rủi ro an ninh mạng	Thực hiện và lưu hồ sơ làm căn cứ xác định cấp độ	Thực hiện và đối chiếu biện pháp bảo vệ theo cấp độ	Thực hiện chuyên sâu, làm căn cứ xem xét cấp độ và biện pháp trọng yếu	Thực hiện chuyên sâu, làm căn cứ xem xét cấp độ và biện pháp trọng yếu
3	Thẩm định hồ sơ	Đơn vị chuyên trách an ninh mạng của chủ quản HTTT	Đơn vị chuyên trách an ninh mạng	Bộ Công an chủ trì thẩm định (trừ HT quân sự, cơ yếu)	Bộ Công an chủ trì thẩm định (trừ HT quân sự, cơ yếu)
4	Phê duyệt cấp độ / phương án bảo đảm ANM	Đơn vị chuyên trách an ninh mạng của chủ quản HTTT phê duyệt; sau đó báo cáo chủ quản HTTT	Chủ quản hệ thống thông tin phê duyệt	Chủ quản hệ thống thông tin phê duyệt	Thủ tướng Chính phủ phê duyệt Danh mục HTTT cấp độ 5; Chủ quản HTTT phê duyệt phương án bảo đảm ANM

Lưu ý: Việc xác định cấp độ cần gắn với đánh giá rủi ro an ninh mạng; kết quả đánh giá rủi ro là một trong các căn cứ quan trọng để xem xét cấp độ và biện pháp bảo vệ phù hợp.

Nguồn tham chiếu: *Nghị định 331/2026/NĐ-CP; Luật An ninh mạng số 116/2025/QH15; TCVN 14423:2026.*

PNE

XÁC ĐỊNH CẤP ĐỘ

Theo NĐ 331/2026/NĐ-CP, cấp độ 1–5 được xác định theo tính chất hệ thống, loại dữ liệu xử lý, đối tượng phục vụ và mức độ ảnh hưởng khi xảy ra sự cố.

CẤP ĐỘ 1

HTTT nội bộ, chỉ xử lý thông tin công cộng.

- Phạm vi hẹp, ảnh hưởng giới hạn.
- Không xử lý dữ liệu cá nhân nhạy cảm, không xử lý bí mật nhà nước.

CẤP ĐỘ 2

HTTT nội bộ có xử lý thông tin riêng hoặc dữ liệu cá nhân, nhưng không xử lý bí mật nhà nước.

- Ảnh hưởng chủ yếu trong phạm vi cơ quan, tổ chức.
- Yêu cầu kiểm soát chặt hơn về truy cập, dữ liệu và vận hành.

CẤP ĐỘ 3

HTTT phục vụ người dân, doanh nghiệp hoặc hệ thống nội bộ quan trọng.

- Có xử lý dữ liệu cá nhân quy mô lớn hoặc cung cấp dịch vụ số diện rộng.
- Có thể tích hợp CSDL dân cư, VNeID hoặc dịch vụ định danh, xác thực điện tử.
- Kết quả đánh giá rủi ro có thể là căn cứ đề xuất nâng cấp độ.

Nguồn tham chiếu: NĐ 331/2026/NĐ-CP; Luật An ninh mạng 116/2025/QH15.

PNE

XÁC ĐỊNH CẤP ĐỘ 4, 5 & ĐÁNH GIÁ RỦI RO

Theo NĐ 331/2026/NĐ-CP, cấp độ 4 và 5 áp dụng cho các hệ thống quan trọng, trọng yếu; kết quả đánh giá rủi ro an ninh mạng là căn cứ quan trọng để xem xét đề xuất nâng cấp độ.

Tiêu chí cấp độ 4

CẤP ĐỘ 4

- HTTT quan trọng, nếu bị tấn công hoặc gián đoạn có thể gây ảnh hưởng nghiêm trọng tới hoạt động ngành, lĩnh vực hoặc hạ tầng thiết yếu.
- Yêu cầu mức sẵn sàng cao, khả năng vận hành liên tục và kiểm soát tăng cường.
- Thường áp dụng với hệ thống trọng yếu phục vụ diện rộng hoặc vận hành quan trọng.

Tiêu chí cấp độ 5

CẤP ĐỘ 5

- HTTT đặc biệt quan trọng, nếu bị xâm phạm có thể ảnh hưởng đặc biệt nghiêm trọng tới an ninh quốc gia, quốc phòng, chủ quyền hoặc hạ tầng quốc gia.
- Áp dụng với hệ thống đặc biệt trọng yếu, yêu cầu bảo vệ ở mức cao nhất.
- Cần cơ chế kiểm soát nghiêm ngặt, giám sát tập trung và phương án ứng cứu chuyên sâu.

Đánh giá rủi ro an ninh mạng là căn cứ quan trọng để xem xét đề xuất nâng cấp độ theo NĐ 331/2026/NĐ-CP.

PNE

THÀNH PHẦN HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

Rà soát và xây dựng hồ sơ theo NĐ 331/2026/NĐ-CP và TCVN 14423:2026; tham khảo cấu trúc TT 12/2022/TT-BTTTT khi còn phù hợp.

01

Văn bản đề nghị thẩm định, phê duyệt

- Văn bản đề nghị của đơn vị/chủ quản hệ thống thông tin.
- Nêu rõ phạm vi, tên HTTT và cấp độ đề xuất.

02

Tài liệu hồ sơ đề xuất cấp độ

- Thuyết minh tổng quan HTTT
- Thuyết minh đề xuất cấp độ
- Thuyết minh phương án bảo đảm an ninh mạng

03

Quy chế / tài liệu quản lý

- Dự thảo hoặc Quy chế về bảo đảm an ninh mạng đã ban hành.
- Các chính sách, quy trình, phân công, phân nhiệm liên quan đến bảo đảm an ninh mạng.

04

Tài liệu thiết kế hệ thống thông tin

- Thiết kế sơ bộ / thiết kế thi công / tài liệu tương đương.
- Sơ đồ mạng, kiến trúc, phân vùng và thành phần bảo vệ.

Nguồn tham chiếu: NĐ 331/2026/NĐ-CP và TCVN 14423:2026; tham khảo cấu trúc TT 12/2022/TT-BTTTT khi còn phù hợp.

PNE

QUY TRÌNH THẨM ĐỊNH, PHÊ DUYỆT CẤP ĐỘ 1, 2

Xác định, thẩm định và phê duyệt cấp độ đối với HTTT cấp độ 1, 2 theo Nghị định 331/2026/NĐ-CP.

Hồ sơ, tài liệu chính

1. Văn bản đề nghị thẩm định, phê duyệt hồ sơ xác định cấp độ
2. Thuyết minh tổng quan hệ thống thông tin
3. Tài liệu thiết kế, mô hình logic/vật lý của hệ thống
4. Thuyết minh căn cứ xác định cấp độ
5. Thuyết minh phương án bảo đảm an ninh mạng

1 ĐƠN VỊ VẬN HÀNH / CHỦ QUẢN HTTT

Lập hồ sơ xác định cấp độ

→

2 ĐƠN VỊ CHUYÊN TRÁCH AN NINH MẠNG

Thẩm định và phê duyệt hồ sơ

→

3 PHÊ DUYỆT CẤP ĐỘ 1, 2

Ban hành quyết định phê duyệt cấp độ

→

4 BÁO CÁO CHỦ QUẢN HTTT

Thực hiện theo quy định nội bộ

- **Đối tượng thực hiện:** Đơn vị vận hành hoặc chủ quản hệ thống thông tin.
- **Cơ quan thẩm định/phê duyệt:** Đơn vị chuyên trách an ninh mạng của chủ quản HTTT.

Lưu ý: Đối với cấp độ 1, 2, đơn vị chuyên trách an ninh mạng của chủ quản HTTT thực hiện thẩm định và phê duyệt; sau khi phê duyệt, kết quả được báo cáo chủ quản HTTT theo quy định.

Nguồn tham chiếu: Nghị định 331/2026/NĐ-CP; Luật An ninh mạng số 116/2025/QH15; TCVN 14423:2026.

PNE

QUY TRÌNH THẨM ĐỊNH, PHÊ DUYỆT CẤP ĐỘ 3

Xác định, thẩm định và phê duyệt cấp độ đối với HTTT cấp độ 3 theo Nghị định 331/2026/NĐ-CP.

Hồ sơ, tài liệu chính

1. Văn bản đề nghị thẩm định hồ sơ xác định cấp độ
2. Thuyết minh tổng quan hệ thống thông tin
3. Tài liệu thiết kế, mô hình logic/vật lý của hệ thống
4. Thuyết minh căn cứ xác định cấp độ
5. Thuyết minh phương án bảo đảm an ninh mạng

1 ĐƠN VỊ VẬN HÀNH / CHỦ QUẢN HTTT

Lập hồ sơ xác định cấp độ

→

2 ĐƠN VỊ CHUYÊN TRÁCH AN NINH MẠNG

Thẩm định hồ sơ

→

3 Ý KIẾN THẨM ĐỊNH

Ban hành văn bản thẩm định

→

4 PHÊ DUYỆT CẤP ĐỘ 3

Chủ quản HTTT phê duyệt cấp độ

- **Đối tượng thực hiện:** Đơn vị vận hành hoặc chủ quản hệ thống thông tin.
- **Cơ quan thẩm định:** Đơn vị chuyên trách an ninh mạng của chủ quản HTTT.
- **Cơ quan phê duyệt:** Chủ quản hệ thống thông tin.

Lưu ý: Đối với cấp độ 3, đơn vị chuyên trách an ninh mạng thực hiện thẩm định; chủ quản HTTT ban hành quyết định phê duyệt cấp độ và tổ chức triển khai phương án bảo đảm an ninh mạng.

Nguồn tham chiếu: Nghị định 331/2026/NĐ-CP; Luật An ninh mạng số 116/2025/QH15; TCVN 14423:2026.

PNE

PHƯƠNG ÁN BẢO ĐẢM AN NINH MẠNG THEO CẤP ĐỘ

Căn cứ Nghị định 331/2026/NĐ-CP, Luật An ninh mạng 2025 và TCVN 14423:2026.

YÊU CẦU VỀ QUẢN LÝ

Chính sách an ninh mạng, quản lý rủi ro, tổ chức nhân sự, quản lý vận hành, quản lý thay đổi, giám sát và ứng cứu sự cố.



YÊU CẦU VỀ KỸ THUẬT

An toàn mạng, an toàn máy chủ/thiết bị đầu cuối, an toàn ứng dụng, an toàn dữ liệu, nhận dạng/xác thực, giám sát nhật ký và sao lưu.



Phương án bảo đảm an ninh mạng phải bám theo cấp độ đề xuất và được chứng minh bằng cấu hình, quy trình và bằng chứng triển khai thực tế.

PNE

THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN NINH MẠNG

Thuyết minh phương án đáp ứng các yêu cầu về **quản lý** tương ứng với cấp độ đề xuất

Thuyết minh phương án đáp ứng các yêu cầu về **kỹ thuật** tương ứng với cấp độ đề xuất

Căn cứ Nghị định 331/2026/NĐ-CP, Luật An ninh mạng số 116/2025/QH15, Thông tư 12/2022/TT-BTTTT và TCVN 14423:2026:

1. **Yêu cầu về quản lý:** chính sách, tổ chức, nhân lực, quản lý rủi ro an ninh mạng, thiết kế/xây dựng, vận hành, ứng cứu sự cố, kết thúc vận hành.
2. **Yêu cầu về kỹ thuật:** an toàn/an ninh mạng, bảo vệ máy chủ, ứng dụng, dữ liệu, kiểm soát truy cập, ghi nhật ký, giám sát, sao lưu và phục hồi.
3. **Biện pháp bảo đảm** phải gắn với cấp độ đã xác định và kết quả đánh giá rủi ro; trường hợp rủi ro cao có thể là căn cứ để đề xuất nâng cấp độ.

Chi tiết đối chiếu thực hiện theo quy định của Nghị định 331/2026/NĐ-CP, thành phần hồ sơ theo Thông tư 12/2022/TT-BTTTT và yêu cầu kiểm soát theo TCVN 14423:2026.

Nguồn tham chiếu: Luật An ninh mạng số 116/2025/QH15; Nghị định 331/2026/NĐ-CP; Thông tư 12/2022/TT-BTTTT; TCVN 14423:2026.

THUYẾT MINH ĐÁP ỨNG CÁC YÊU CẦU VỀ QUẢN LÝ

YÊU CẦU VỀ QUẢN LÝ

1. Chính sách bảo vệ an ninh mạng
- Ban hành chính sách
- Phổ biến / áp dụng
- Rà soát, cập nhật

2. Tổ chức bảo đảm an ninh mạng
- Đơn vị/đầu mối chuyên trách
- Phối hợp nội bộ và bên thứ ba

3. Bảo đảm nguồn nhân lực
- Tuyển dụng / sàng lọc
- Đào tạo, nâng cao nhận thức
- Thay đổi / chấm dứt công việc

4. Quản lý rủi ro và thiết kế hệ thống
- Đánh giá rủi ro ANM
- Yêu cầu ANM trong thiết kế
- Thử nghiệm / nghiệm thu

5. Quản lý vận hành hệ thống
- Quản lý an toàn mạng
- Quản lý máy chủ, ứng dụng, dữ liệu
- Quản lý sự cố và ứng cứu
- Giám sát, nhật ký
- Quản lý điểm yếu
- Quản lý người sử dụng

6. Yêu cầu bổ sung theo NĐ 331
- Phương án bảo vệ dữ liệu cá nhân/BMNN
- Quản lý bên thứ ba, nhà thầu
- Kế hoạch duy trì, kết thúc, khôi phục

Nội dung thuyết minh phải thể hiện đầy đủ yêu cầu quản lý tương ứng với cấp độ đề xuất và bằng chứng triển khai thực tế.

PNE

THUYẾT MINH ĐÁP ỨNG CÁC YÊU CẦU VỀ KỸ THUẬT

YÊU CẦU VỀ KỸ THUẬT

1. Bảo đảm an toàn mạng

- Thiết kế phân vùng mạng
- Kiểm soát truy cập mạng
- Phòng chống xâm nhập
- Nhật ký hệ thống mạng

2. Bảo đảm an toàn máy chủ/thiết bị đầu cuối

- Xác thực
- Kiểm soát truy cập
- Chống mã độc / EDR
- Nhật ký hệ thống
- Cứng hóa cấu hình

3. Bảo đảm an toàn ứng dụng và danh tính

- Quản lý tài khoản / MFA
- Kiểm soát truy cập
- Bảo mật thông tin liên lạc
- Chống chối bỏ
- An toàn ứng dụng và mã nguồn

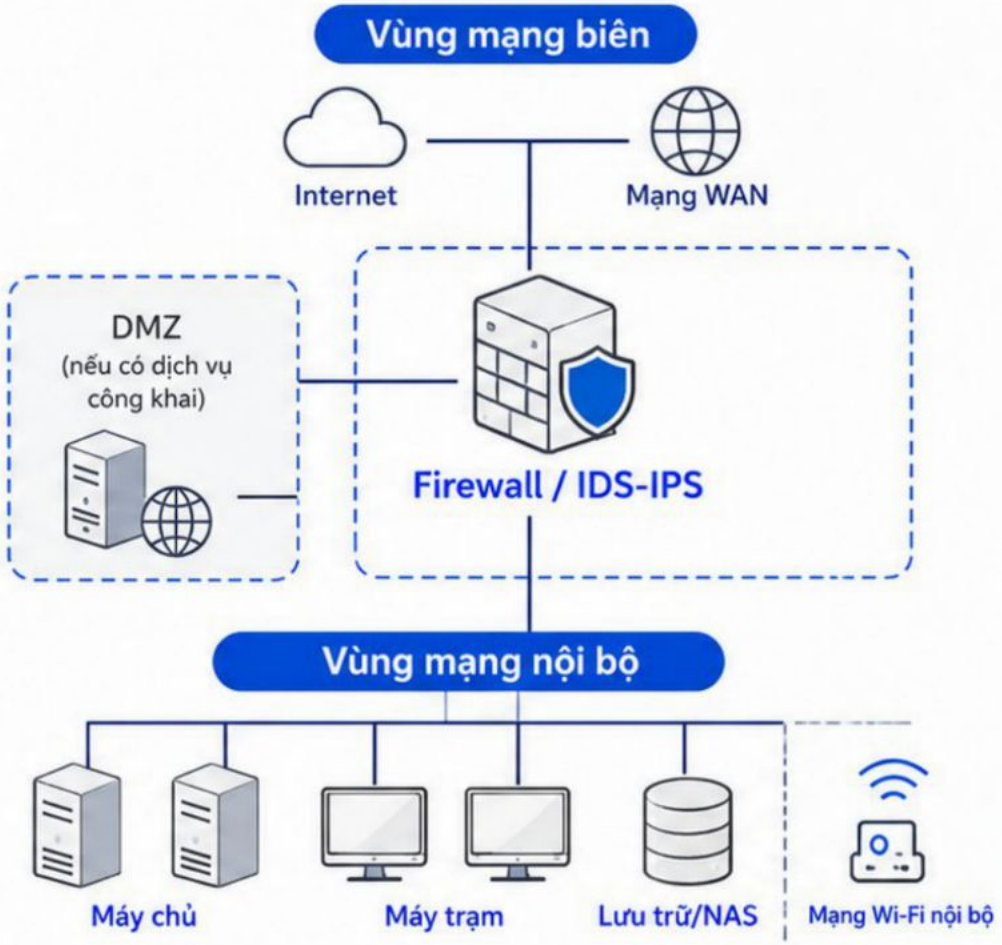
4. Bảo đảm an toàn dữ liệu

- Toàn vẹn dữ liệu
- Bảo vệ / mã hóa dữ liệu
- Sao lưu dự phòng
- Giám sát truy cập dữ liệu
- DLP khi áp dụng

Biện pháp kỹ thuật phải phù hợp cấp độ đề xuất và được thuyết minh bằng kiến trúc, cấu hình, log, cơ chế giám sát và bằng chứng kiểm tra.

PNE

YÊU CẦU VỀ THIẾT KẾ HỆ THỐNG ĐẠT AN NINH MẠNG CẤP ĐỘ 1



Phương án thiết kế tham chiếu theo NĐ 331/2026/NĐ-CP và TCVN 14423:2026:

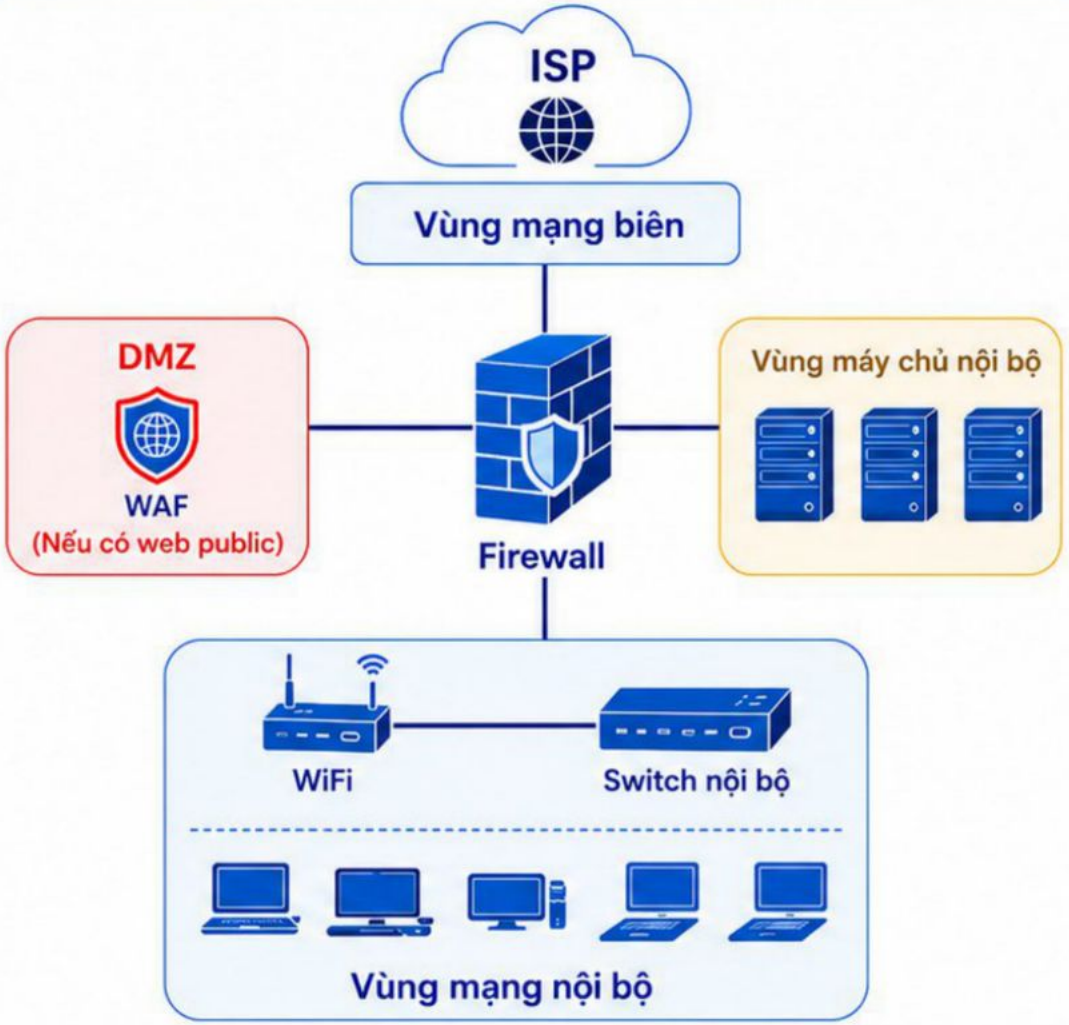
1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn *(sử dụng VPN hoặc phương án tương đương khi cần).*

2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập *(Firewall hoặc giải pháp tương đương).*

3. Có phương án phòng chống mã độc cho máy chủ và máy trạm; thực hiện sao lưu và lưu nhật ký tối thiểu để phục vụ vận hành.

PNE

YÊU CẦU VỀ THIẾT KẾ HỆ THỐNG ĐẠT AN NINH MẠNG CẤP ĐỘ 2

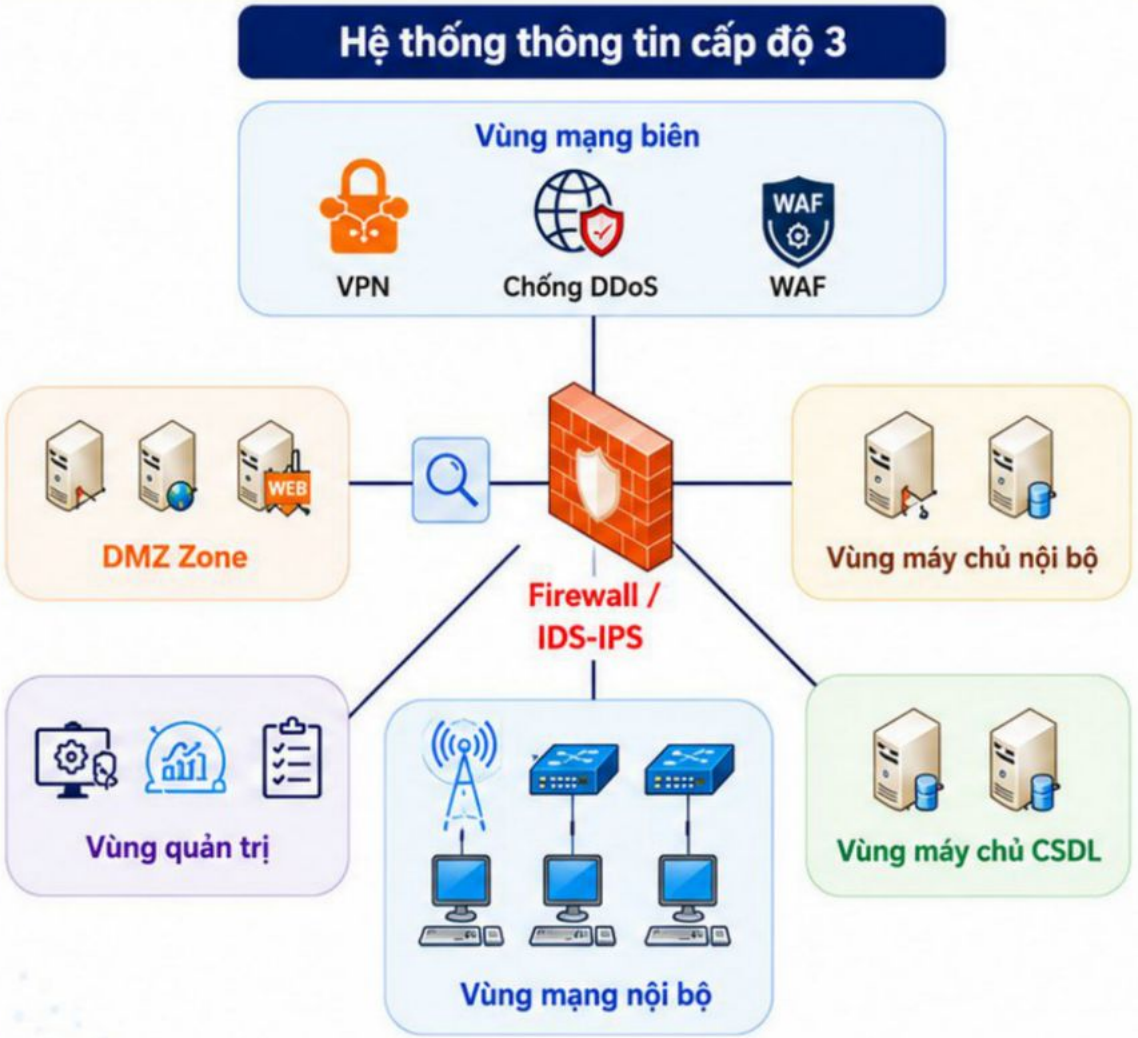


Phương án thiết kế tham chiếu theo NĐ 331/2026/NĐ-CP và TCVN 14423:2026:

1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn *(VPN hoặc giải pháp tương đương).*
2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập *(Firewall tích hợp hoặc IDS/IPS).*
3. Có phương án phòng chống mã độc cho máy chủ và máy trạm.
4. Có phương án bảo vệ ứng dụng web công khai *(WAF hoặc giải pháp tương đương)* khi hệ thống có web public.
5. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử *(anti-spam, anti-malware cho email)* nếu có dịch vụ email.
6. Có phương án dự phòng cho các thiết bị mạng chính và cơ chế sao lưu/khôi phục phù hợp.

PNE

YÊU CẦU VỀ THIẾT KẾ HỆ THỐNG ĐẠT AN NINH MẠNG CẤP ĐỘ 3

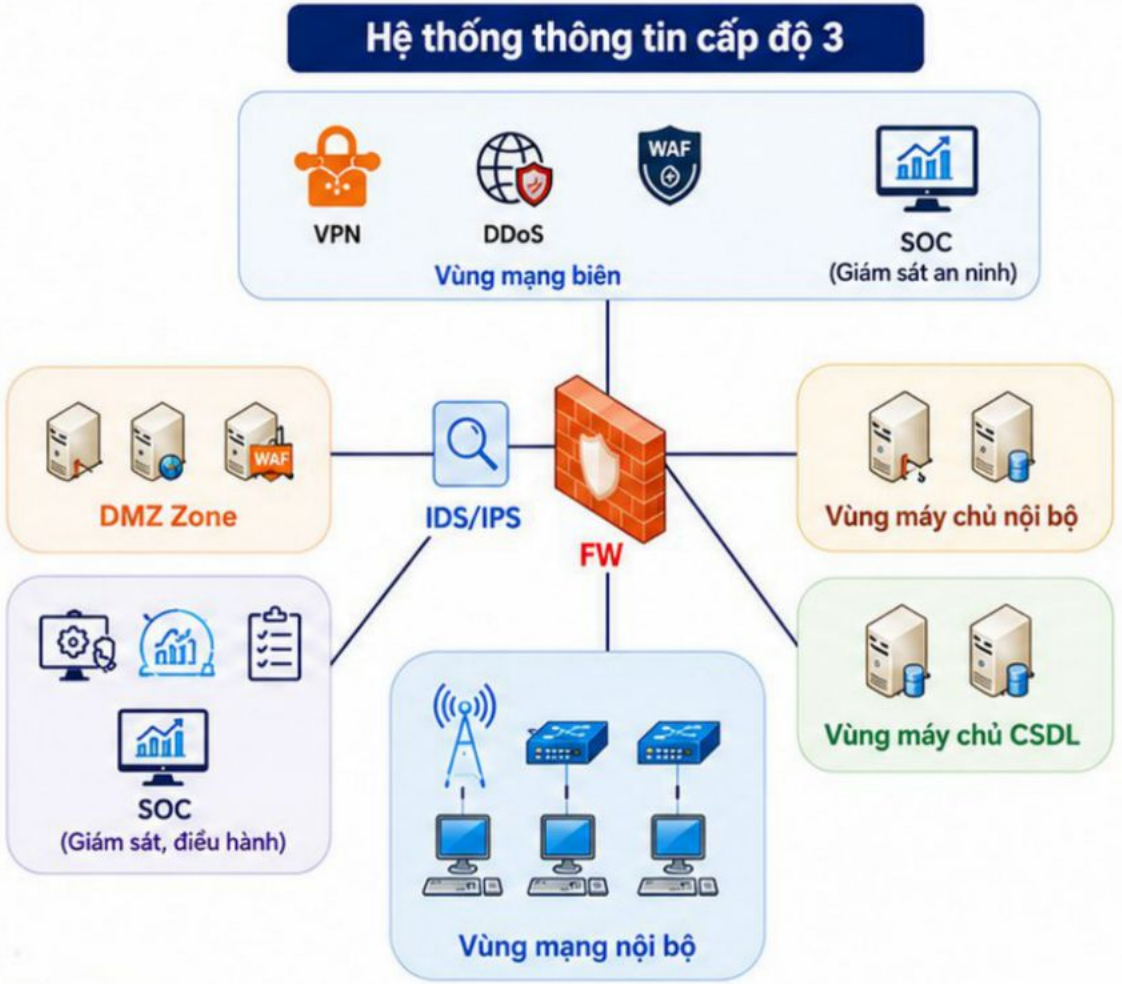


Phương án thiết kế tham chiếu theo NĐ 331/2026/NĐ-CP và TCVN 14423:2026:

1. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn (VPN).
2. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập (*Firewall tích hợp hoặc IDS/IPS*).
3. Có phương án cân bằng tải hoặc dự phòng nóng cho các thiết bị mạng chính.
4. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu và dữ liệu trọng yếu.
5. Có phương án phát hiện và ngăn chặn mã độc trên môi trường mạng.
6. Có phương án chống tấn công từ chối dịch vụ đối với dịch vụ trực tuyến/công khai.
7. Có phương án phòng chống tấn công mạng cho ứng dụng web (*WAF*).
8. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có).

PNE

YÊU CẦU VỀ THIẾT KẾ HỆ THỐNG ĐẠT AN NINH MẠNG CẤP ĐỘ 3 (TIẾP)



Phương án thiết kế tham chiếu theo NĐ 331/2026/NĐ-CP và TCVN 14423:2026:

9. Có phương án quản lý truy cập lớp mạng (NAC hoặc giải pháp tương đương đối với mạng nội bộ quan trọng).
10. Có phương án giám sát hệ thống thông tin tập trung *(NOC / Network Monitoring)*.
11. Có phương án giám sát an ninh mạng tập trung *(SIEM/SOC hoặc giải pháp tương đương)*.
12. Có phương án quản lý sao lưu, lưu trữ và khôi phục tập trung.
13. Có phương án quản lý tập trung phần mềm phòng chống mã độc trên máy chủ và máy trạm (*AntiVirus/EDR*).
14. Có phương án phòng, chống thất thoát dữ liệu (DLP) khi hệ thống xử lý dữ liệu nhạy cảm, dữ liệu cá nhân hoặc dữ liệu trọng yếu.
15. Có phương án duy trì ít nhất 02 kết nối Internet hoặc 02 tuyến kết nối dự phòng cho dịch vụ quan trọng khi cần.
16. Có phương án bảo đảm an toàn cho mạng không dây, thiết bị di động và điểm truy cập không dây (nếu có).

PNE

BỐI CẢNH & THÁCH THỨC CỦA DOANH NGHIỆP

Những yêu cầu pháp lý và khó khăn phổ biến khi triển khai hồ sơ xác định cấp độ an ninh mạng hệ thống thông tin.

01

Yêu cầu pháp lý

- Luật An ninh mạng số 116/2025/QH15.
- Nghị định 331/2026/NĐ-CP về xác định cấp độ và bảo vệ an ninh mạng đối với HTTT.
- TCVN 14423:2026 là chuẩn đối chiếu các yêu cầu kiểm soát.

02

Áp lực tuân thủ & chế tài

- Nghị định 330/2026/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân.
- Hồ sơ thiếu căn cứ hoặc triển khai không đầy đủ có thể làm tăng rủi ro tuân thủ.

03

Khó khăn thực tế

- Thiếu thông tin đầu vào, thiếu bằng chứng kỹ thuật và vận hành.
- Chưa đồng bộ giữa đơn vị vận hành, đơn vị chuyên trách an ninh mạng và chủ quản HTTT.
- Dễ phát sinh rework và kéo dài thời gian hoàn thiện hồ sơ.



Mục tiêu là xây dựng bộ hồ sơ **đúng pháp lý, đủ nội dung** và có thể **triển khai thực tế**; đồng thời giảm rủi ro tuân thủ theo **NĐ 330/2026/NĐ-CP.**

Nguồn tham chiếu: Luật An ninh mạng số 116/2025/QH15; NĐ 331/2026/NĐ-CP; NĐ 330/2026/NĐ-CP; TCVN 14423:2026.

PNE

MAPPING RỦI RO TUÂN THỦ & CHẾ TÀI THEO NĐ 330/2026/NĐ-CP

Đối chiếu các khoảng trống thường gặp với rủi ro tuân thủ và tác động pháp lý cần lưu ý.

Khoảng trống / Gap	Rủi ro tuân thủ	Tác động / Chế tài cần lưu ý	Mức ưu tiên
1 Chưa lập hoặc chưa điều chỉnh hồ sơ xác định cấp độ	Vi phạm nghĩa vụ xác định cấp độ	Nguy cơ bị yêu cầu khắc phục, kéo dài tiến độ; trường hợp nghiêm trọng có thể phát sinh rủi ro xử phạt theo NĐ 330	Cao
2 Hồ sơ thiếu căn cứ/ tài liệu bắt buộc	Không đáp ứng yêu cầu thẩm định	Phải bổ sung, rework, kéo dài thời gian phê duyệt	Cao
3 Chưa ban hành quy chế/ phương án bảo đảm ANM đồng bộ	Thiếu cơ sở triển khai và chứng minh tuân thủ	Tăng rủi ro bị yêu cầu khắc phục và kiểm tra lại	Cao
4 Thiếu bằng chứng kỹ thuật, vận hành	Khó chứng minh đáp ứng yêu cầu TCVN 14423:2026	Giảm mức độ sẵn sàng thẩm định, tăng rework	Trung bình – Cao
5 Biện pháp bảo vệ theo cấp độ chưa triển khai đầy đủ	Rủi ro an ninh mạng và rủi ro tuân thủ tăng cao	Ảnh hưởng an toàn hệ thống, dữ liệu và uy tín tổ chức	Cao

Ý nghĩa của việc mapping

- Xác định đúng mức độ ưu tiên khắc phục.
- Gắn yêu cầu pháp lý với hiện trạng thực tế của hệ thống.
- Hỗ trợ lãnh đạo ra quyết định đầu tư và triển khai.

NĐ 330/2026/NĐ-CP là căn cứ quan trọng để đánh giá mức độ rủi ro tuân thủ và hậu quả pháp lý liên quan.

Nguồn tham chiếu: NĐ 330/2026/NĐ-CP; NĐ 331/2026/NĐ-CP; TCVN 14423:2026.

PNE

QUY TRÌNH THỰC HIỆN DỊCH VỤ CỦA PNE

Các bước triển khai dịch vụ hỗ trợ xác định cấp độ và xây dựng hồ sơ bảo đảm an ninh mạng.

01 — Khởi động dự án

Thống nhất phạm vi, đầu mối và kế hoạch triển khai

02 — Khảo sát & thu thập thông tin

Thu thập tài liệu, kiến trúc, hiện trạng kỹ thuật và vận hành

03 — Đánh giá & xác định cấp độ

Đối chiếu tiêu chí, đánh giá rủi ro và xác định cấp độ phù hợp

04 — Xây dựng hồ sơ

Soạn HSĐXCĐ, Quy chế và Phương án bảo đảm ANM

05 — Rà soát & hoàn thiện

Đối soát evidence, bổ sung gap và hoàn thiện hồ sơ

06 — Bàn giao & hỗ trợ thẩm định

Bàn giao sản phẩm và hỗ trợ giải trình khi cần

Đầu ra theo từng giai đoạn

- Phạm vi rõ ràng
- Dữ liệu đầu vào đầy đủ
- Cấp độ đề xuất
- Bộ hồ sơ hoàn chỉnh
- Hồ sơ sẵn sàng
- Sẵn sàng thẩm định

Trong quá trình thực hiện, đơn vị triển khai đồng thời rà soát khoảng trống tuân thủ và mapping rủi ro/chế tài liên quan theo NĐ 330/2026/NĐ-CP.

Nguồn tham chiếu: Luật An ninh mạng số 116/2025/QH15; NĐ 331/2026/NĐ-CP; NĐ 330/2026/NĐ-CP; TCVN 14423:2026.

PNE

SẢN PHẨM BÀN GIAO CỦA DỊCH VỤ

Các đầu ra chính sau khi hoàn thành dịch vụ hỗ trợ xây dựng hồ sơ cấp độ.

01



Hồ sơ đề xuất cấp độ (HSĐXCĐ)

02



Quy chế bảo đảm an ninh mạng

03



Phương án bảo đảm an ninh mạng theo cấp độ

04



Ma trận Gap – Rủi ro – Chế tài – Khuyến nghị

05



Bộ evidence đối soát kỹ thuật, vận hành và tài liệu

06



Hỗ trợ giải trình, rà soát và hoàn thiện trước thẩm định

ĐIỂM NHẤN

- Hồ sơ được xây dựng đồng bộ giữa pháp lý, kỹ thuật và vận hành.
- Có đối chiếu rủi ro tuân thủ liên quan theo NĐ 330/2026/NĐ-CP.
- Tăng mức độ sẵn sàng trình thẩm định/phê duyệt.

Nguồn tham chiếu: NĐ 331/2026/NĐ-CP; NĐ 330/2026/NĐ-CP; TCVN 14423:2026.

PNE

GIÁ TRỊ PHƯƠNG NAM EDU MANG LẠI

Lợi ích dành cho khách hàng khi triển khai dịch vụ hỗ trợ xây dựng hồ sơ cấp độ.

01

Đúng pháp lý

- Bám theo Luật ANM, NĐ 331/333/330 và TCVN 14423:2026.
- Đồng bộ hồ sơ với yêu cầu hiện hành.

02

Sát thực tế

- Đối chiếu hiện trạng hệ thống, evidence kỹ thuật và vận hành.
- Hạn chế tình trạng hồ sơ lý thuyết, khó triển khai.

03

Giảm rủi ro tuân thủ

- Nhận diện sớm các khoảng trống có thể dẫn tới rủi ro pháp lý.
- Có mapping Gap – Rủi ro – Chế tài theo NĐ 330.

04

Sẵn sàng thẩm định

- Tăng khả năng hoàn thiện hồ sơ đúng tiến độ.
- Hỗ trợ phối hợp giải trình và hoàn thiện trước phê duyệt.

Kết quả cuối cùng: Bộ hồ sơ đầy đủ, nhất quán, có khả năng áp dụng thực tế và hỗ trợ tổ chức nâng cao mức độ sẵn sàng tuân thủ.

Nguồn tham chiếu: Luật An ninh mạng số 116/2025/QH15; NĐ 331/2026/NĐ-CP; NĐ 330/2026/NĐ-CP; TCVN 14423:2026.

PNE

SECURITY OPERATION CENTER (SOC)

TRUNG TÂM VẬN HÀNH AN NINH MẠNG

GIÁM SÁT LIÊN TỤC

SOC hoạt động 24/7 để giám sát các hệ thống mạng và phát hiện sớm các mối đe dọa.

PHÁT HIỆN VÀ CẢNH BÁO SỚM

Sử dụng các công cụ phân tích và công nghệ machine learning để phát hiện các hành vi bất thường và các mối đe dọa tiềm ẩn.



ỨNG PHÓ VỚI SỰ CỐ

Khi phát hiện sự cố, SOC sẽ tiến hành các biện pháp ứng phó nhanh chóng để giảm thiểu thiệt hại và khôi phục hoạt động bình thường.

ĐIỀU TRA TRUY VẾT

Tiến hành điều tra nguyên nhân gốc rễ để ngăn chặn sự cố tương tự trong tương lai.

BÁO CÁO, ĐỀ XUẤT

Cung cấp các báo cáo chi tiết về các sự cố đã xảy ra, quản lý các rủi ro an ninh mạng, từ đó đề xuất các biện pháp bảo vệ phù hợp.

PNE

SECURITY OPERATION CENTER (SOC)

KHÓ KHĂN KHI TRIỂN KHAI VÀ VẬN HÀNH SOC CỦA CÁC DOANH NGHIỆP







Thiếu nguồn lực

1. Thiếu nguồn lực chuyên trách về an toàn thông tin

Công cụ

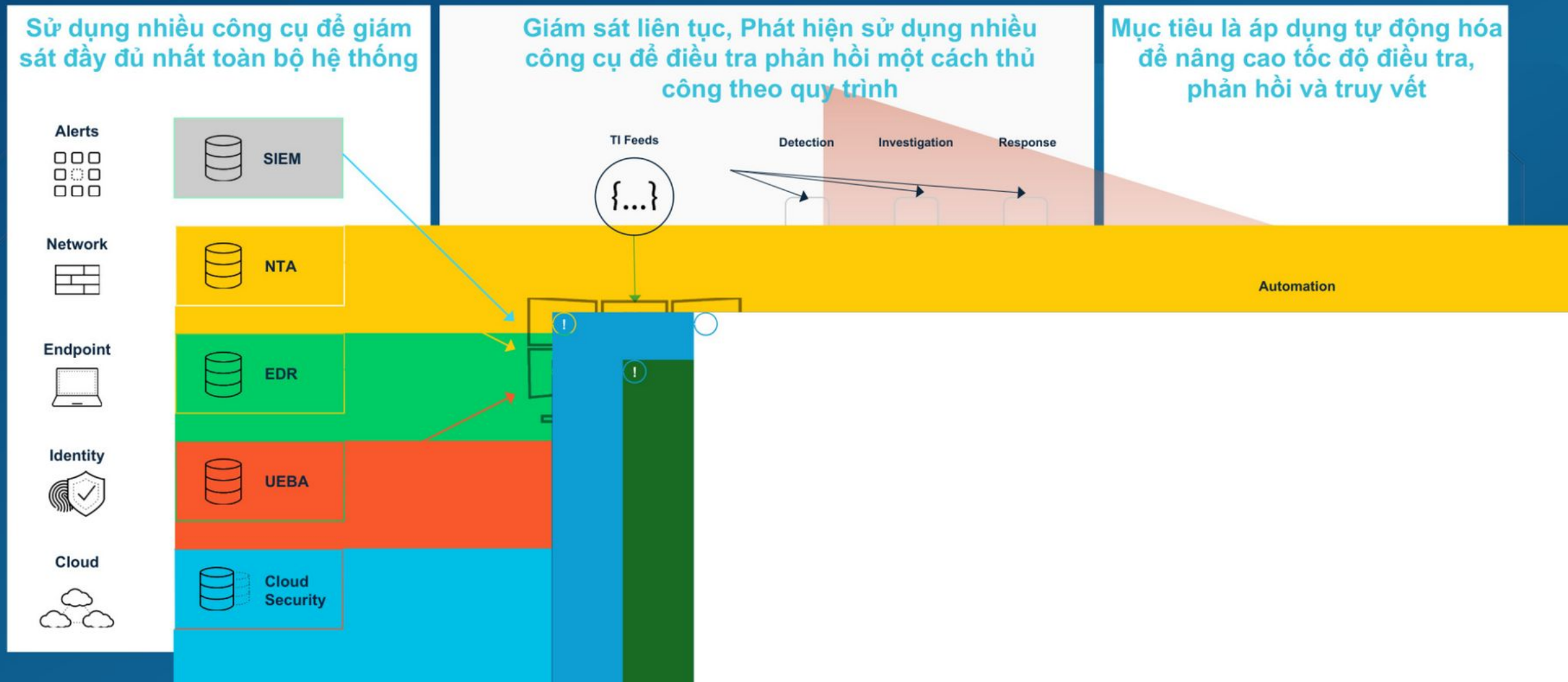
2. Quá nhiều công cụ riêng lẻ dẫn đến việc thiếu một cái nhìn tổng thể về an toàn thông tin cho toàn bộ hệ thống, từ đó làm giảm khả năng phản ứng và xử lý sự cố một cách nhanh chóng.

Quy trình

3. Thiếu quy trình xử lý hoặc quy trình xử lý sự cố phức tạp và không rõ ràng dẫn đến những khó khăn trong việc phản ứng và giải quyết sự cố.

SECURITY OPERATION CENTER (SOC)

HOẠT ĐỘNG CỦA TRUNG TÂM VẬN HÀNH AN NINH MẠNG



DỊCH VỤ SOC

Dịch vụ Giám sát và Quản lý ATTT (SOC) bao gồm:

Nhân sự chuyên trách

- Vận hành giám sát & phát hiện
- Hỗ trợ phản ứng và xử lý sự cố
- Phân tích và điều tra
- Quản lý rủi ro
- Báo cáo định kỳ

Công nghệ tiên tiến chính hãng

- Nền tảng giám sát ATTT hợp nhất:
Open XDR, SIEM, IDS, APT Sandbox, NTA, UBA, SOAR, Case Management
- ASM, EDR, Theat Intelligence, BEP (Bussiness Email Protection)
- Áp dụng AI và Machine

Quy trình và hỗ trợ

- Quy trình vận hành tiêu chuẩn quốc tế
- Đầy đủ cấp độ hỗ trợ Tier 1, Tier 2, Tier 3
- Liên tục cải tiến đảm bảo thông suốt, hiệu quả

Tài liệu giới thiệu PNE – thông tin năng lực, hạ tầng và khách hàng tham chiếu từ tài liệu đối tác; cần xác nhận trước khi sử dụng.

MÔ HÌNH CUNG CẤP DỊCH VỤ

SoC Manager
Security Operators (Tier 1)
Security Analysts (Tier 2, Tier 3)
Red Team, Blue Team



CS
OC

Quản lý giám sát tập trung 24x7
Kiến trúc Multi-Tenant
Thu thập dữ liệu và quản lý log riêng biệt
Quản trị phân cấp



Custom
er 1



Custom
er 2



Custom
er 3

PNE

NỀN TẢNG GIÁM SÁT TOÀN DIỆN

Giám sát toàn diện 24/7

Giám sát và rà soát các mối đe dọa trên hệ thống CNTT của khách hàng cả môi trường On-Premise & Cloud 24/7/365

Thu thập dữ liệu và phân tích tự động

IDS: phát hiện dấu hiệu tấn công xâm nhập ứng dụng dựa trên Machine Learning

NTA: phân tích lưu lượng mạng, phát hiện các hành vi bất thường trên mạng

UBA: phân tích hành vi người dùng, phát hiện thay đổi bất thường của người dùng

APT Sandbox: phát hiện mã độc chưa biết, các mối đe dọa APT, Zero-day

Quản trị tập trung

Giao diện quản trị tập trung giám sát toàn diện, cung cấp giao diện portal riêng biệt cho từng khách hàng (Multi Tenant)

Phát hiện sớm và tự động phản hồi

Next Gen SIEM: công cụ quản lý thông tin và sự kiên ATTT thế hệ mới, tự động iên kết các sự kiện tạo thành sự cố dựa trên AI và ML,

SOAR: phản ứng lại mối đe dọa một cách tự động.

OPEN

Thu thập và phân tích dữ liệu toàn diện từ các điểm cuối, mạng, đám mây, email, ứng dụng và định danh.

CÁC CẤP ĐỘ HỖ TRỢ

TIER 1

GIÁM SÁT AN NINH
Giám sát 24x7
Phân tích, xác minh cảnh báo
Phân loại sự cố

XỬ LÝ SỰ CỐ CƠ BẢN
Thực hiện các biện pháp ngăn chặn ban đầu
Ghi chép và báo cáo
Theo dõi và cập nhật

VẬN HÀNH BẢO TRÌ
Vận hành các công cụ
Cập nhật quy trình

TIER 2

PHÂN TÍCH ĐIỀU TRA SỰ CỐ

XỬ LÝ SỰ CỐ

CẢI TIẾN NÂNG CAO NĂNG LỰC PHÒNG THỦ

TIER 3

PHÂN TÍCH XỬ LÝ SỰ CỐ NÂNG CAO
Phân tích chuyên sâu để xác định nguyên nhân gốc rễ
Xây dựng kịch bản ứng phó
Phân tích mã độc chuyên sâu
Phân tích xử lý các sự cố phức tạp

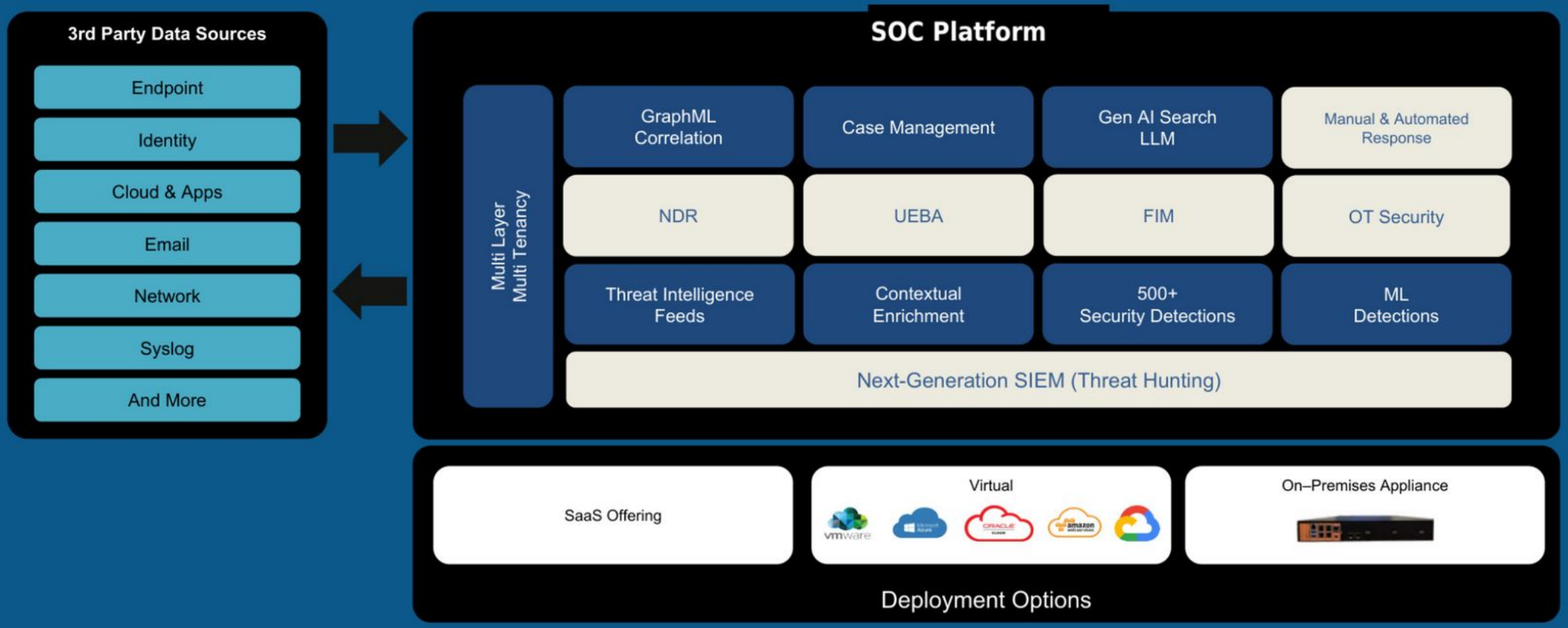
ĐIỀU TRA SỐ
Điều tra xử lý các sự cố phức tạp
Điều tra số trên các thiết bị bị xâm nhập

SĂN TÌM MỐI ĐE DỌA
Phát triển, tối ưu các quy tắc phát hiện
Nghiên cứu mối đe dọa, phân tích thông tin tình báo
Đánh giá và báo cáo nguy cơ an ninh định kỳ

CÔNG NGHỆ

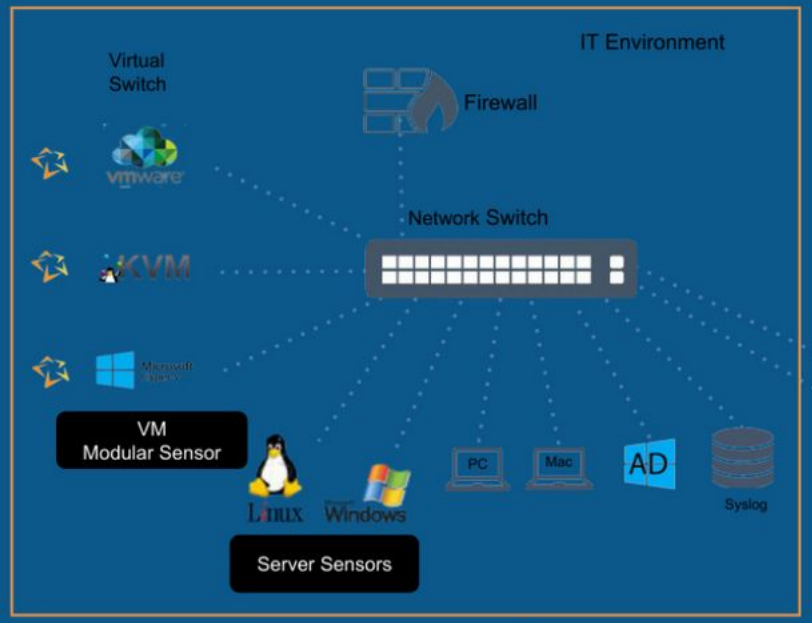
Automation-Driven Open Security Operation Platform

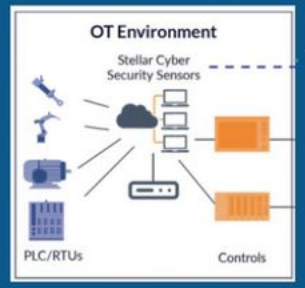
Single Platform. Single License.



PHƯƠNG THỨC KẾT NỐI

Complete Visibility and Integrations





MGT-int

Span-port



Modular Sensors

- Log Forwarder **SIEM**
- Network Visibility **NDR**
- IDS
- Parsing
- Filtering
- Response Action
- Vulnerability Scanner
- Sensor Aggregator

API Integrations

- Identity
- EDR
- PaaS
- Vulnerability Mgmt.
- Firewalls
- SaaS Apps

Active Directory
BlackBerry CYLANCE
ORACLE
tenable
CHECK POINT
Office 365



SOC Tier 1,2,3

Đội ngũ an ninh mạng

PNE



ƯU ĐIỂM CỦA DỊCH VỤ SOC PNE

Triển khai nhanh chóng

Nhờ vào việc sử dụng các công cụ chính hãng việc tích hợp và tối ưu nhanh chóng, thời gian triển khai SOC đã được rút ngắn đáng kể.

Khả năng tương thích

Có khả năng tương thích cao với hệ thống khách hàng, không làm giảm hiệu suất, và không yêu cầu băng thông mạng quá lớn.

PHÁT HIỆN SỚM

Tận dụng trí tuệ nhân tạo và học máy, tương quan để nhận diện các mối đe dọa tinh vi kết hợp với đội ngũ kỹ thuật dày dặn kinh nghiệm mang lại hiệu quả về thời gian phát hiện và độ chính xác

Dashboard trực quan

Cung cấp tài khoản Portal SOC, các Dashboard hiển thị thông tin trực quan
Khả năng hiển thị sự kiện được ánh xạ (map) theo MITRE ATT&CK Framework

Khả năng mở rộng và hỗ trợ

Đối tác MSSP của các hãng bảo mật những hãng bảo mật hàng đầu, giúp cung cấp dễ dàng các công cụ bổ sung nhằm nâng cao hiệu quả điều tram, phân tích xử lý sự cố.