

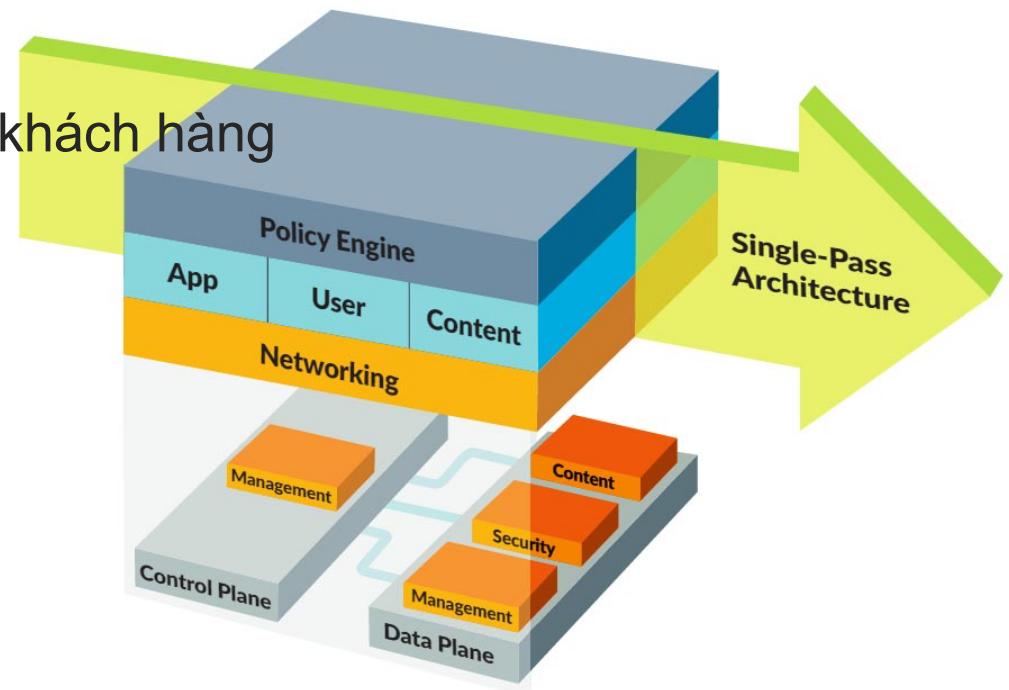
Next-Generation Security Platform

Hiep Nguyen
CCIE, CISSP
Security Solution Consultant

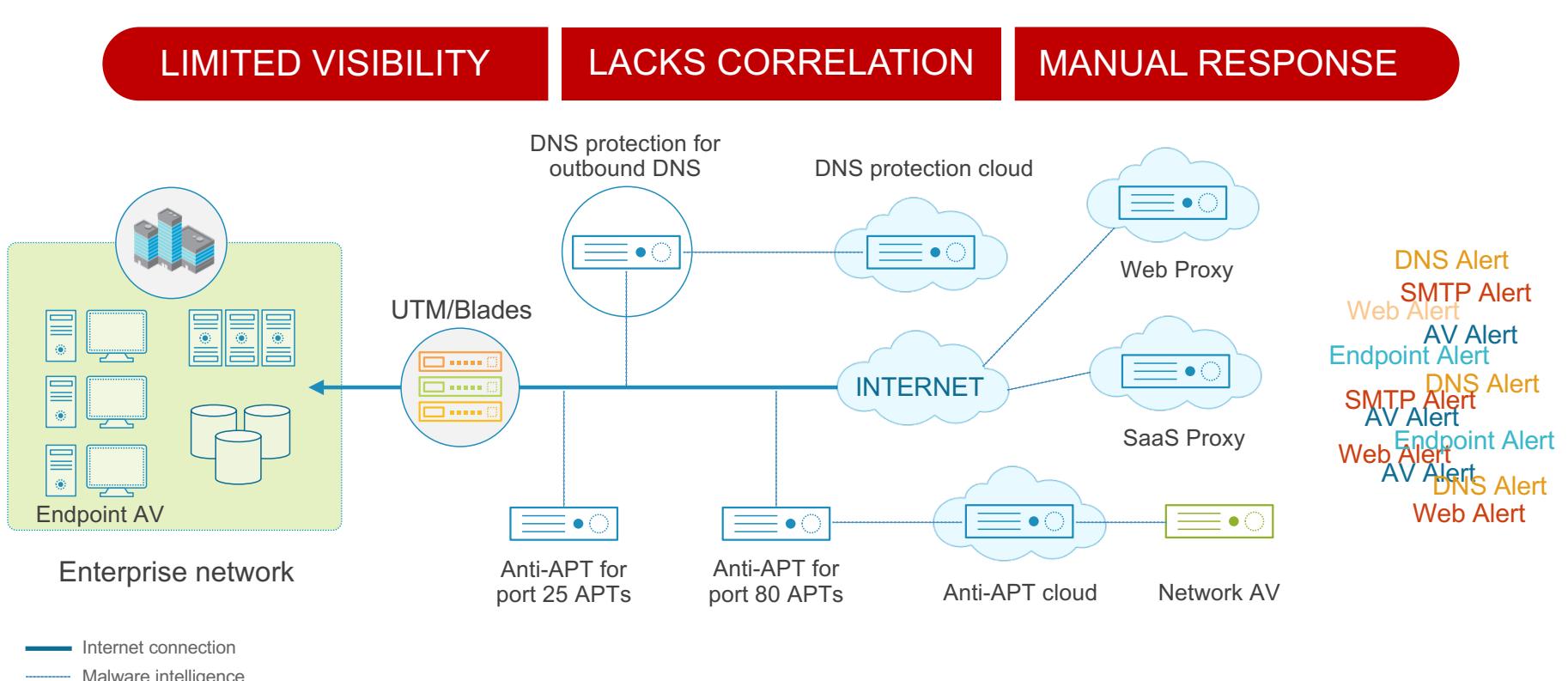


Nội dung

1. Cách tiếp cận về ANTT của Palo Alto Networks
2. Tính năng mới của PAN-OS 8.0
3. Các dịch vụ Palo Alto Networks hỗ trợ khách hàng
4. Q&A



Failure of the legacy “defense in depth” approach



CẦN MỘT CÁCH TIẾP CẬN MỚI VÀ THỰC TẾ HƠN

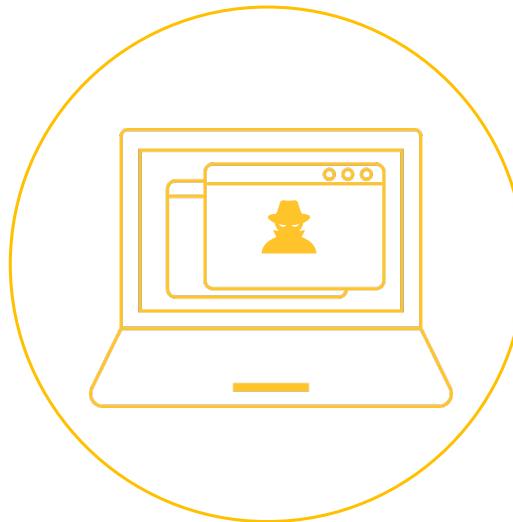


DETECTION VÀ REMEDIATION LÀ KHÔNG ĐỦ

Yêu cầu 1: có thể sử dụng dịch vụ trên mạng một cách an toàn



Người dùng

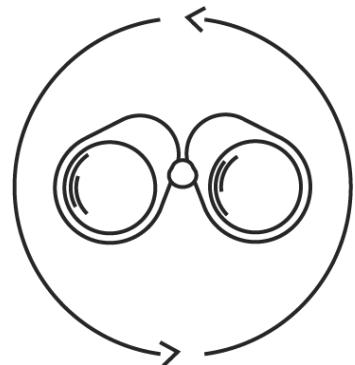


Ứng dụng

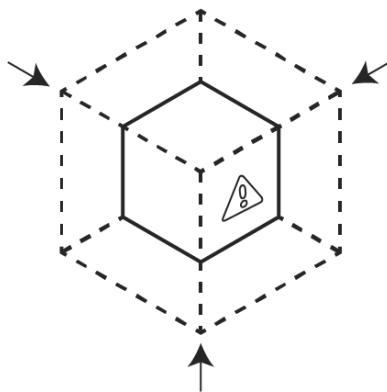


Nội dung

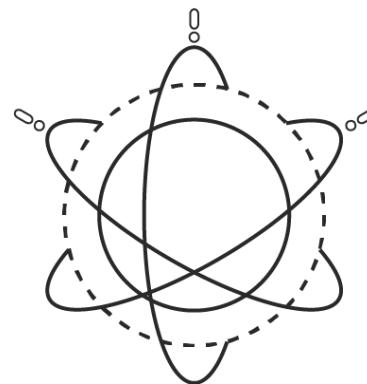
Yêu cầu 2: Tập trung ngăn chặn các hiểm họa



Tường
minh



Giảm thiểu
nguy cơ



Ngăn chặn
hiểm họ
đã biết



Ngăn chặn
hiểm họ
chưa biết

Các chức năng ngăn chặn cần có

TƯỜNG MINH

- Giám sát và kiểm soát được toàn bộ ứng dụng, người dùng, nội dung
- Dữ liệu mã hoá
- Định danh, tài khoản người dùng

GIẢM THIỂU NGUY CƠ

- Cho phép sử dụng app cho công việc
- Chặn các app không hợp lệ
- Giới hạn chức năng
- Giới hạn loại file sử dụng
- Chặn website

NGĂN CHẶN HIỂM HỌA ĐÃ BIẾT

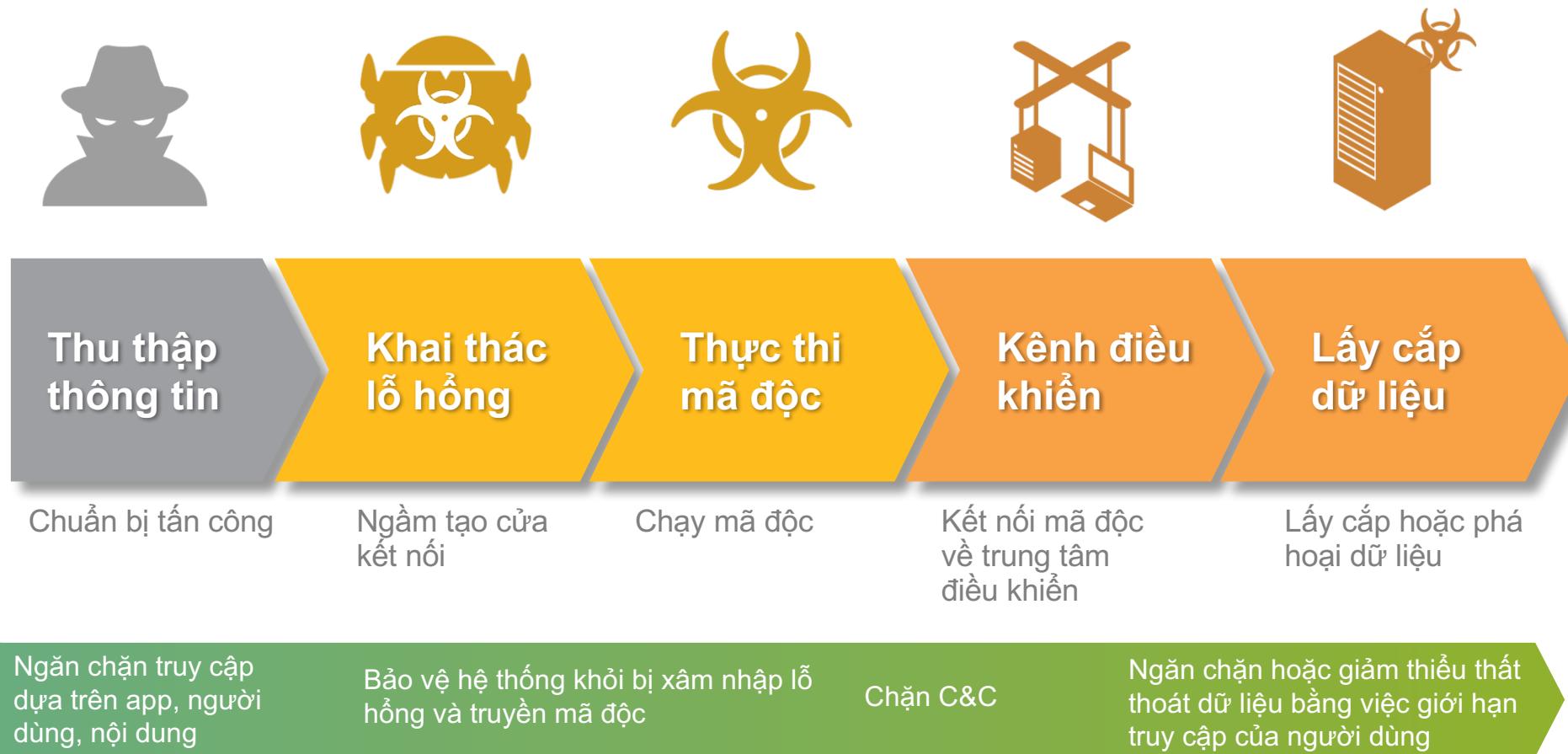
- Malware
- Exploits
- Command & control
- Trang web xấu
- Domain xấu
- Lấy cắp tài khoản

NGĂN CHẶN HIỂM HỌA CHƯA BIẾT

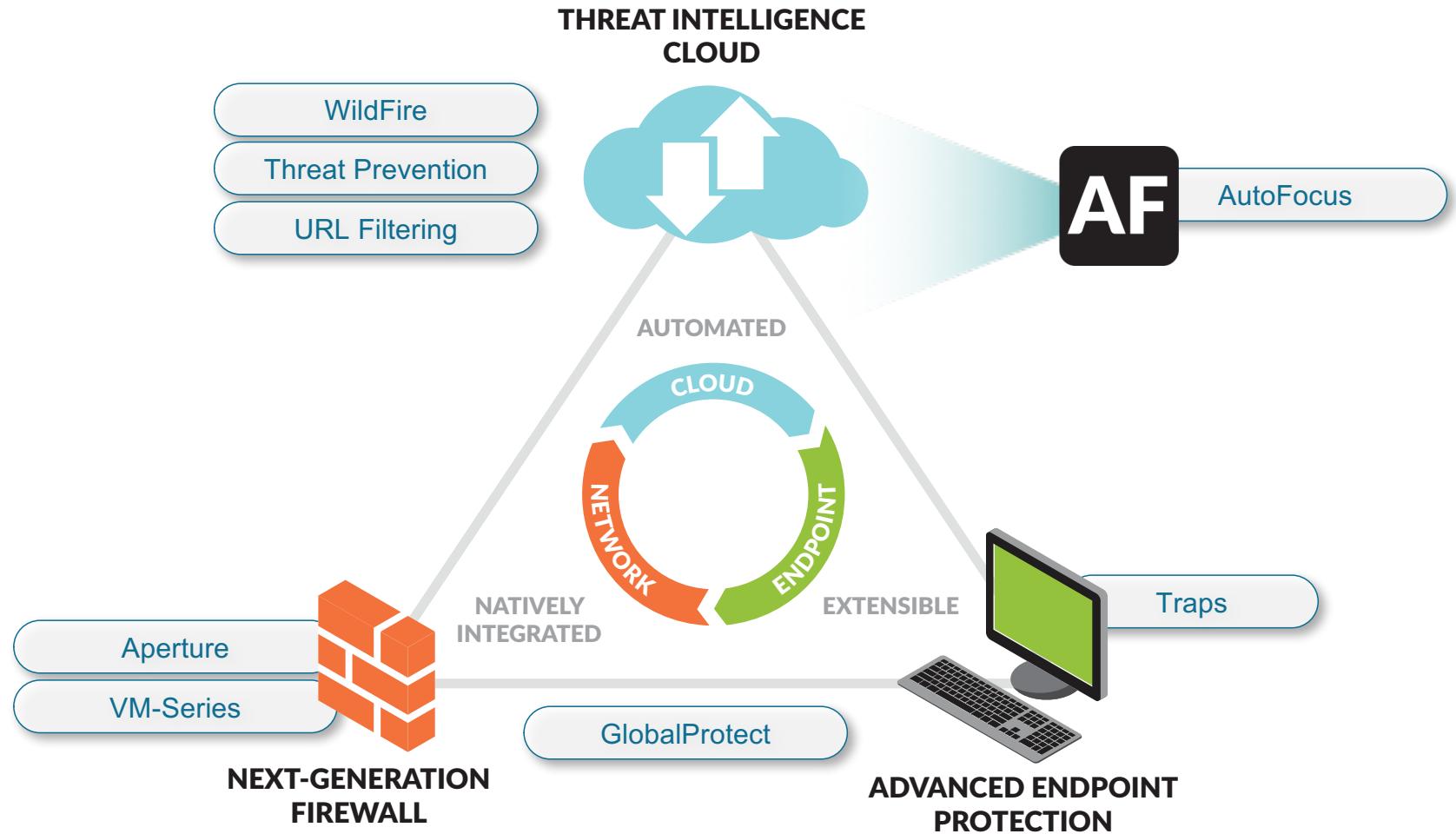
- Phân tích động
- Phân tích tĩnh
- Machine learning
- Tập trung vào kỹ thuật tấn công
- Phân tích hành vi bất thường

Network | Endpoint | Cloud

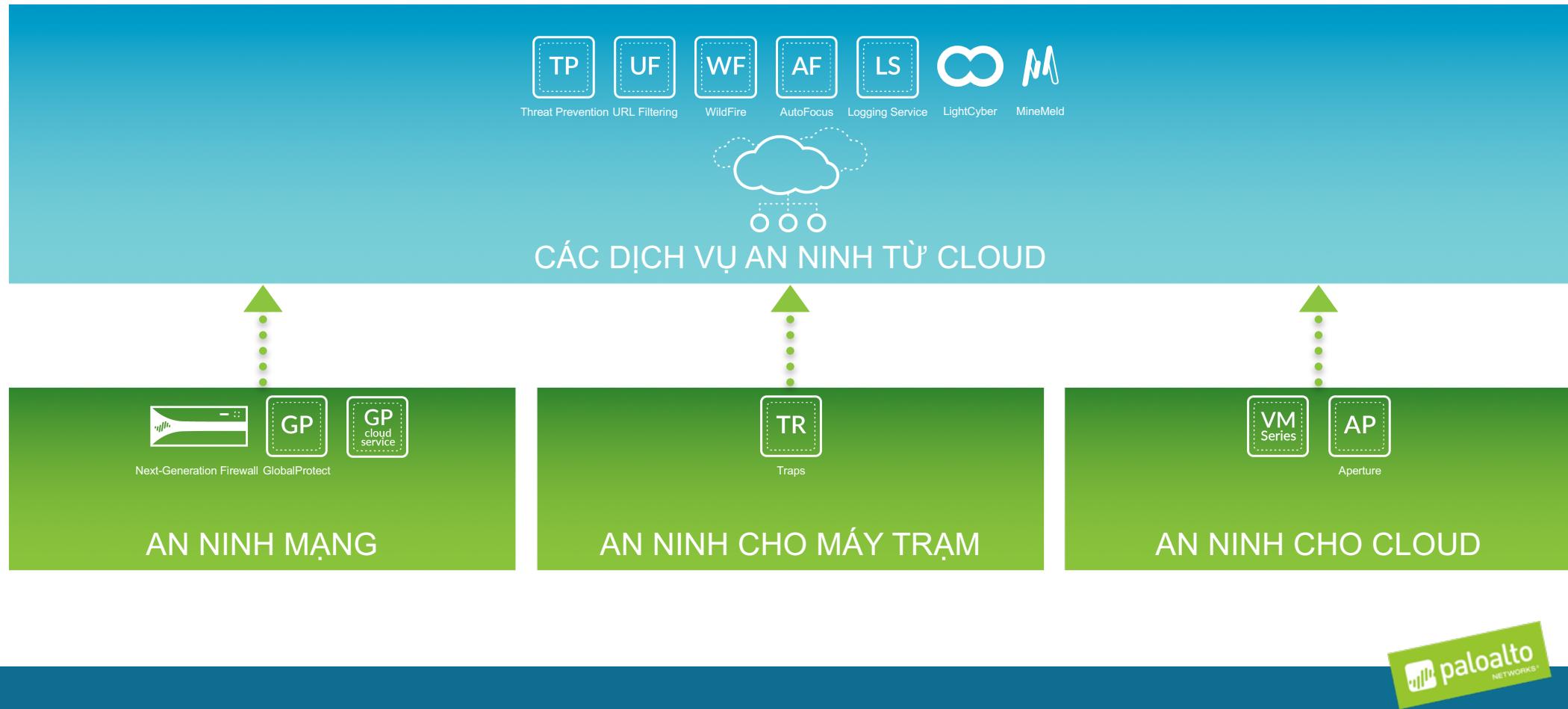
Và cần phải ngăn chặn ở mọi khâu của cuộc tấn công



Nền tảng bảo mật gồm 3 thành phần



Các dịch vụ trên nền tảng Palo Alto Networks



Tự động

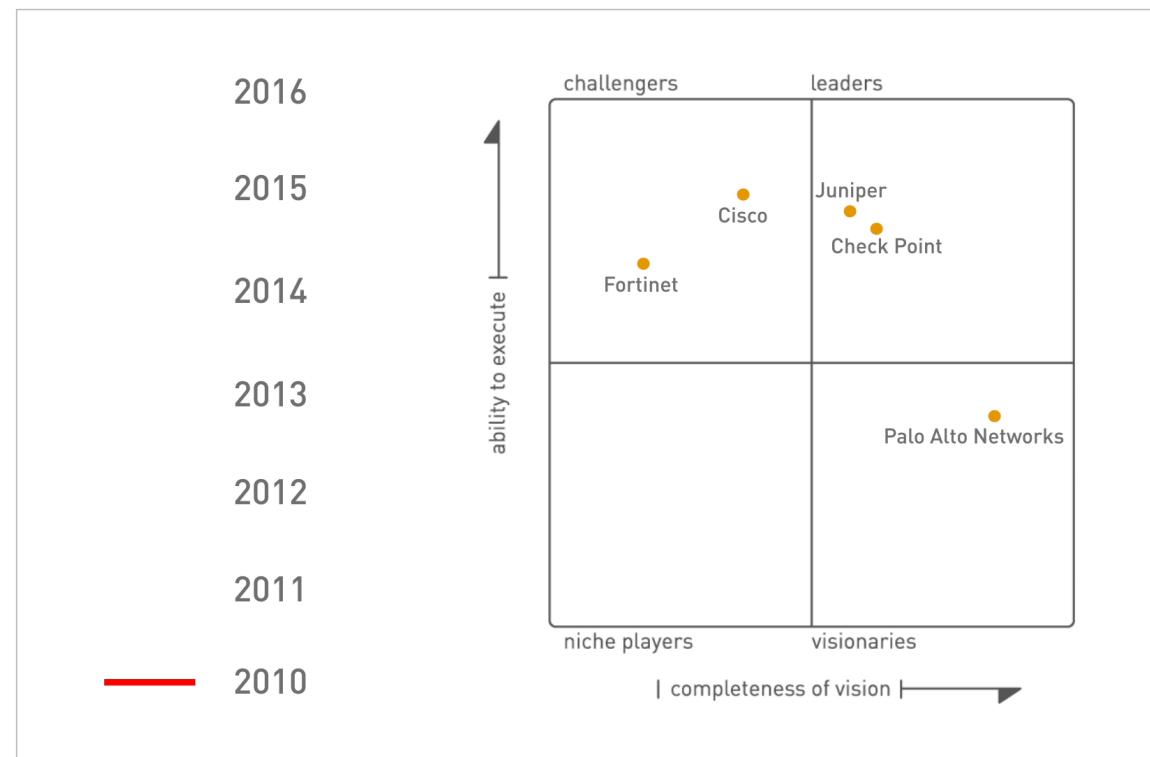
Prevention – Ngăn chặn

Dịch vụ từ cloud



07 năm ở nhóm Leaders của Gartner Enterprise Firewalls

- Palo Alto Networks is positioned as a leader in the Gartner Magic Quadrant for enterprise network firewalls*
- Palo Alto Networks is highest in execution and most visionary within the leaders quadrant



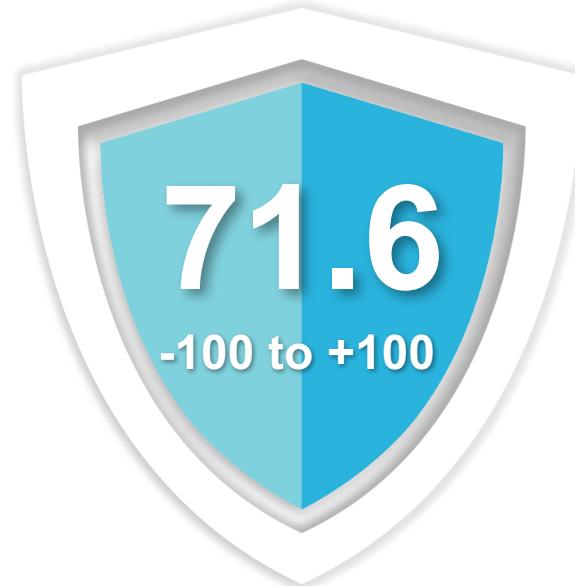
*Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Greg Young, Jeremy D'Hoinne, and Rajpreet Kaur, May 2016

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Tập trung cho sự Hiệu quả và Hài lòng của khách hàng



Độ hài lòng

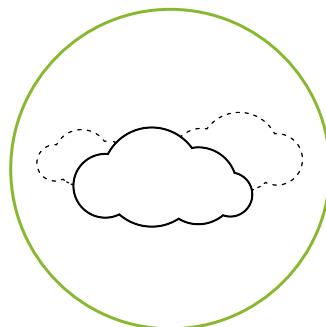


Tỷ lệ giới thiệu
tiếp sản phẩm

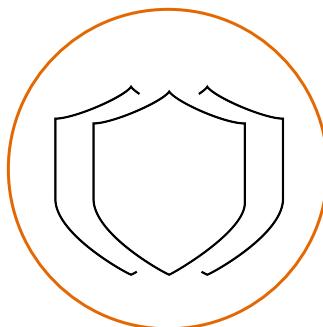
<PAN-OS 8.0>



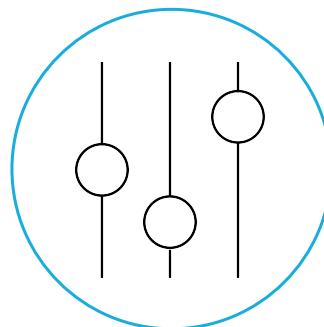
Các tính năng mới của phiên bản 8.0



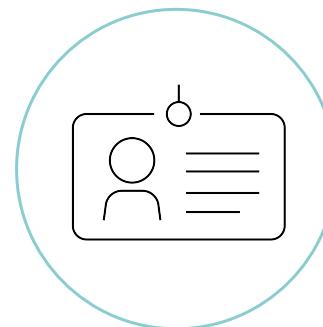
BẢO MẬT NỀN TẢNG
CLOUD



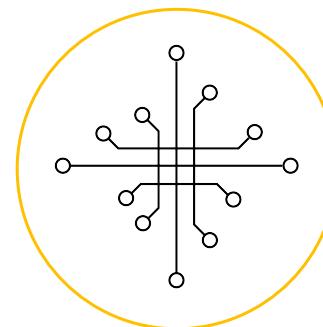
NGĂN CHẶN BẰNG
NHIỀU KỸ THUẬT
HƠN



TỐI ƯU QUẢN TRỊ

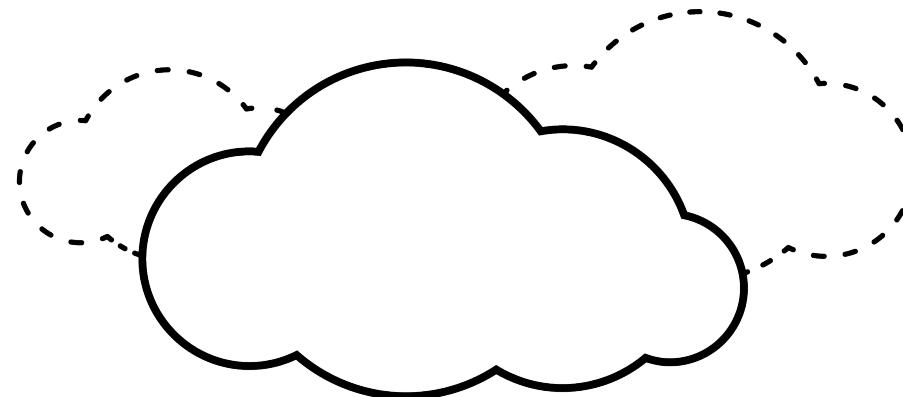


CHỐNG LẤY CẮP TÀI
KHOẢN

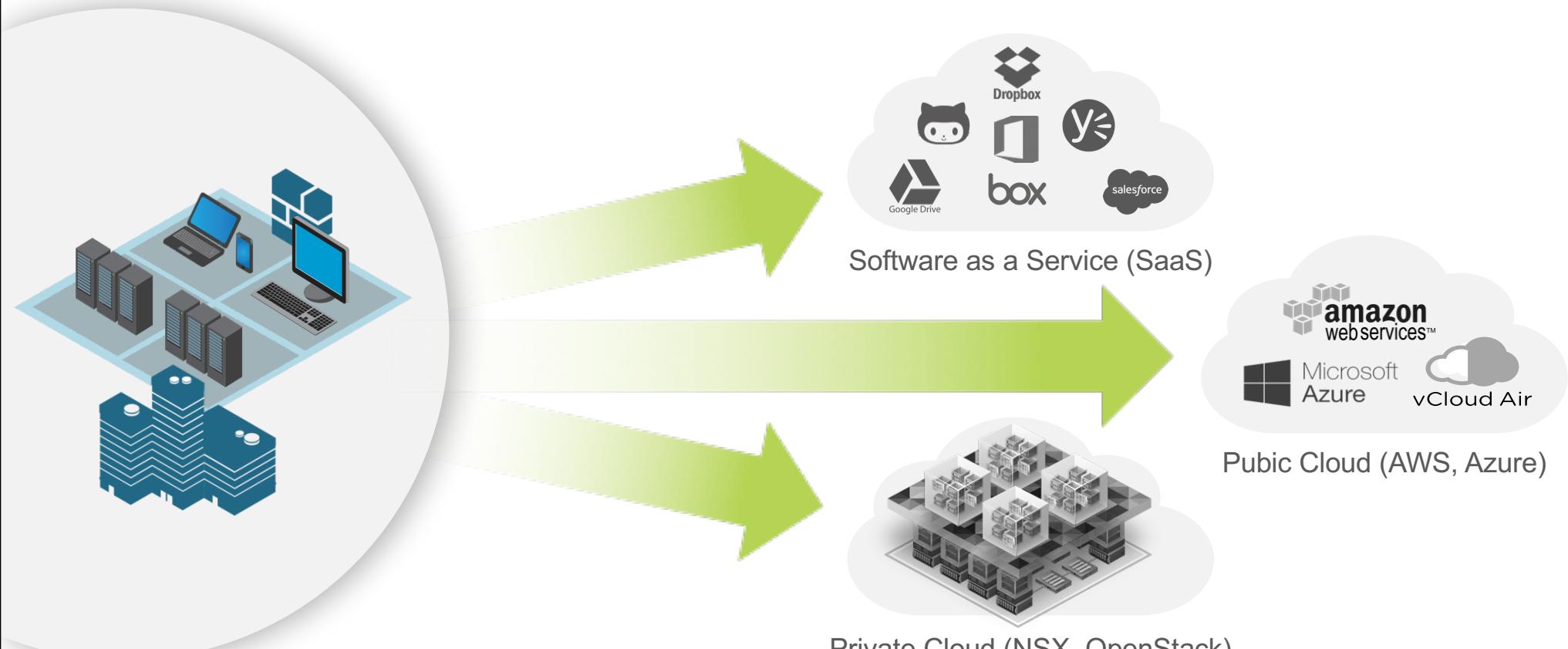


PHẦN CỨNG MỚI
MÃ HOÁ MẠNH

BẢO MẬT CLOUD

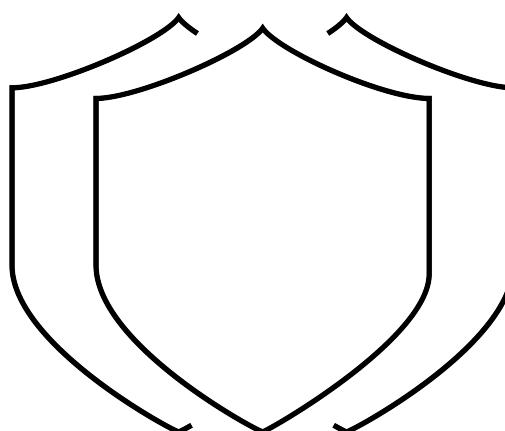


Mở rộng tính năng bảo mật trên SaaS, IaaS, PaaS, Private cloud

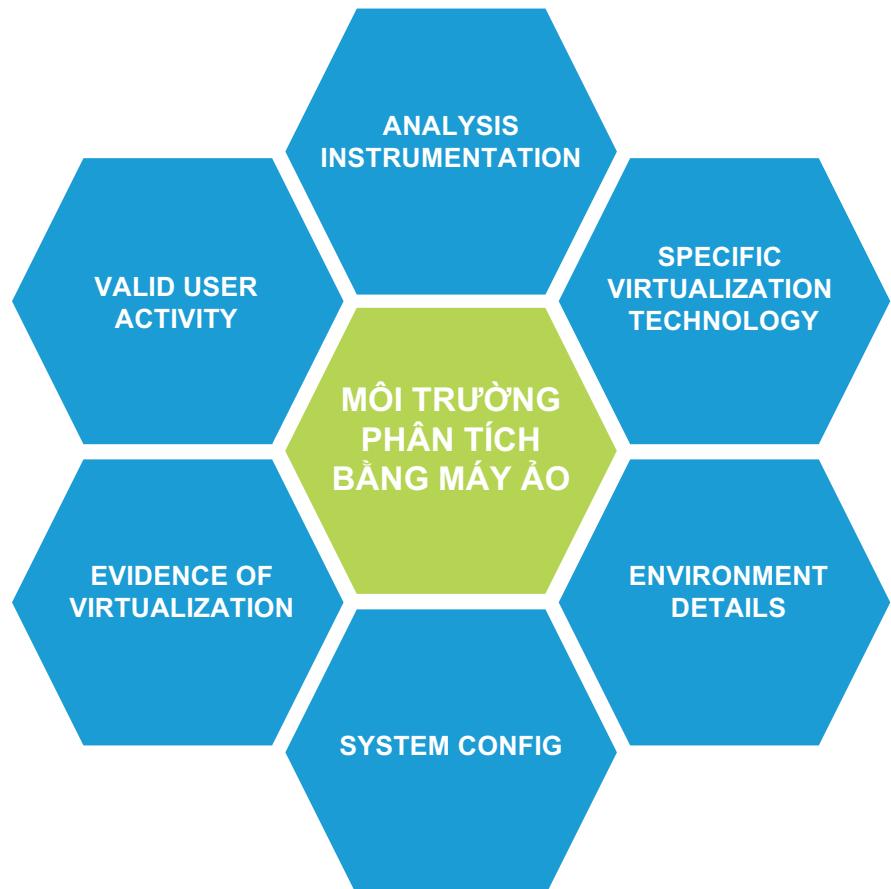


NGĂN CHẶN BẰNG NHIỀU KỸ THUẬT HƠN NỮA

Các công nghệ mới của Threat Intelligence



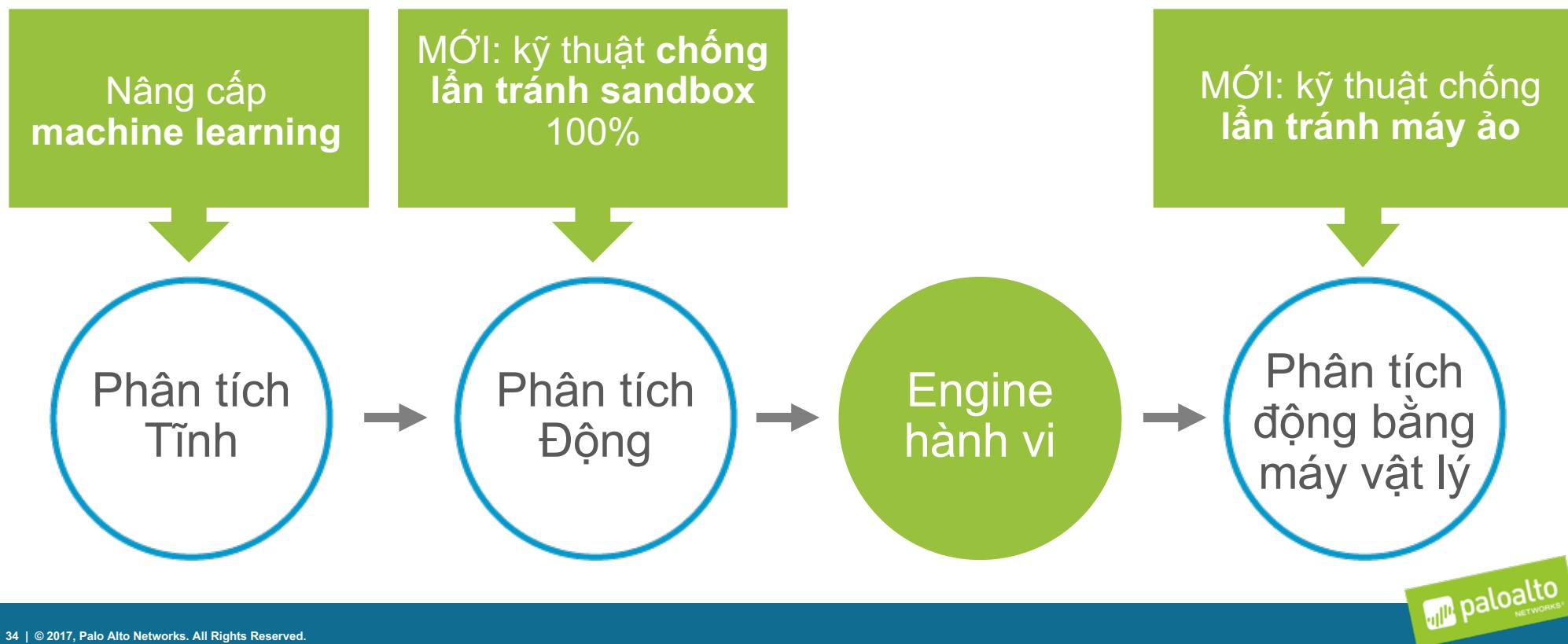
Giải pháp phân tích động bằng Máy ảo đã không còn hiệu quả



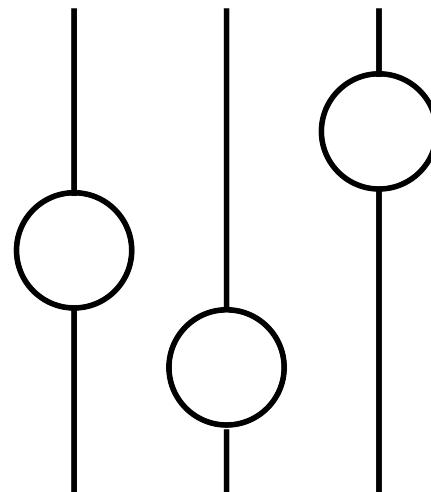
Hầu hết Malware kỹ thuật cao hiện nay đều đã tích hợp các công nghệ phát hiện sandbox ảo

Tất cả các hãng bảo mật, bao gồm cả Palo Alto Networks đều sử dụng chung kỹ thuật sandbox ảo opensource

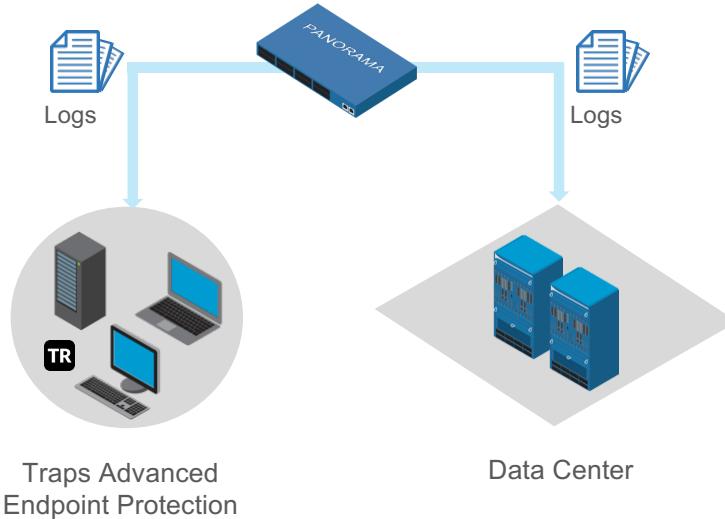
Công nghệ phân tích động mới của PAN 8.0



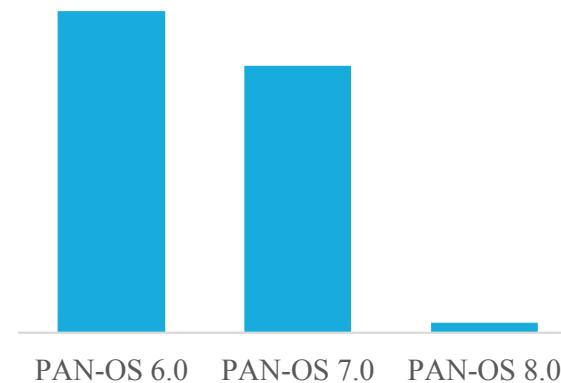
TỐI ƯU QUẢN TRỊ



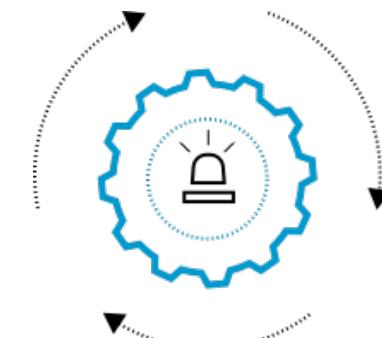
Các cải tiến chính trong tính năng quản trị của PAN OS 8.0



Thu thập dữ liệu từ
nhiều nguồn

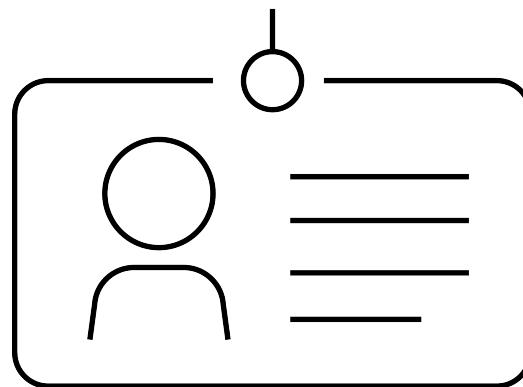


Cải tiến tốc độ
truy vấn log

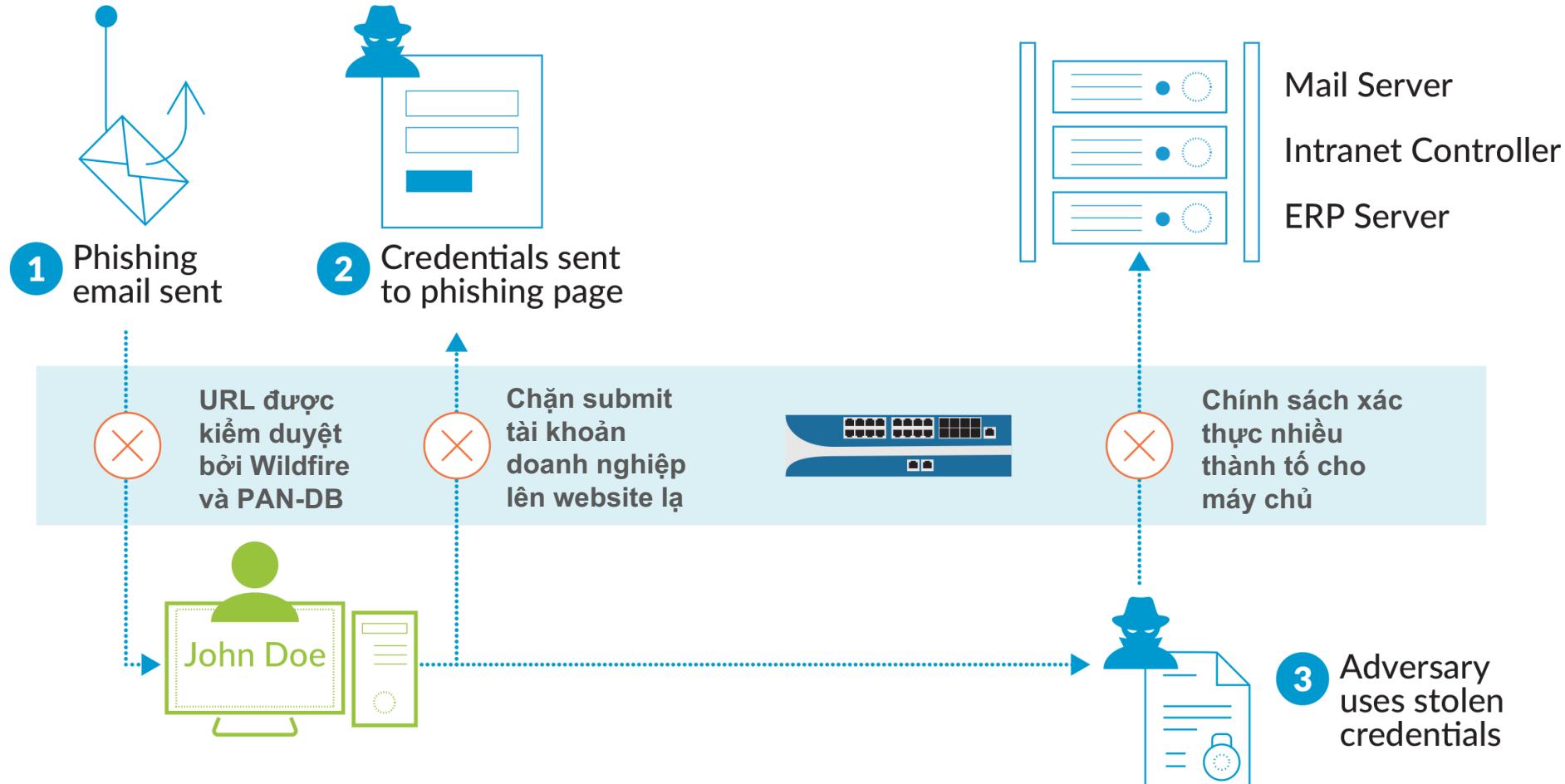


Tự động
thực thi tác vụ

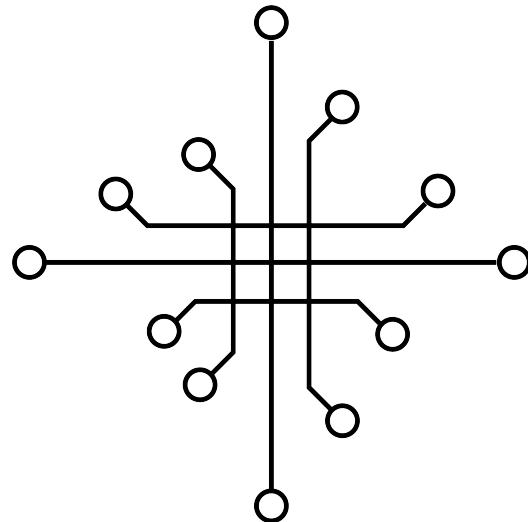
CHỐNG LẤY CẮP TÀI KHOẢN



Giải pháp chống lấy cắp tài khoản nhiều lớp



CÁC PHIÊN BẢN PHẦN CỨNG MỚI



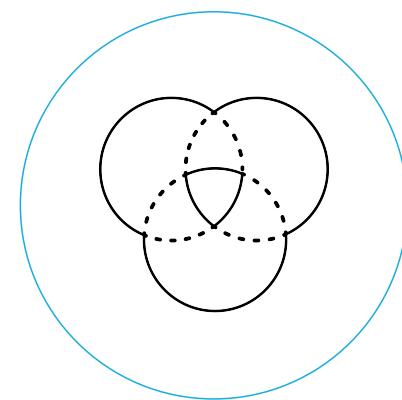
Phần cứng mới dành cho các tính năng



Trung tâm dữ liệu



Dữ liệu mã hóa



Hybrid Cloud và SaaS

Phần cứng mới

PA-800 SERIES



PA-5200 SERIES



PA-220



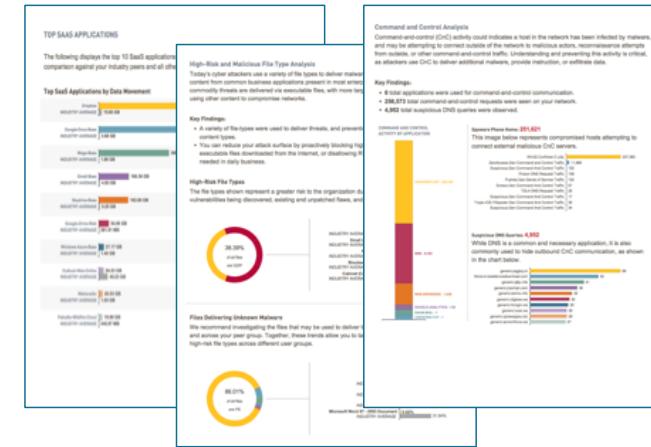
- ✓ Up to 10x performance and capacity increases
- ✓ Front-to-back cooling
- ✓ Higher port density, flexible I/O, & hardware resiliency
- ✓ Up to 10x decryption performance increase
- ✓ Up to 35x SSL session capacity increase

Các dịch vụ Palo Alto Networks hỗ trợ khách hàng



Dịch vụ đánh giá rủi ro của các ứng dụng trên mạng khách hàng

- Đánh giá rủi ro các ứng dụng đang chạy thực tế trên mạng
- Đánh giá ứng dụng, người dùng, lưu lượng, hiểm họa, lỗ hổng, mã độc
- Đặt lịch với đại diện của Palo Alto Networks ngay hôm nay



CHÚNG TÔI SẼ ĐẶT THIẾT BỊ
TRÊN MẠNG KHÁCH HÀNG

CHÚNG TÔI LẮNG NGHE DỮ
LIỆU TRONG 1 TUẦN

CHÚNG TÔI LẬP BÁO CÁO
VÀ TRÌNH BÀY CHO ĐỘI VẬN
HÀNH BẢO MẬT

Dịch vụ đào tạo lab trong 4 ngày

Trải nghiệm hands-on với các kịch bản khác nhau để chống tấn công và quản lý an ninh mạng trên nền tảng của Palo Alto Networks

- Trên 20,000 người tham gia năm FY17
- Có 4-6 nội dung lab
- Đăng ký online:
www.paloaltonetworks.com/events/test-drive.html
- Hoặc liên hệ kỹ sư của Palo Alto Networks tại khu vực muốn tham gia



Palo Alto Networks

Thành lập năm **2005**; sản phẩm đầu tiên bán trên thị trường **2007**

Có hơn **39,500** khách hàng in **150+ quốc gia**

49% YoY tăng trưởng với số lượng khách hàng tăng nhanh

Trên **85** trong số Fortune 100 và **60%** trong số Global 2000 sử dụng

Được các giải thưởng về hỗ trợ sau bán hàng của **J.D. Power** và **TSIA**

Đội ngũ **4,500** nhân sự