Công ty CP Công nghệ mạng Lancs Việt Nam

LANCS NETWORKS

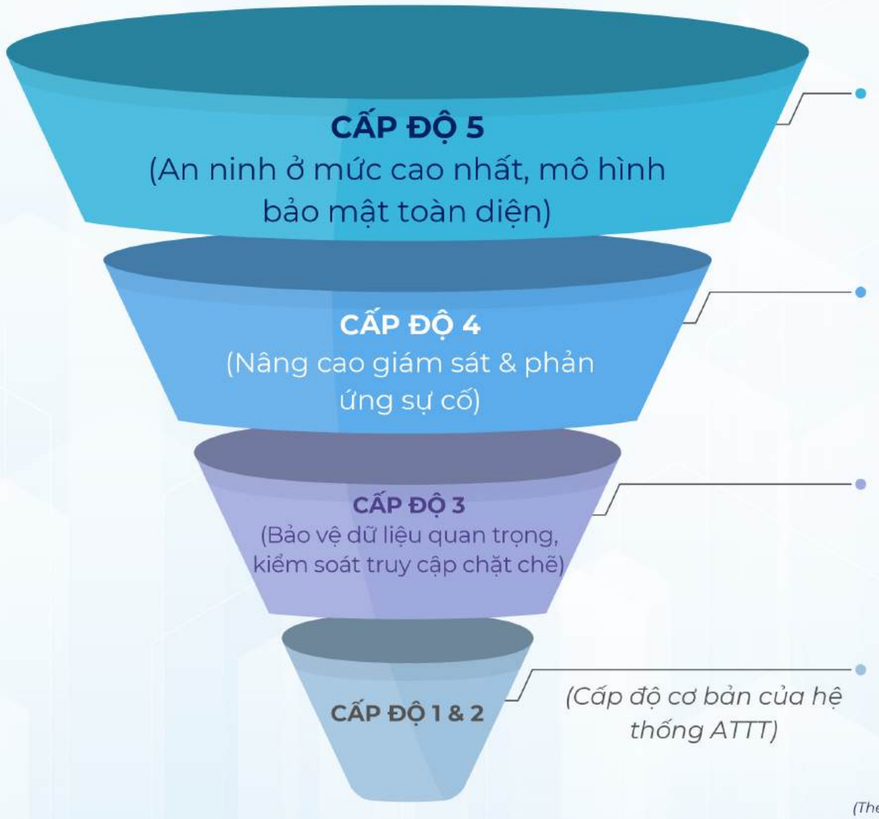
HỆ THỐNG QUẢN LÝ HẠ TẦNG CNTT VÀ ĐẢM BẢO TRUY CẬP MẠNG TẬP TRUNG TIN CẬY, KIỂM SOÁT CẤU HÌNH ĐẶC QUYỀN

LINKSAFE

NỘI DUNG

1 CÁC QUY ĐỊNH VỀ AN TOÀN THÔNG TIN

An toàn hệ thống thông tin theo cấp độ theo NĐ 85/2016/NĐ-CP là cách phân loại và áp dụng các biện pháp bảo vệ tương ứng với mức độ quan trọng, độ mật và phạm vi ảnh hưởng của từng hệ thống, nhằm đảm bảo an ninh, an toàn trong quá trình vận hành và xử lý thông tin.



Cấp độ 5: Mô hình bảo mật toàn diện:
- Bảo vệ toàn bộ hạ tầng và dữ liệu tối mật.
- Chống tấn công APT, Zero-day với AI Security Analytics.
- Hệ thống bảo mật đa lớp, phòng thủ chủ động trước các mối đe dọa tiên tiến.

Cấp độ 4: Nâng cao giám sát & phản ứng sự cố:
- Giám sát 24/7, phát hiện sớm và phản ứng tự động với sự cố an ninh.
- Mở rộng kiểm soát hệ thống, bảo vệ dữ liệu và phục hồi khi có sự cố.
- Tăng cường bảo mật hạ tầng mạng bằng kiến trúc Zero Trust.

Cấp độ 3: Bảo vệ dữ liệu, kiểm soát truy cập:
- Yêu cầu xác thực người dùng chặt chẽ (MFA, quản lý danh tính).
- Cơ chế mã hóa dữ liệu & bảo vệ thông tin nội bộ.
- Giám sát hệ thống để phát hiện và phản ứng với các rủi ro bảo mật.

Yêu cầu đối với các hệ thống cấp độ 3 trở lên

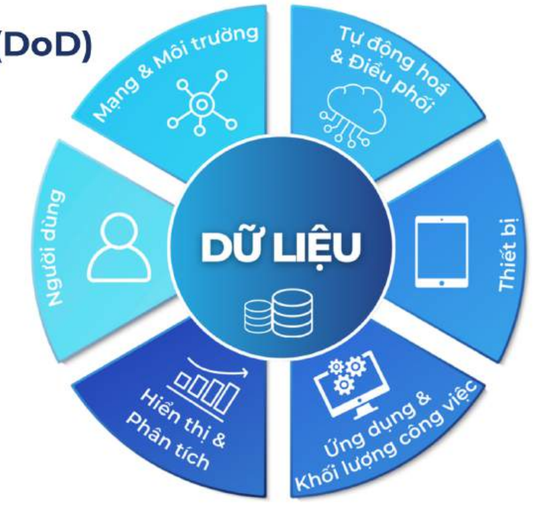
(Theo Công văn số 708/BTTTT-CATTT 2024)

- Đáp ứng **mô hình bảo đảm ATTT 4 lớp:** (1) Lực lượng tại chỗ; (2) Giám sát, bảo vệ; (3) Kiểm tra, đánh giá ATTT; (4) Kết nối, chia sẻ thông tin.
- Có phương án/phần mềm cụ thể **bảo vệ thiết bị, mạng, dữ liệu, ứng dụng, người dùng.**

1 CÁC QUY ĐỊNH VỀ AN TOÀN THÔNG TIN

Kiến trúc Zero Trust - BQP Hoa Kỳ (DoD)

Nguyên tắc **"không tin tưởng, xác minh liên tục, phân quyền tối thiểu".**



Khung kiến trúc Zero Trust DOD

Nguyên tắc 1:

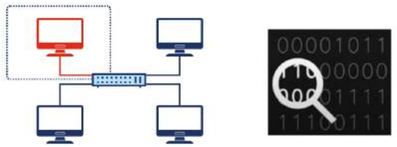
Không tin tưởng, xác minh liên tục, mã hóa toàn diện.

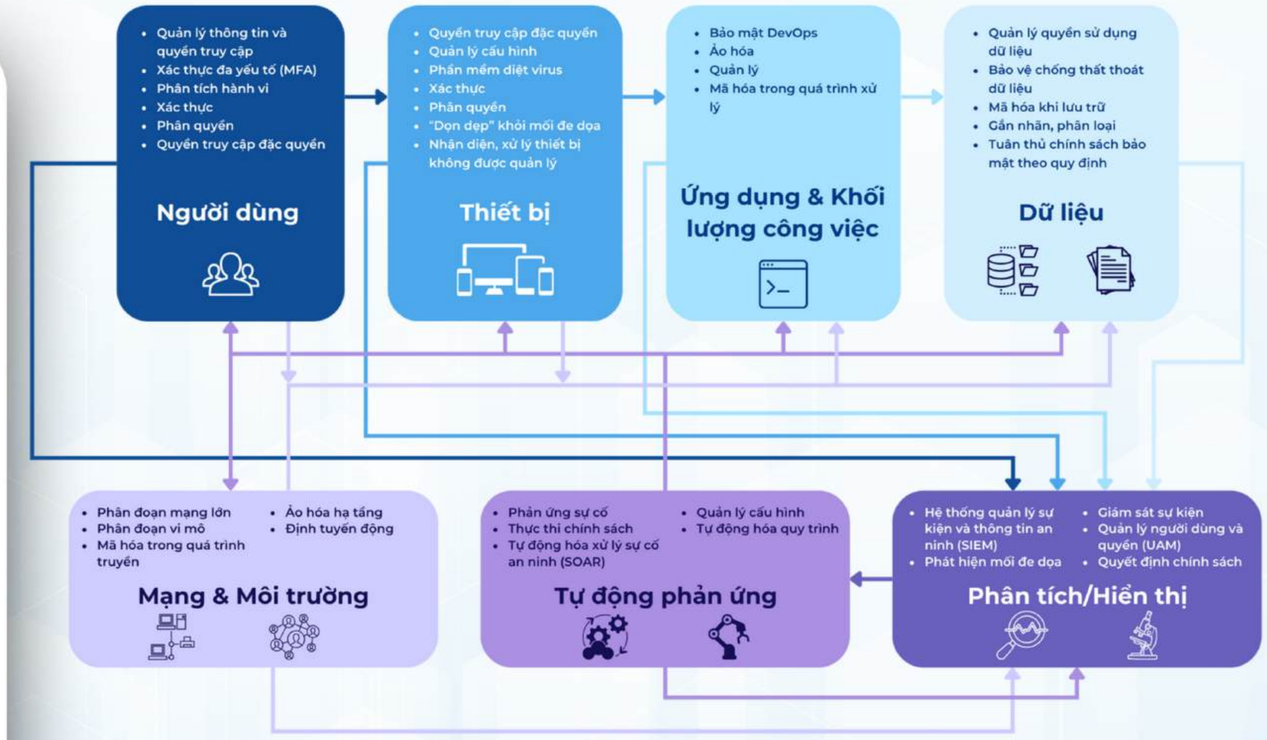
Nguyên tắc 2:

Phân quyền tối thiểu, cô lập nguy cơ

Nguyên tắc 3:

Chuẩn hoá log, chủ động phân tích và xử lý thông tin trên toàn hệ thống.





Mô hình bảo mật Zero Trust là sự kết hợp đồng bộ giữa:

- **4 đối tượng chính phục vụ hoạt động CNTT**: Người dùng, Thiết bị, Ứng dụng & Khối lượng công việc, Dữ liệu.
- **3 trụ cột hỗ trợ:** Mạng & Môi trường; Tự động phản ứng; Phân tích/Hiển thị

2 GIỚI THIỆU GIẢI PHÁP LINKSAFE - ĐÁP ỨNG CÁC QUY ĐỊNH VỀ ATTT

LINKSAFE - Giải pháp được phát triển theo kiến trúc **Zero Trust** và tiêu chuẩn quốc gia về ATTT.

Giải pháp cung cấp một **hệ sinh thái bảo mật và an toàn thông tin toàn diện** từ hạ tầng đến quản trị hệ thống, giúp cải thiện hiệu quả quản lý và giám sát mạng, an toàn thông tin toàn diện trước các mối đe dọa hiện đại.

- Đáp ứng hệ thống An toàn thông tin tối thiểu **cấp độ 3** - Dễ dàng tích hợp lên **cấp độ 4,5**
- Tự chủ công nghệ, bảo mật dữ liệu quốc gia.
- Hệ sinh thái đồng bộ, tương thích với hạ tầng và chính sách bảo mật sẵn có.

THÀNH PHẦN GIẢI PHÁP

1. Quản lý hạ tầng CNTT

Quản lý và giám sát trạng thái hoạt động của hạ tầng CNTT.

2. Quản lý truy cập đặc quyền

Theo dõi, giám sát, phát hiện và đảm bảo an toàn quyền truy cập tài nguyên.

3. Truy cập không tin cậy

Xác thực liên tục người dùng, thiết bị, yêu cầu truy cập dựa trên ngữ cảnh.

2.1 TỔNG QUAN MODULE QUẢN LÝ HẠ TẦNG CNTT - LINKSAFE IFM

LINKSAFE IFM (IT Infrastructure Management) - cho phép quản lý toàn bộ hạ tầng CNTT nhằm tối ưu hoá hiệu quả vận hành, đầu tư và quản trị vận hành an toàn, tin cậy, giảm thiểu các sai sót, chống lại các hành vi cố ý tạo sai sót trong quá trình vận hành. Hỗ trợ cảnh báo các lỗ hổng bảo mật có thể có của hệ thống.

Tối ưu chi phí đầu tư & vận hành

Giảm chi phí quản trị hạ tầng, nâng cao hiệu suất sử dụng tài nguyên CNTT nhờ quản lý tập trung – chủ động – tự động hóa.

Tích hợp hệ sinh thái bảo mật toàn diện

Hoạt động liền mạch với các module khác trong hệ sinh thái LINKSAFE, tạo thành kiến trúc quản lý & bảo mật toàn diện.

Tích hợp linh hoạt với hệ thống nội bộ

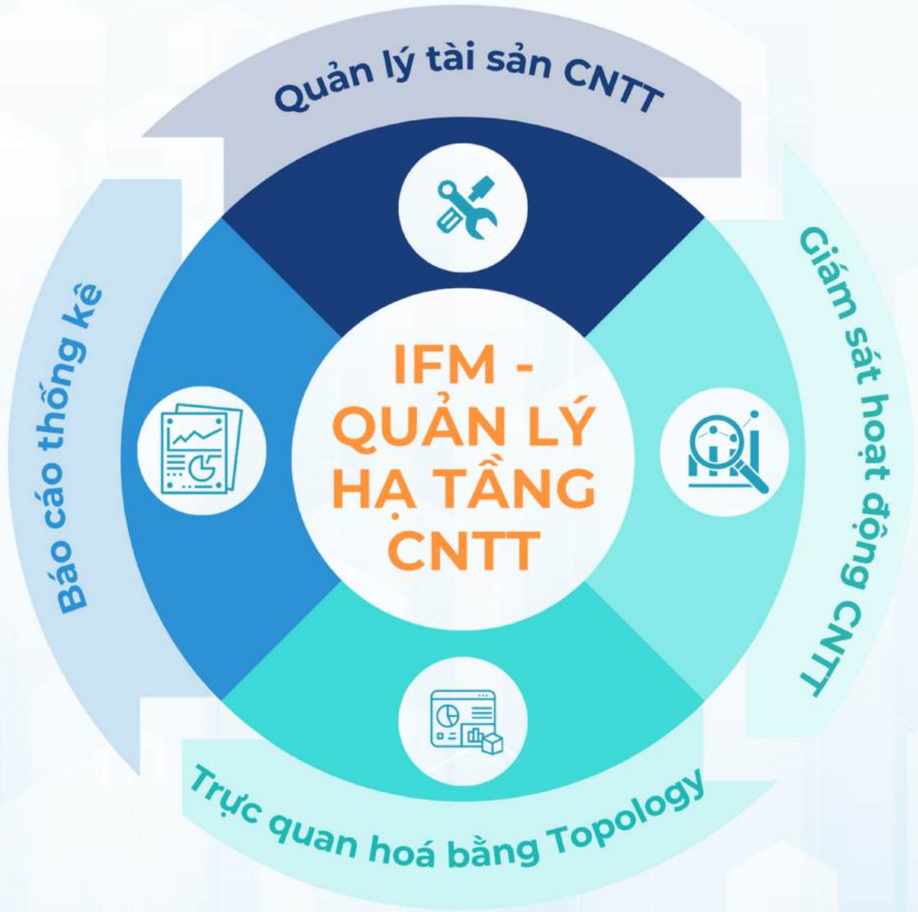
Kết nối được với các nền tảng nội bộ sẵn có, không làm gián đoạn hệ thống đang vận hành.

Sẵn sàng kết nối với hệ thống bên thứ 3

Dễ dàng tích hợp với các giải pháp từ đối tác/bên thứ ba, đảm bảo kết nối linh hoạt trong tương lai.

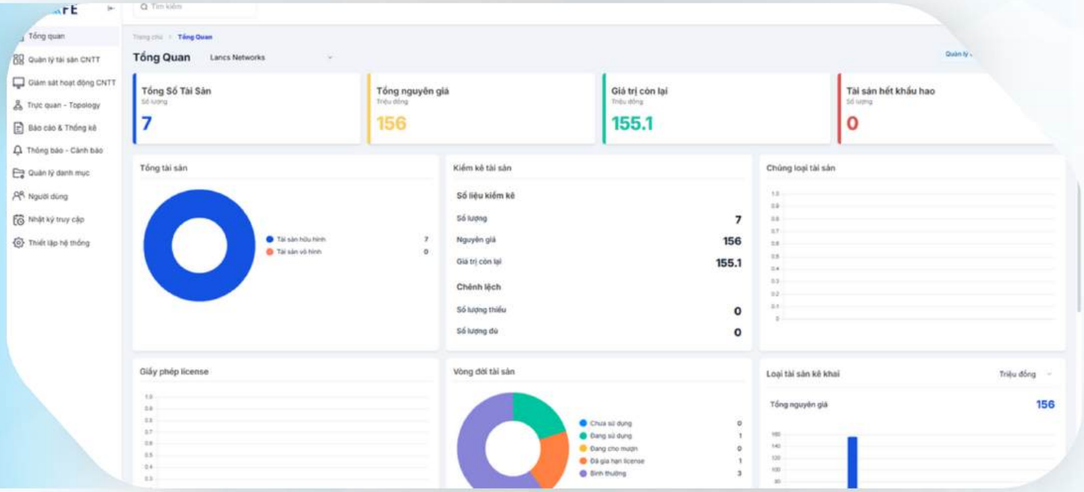
Tuân thủ quy định & tiêu chuẩn pháp lý

Đáp ứng tiêu chuẩn bảo mật ISO 27001, PCI DSS, Nghị định 85/2016/NĐ-CP và phù hợp với khung Zero Trust của DoD.



2.1 LINKSAFE IFM - QUẢN LÝ TẬP TRUNG HẠ TẦNG CNTT PHÂN TÁN

Giao diện Dashboard - Quản lý tài sản



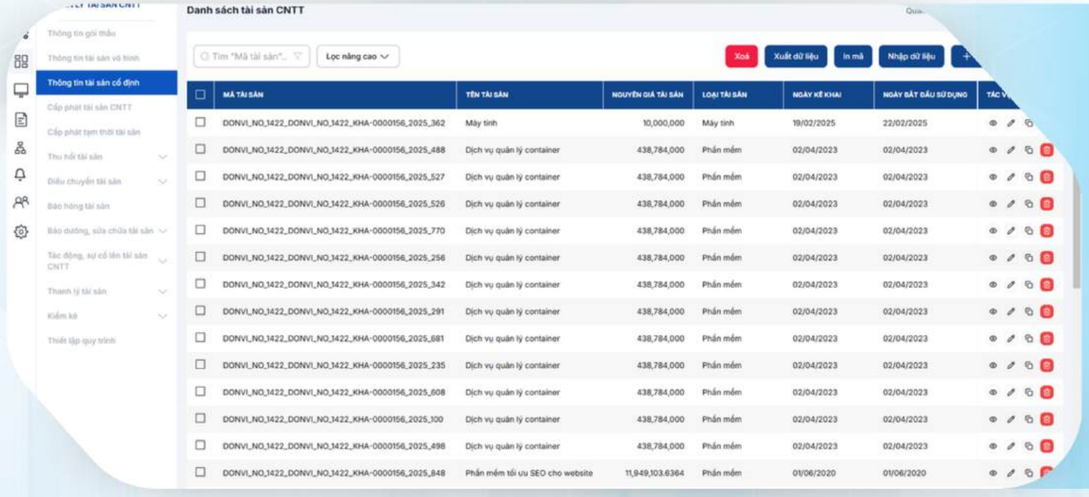
Nắm rõ toàn bộ tài sản CNTT/OT đang sở hữu và vị trí vận hành trên một hệ thống duy nhất.

Quản lý minh bạch vòng đời thiết bị từ cấp phát – vận hành – bảo trì – thanh lý.

Dễ dàng **theo dõi tình trạng của thiết bị** để lên kế hoạch sử dụng và bảo dưỡng hợp lý.

Phát hiện sớm thiết bị gặp sự cố hoặc hỏng hóc nhờ cảnh báo theo thời gian thực.

Ra quyết định đầu tư, nâng cấp chính xác dựa trên dữ liệu tài sản và tình trạng vận hành.

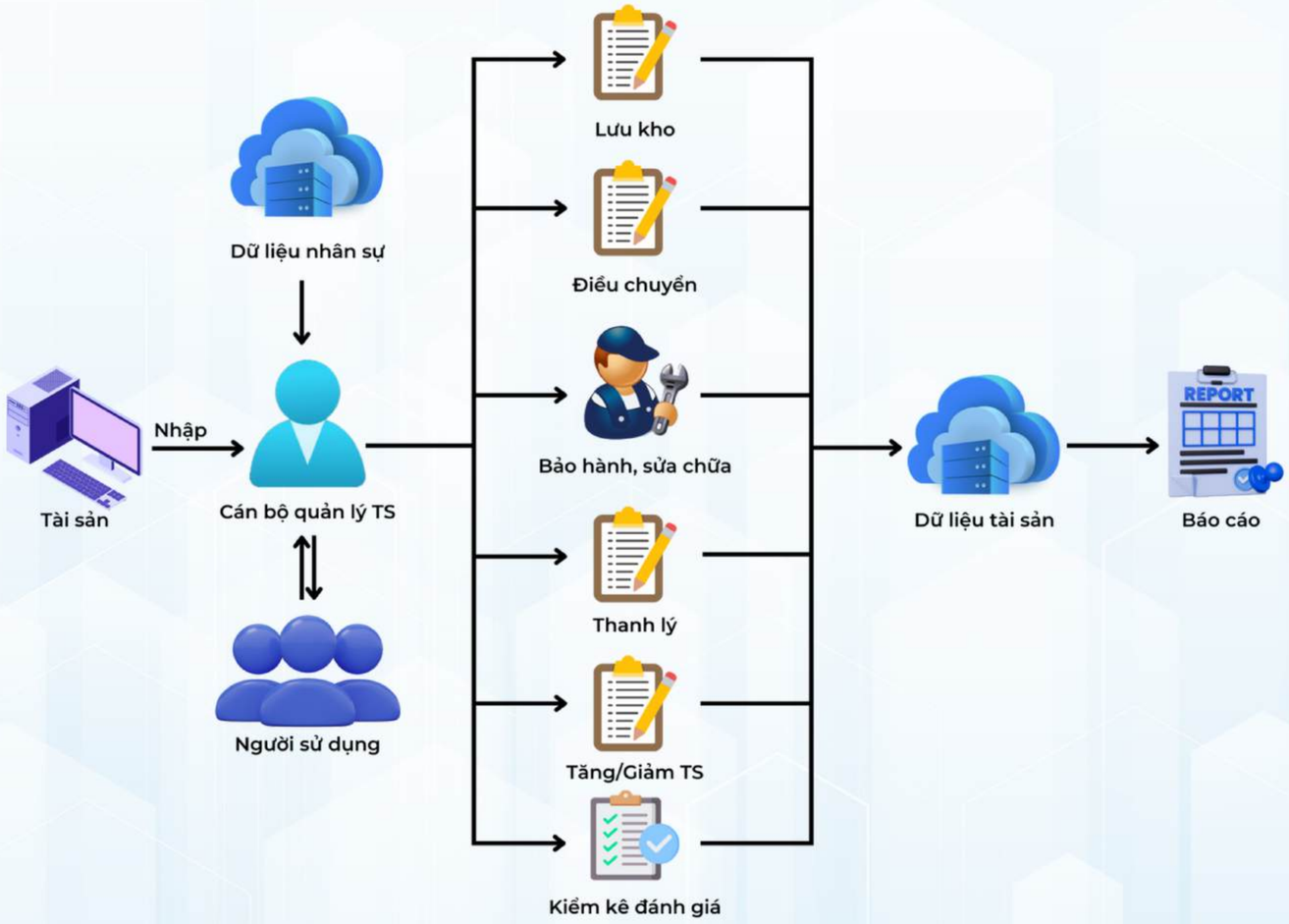


Giao diện Quản lý tài sản CNTT

2.1 LINKSAFE IFM - QUẢN LÝ TẬP TRUNG HẠ TẦNG CNTT PHÂN TÁN

Giải pháp toàn diện giúp quản lý tài sản CNTT trong toàn bộ vòng đời từ khi mua sắm, sử dụng đến thanh lý

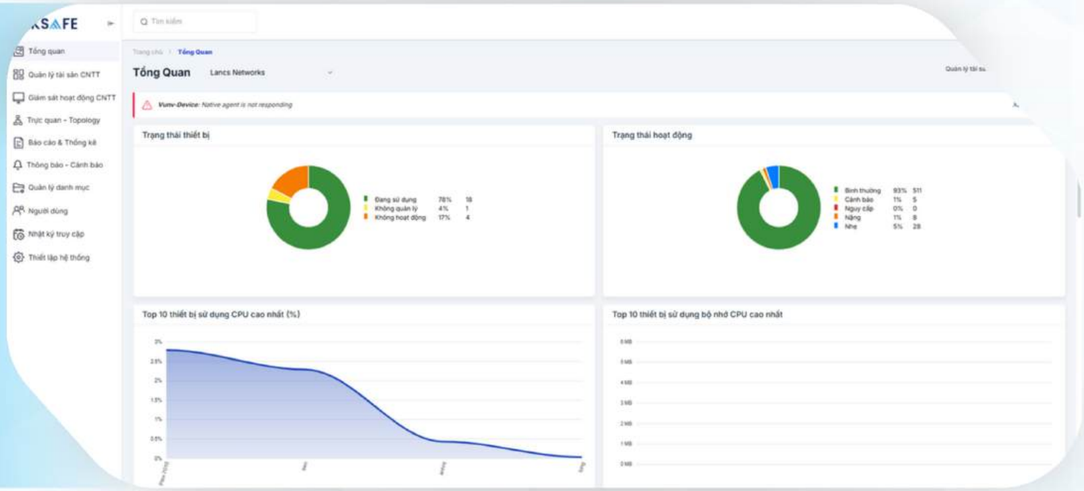
- Quản lý danh mục tài sản bao gồm nhà cung cấp, nhà sản xuất, loại tài sản, hợp đồng, trạng thái hoạt động.
- Ghi nhận, lưu trữ thông tin mua sắm tài sản hợp đồng, hóa đơn, hồ sơ kỹ thuật kèm theo.
- Quản lý vị trí lắp đặt, cấu hình, người chịu trách nhiệm của tài sản CNTT.
- Quản lý thông suốt các giai đoạn của tài sản từ Cấp phát, thu hồi, điều chuyển, báo hỏng, bảo trì sửa chữa và thanh lý.
- Lưu vết lịch sử sử dụng, bảo trì, sự cố trên từng thiết bị, tích hợp hệ thống cảnh báo theo thời gian thực.



Quy trình Quản lý tài sản CNTT

2.1 LINKSAFE IFM - TỰ ĐỘNG HÓA THU THẬP HOẠT ĐỘNG HẠ TẦNG CNTT

Giao diện Dashboard - Giám sát hoạt động



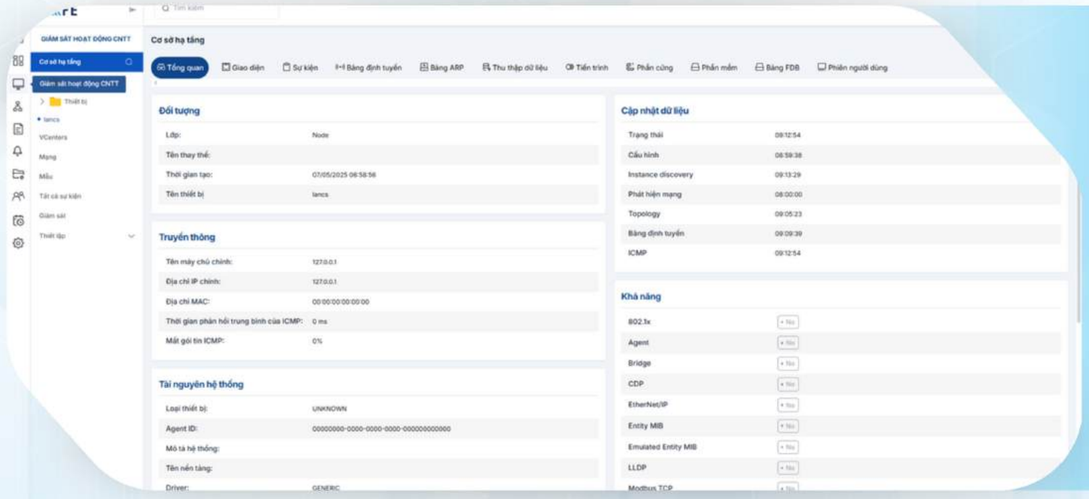
Phản ứng nhanh trước sự cố với cảnh báo tức thời khi mất kết nối, lỗi phần cứng,...

Giảm gián đoạn hệ thống – tối ưu chi phí vận hành nhờ phát hiện sớm vấn đề và phân bổ tài nguyên hợp lý.

Nắm bắt tình trạng hệ thống theo thời gian thực (CPU, RAM, băng thông...).

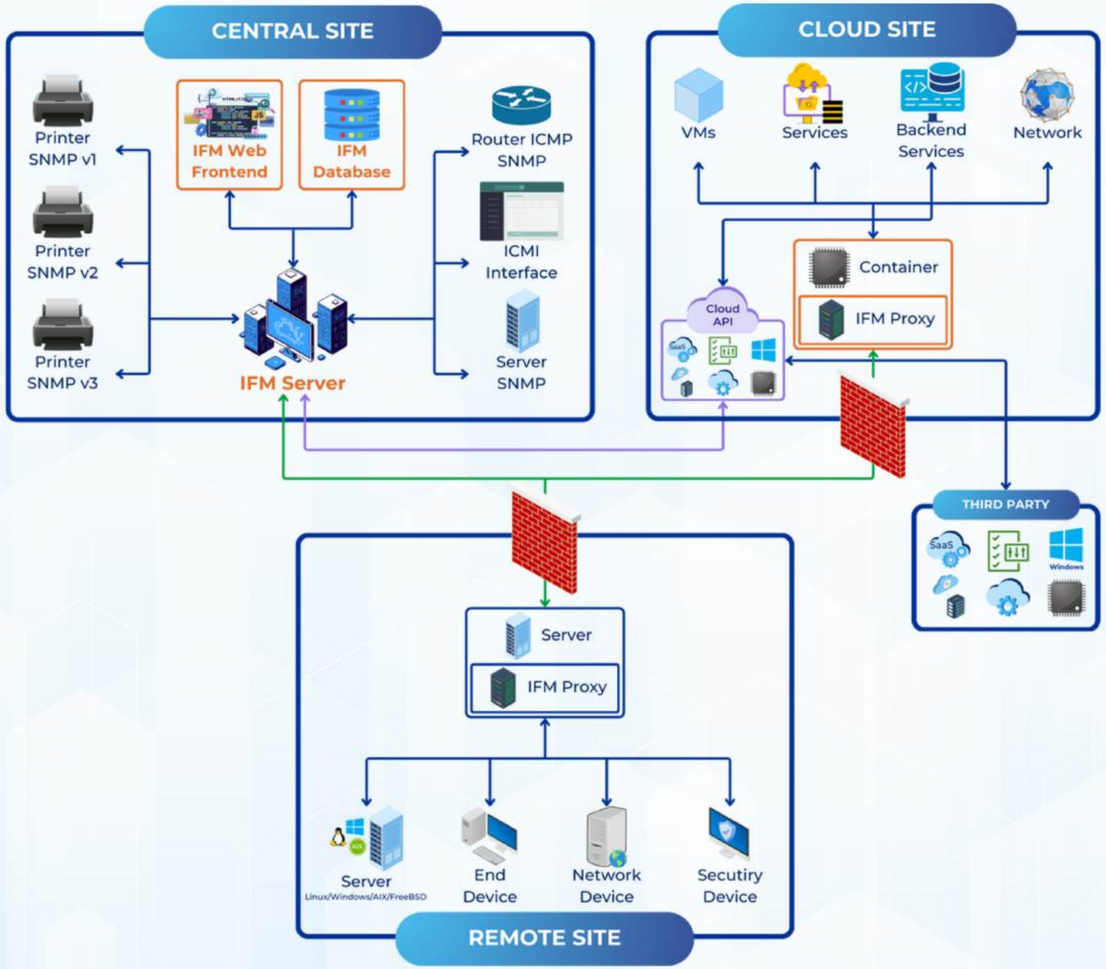
Không còn mất thời gian kiểm tra thủ công – dữ liệu tự động cập nhật liên tục.

Dự báo sớm nguy cơ quá tải hoặc thiếu hụt thiết bị nhờ phân tích xu hướng hiệu suất.



Giao diện Giám sát hoạt động CNTT

2.1 LINKSAFE IFM - TỰ ĐỘNG HÓA THU THẬP HOẠT ĐỘNG HẠ TẦNG CNTT



Mô hình giám sát hoạt động CNTT

Theo dõi hiệu suất thiết bị: Giám sát CPU, RAM, băng thông, ổ cứng của máy chủ, thiết bị mạng,...

Tự động thu thập số liệu: thông qua giao thức SNMP và IFM Agent cập nhật dữ liệu thời gian thực thiết bị.

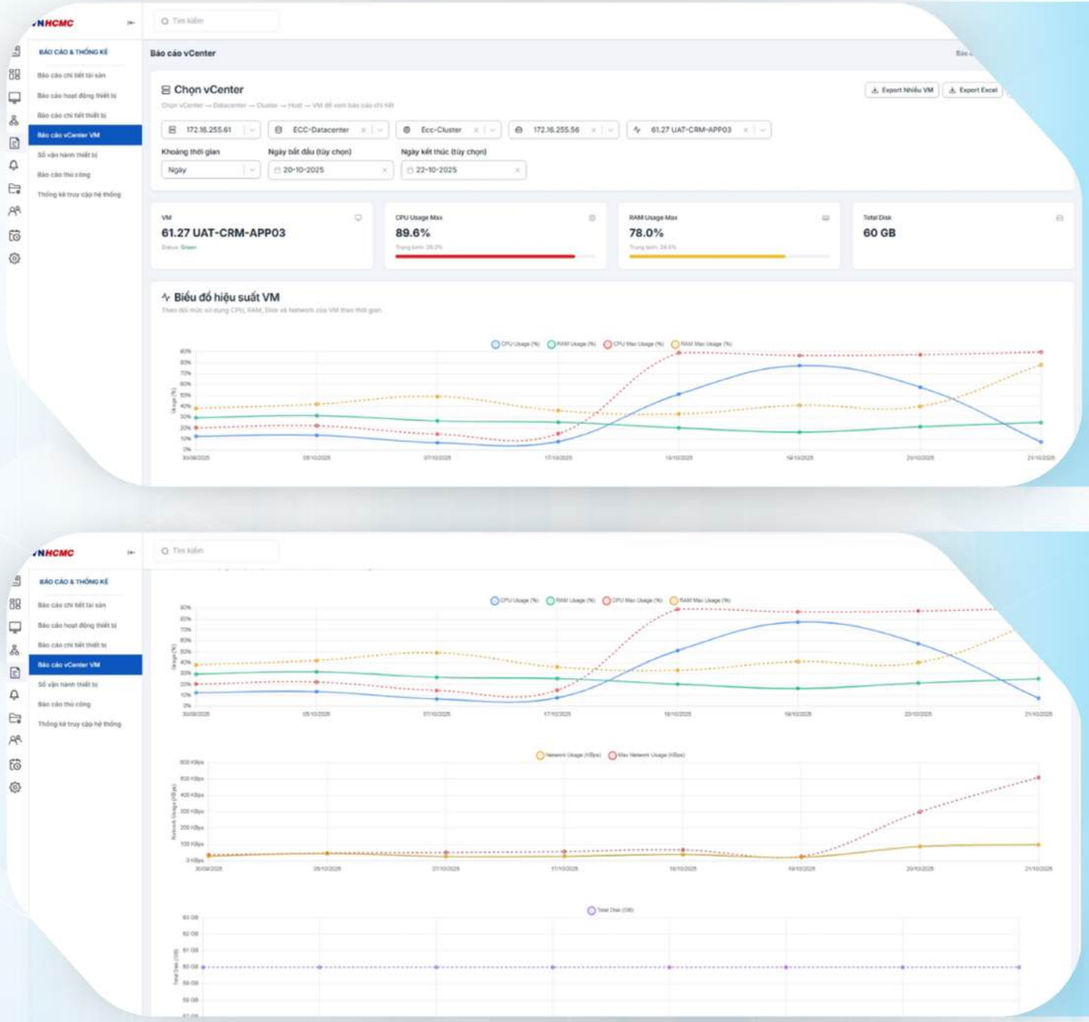
Phân tích, dự đoán sự cố: Phân tích xu hướng hiệu suất thiết bị, phát hiện bất thường để có biện pháp xử lý.

Cảnh báo tức thời khi có sự cố bất thường: Gửi cảnh báo ngay khi phát hiện sự cố (mất kết nối, lỗi phần cứng...).

2.1 LINKSAFE IFM - THU THẬP VÀ QUẢN LÝ HỆ THỐNG ẢO HÓA VCENTER CỦA VMWARE

Tự động thu thập, chuẩn hóa và giám sát toàn diện tài nguyên trong hệ thống ảo hóa vCenter của VMware

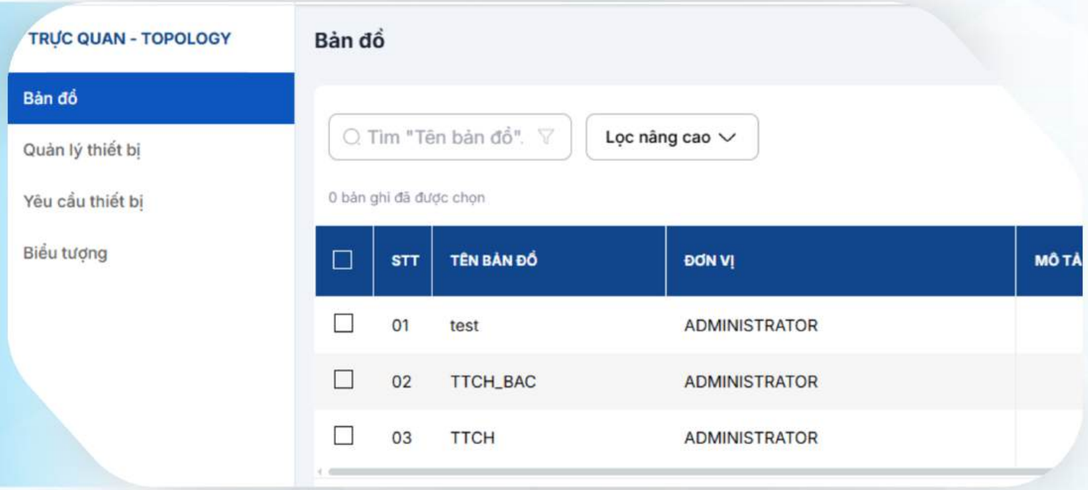
- Thu thập chi tiết tài nguyên (CPU, RAM, Disk, Network) và các sự kiện/cảnh báo từ vCenter.
- Tổng hợp báo cáo theo các cấp: VM, host, cluster, datastore, datacenter.
- Tích hợp dữ liệu để hiển thị trong Topology hệ thống, liên kết dữ liệu thu thập từ agent và SNMP.
- Khai báo & quản lý danh sách vCenter, phân loại theo khu vực.
- Kết nối và thu thập dữ liệu tự động qua tài khoản read-only bảo mật.
- Theo dõi thời gian thực tình trạng hoạt động của máy ảo, host ESXi, datastore, cluster và datacenter.



Giao diện Báo cáo hệ thống ảo hóa VCenter

2.1 LINKSAFE IFM - MÔ HÌNH HÓA BẢN ĐỒ MẠNG

Giao diện các bản đồ chi nhánh trong hệ thống



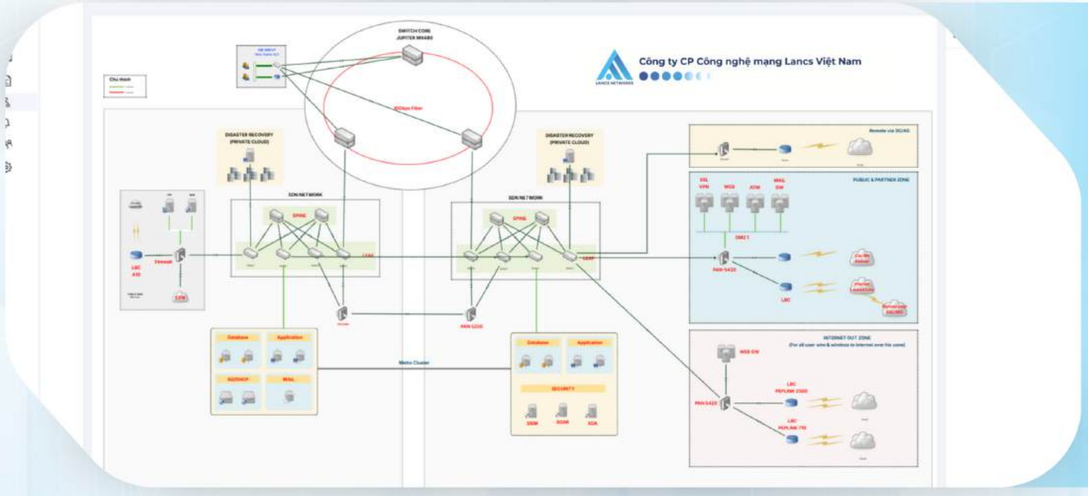
Tiết kiệm thời gian xác định nguyên nhân sự cố và rút ngắn thời gian khắc phục (MTTR).

Giúp quản trị viên và lãnh đạo **có cái nhìn tổng thể về kiến trúc mạng** để tối ưu thiết kế, nâng cấp hoặc mở rộng hệ thống.

Hình dung **toàn bộ hệ thống CNTT trên một sơ đồ trực quan** – biết rõ thiết bị nào đang kết nối với thiết bị nào.

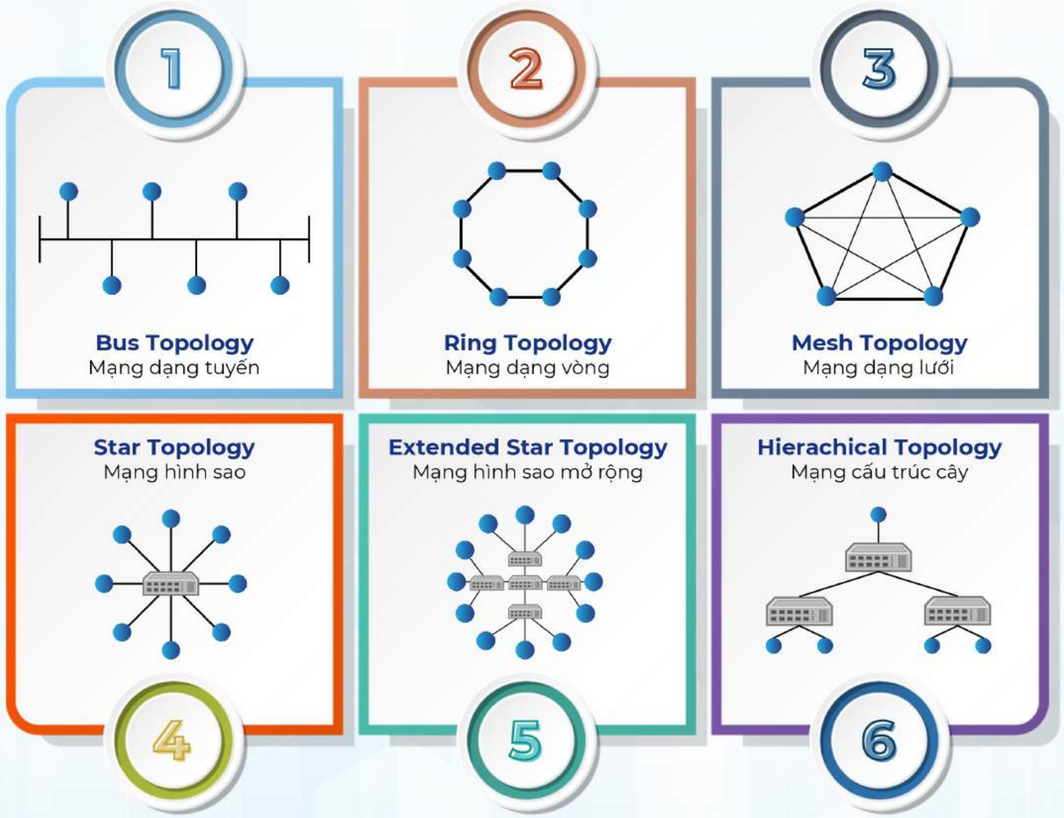
Tập trung kiểm soát trạng thái hoạt động của từng thành phần hệ thống theo thời gian thực.

Phát hiện nhanh vị trí xảy ra lỗi hoặc mất kết nối ngay trên topology – không cần dò thủ công từng thiết bị.



Giao diện Bản đồ mạng hệ thống

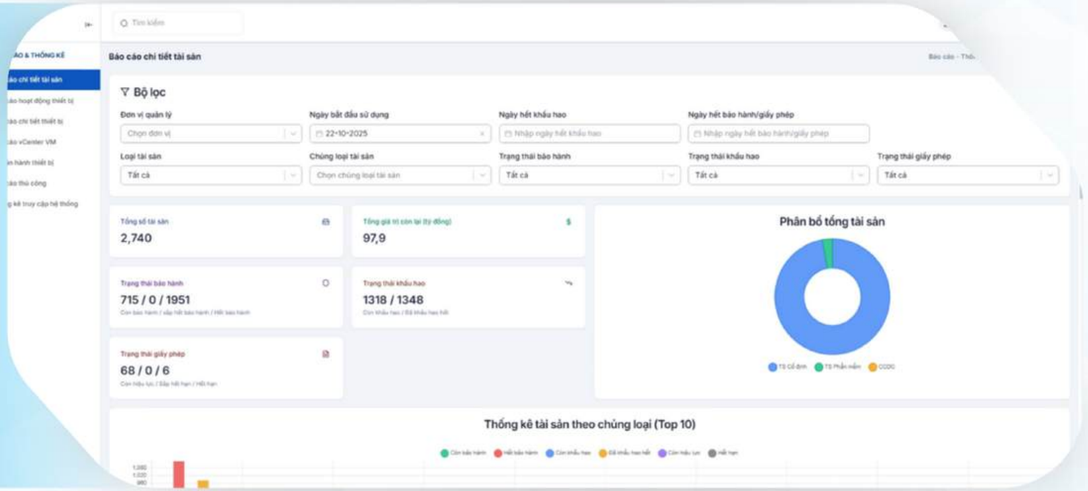
2.1 LINKSAFE IFM - MÔ HÌNH HÓA BẢN ĐỒ MẠNG



- **Hiển thị toàn bộ hệ thống theo mô hình trực quan:** Cho phép quản trị viên theo dõi mối quan hệ giữa các thiết bị bao gồm thiết bị mạng, máy chủ, endpoint.
- **Tự động cập nhật trạng thái thiết bị và kết nối:** Đồng bộ trạng thái, tích hợp chỉ số hiệu suất của các thiết bị với hệ thống giám sát, phân lớp theo từng bộ phận.
- **Phát hiện và đánh dấu các sự cố trên topology:** Hiển thị cảnh báo lỗi hoặc mất kết nối trên sơ đồ topology, dễ dàng theo dõi xu hướng sự cố.

2.1 LINKSAFE IFM - BÁO CÁO THỐNG KÊ HIỆU QUẢ

Giao diện Báo cáo chi tiết tài sản CNTT

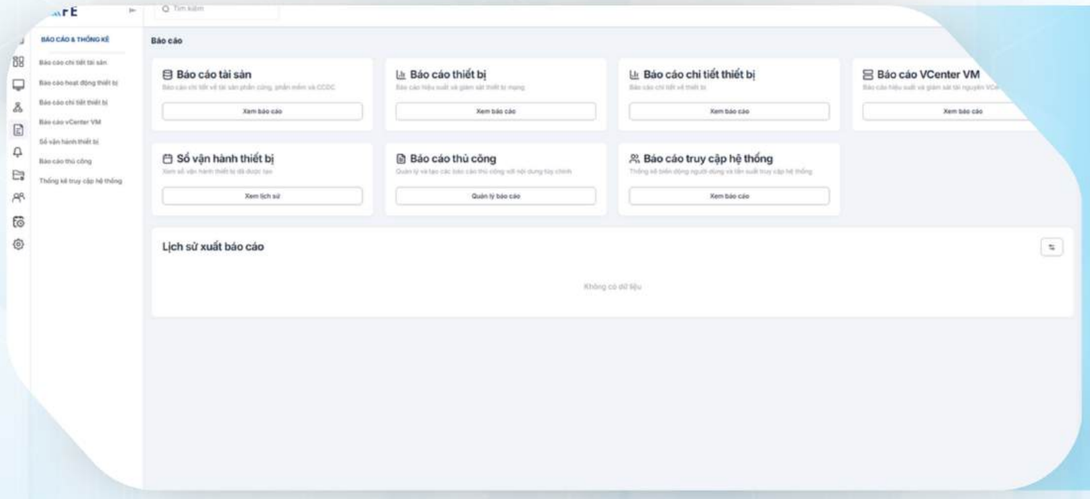


Hỗ trợ nhà quản lý đưa ra quyết định chính xác **dựa trên số liệu,** phục vụ lập kế hoạch nâng cấp hạ tầng.

Giúp quản trị viên và lãnh đạo **đánh giá hiệu suất vận hành hệ thống CNTT** để tối ưu chi phí đầu tư và bảo trì.

Có thể sử dụng nhiều **định dạng báo cáo theo mẫu có sẵn**, không cần lập báo cáo thủ công.

Nhận **báo cáo tự động và cảnh báo sớm** khi tài nguyên CNTT có dấu hiệu bất thường.



Giao diện Quản lý mẫu định dạng báo cáo

2.1 LINKSAFE IFM - BÁO CÁO THỐNG KÊ HIỆU QUẢ

Cung cấp báo cáo chi tiết

Báo cáo chi tiết về số lượng, tình trạng, tổng hợp hiệu suất sử dụng, ghi nhận sự cố.

Tuỳ chỉnh báo cáo theo yêu cầu

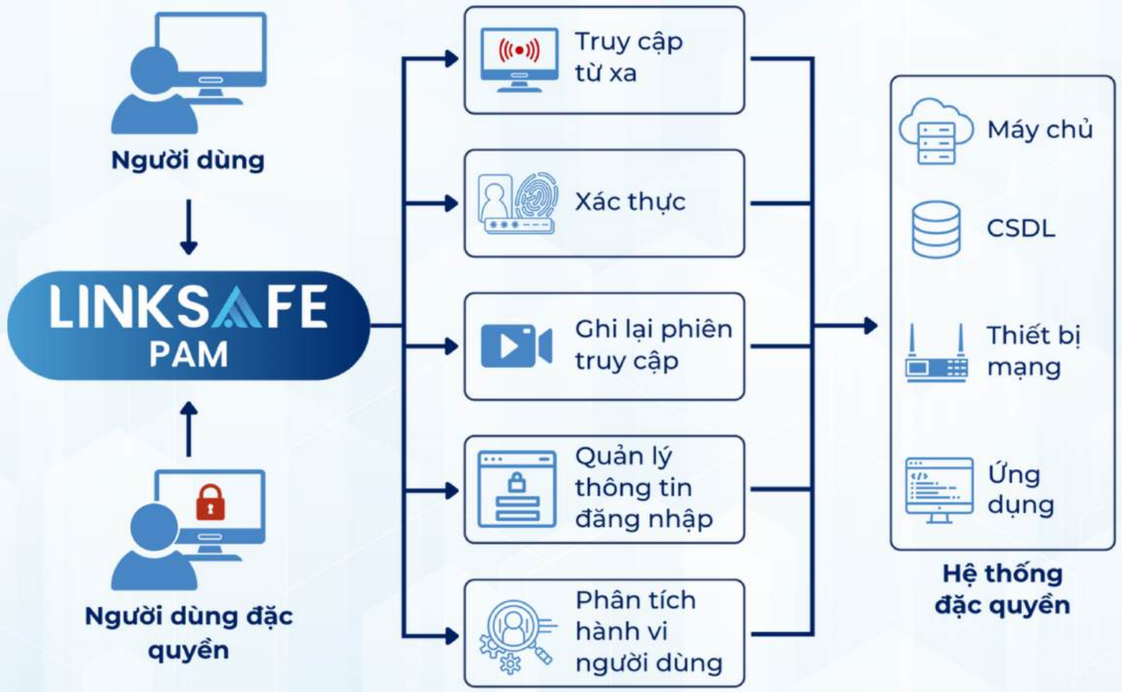
Hỗ trợ nhiều định dạng, tùy chỉnh nội dung báo cáo theo tiêu chí phù hợp.

Tích hợp báo cáo tự động

Thiết lập gửi báo cáo định kỳ, cảnh báo về xu hướng sử dụng tài nguyên bất thường.

2.2 TỔNG QUAN MODULE QUẢN LÝ TRUY CẬP ĐẶC QUYỀN - LINKSAFE PAM

LINKSAFE PAM (Privileged Access Management) - Module giúp doanh nghiệp quản lý, giám sát và kiểm soát tài khoản đặc quyền, bảo vệ hệ thống khỏi lạm dụng, rò rỉ dữ liệu, đảm bảo tuân thủ và tăng cường an toàn thông tin.



Mô hình hoạt động giải pháp LINKSAFE PAM

TÍNH NĂNG GIẢI PHÁP

Quản lý thông tin xác thực người dùng

- Lưu trữ mật khẩu an toàn.
- Quản lý người dùng đặc quyền.
- Tự động đăng nhập.

Kiểm soát truy cập

- Thiết lập chính sách truy cập dữ liệu.
- Quản lý các phiên truy cập đang hoạt động.
- Cho phép truy cập theo từng yêu cầu cụ thể.

Xác thực và Phân quyền

- Xác minh danh tính người dùng khi đăng nhập.
- Phân quyền truy cập theo chức năng, vai trò.
- Quản lý các phiên làm việc của người dùng.

Quản lý truy cập từ xa

- Hỗ trợ truy cập từ xa.
- Ghi lại toàn bộ phiên làm việc, tiến trình
- Cho phép chạy lệnh từ xa.

Quản lý hệ thống

- Áp dụng chính sách quản lý người dùng theo vai trò.
- Thu thập và phân tích nhật ký hoạt động.
- Quản lý các kết nối từ hệ thống khác, tích hợp API kết nối

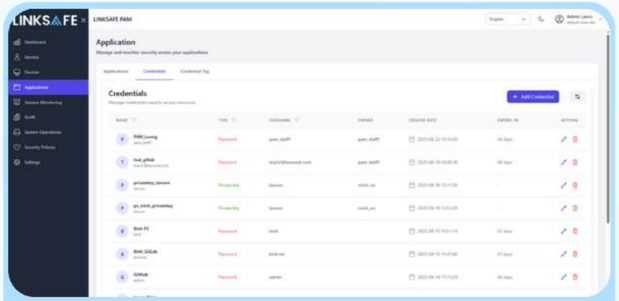
Quản lý nhật ký

- Ghi lại toàn bộ nhật ký hoạt động trên hệ thống.
- Cho phép truy vấn sự kiện theo thời gian.
- Lưu trữ nhật ký.

2.2 LINKSAFE PAM - QUẢN LÝ THÔNG TIN XÁC THỰC NGƯỜI DÙNG

Lưu trữ mật khẩu an toàn

Lưu trữ mật khẩu tài khoản đặc quyền trong kho mật khẩu (Vault) với cơ chế mã hóa cấp cao.



Giao diện quản lý mật khẩu

Quản lý tập trung người dùng đặc quyền

Tập trung toàn bộ tài khoản admin, service account, root... từ các hệ thống khác nhau (Server, DB, Network...) để quản lý theo vòng đời.

Cơ chế Just in Time Access

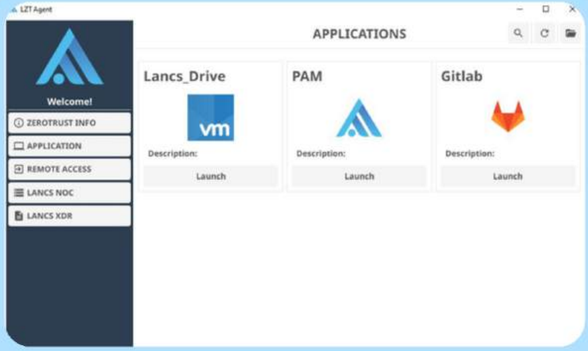
Chỉ cấp quyền trong thời gian cần thiết và tự động thu hồi sau phiên truy cập.

Đăng nhập tự động - Auto Login

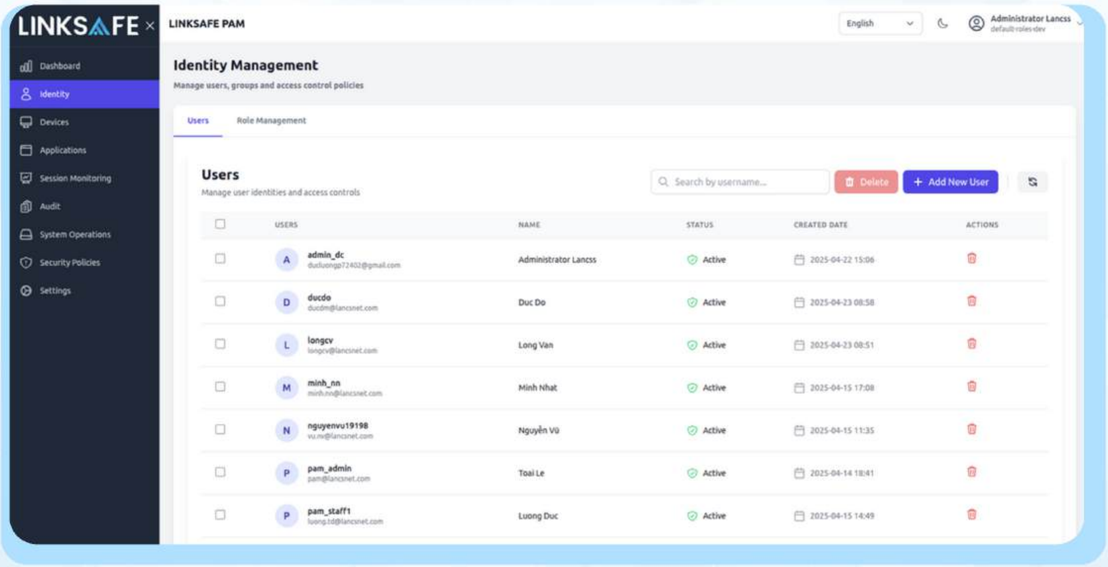
Cho phép đăng nhập vào hệ thống nội bộ quan trọng mà người dùng không cần biết mật khẩu.

Hỗ trợ auto-login cho:

- Web quản trị
- Ứng dụng nội bộ/ phần mềm DN
- Giao thức SSH, RDP, VNC



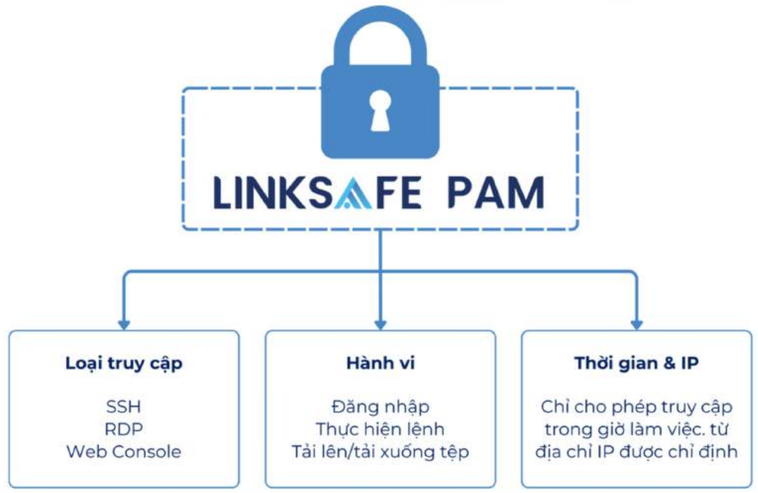
Giao diện các tài nguyên được phân quyền đăng nhập tự động



2.2 LINKSAFE PAM - KIỂM SOÁT TRUY CẬP

Thiết lập chính sách truy cập

- Chính sách linh hoạt, dễ tùy chỉnh.
- Có thể kết hợp với hệ thống phân quyền hiện có như AD, LDAP, IAM.



Mô tả tính năng: Thiết lập chính sách truy cập

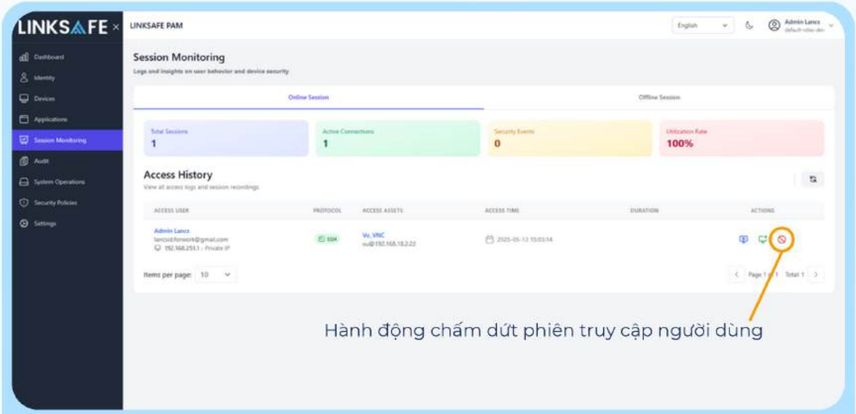
Can thiệp phiên truy cập thời gian thực

Quản trị viên có thể theo dõi, giám sát, ghi nhận và kiểm soát phiên truy cập theo thời gian thực.

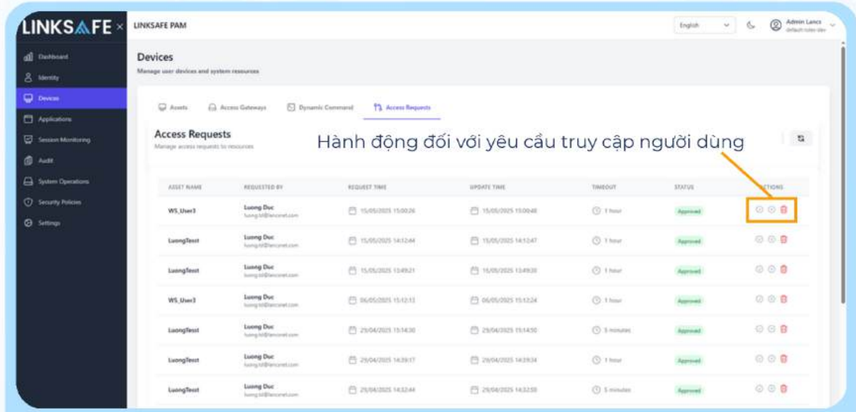
- **Xem trực tiếp** phiên truy cập đang diễn ra của người dùng.
- **Tham gia (join) phiên** để hỗ trợ kỹ thuật.
- **Chấm dứt phiên truy cập** ngay lập tức nếu phát hiện hành vi nguy hiểm.

Xét duyệt truy cập tài nguyên

Phê duyệt hoặc từ chối yêu cầu truy cập tài nguyên quan trọng từ người dùng, kiểm duyệt lý do truy cập.



Giao diện chấm dứt phiên truy cập



Giao diện phê duyệt yêu cầu truy cập người dùng

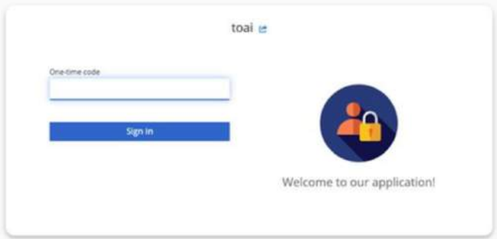
2.2 LINKSAFE PAM - XÁC THỰC VÀ PHÂN QUYỀN

Xác thực người dùng

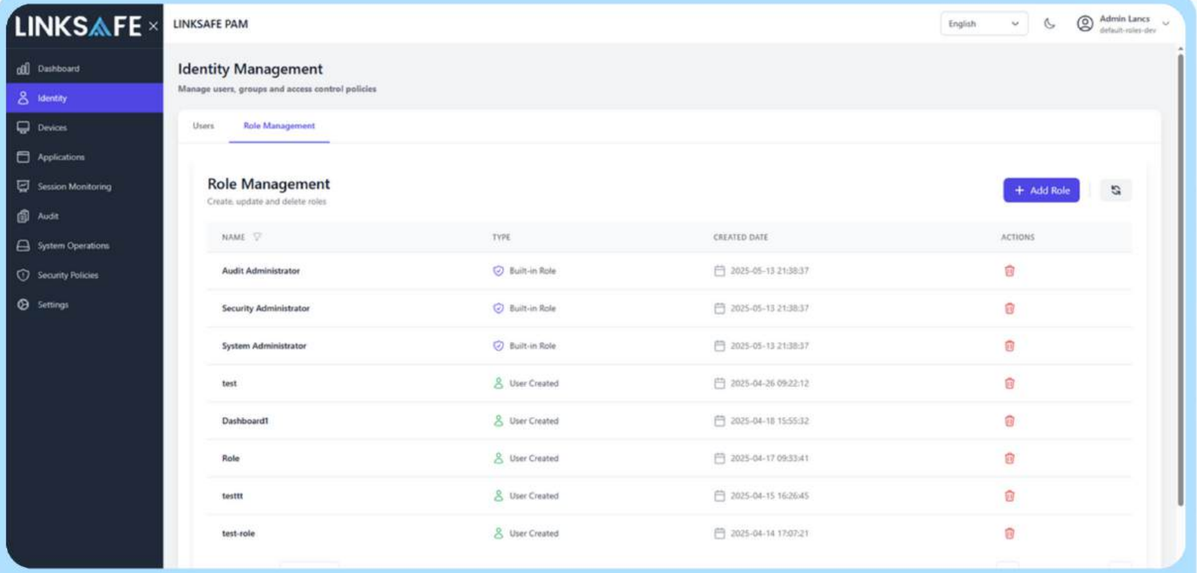
Xác minh danh tính người dùng trước khi cấp quyền truy cập vào tài nguyên đặc quyền.

Hỗ trợ phương thức xác thực

- Username/ Password
- MFA
- SAML / OIDC Token
- LDAP / Active Directory



Giao diện màn hình đăng nhập có yêu cầu xác thực từ phía người dùng



Giao diện quản lý vai trò và phân quyền cho người dùng

Phân quyền & quản lý vai trò (RBAC)

Phân loại người dùng theo vai trò và cấu hình chính sách cho từng vai trò.

Quản lý phiên làm việc

Quản lý toàn bộ quá trình truy cập của người dùng đặc quyền đến tài nguyên (máy chủ, CSDL...).

2.2 LINKSAFE PAM - QUẢN LÝ TRUY CẬP TỪ XA

Ghi lại phiên làm việc

Tự động ghi lại toàn bộ thao tác của người dùng trong phiên truy cập, bản ghi có thể phát lại để hỗ trợ truy vết khi có sự cố hoặc kiểm toán nội bộ.

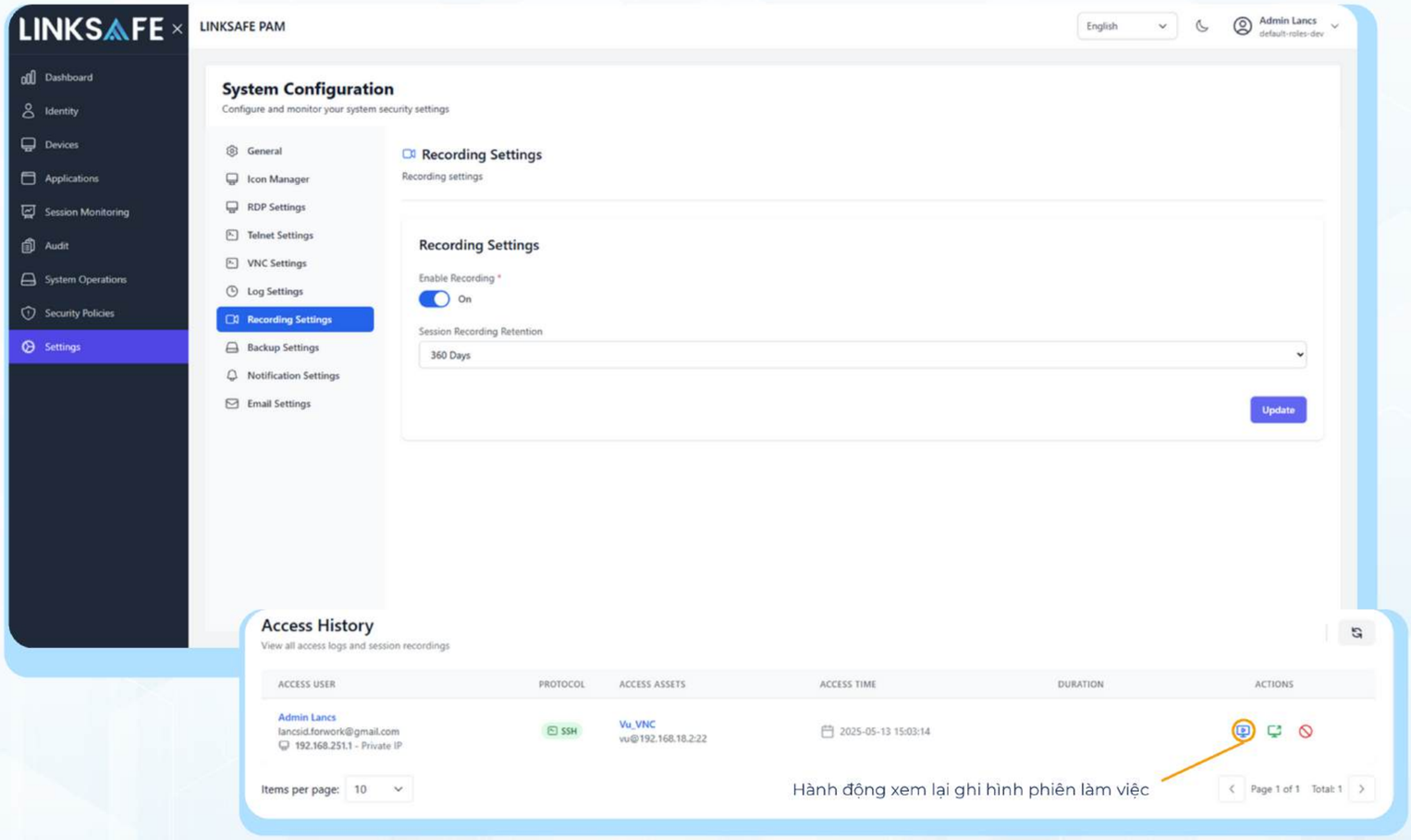
Hỗ trợ truy cập từ xa

Cho phép người dùng kết nối từ xa đến hệ thống đích, được thực hiện thông qua Gateway trung gian, không cần lộ địa chỉ IP thực của máy chủ.

Hỗ trợ thực thi lệnh Command

Cho phép người dùng truy cập dòng lệnh SSH ngay trên trình duyệt web để điều khiển máy chủ từ xa.

Giao diện thiết lập ghi lại phiên làm việc



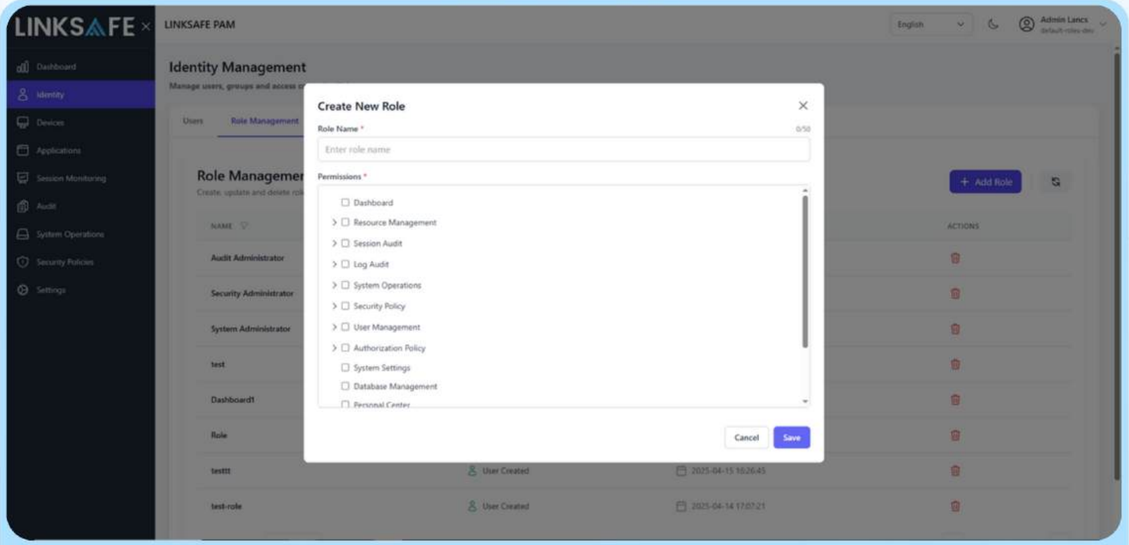
2.2 LINKSAFE PAM - QUẢN LÝ HỆ THỐNG

Thiết lập chính sách quản lý người dùng

Cho phép quản trị viên tạo nhóm người dùng, gán vai trò và thiết lập quyền cụ thể theo từng nhóm.

Thiết lập Permissions

Ai được quyền truy cập vào hệ thống nào?

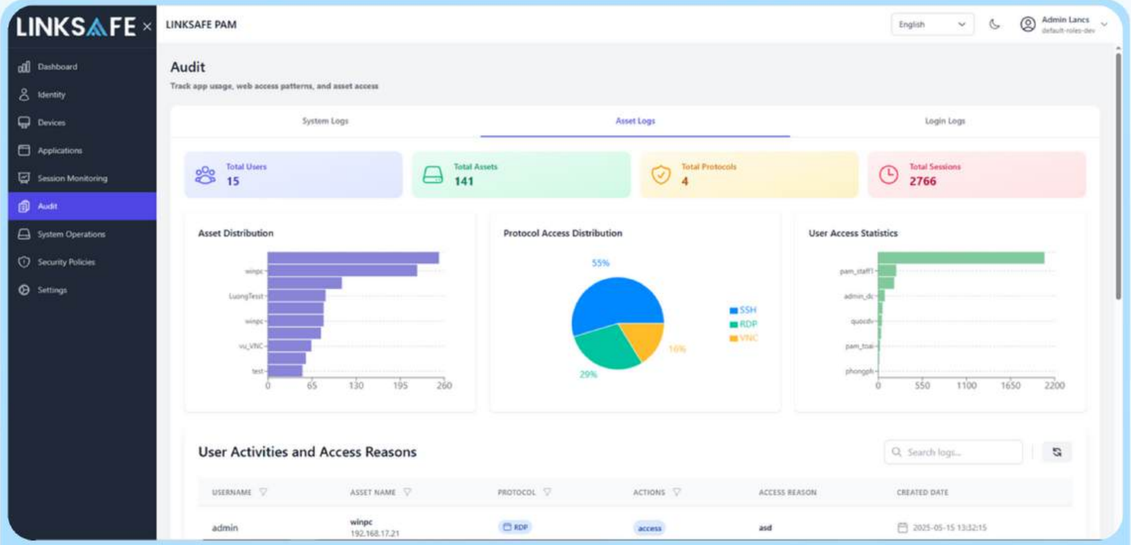


Giao diện thiết lập chính sách cho vai trò người dùng

Thu thập, lưu trữ & phân tích log

Nhật ký hoạt động được lưu trữ tập trung và mã hóa an toàn, dễ dàng truy xuất khi cần điều tra hoặc kiểm toán.

- **Logs hệ thống** (System logs).
- **Logs tài sản** (Asset logs).
- **Logs đăng nhập** (Login logs).



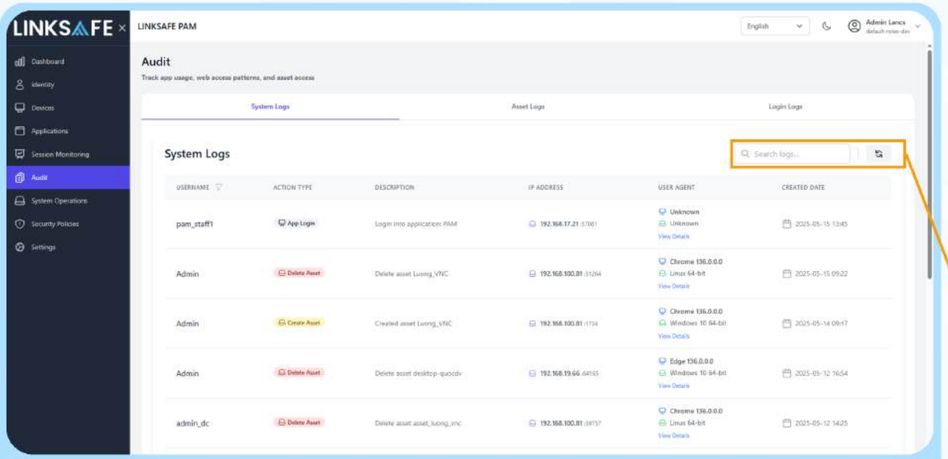
Giao diện Giám sát logs của hệ thống, asset, user

2.2 LINKSAFE PAM - QUẢN LÝ NHẬT KÝ

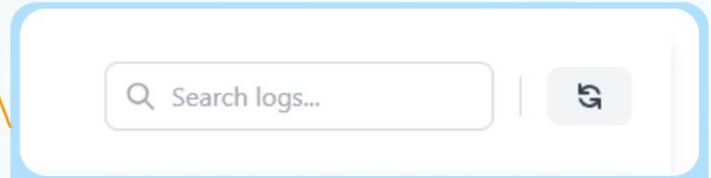
Thu thập nhật ký hoạt động

Hệ thống tự động ghi lại tất cả các hoạt động liên quan đến người dùng và hệ thống.

- Thời gian **đăng nhập/đăng xuất.**
- **Hành động** thực hiện.
- **Đối tượng** thực hiện hành động.



Giao diện nhật ký hoạt động trong hệ thống



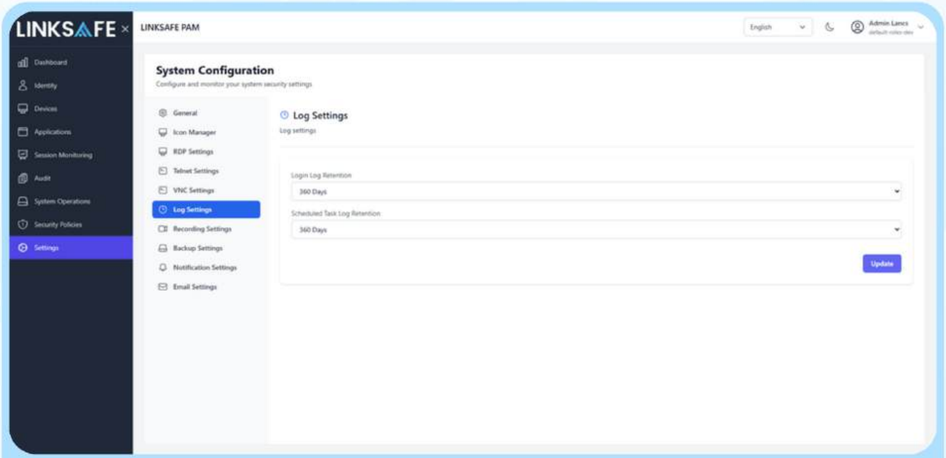
Thành phần tìm kiếm trong bảng logs

Tìm kiếm & truy vấn nhật ký hoạt động

Cho phép tìm kiếm và hỗ trợ lọc thông tin cụ thể trong log theo người dùng, địa chỉ IP, tag...

Lưu trữ nhật ký hoạt động

Toàn bộ nhật ký được lưu trữ tập trung theo thời gian thực, được mã hóa và cấu hình thời gian lưu trữ.



Giao diện cấu hình thời gian lưu trữ nhật ký hoạt động

2.3 TỔNG QUAN MODULE TRUY CẬP KHÔNG TIN CẬY - LINKSAFE ZTNA

LINKSAFE ZTNA (Zero Trust Network Access) - Module bảo mật tiên tiến, áp dụng mô hình "Zero Trust" (không tin tưởng mặc định) để kiểm soát truy cập mạng, giúp xác minh liên tục danh tính người dùng và thiết bị đối với người dùng trong mạng nội bộ và từ xa, đảm bảo chỉ những đối tượng đáng tin cậy mới được phép truy cập tài nguyên hệ thống.

Tính năng chính

Quản lý danh tính, thiết bị

Theo dõi, xác thực, và kiểm soát quyền truy cập dựa trên danh tính người dùng

Quyền truy cập tối thiểu

Chỉ cấp quyền truy cập cần thiết, giảm thiểu rủi ro truy cập trái phép.

Kiểm soát truy cập theo ngữ cảnh

Điều chỉnh quyền truy cập dựa trên vị trí, thời gian, thiết bị, và ngữ cảnh.

Thiết lập chính sách quản lý truy cập mạng

Thiết lập và áp dụng các chính sách truy cập, đảm bảo kiểm soát linh hoạt và an toàn toàn hệ thống.

Giám sát & quản lý tập trung

Hỗ trợ quản lý tập trung các thiết bị mạng, thống kê, giám sát hoạt động truy cập và tạo báo cáo chi tiết.

Truy cập từ xa an toàn (VPN)

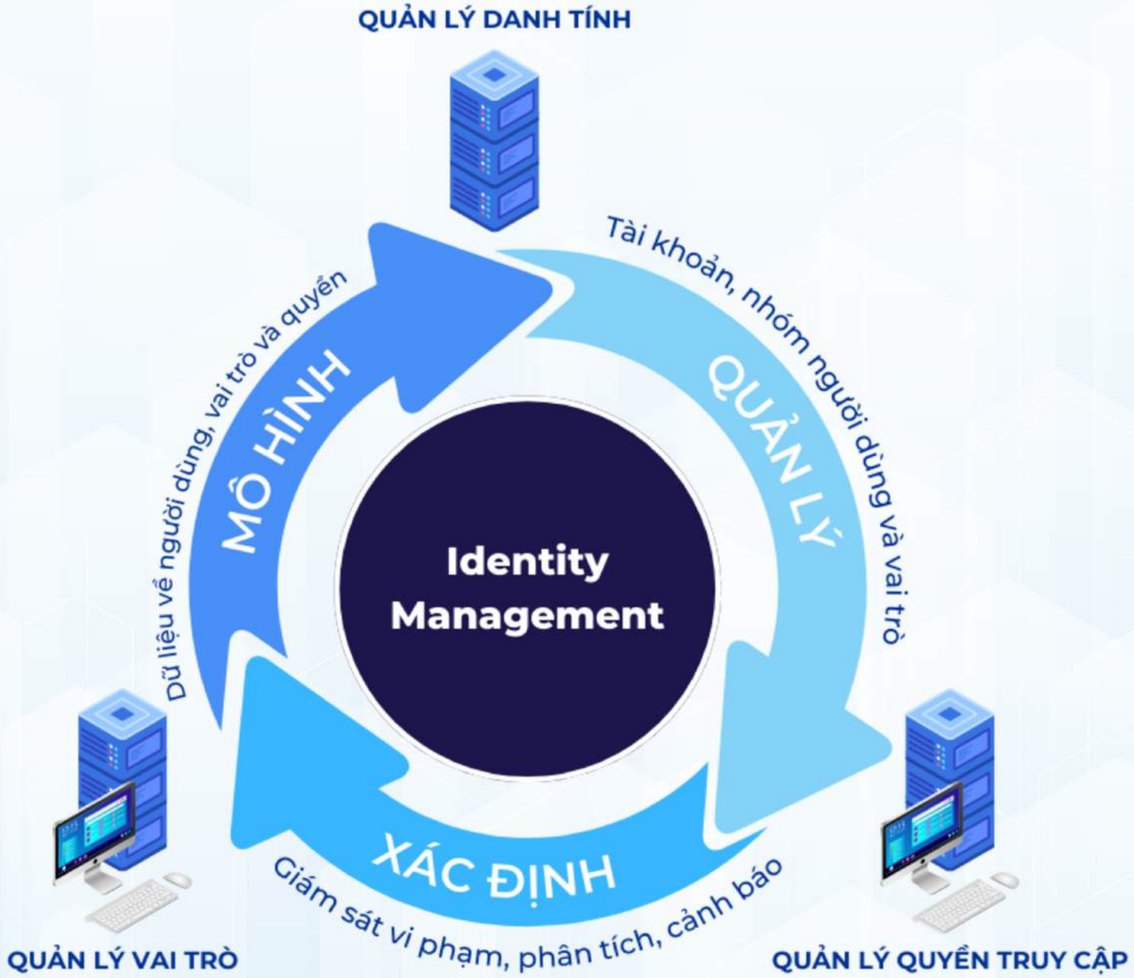
Cung cấp truy cập an toàn từ client đến gateway.

Bảo mật toàn diện với nguyên tắc *"Never trust, always verify"*

Tiết kiệm chi phí đầu tư xây dựng cơ sở hạ tầng mạng

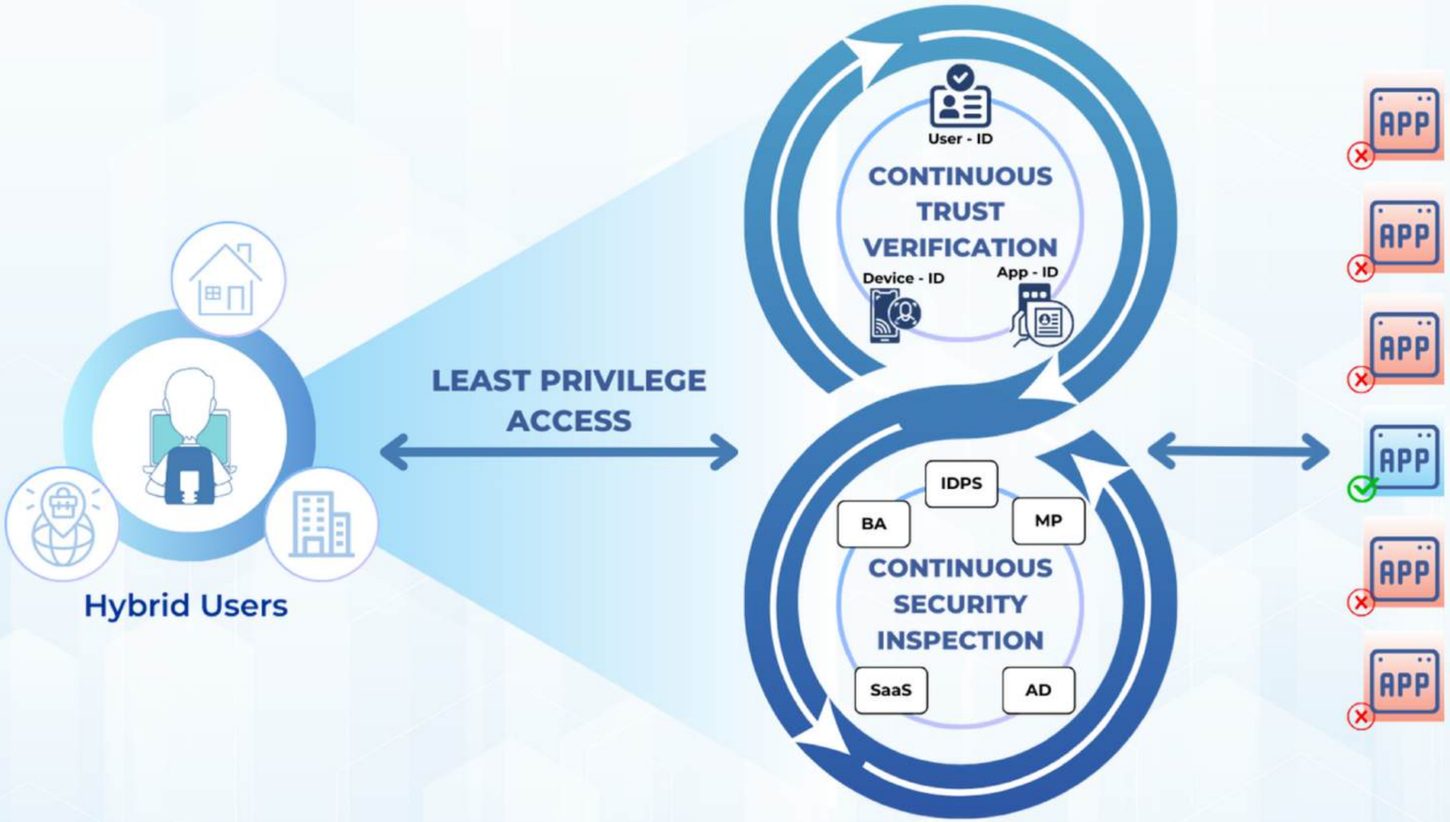
Truy cập từ xa an toàn mọi lúc, mọi nơi.

2.3 LINKSAFE ZTNA - QUẢN LÝ DANH TÍNH



- ***Quản lý danh tính người dùng***, bao gồm quản lý danh sách, hồ sơ và thông tin người dùng.
- ***Quản lý phương thức xác thực/ đăng nhập***, bao gồm:
  - Xác thực đa yếu tố: OTP, tin nhắn SMS, email.
  - Đăng nhập với mật khẩu, không mật khẩu với Passkeys hoặc với token phần cứng (theo chuẩn FIDO2/ Webauthn).
- ***Quản lý quyền truy cập***, bao gồm quản lý tài nguyên web, quyền, chính sách; phân quyền theo vai trò (RBAC) và thuộc tính (ABAC).
- Tích hợp dữ liệu về người dùng từ các hệ thống quản lý sẵn có.
- Hỗ trợ xuất ra luồng log theo chuẩn syslog, sẵn sàng tích hợp với các hệ thống SIEM.
- Quản lý trạng thái ATTT của người dùng bằng các yếu tố posture: GeoLocation, OS, version, phần mềm, trạng thái tuân thủ.
- Quản lý truy cập đặc quyền (PAM) thông qua các giao thức SSH/RDP/VNC.

2.3 LINKSAFE ZTNA - QUYỀN TRUY CẬP TỐI THIỂU



- Xác định, gán quyền truy cập và điều chỉnh quyền truy cập cho vai trò; Tạo và quản lý các nhóm người dùng.
- Xác định, kiểm tra thuộc tính người dùng và ngữ cảnh trước khi cấp quyền.
- Cấp quyền thu cập tạm thời, có thể điều chỉnh quyền truy cập thời gian thực và thu hồi quyền khi phát hiện rủi ro
- Phân đoạn mạng và cô lập tài nguyên, giảm rủi ro lây lan khả năng xâm nhập vào hệ thống.
- Tích hợp với hệ thống giám sát SIEM; theo dõi lịch sử truy cập, ghi lại yêu cầu truy cập và cấp quyền truy cập theo yêu cầu.
- Áp dụng các chính sách truy cập dựa trên ngữ cảnh.

2.3 LINKSAFE ZTNA - KIỂM SOÁT TRUY CẬP THEO NGỮ CẢNH

- Kiểm soát truy cập dựa theo giới hạn địa lý, thời gian, ứng dụng và chính sách.
- Kiểm tra phiên bản hệ điều hành, các phần mềm, trạng thái tuân thủ và quy trình chạy trên thiết bị cuối.
- Tạo các backlist, whitelist, tag... cho các thông tin của thiết bị.
- Phân tích hành vi đăng nhập, truy cập ứng dụng; Phát hiện với các hành vi bất thường và cảnh báo, tự động phản ứng.
- Xác định loại mạng và điều chỉnh quyền truy cập theo loại mạng.
- Phân tích hành vi người dùng và thực thể (UEBA).

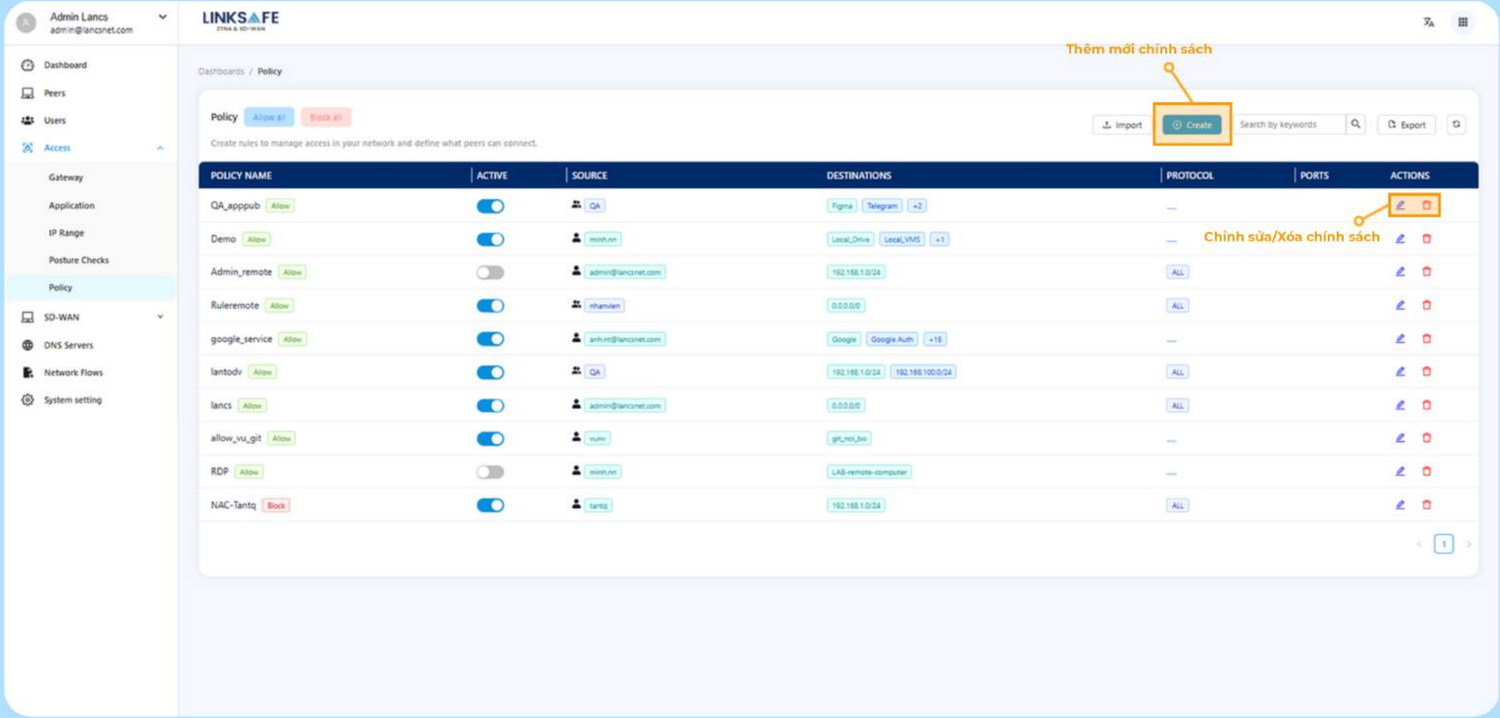
2.3 LINKSAFE ZTNA - THIẾT LẬP CHÍNH SÁCH QUẢN LÝ TRUY CẬP MẠNG

Chính sách quản lý mạng

Cho phép thiết lập, áp dụng và phân phối các chính sách mạng một cách chi tiết và tự động cho toàn bộ hệ thống: loại lưu lượng, ứng dụng và người dùng

Chính sách quản lý truy cập

Thiết lập và cập nhật các chính sách truy cập theo ngữ cảnh như: thiết bị đầu cuối, thời gian, vị trí, hoặc mức độ rủi ro – đảm bảo chỉ những truy cập hợp lệ, đúng người, đúng thời điểm mới được phép kết nối.



Giao diện Quản lý chính sách quản lý truy cập mạng

2.3 LINKSAFE ZTNA - GIÁM SÁT & QUẢN LÝ TẬP TRUNG

Quản lý tập trung theo thời gian thực

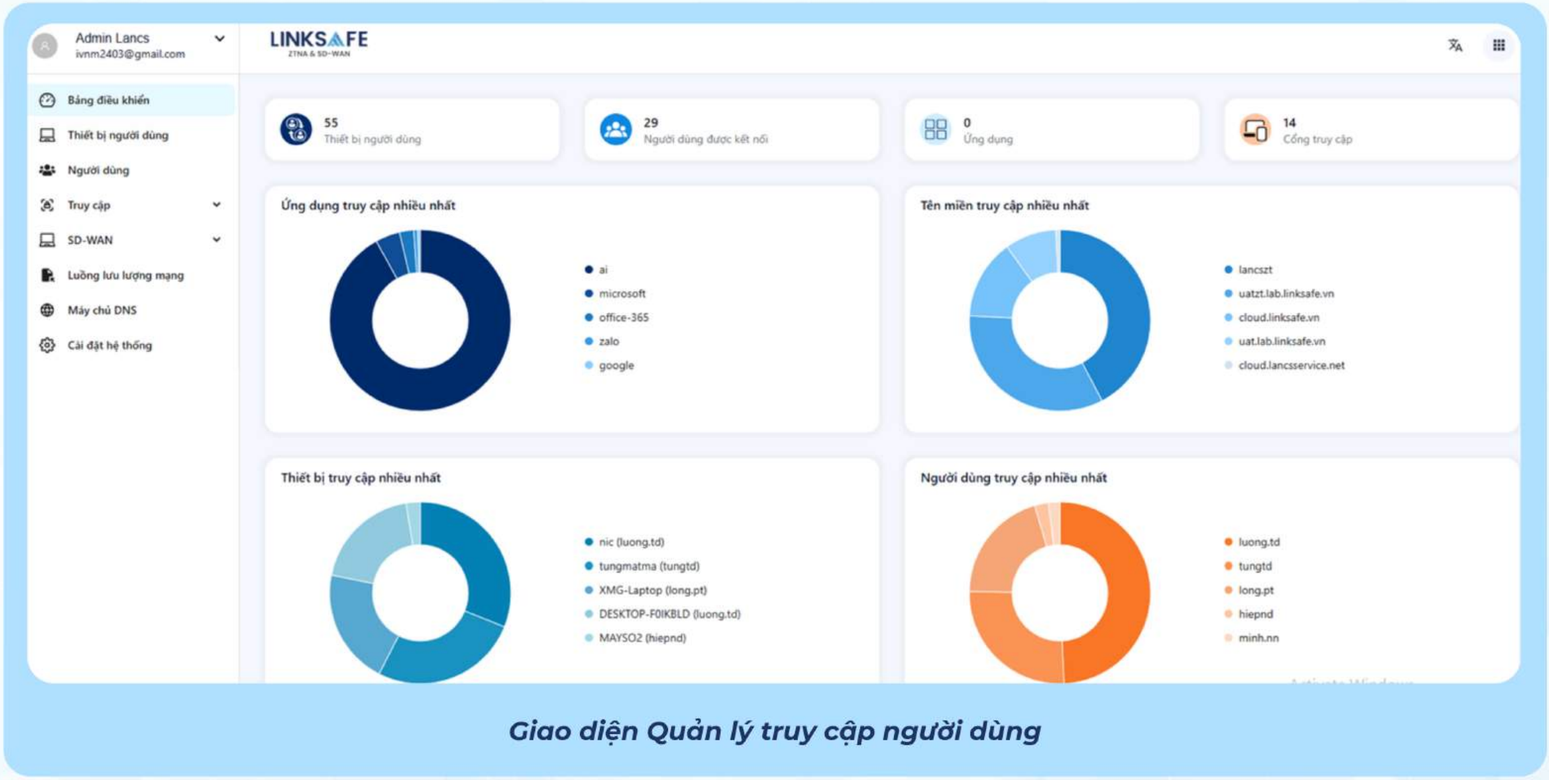
Toàn bộ thiết bị mạng, hoạt động (lưu lượng, kết nối, ứng dụng, người dùng...) được theo dõi tập trung thông qua giao diện quản lý trực quan.

Cảnh báo và phản hồi thông minh

Hệ thống có khả năng gửi cảnh báo tức thời (real-time alert) khi phát hiện truy cập trái phép, bất thường hoặc vượt chính sách.

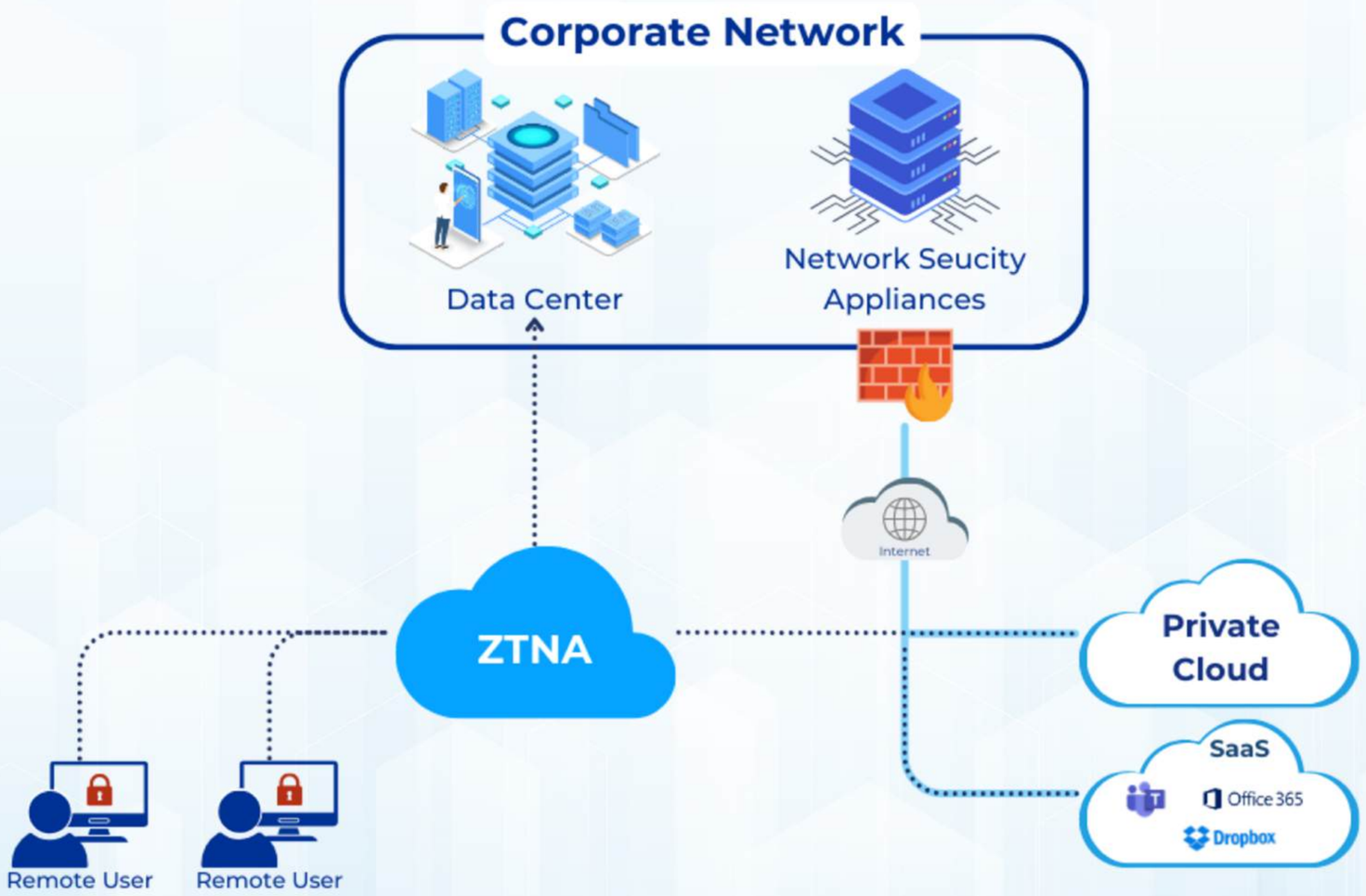
Báo cáo chi tiết và tùy biến

Tự động tạo các báo cáo định kỳ về hiệu suất mạng, trạng thái truy cập và sự kiện bảo mật theo thời gian, người dùng, thiết bị, ứng dụng...



Giao diện Quản lý truy cập người dùng

2.3 LINKSAFE ZTNA - TRUY CẬP TỪ XA AN TOÀN



- Mã hóa toàn bộ dữ liệu được truyền tải giữa người dùng từ xa và các tài nguyên trong mạng thông qua Wireguard / TLS.
- Thiết lập các chính sách kết nối cho người dùng truy cập từ xa.
- Bảo mật truy cập tới các ứng dụng, trang web nội bộ và ứng dụng, dịch vụ triển khai trên cloud.
- Đảm bảo an toàn và bảo mật thông tin cho các kết nối từ xa, kiểm soát chặt chẽ truy cập vào tài nguyên của tổ chức

TRÂN TRỌNG CẢM ƠN

LIÊN HỆ CHÚNG TÔI

info@lancsnet.com

www.lancsnet.com

+84 8680275 959

Trụ sở: Tầng 2, Số 236 Âu Cơ, Phường Hồng Hà, Hà Nội, Việt Nam.

Văn phòng: BT35 - TT3, KĐT thành phố Giao Lưu, Đường Phạm Văn Đồng, Phường Phú Diễn, Hà Nội, Việt Nam.