FPT CLOUD
by FPT Smart Cloud

GIẢI PHÁP

Bảo mật & An toàn dữ liệu cho doanh nghiệp

Theo giới chuyên gia, trong lĩnh vực an ninh mạng, khó có khái niệm "an toàn" vĩnh viễn. Từ các vụ việc bị tấn công mạng gần đây tại Việt Nam, đã đến lúc các tổ chức, doanh nghiệp chuyển từ tư duy “chữa bệnh” sang “phòng bệnh”.

I. Rủi ro tấn công mạng tại Việt Nam

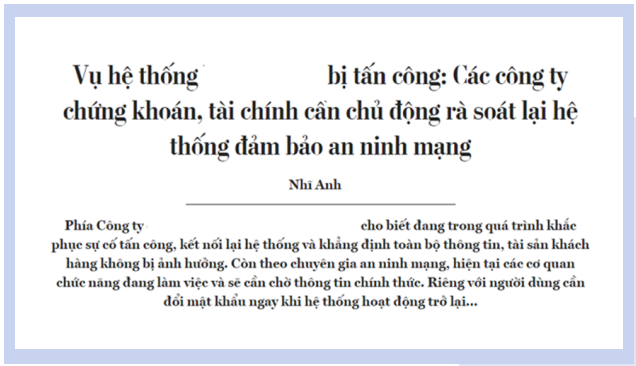
1. Sự cố tấn công Ransomware vào doanh nghiệp

Các sự cố tấn công mạng:

- Vào tháng 03/2024, một công ty chứng khoán tại Việt Nam đã trở thành điểm nóng trên bản đồ của các cuộc tấn công ransomware quốc tế
- Ngày 29/7/2016, tin tặc có nguồn gốc Trung Quốc đã thực hiện cuộc tấn công mạng vào hệ thống thông tin của một hãng hàng không lớn tại Việt Nam
- Ngày 12/5/2017, cuộc tấn công ransomware lớn nhất thế giới xảy ra, virus wannacry lây nhiễm vào 200.000 hệ thống, với 150 lãnh thổ quốc gia

Thiệt hại:

- Gây gián đoạn hoạt động kinh doanh doanh nghiệp
- Dữ liệu quan trọng có nguy cơ mất vĩnh viễn, không thể khôi phục
- Ảnh hưởng đến trải nghiệm khách hàng và uy tín của doanh nghiệp

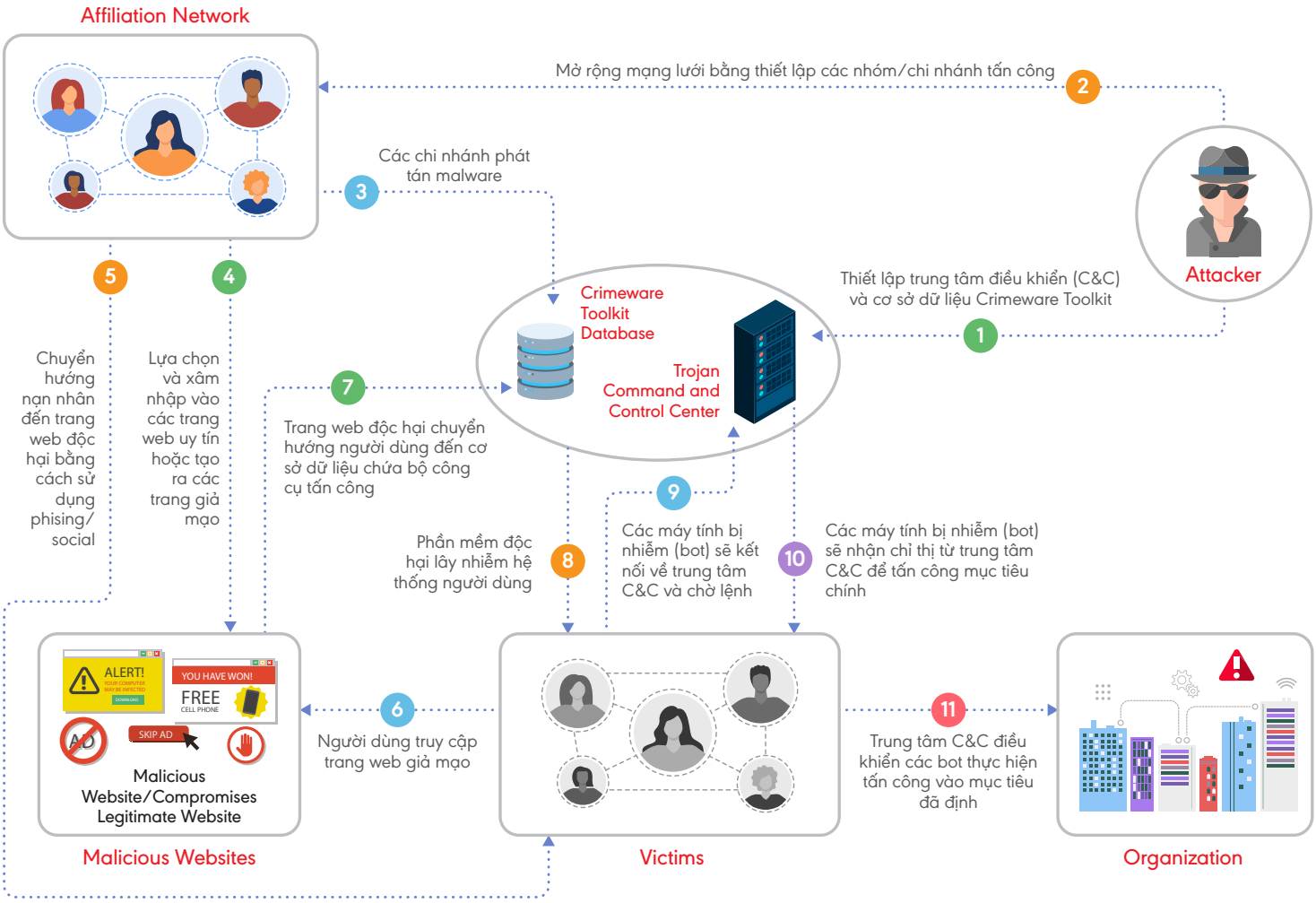


Vụ hệ thống bị tấn công: Các công ty chứng khoán, tài chính cần chủ động rà soát lại hệ thống đảm bảo an ninh mạng

Nhi Anh

Phía Công ty cho biết đang trong quá trình khắc phục sự cố tấn công, kết nối lại hệ thống và khẳng định toàn bộ thông tin, tài sản khách hàng không bị ảnh hưởng. Còn theo chuyên gia an ninh mạng, hiện tại các cơ quan chức năng đang làm việc và sẽ cần chờ thông tin chính thức. Riêng với người dùng cần đổi mật khẩu ngay khi hệ thống hoạt động trở lại...

2. Phương pháp tấn công phổ biến



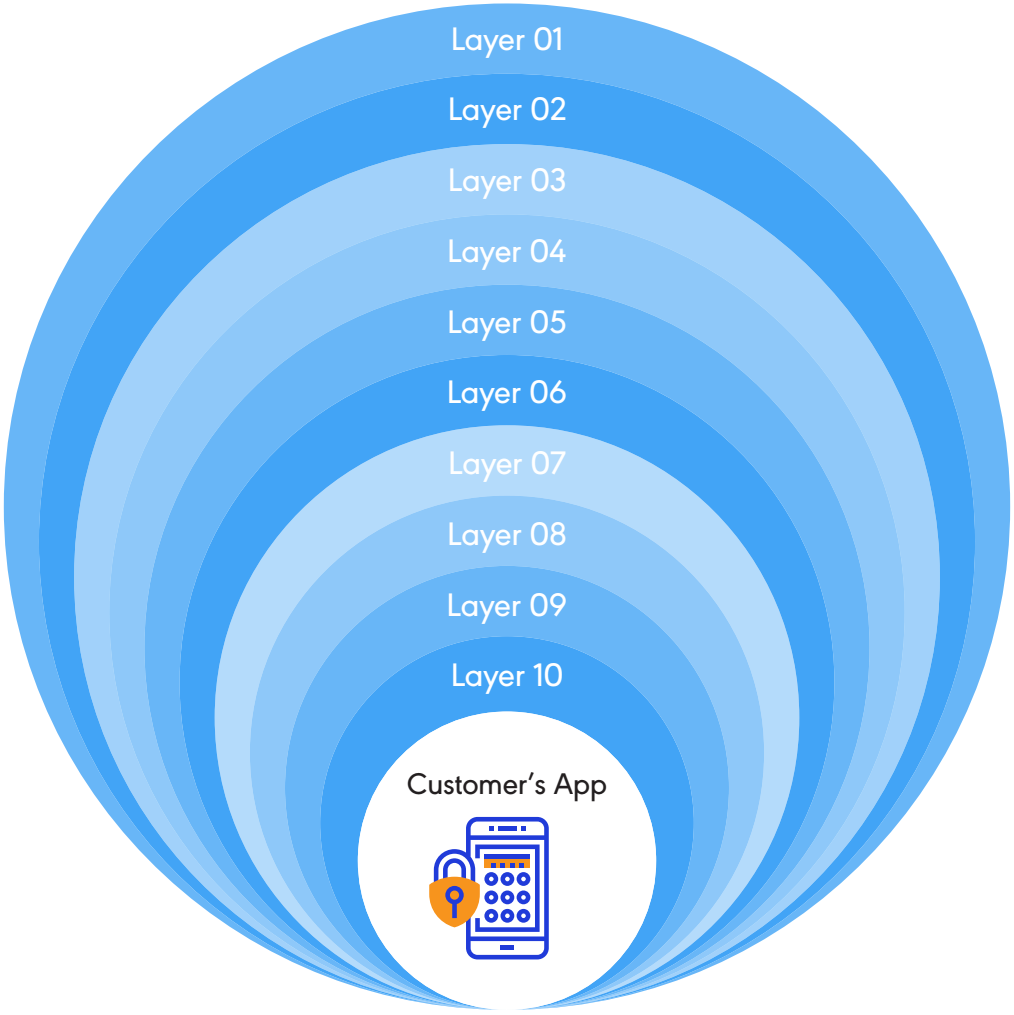
3. Rủi ro bảo mật doanh nghiệp gặp phải

- Người dùng nhiễm mã độc malware tấn công vào hệ thống
- Các kết nối từ on-prem lên Cloud
- Lỗ hổng bảo mật và ứng dụng phiên bản quá cũ
- Malware/Ransomware, Bảo mật hạ tầng
- Lây nhiễm mã độc, huỷ phương thức xác thực
- Web/API attack

II. Giải pháp đảm bảo an toàn bảo mật cho doanh nghiệp

1. Mô hình kiến trúc bảo mật nhiều lớp - Defense in Depth

Hệ thống ứng dụng của doanh nghiệp được khuyến nghị sử dụng 10 lớp bảo mật, đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng (theo tiêu chuẩn cốt lõi CIA) cho toàn bộ hệ thống.



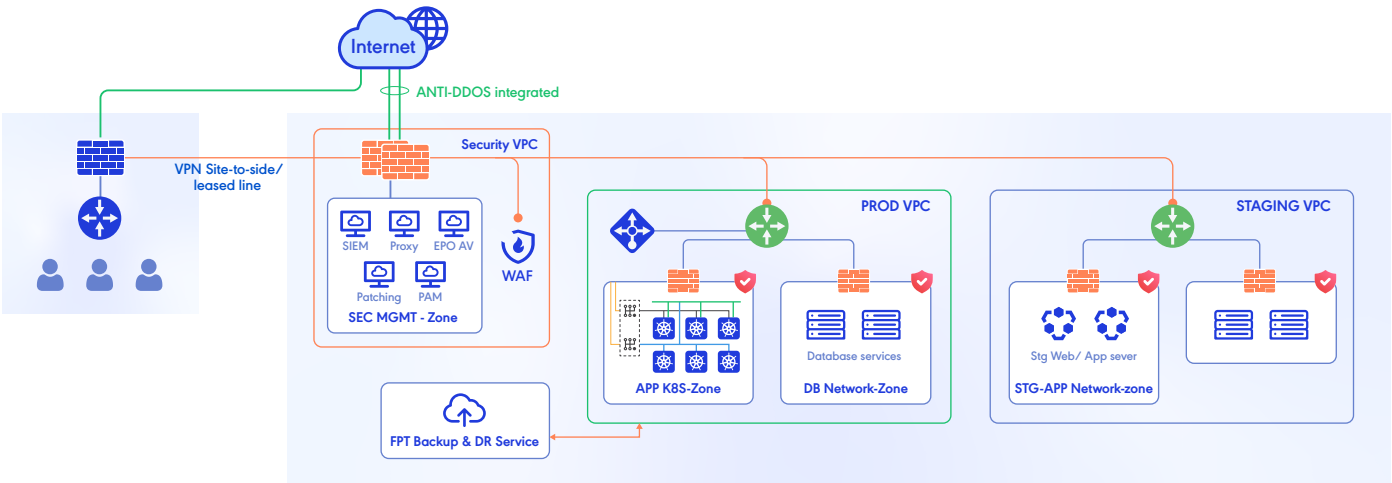
Layer 01: Chính sách bảo mật và đào tạo nhân sự
Layer 02: Bảo mật mạng (Network Security)
Layer 03: Kiểm soát truy cập (Access Control)
Layer 04: Bảo mật đầu cuối (Endpoint Security)
Layer 05: Bảo mật ứng dụng (Application Security)
Layer 06: Lỗ hổng bảo mật và bản vá (Vulnerabilities and Patching)
Layer 07: Bảo mật container (Container Security)
Layer 08: Bảo mật dữ liệu (Data Security)
Layer 09: SOC, Thông báo sự cố, Giám sát 24/7
Layer 10: Backup & DR

2. Các yếu tố vận hành an toàn

Để vận hành một cách an toàn, doanh nghiệp cần chú ý đến các yếu tố:

CÔNG NGHỆ	Layer 1: Security	Đào tạo nhân sự, chính sách và quy định về bảo mật an toàn thông tin
	Layer 2: Network Security	Next-gen Firewall, VPN, IDPS, Web proxy, DDOS, Threat Intelligence
	Layer 3: Access Control	PAM, MFA
	Layer 4: Endpoint Security	Antimalware, Host IDPS, Host Firewall, Device Control, EDR
	Layer 5: Application Security	WAF, scan code, pentest/threat hunting
	Layer 6: Vulnerabilities and Patching	Đánh giá lỗ hổng bảo mật (Vulnerabilities Assessment), Bản vá lỗ hổng (Patching)
	Layer 7: Container Security	Image scanning, runtime protection
	Layer 8: Data Security	Mã hóa dữ liệu (Data Encryption), DLP Endpoint
	Layer 9: SOC	SIEM, Threat Intelligence
	Layer 10: Backup/DR	Backup, DR
QUY TRÌNH	Quy trình nội bộ	Quy trình xử lý sự cố (Incident response process), Quy trình đánh giá/ vá lỗ hổng bảo mật (Vulnerabilities/Patching process), Quy trình quản lý vận hành (Change management process)
CON NGƯỜI	Đội ngũ nhân sự	Tập hợp các chuyên gia bảo mật
	Chứng chỉ	Yêu cầu các chứng chỉ chuyên môn về bảo mật

3. Mô hình bảo mật tổng quan cho khách hàng trên Cloud



4. Các yếu tố công nghệ để vận hành an toàn

4.1. Layer I: Chính sách bảo mật và đào tạo nhân sự

- Tuân thủ chính sách ATTT chung của công ty
- Đào tạo nội bộ về các kỹ thuật tấn công, nâng cao nhận thức ATTT cho quản trị viên hệ thống
- Xây dựng tài liệu, quy trình đáp ứng các chuẩn an toàn thông tin quốc tế như: ISO27K, PCIDSS...

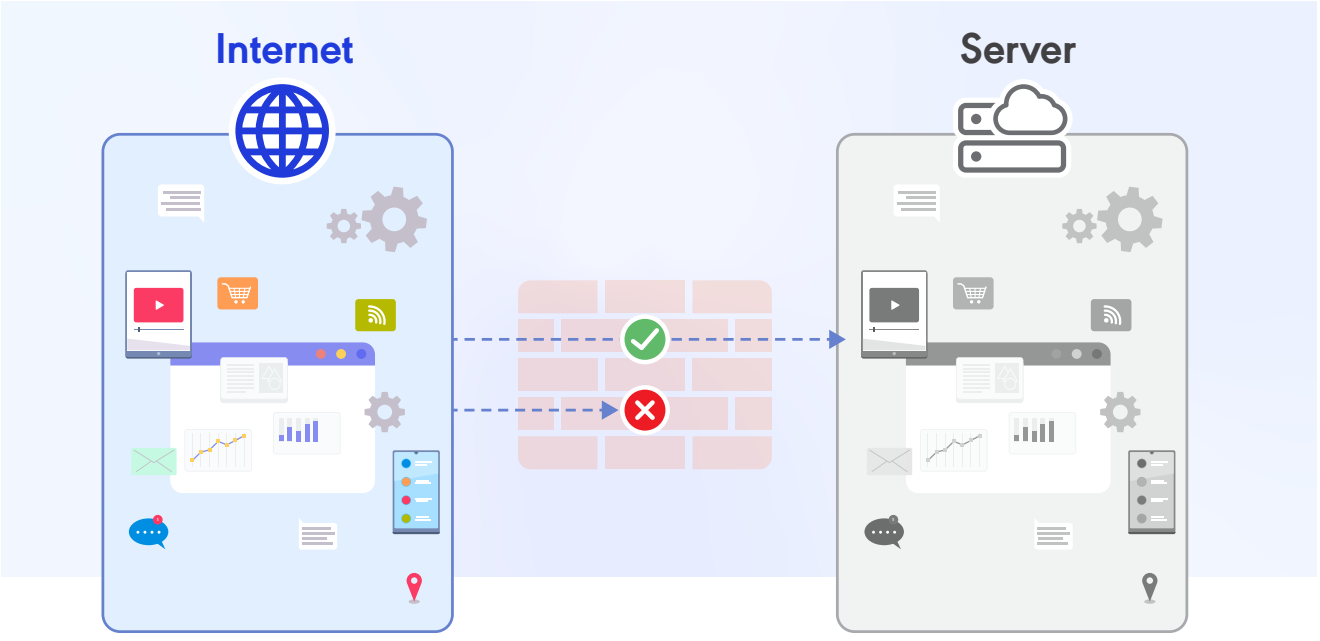
4.2. Layer II: Network Security

a. Giải pháp NGFW (Next Gen Firewall)

- Layer thứ nhất, NGFW thiết lập bảo mật mức Network: Cô lập các thành phần quan trọng sử dụng subnet, firewall, routing table, giới hạn inbound/outbound traffic, bật các tính năng nâng cao như Stateful Firewall, IDS & IPS, Antibot, AntiMalware, URL Filtering, Application Control, VPN...
- Layer thứ 2, the Distributed FW (Network Security Group), được tích hợp trong vRouter, giúp chia và điều khiển kết nối giữa các subnet mạng

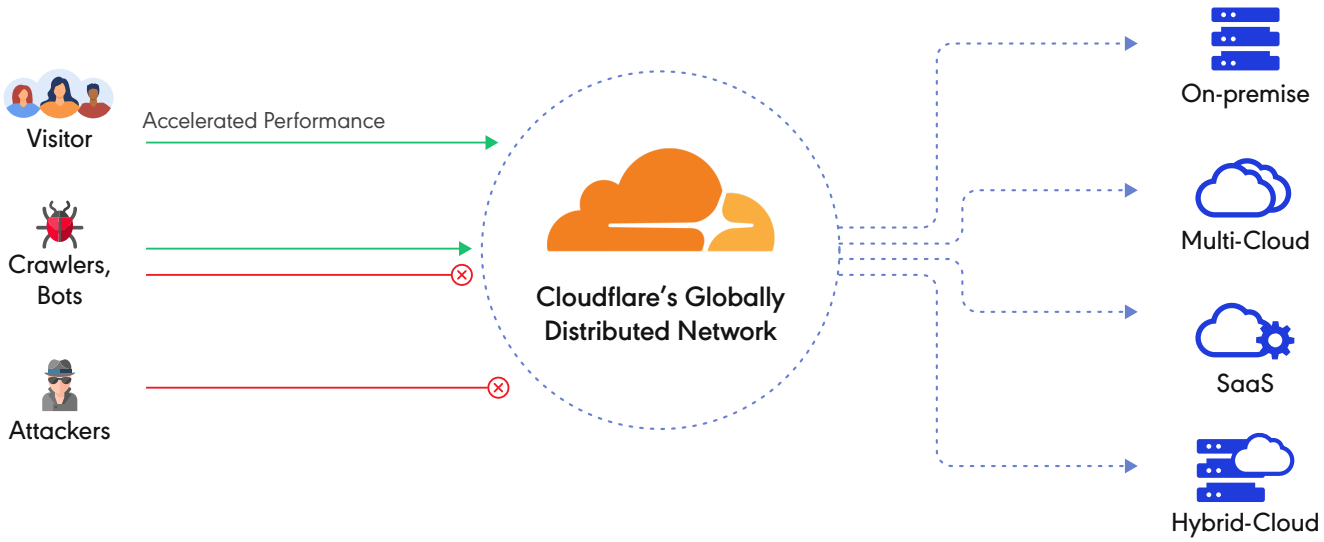
b. Giải pháp Web Proxy

- Chiều truy cập inbound/outbound của hệ thống được bảo vệ bằng Web Proxy
- Web Proxy thiết lập bảo mật truy cập internet sử dụng các tính năng Caching, Antivirus, Anti-Malware, Web and Geo Reputation...
- Lợi ích:
  - Antimalware & và các mã độc zero-day
  - Lọc URL và danh mục
  - Giải mã SSL



c. Giải pháp Anti-DDoS

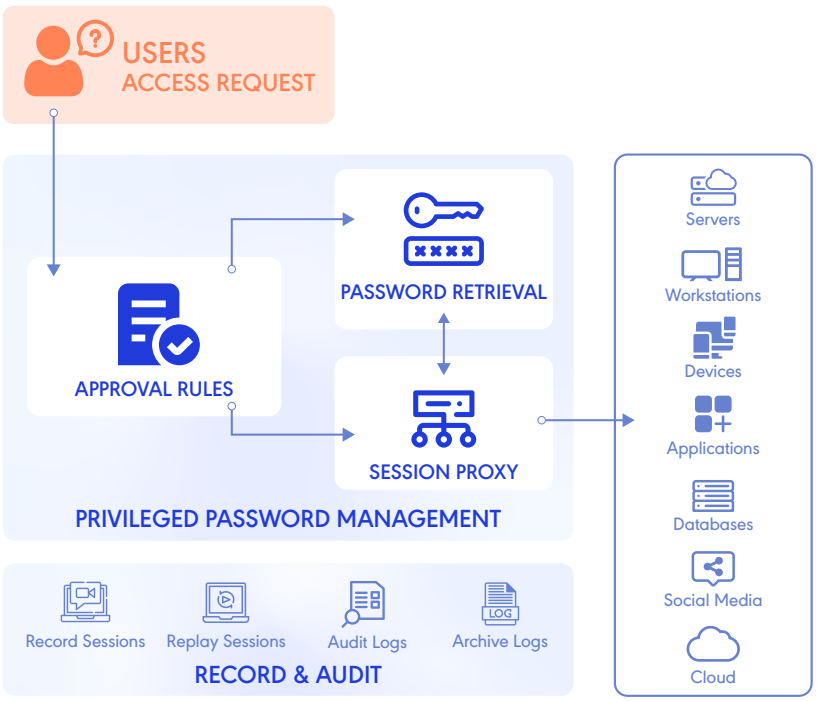
- Phòng chống tấn công DDoS Layer 3, 4 và Layer 7
- Được chia thành 3 loại tấn công: Volumetric Attacks, Protocol Attacks, Application Attacks
- Anti DDoS layer 4 phát hiện và ngăn chặn tấn công UDP Flood, ICMP Flood (Gbps); syn flood attack, ack flood (pps)...
- Anti DDoS layer 7 ngăn chặn các tấn công vào tài nguyên dịch vụ của ứng dụng, VD: http get/post attack, slowloris attack (rps)...



4.3. Layer III: Access control

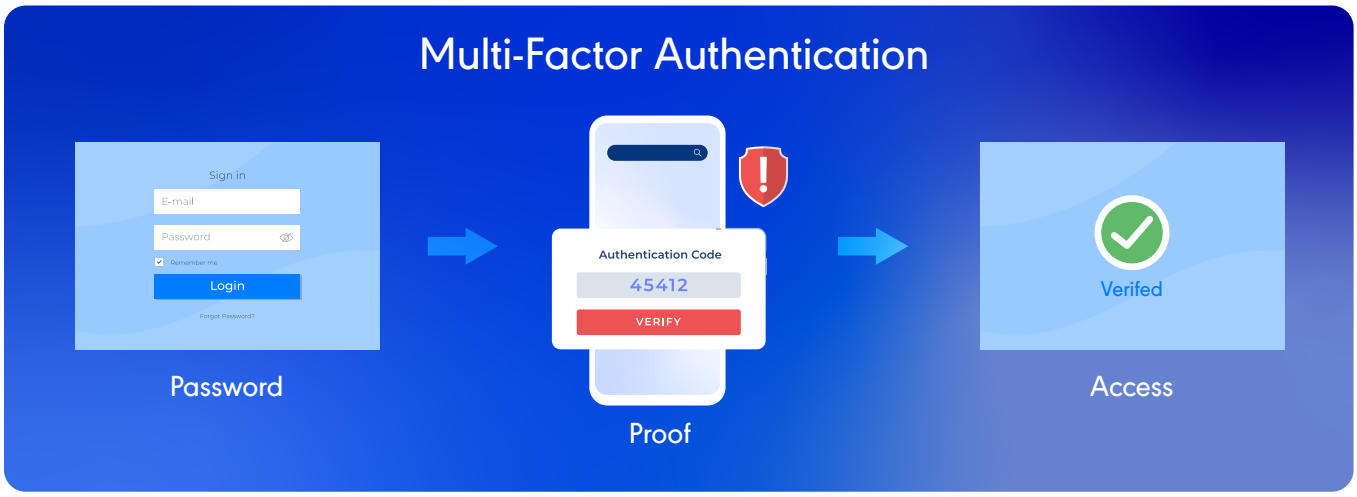
a. Giải pháp PAM (Privileged Access Management)

- Privileged Account Management là một giải pháp quản lý tập trung các mật khẩu đặc quyền như Administrators, Root, DBA,... của hệ thống. PAM dựa trên chính sách thống nhất, giám sát các tài khoản và các hoạt động liên quan đến mật khẩu đặc quyền từ các trung tâm dữ liệu cũng như trên môi trường cloud
- Lợi ích mang lại:
  - Kiểm soát các truy cập đặc quyền, quản lý mật khẩu tập trung cho các tài khoản đặc quyền, giám sát hành vi truy cập và lưu bằng chứng (log, video) trên cùng một giải pháp chuyên dụng
  - Cung cấp thông tin chính xác: Ai đang sử dụng tài khoản đặc quyền nào, truy cập đến hệ thống đích nào, đang thực thi/thao tác hành động gì đồng thời cung cấp cơ chế ngăn chặn tự động theo thời gian thực



b. Giải pháp MFA (Multi-factor Authentication)

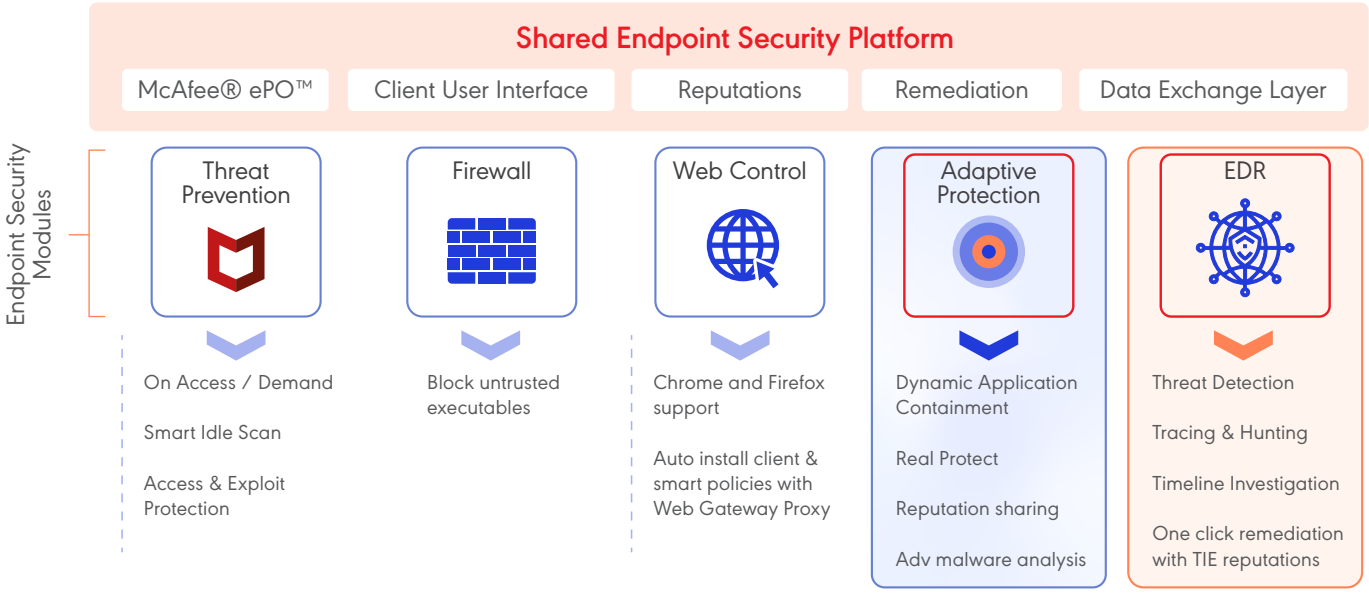
- Hệ thống MFA được triển khai trên các tenant của KH
- Quản trị viên truy cập vào VPN (NGFW/PAM) qua máy tính, từ đó radius nhận yêu cầu xác thực và kiểm tra thông tin với AD
- AD xác minh thông tin (user, password) và trả về kết quả xác thực cho radius, sau đó radius gửi mã OTP đến quản trị viên



4.4. Layer IV: Endpoint security

Giải pháp Endpoint Security

- Endpoint Security là giải pháp giúp bảo vệ thiết bị endpoint (Windows Workstation, Windows Server, Linux Server, MacOS) giúp ngăn chặn & phản ứng với các rủi ro (malware, virus, exploit) trên thiết bị endpoint
- EDR (Endpoint Detection & Response) giải pháp phòng chống điểm cuối nâng cao, giúp phát hiện ngăn chặn các mã độc chưa biết, các cuộc tấn công nâng cao APT, mã độc dạng fileless
- Lợi ích:
  - Phòng chống malware, antivirus, trojan, backdoor
  - Host IPS, HostFW, Device Control

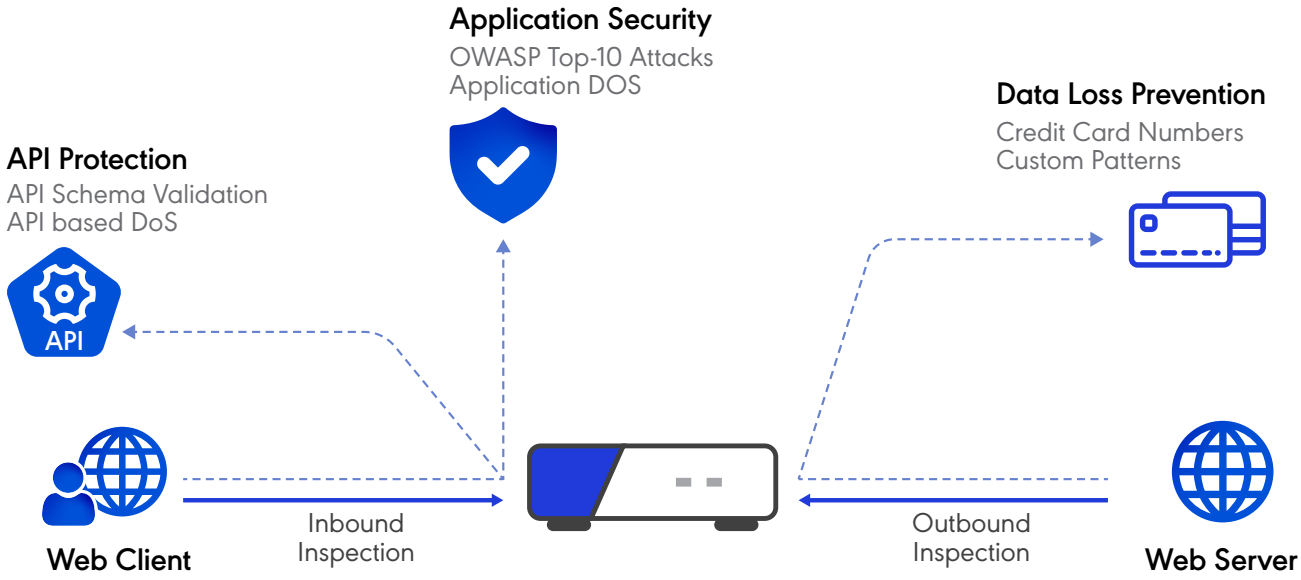


4.5. Layer V: Application Security

a. Giải pháp WAF (Web Application Firewall)

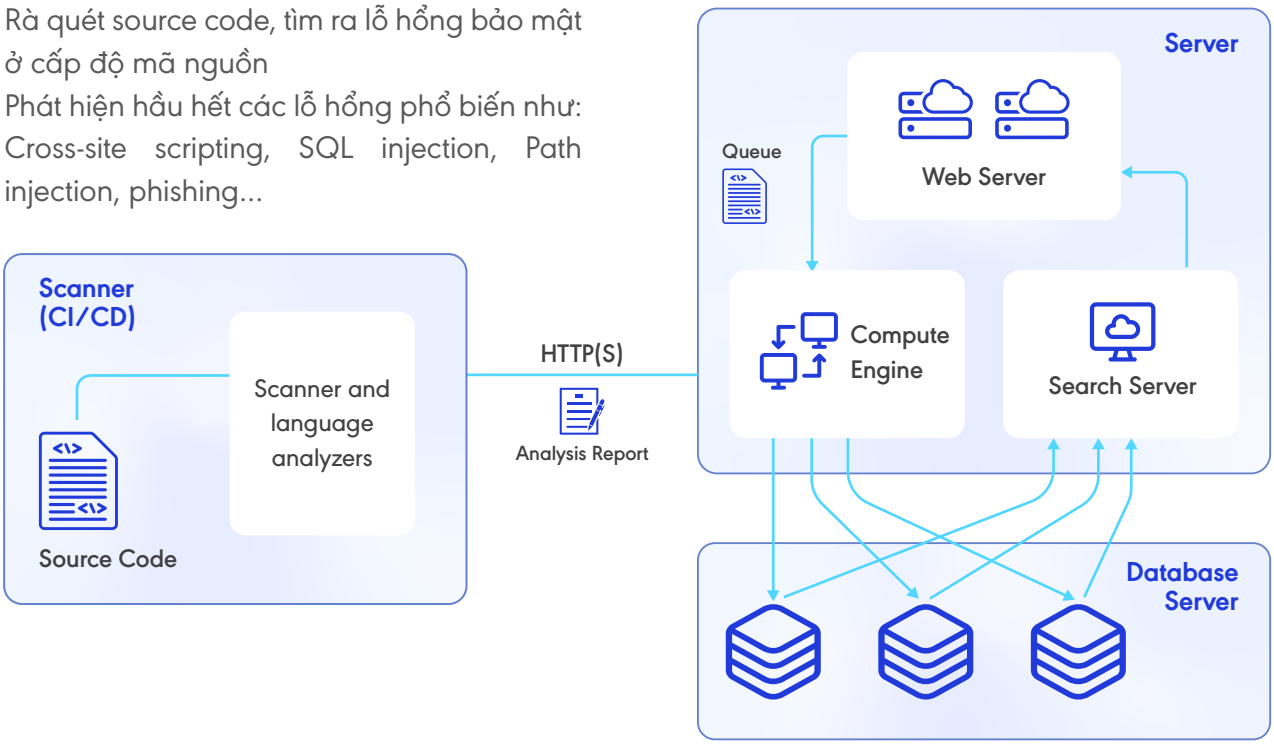
WAF giúp bảo vệ ứng dụng web trước các tấn công ứng dụng web phổ biến như: DOS, SQL Injection, Cross Site Scripting (XSS) và các loại tấn công web khác...

- Giúp bảo vệ ứng dụng websites từ top 10 OWASP attacks
- Dễ dàng sử dụng: Tối ưu rules, thay đổi nhanh chóng khi cần thiết
- Liên tục update: Bảo vệ ứng dụng WEB chống lại các tấn công và lỗ hổng mới nhất



b. Giải pháp Scan Code

- Hệ thống phần mềm scan security code, được sử dụng cho các đội DEV
- Lợi ích:
  - Rà quét source code, tìm ra lỗ hổng bảo mật ở cấp độ mã nguồn
  - Phát hiện hầu hết các lỗ hổng phổ biến như: Cross-site scripting, SQL injection, Path injection, phishing...



c. Dịch vụ Pentest

Dịch vụ kiểm thử xâm nhập (Penetration Testing): là quá trình mô phỏng lại toàn bộ quy trình, cách thức tấn công vào hệ thống CNTT. Bằng việc tạo ra các cuộc tấn công mạng theo kịch bản nhằm tìm ra lỗ hổng bảo mật mà tin tặc có thể khai thác để chiếm quyền điều khiển hoặc tấn công bằng ransomware

- Pentest ứng dụng trên môi trường UAT trước khi public
- Pentest các tính năng mới
- Threat hunting từ internet và internal

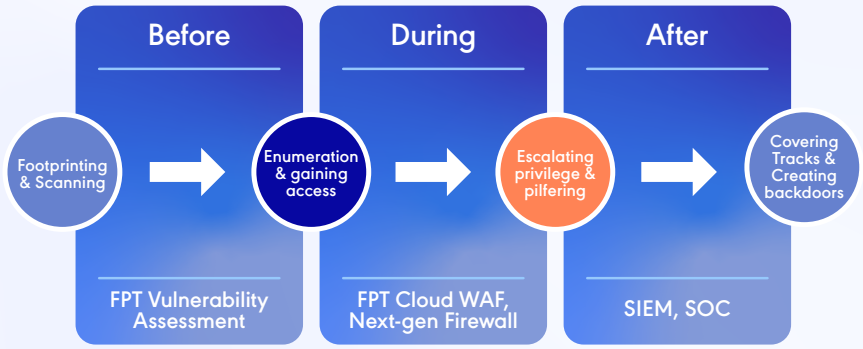
Mục tiêu

- Tìm ra lỗ hổng Web/API trước kẻ tấn công, giảm thiểu thiệt hại
- Duy trì danh tiếng, uy tín trước khách hàng
- Đáp ứng các tiêu chuẩn bảo mật ISO27k, PCI/DSS

4.6. Layer VI: Vulnerabilities & Patch management

a. Giải pháp VA (Vulnerability Assessment)

- Vulnerability Assessment – Dịch vụ rà quét lỗ hổng bảo mật cho Web application và Network
- Vai trò: Đánh giá điểm yếu bảo mật của hệ thống bằng việc rà quét các loại lỗ hổng đã biết, đánh giá mức độ nghiêm trọng và đưa ra gợi ý khắc phục
- Lợi ích
  - Bảo vệ hệ thống website một cách toàn diện
  - Phát hiện và khắc phục các nguy cơ an ninh trước khi cuộc tấn công diễn ra
  - Dễ dàng triển khai với mạng diện rộng và tích hợp với SIEM, SOC



b. Giải pháp Patching Management

Patching management là giải pháp quản lý bản vá bảo mật cho các hệ điều hành Windows, Linux và các ứng dụng cài đặt trên các OS đó.

Lợi ích mang lại:

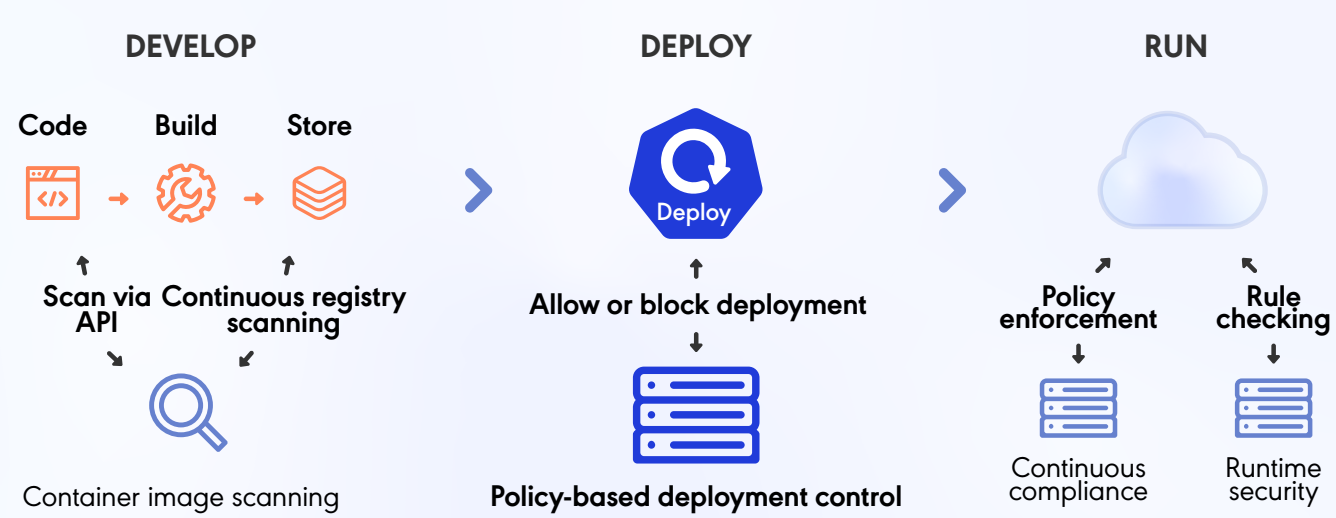
- Cung cấp các bản vá cho đa dạng hệ điều hành
- Đánh giá rủi ro bảo mật và lỗ hổng trên đa dạng các nền tảng như Windows, Linux
- Xem thông tin patch and compliance cho các thiết bị đã quét

- Đặt lịch tự động vá bao gồm cập nhật nội dung, quét thiết bị và tải về bản vá
- Tải, triển khai và cài đặt bản vá đã được nghiên cứu và kiểm thử
- Kiểm tra trạng thái của triển khai patch và cài đặt trên các thiết bị được quét

4.7. Layer VII: Container Security

Giải pháp Container Security

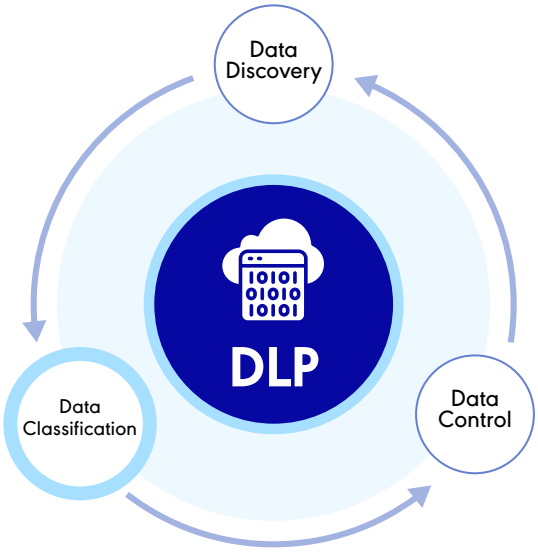
- Container security bao gồm các biện pháp bảo vệ các ứng dụng được lưu trên container và infrastructure trong suốt vòng đời
- Các tính năng:
  - Phát hiện các attack từ network
  - Phát hiện malware trên các image, container
  - Dò quét lỗ hổng trên các image, container, application
  - Tìm kiếm clear text credential và các key mã hoá
  - Bảo vệ malware theo thời gian thực
  - Ngăn chặn các tấn công đã biết và chưa biết dựa vào các signature và behavioral



4.8. Layer VIII: Data Security - Data Encryption

Giải pháp Container Security

No.	Hạng mục	Mô tả	Biện pháp sử dụng
1	Network	Các ứng dụng Web	Sử dụng giao thức HTTPS: thuật toán mã hóa TLS
2		Kết nối VPN Client to site	Mã hoá kết nối sử dụng IPSEC
3		Kết nối quản trị	Sử dụng SSH
4	SAN Storage	Mã hóa lớp SAN	Mã hóa cấp độ 2 ở mức SAN Storage: Mã hóa với thuật toán XTS-AES-256
5	Database	Mã hoá mức database	Thuật toán sử dụng AES-256, AES-128
6	Backup	Mã hóa dữ liệu backup	Thuật toán sử dụng AES-256

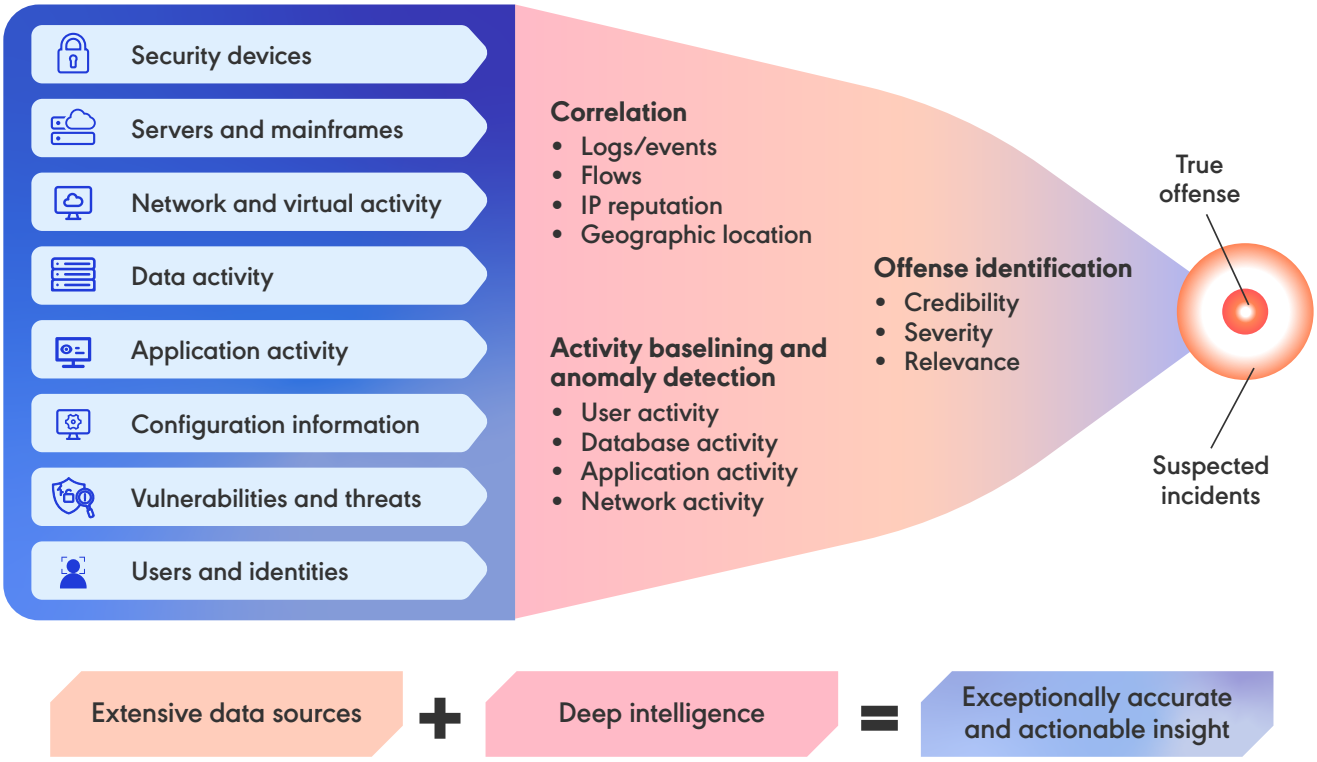


4.9. Layer IX: Giám sát, phân tích sự kiện an ninh (SOC)

Giải pháp SIEM – Security Monitoring

- SIEM (Security information and event management) là giải pháp quản lý, phân tích sự kiện an toàn thông tin và đưa ra các cảnh báo ATTT kịp thời cho người quản trị
- Các hệ thống Host, VM, Firewall, WAF, AV, Windows, Linux, App, DB... được đẩy log về hệ thống SIEM nhằm mục đích phân tích dữ liệu, phát hiện detection, phân tích, truy tìm dấu vết các sự kiện an ninh

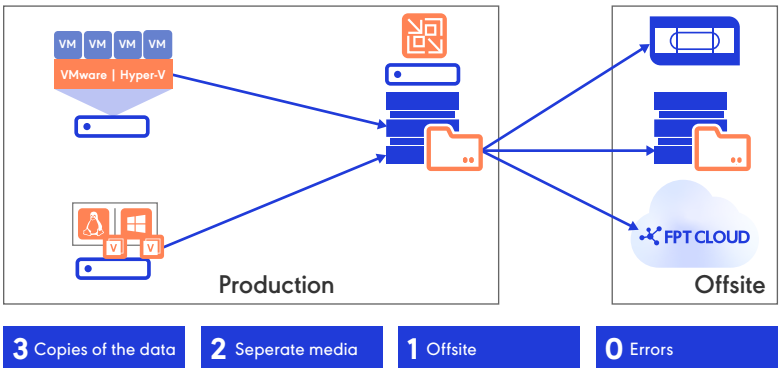
- Lợi ích mang lại:
  - Thu thập dữ liệu từ nhiều log source
  - Ghi nhật ký hoạt động quản lý
  - Liên kết tương quan sự kiện
  - Điều tra sự kiện
  - Giám sát và ứng phó với sự cố



- SOC team thực hiện việc giám sát & phân tích sự kiện an toàn thông thông tin:
  - SOC L1: Giám sát các alert trên hệ thống SIEM, tạo các ticket hoặc gọi điện khi phát hiện sự cố tấn công: DDoS, malware behavior...
  - SOC L2: Phân tích các sự kiện security L1 chuyển lên, xác định các cảnh báo false positive, điều tra nguyên nhân, đưa ra biện pháp xử lý. Nếu đúng cảnh báo positive thực hiện thông báo đến các owner thuộc các đơn vị liên quan... trực tiếp xử lý

4.10. Layer X: Backup & DR

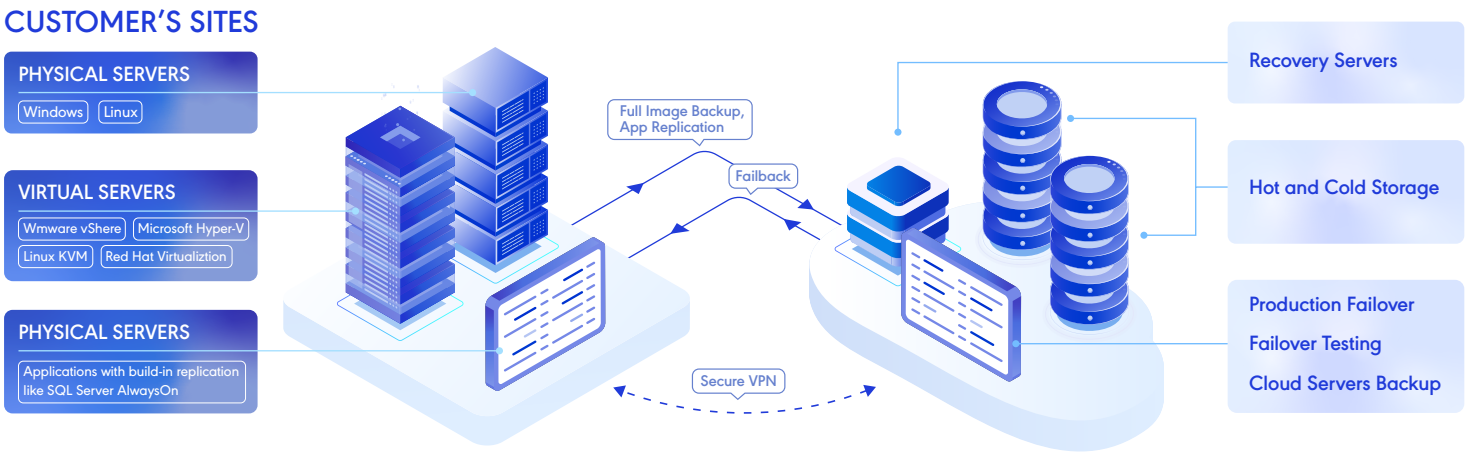
- Sao lưu đa nguồn dữ liệu: Hỗ trợ sao lưu từ đa nguồn: máy chủ vật lý, máy chủ ảo, thư mục tệp tin...
- Sao lưu đa nền tảng: Hỗ trợ sao lưu từ hạ tầng on-premise, hạ tầng tính toán Cloud, hoặc giữa các zone trong FPT Cloud
- Hỗ trợ đa hệ điều hành: Tương thích với các hệ điều hành phổ biến (Windows, Linux, MacOS)
- Quy tắc sao lưu dữ liệu 3-2-1



Giải pháp khôi phục dữ liệu sau thảm họa giúp hệ thống của khách hàng luôn được đảm bảo sẵn sàng vận hành khi có bất kỳ sự cố nào ngoài mong muốn xảy ra.

- Di chuyển từ On-Premise lên vCloud
- Di chuyển từ vCloud tới On-Premise
- Failover On-Premise to vCloud
- Failover vCloud to On-Premise
- DR vCloud to another vCloud site
- DR to another region

- Đặc điểm:
  - Khởi tạo: Khởi tạo dịch vụ đơn giản bằng cách sao chép các máy ảo cần bảo vệ lên trên nền tảng điện toán đám mây thông qua cổng quản trị tập trung
  - Phân tích, báo cáo: Tính năng tự động tính toán giá trị RPO và hiển thị đồ hoạ các thông tin liên quan lên băng thông mạng sao chép dữ liệu, tổng dung lượng đã được nhân bản trên Cloud
  - Cho phép giả lập tình huống: Tính năng thử nghiệm giả lập tình huống thảm hoạ cho khách hàng mà không làm ảnh hưởng đến hệ thống thực nhằm diễn tập các tình huống sẵn sàng cho người quản trị và tính toán các thông số RTO cho hệ thống DR



FPT CLOUD
by FPT Smart Cloud

III. Giải pháp
Bảo mật an toàn thông tin toàn diện cho Doanh nghiệp

1. Hệ sinh thái dịch vụ FPT Cloud

Platform Services

Container Services
- Dedicated K8S
- Managed K8S
- K8S with GPU
- Container Registry
- App Catalog

DevOps
- CI/CD Pipeline

Monitoring
- Platform Monitoring (K8S,DB,...)
- Infrastructure Monitoring
- Distributed Tracing
- Log Management
- Incident Management
- Reporting

Integration Services
- API Management
- CMS
- FPT Message Bus
- Kafka as a Service

Database Services
- Database Engine for MySQL
- Database Engine for Redis
- Database Engine for MariaDB
- Data Integration (Kafka)
- Database Engine for PostgreSQL
- Database Engine for MongoDB
- Database Engine for MS SQL
- Open Search

AI Services
- FPT AI Chat
- FPT AI Read
- FPT AI Enhance
- FPT AI Engage
- FPT AI Mentor
- FPT AI eKYC
- FPT AI Car Damage
- Speech synthesis
- Speech Recognition
- Liveness Detection
- FaceMatch
- Identification Paper extraction
- Sentiment Detection

Security & Management
- Cloud WAF
- Cloud VA
- Next-Gen Firewall
- Cloud Guard
- Compliance service
- Endpoint security
- Anti DDoS
- Key Vault
- IAM

Infrastructure Services

Compute
- Cloud Server
- GPU Server
- Cloud Backup & DR
- Cloud Desktop

Storage
- FPT Object Storage
- File Storage
- Cloud Drive
- Unified Object Storage

Networking
- FPT Load Balancer
- VPN Service
- VPC Peering
- IPv6 Support

Datacenter Infrastucture

2. FPT Cloud – Cyber Security Services

2.1. Security Group

- Cho phép nhóm các server vào các group, thiết lập rule allow in/out
- Tường lửa Layer 4
- Cho phép apply network policy rule đến từng server

2.2. FPT Cloud Web Application Firewall

- Made by FPT
- OWASP standard
- Hỗ trợ SSL
- Virtual patching
- Anti BotNet

2.3. Endpoint Security

- Checkpoint Harmony
- McAfee (Trellix)

2.4. Firewall 3rd Partner

- Checkpoint
- Fortinet
- Hỗ trợ hầu hết các dạng virtual appliance
- Hỗ trợ model license khách hàng tự mua

2.5. Web Application Firewall (3rd)

- Checkpoint Appsec
- Fortinet WAF
- Hỗ trợ model Subscription
- Hỗ trợ hầu hết các dạng virtual appliance

2.6. Anti-DDos

- On-Demand
- Akamai
- CloudFlare

2.7. Vunerability Assessment (VA)

- Quét lỗ hổng ứng dụng
- Quét đường truyền
- Đánh giá cấu hình VPC
- Quét thủ công/tự động theo lịch
- Thông báo tự động

2.8. Content Delivery Network (CDN)

- Akamai
- CloudFlare

2.9. Threat Detection: FPT Cloud Guard

- Giám sát tài nguyên
- Activity Log
- DDoS Attack Detection
- Internet Attack Detection
- Scanned Attack Detection
- Malware Infected Detection

FPT Cloud – Đồng hành cùng doanh nghiệp chuyển đổi số an toàn và bền vững

- Bảo mật đa lớp trên toàn mô hình hệ thống
- Tích hợp các giải pháp công nghệ bảo mật hàng đầu từ: Checkpoint, Imperva...
- Bảo mật An ninh mạng, đa dạng tùy chọn sao lưu
- Đánh giá hệ thống định kỳ và báo cáo rủi ro cho khách hàng
- Tích hợp Trí tuệ nhân tạo và hệ thống cảnh báo tự động đa kênh với robot ảo 24/7
- Đội ngũ chuyên gia tư vấn hàng đầu, kỹ sư giám sát và hỗ trợ 24/7/365

Tiêu chuẩn cao nhất về an toàn thông tin ở tầng Dịch vụ

TÜV NORD ISO/IEC 27017 · TÜV NORD ISO/IEC 27018 · TÜV NORD ISO/IEC 27001 · AICPA SOC · PCI DSS COMPLIANT · ISO 9001:2015 BUREAU VERITAS Certification · UKAS MANAGEMENT SYSTEMS 0008

Tiêu chuẩn tầng Data Center

ANSI/TIA-942-2017 FACILITIES RATED 3 TIA-942 · PCI DSS CERTIFIED · TIER III FACILITY UPTIME INSTITUTE CERTIFIED · ISO 27017:2015 · ISO 9001:2015 · ISO 27001:2013

Liên hệ chúng tôi

Hà Nội: FPT Tower, 10 Phạm Văn Bạch, Dịch Vọng, Cầu Giấy

TP. Hồ Chí Minh: PJICO Tower, 186 Điện Biên Phủ, Phường 6, Quận 3

fptcloud.com

support@fptcloud.com

1900 638 399