

Hệ thống phát hiện, tìm kiếm và phát  
hiện xâm nhập – NT204.P21.ANTT

Nhóm 11

# TREND MICRO APEX ONE

GV: Đỗ Hoàng Hiển – Đỗ Thị Phương Uyên



# THÀNH VIÊN NHÓM

Nguyễn Khánh Linh – 22520769

Phạm Thị Cẩm Tiên – 22521473

Nguyễn Phúc Nhi – 22521041

Võ Hoàng Huy – 19521639



# NỘI DUNG

01.

KHÁI NIỆM  
CƠ BẢN

02.

MÔ HÌNH  
MẠNG

03.

CẤU HÌNH  
VÀ CÀI ĐẶT

04.

TRIỂN KHAI

05.

TỔNG KẾT



01.

# KHÁI NIỆM CƠ BẢN



# KHÁI NIỆM CƠ BẢN

- Trend Micro Apex One là một nền tảng an ninh mạng toàn diện, cung cấp khả năng bảo vệ điểm cuối tại chỗ (on-premise) và trên nền tảng đám mây (based-cloud).
- Việc sử dụng Apex One là cần thiết vì nó cung cấp giải pháp bảo mật endpoint toàn diện với nhiều tính năng nâng cao.



# KHÁI NIỆM CƠ BẢN

## Một số tính năng nổi bật của Trend Micro Apex One

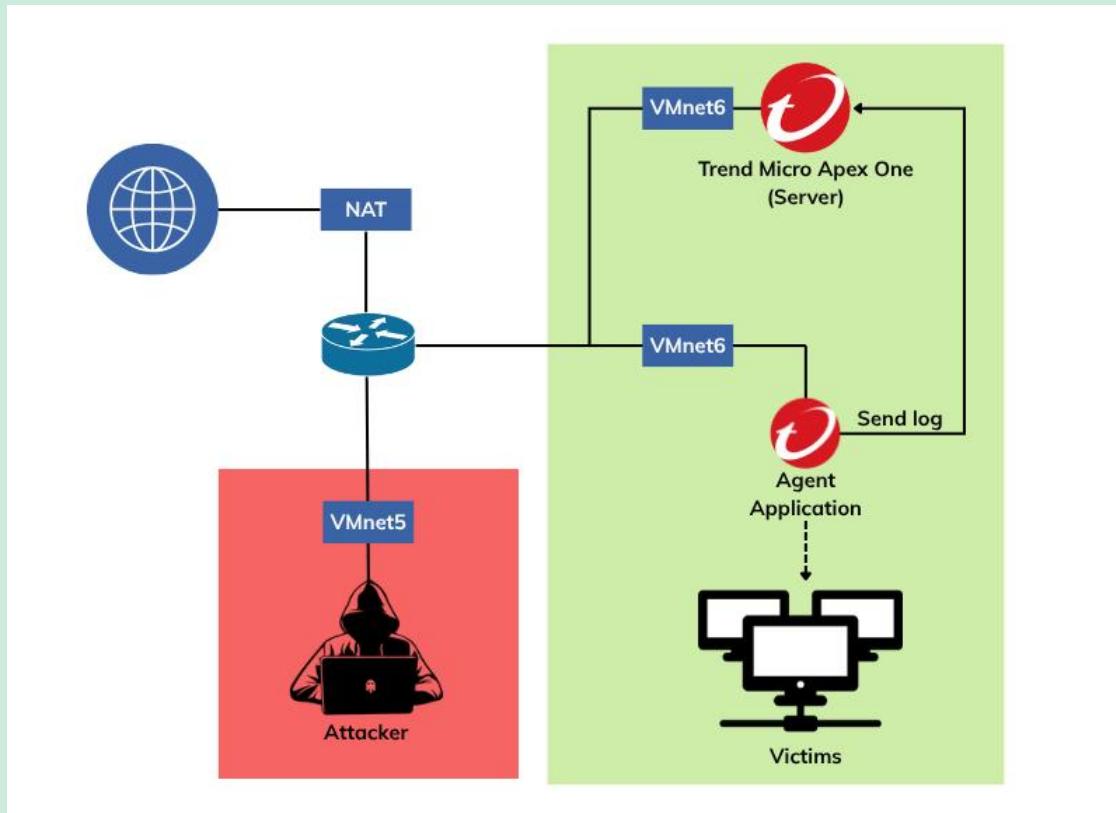
- Bảo vệ chống lại phần mềm độc hại
- Chống khai thác lỗ hổng
- Phát hiện và phản hồi điểm cuối
- Kiểm soát hành vi
- Tích hợp bảo vệ Email và web
- Tự động hóa phản hồi và tích hợp với SIEM/XDR
- Quản lý và báo cáo tập trung



# 02. MÔ HÌNH MẠNG



# MÔ HÌNH MẠNG



03.

# CẤU HÌNH VÀ CÀI ĐẶT



# CẤU HÌNH VÀ CÀI ĐẶT

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.10.0
VMnet2	Host-only	-	Connected	Enabled	10.81.73.0
VMnet3	Host-only	-	Connected	Enabled	192.168.73.0
VMnet4	Host-only	-	Connected	Enabled	192.168.40.0
VMnet5	Host-only	-	Connected	Enabled	10.81.69.0
VMnet6	Host-only	-	Connected	Enabled	192.168.69.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.64.0



# CẤU HÌNH VÀ CÀI ĐẶT

## Cấu hình cho Router

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file D:\ubuntu-24.04.2...
Network Adapter	Custom (VMnet8)
Network Adapter 2	Custom (VMnet5)
Network Adapter 3	Custom (VMnet6)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine:  MB

128 GB  
64 GB  
32 GB  
16 GB  
8 GB  
4 GB

■ Maximum recommended memory  
(Memory swapping may occur beyond this size.)

# CẤU HÌNH VÀ CÀI ĐẶT

```
GNU nano 7.2                                     /etc/netplan/50-cloud-init.yaml *
```

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: true
    ens37:
      dhcp4: no
      addresses: [10.81.69.1/24]
      nameservers:
        addresses: [10.81.69.1, 8.8.8.8]
    ens38:
      dhcp4: no
      addresses: [192.168.69.1/24]
      nameservers:
        addresses: [192.168.69.1, 8.8.8.8]
```

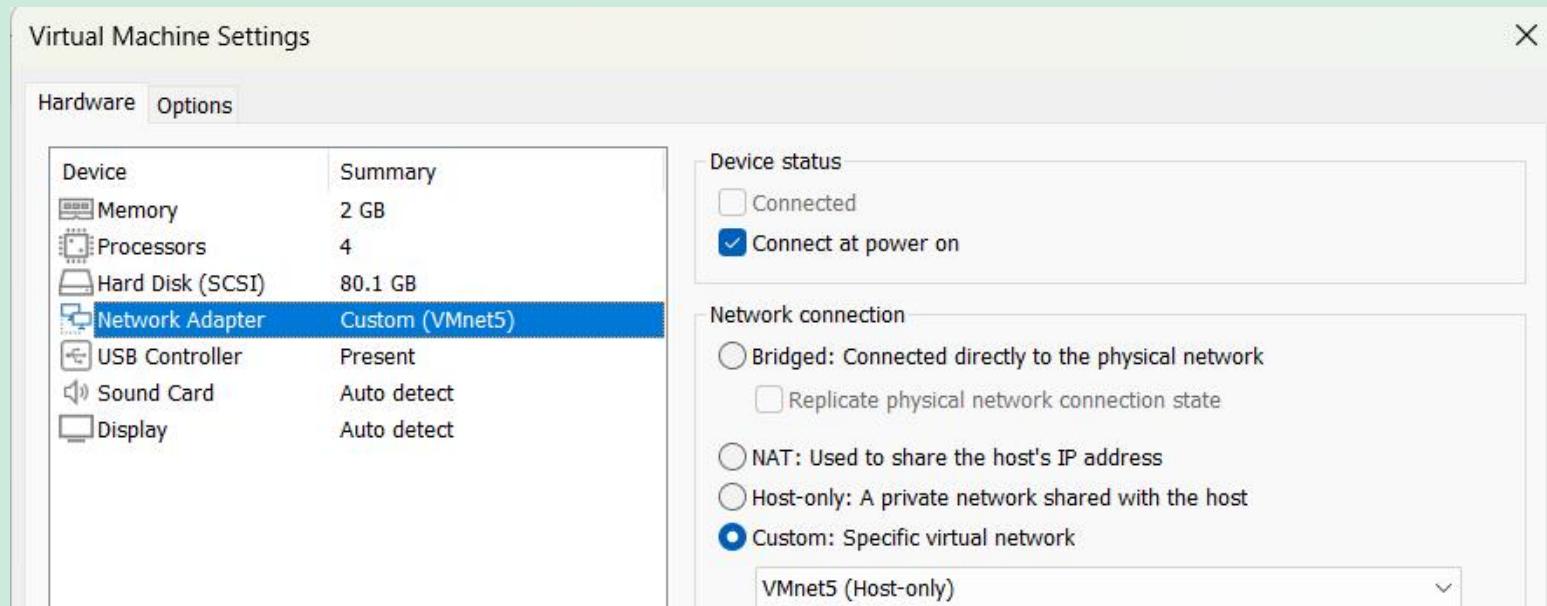


# CẤU HÌNH VÀ CÀI ĐẶT

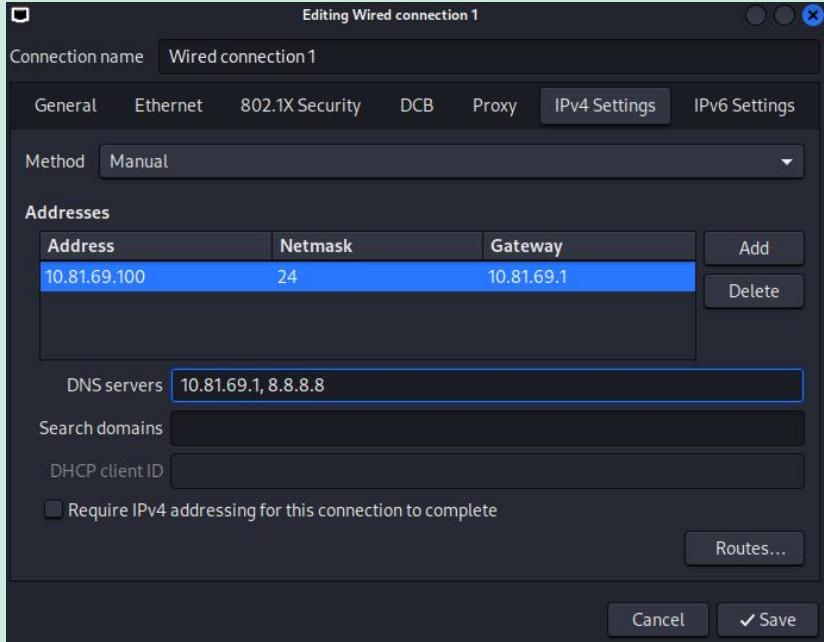
```
victim@victim:~$ sudo netplan apply
victim@victim:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d0:d2:e3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.64.145/24 metric 100 brd 192.168.64.255 scope global dynamic ens33
        valid_lft 1784sec preferred_lft 1784sec
        inet6 fe80::20c:29ff:fed0:d2e3/64 scope link
            valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d0:d2:f7 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.81.69.1/24 brd 10.81.69.255 scope global ens37
        valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:fed0:d2f7/64 scope link
            valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d0:d2:ed brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet 192.168.69.1/24 brd 192.168.69.255 scope global ens38
        valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:fed0:d2ed/64 scope link
            valid_lft forever preferred_lft forever
victim@victim:~$ _
```

# CẤU HÌNH VÀ CÀI ĐẶT

## Cấu hình cho Attacker



# CẤU HÌNH VÀ CÀI ĐẶT



```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd 00:00:00:00:00:00 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:30:ce:64 brd ff:ff:ff:ff:ff:ff
        inet 10.81.69.100/24 brd 10.81.69.255 scope global eth0
            valid_lft forever preferred_lft forever
            inet6 fe80::1c88:74e:1208:fc27/64 scope link noprefixroute
                valid_lft forever preferred_lft forever

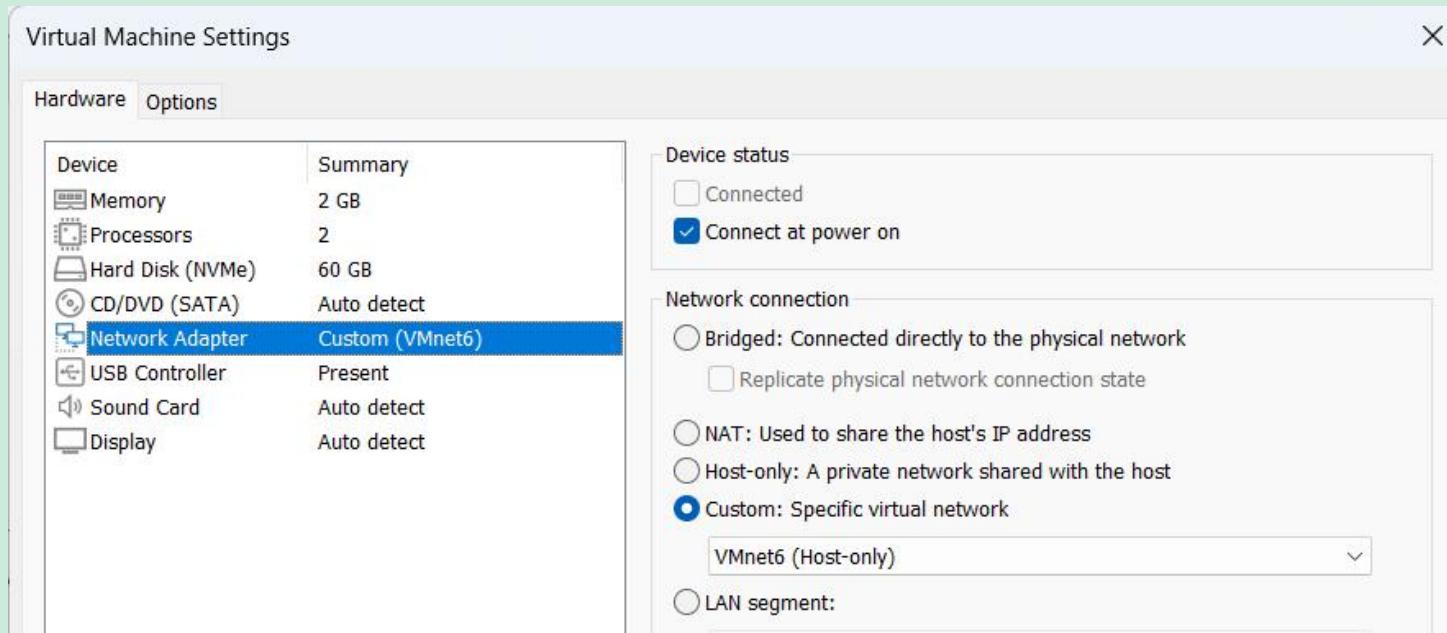
(kali㉿kali)-[~]
$ ip route
default via 10.81.69.1 dev eth0 proto static metric 100
10.81.69.0/24 dev eth0 proto kernel scope link src 10.81.69.100 metric 100

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.81.69.100 netmask 255.255.255.0 broadcast 10.81.69.255
        inet6 fe80::1c88:74e:1208:fc27/64 brd fe80::ff:ff:fe88:74e:1208:fc27/64 scopeid 0x20<link>
            ether 00:0c:29:30:ce:64 txqueuelen 1000 (Ethernet)
            RX packets 97 bytes 5820 (5.6 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 109 bytes 28156 (27.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

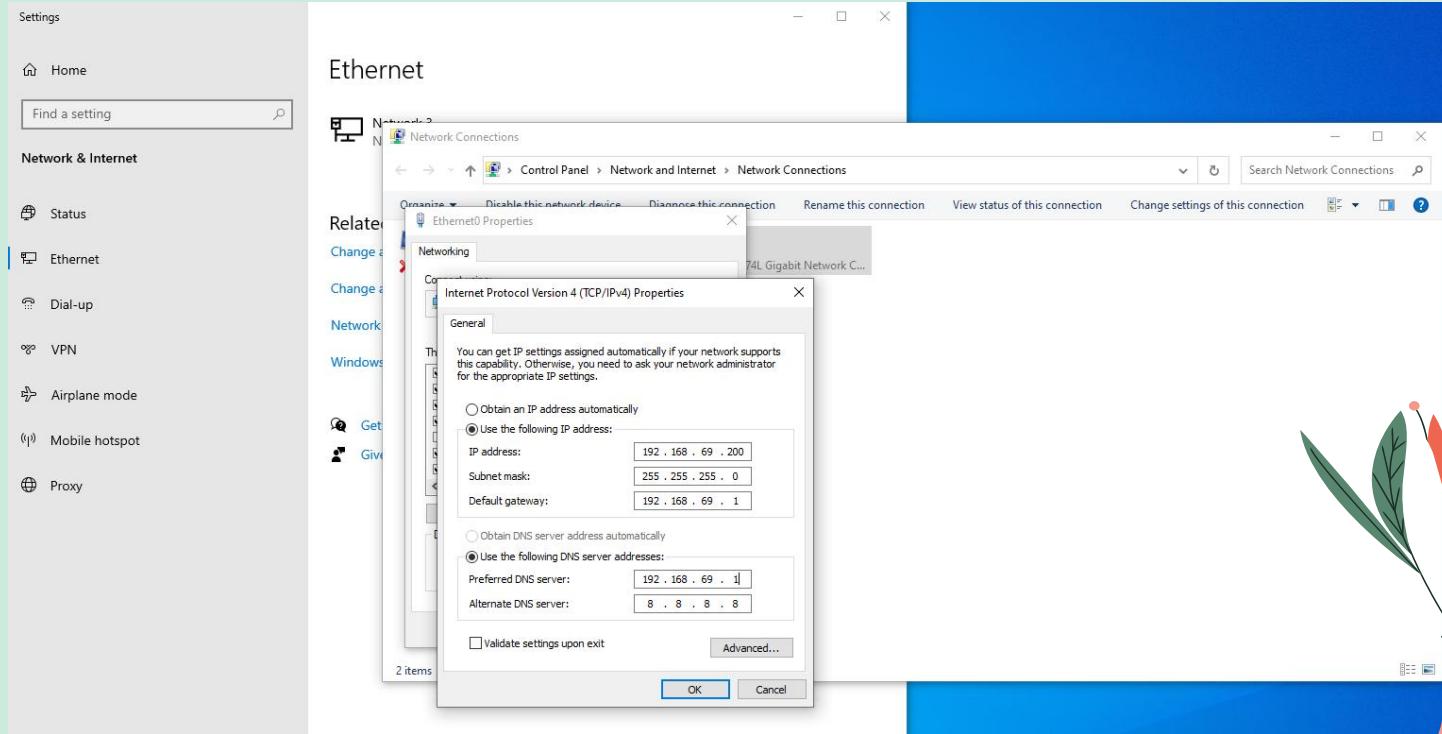
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 8 bytes 480 (480.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 480 (480.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

# CẤU HÌNH VÀ CÀI ĐẶT

## Cấu hình cho Victim



# CẤU HÌNH VÀ CÀI ĐẶT



# CẤU HÌNH VÀ CÀI ĐẶT

```
c:\ Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\victim>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::9926:cef7:f9e1:d9ad%14
    IPv4 Address . . . . . : 192.168.69.200
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.69.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

C:\Users\victim>
```



# CẤU HÌNH VÀ CÀI ĐẶT

## Cấu hình định tuyến cho Router

```
router@router:~$ echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf  
net.ipv4.ip_forward=1  
router@router:~$ sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE  
router@router:~$
```



# CẤU HÌNH VÀ CÀI ĐẶT

## Cài đặt Agent trên Victim

Sau khi đăng ký, ta truy cập vào Vision One Central:

**Bước 1:** Tại Service Management → Product Instance → Create Product Instance → Standard Endpoint Protection → Điền thông tin → Chờ connect

# CẤU HÌNH VÀ CÀI ĐẶT

The screenshot shows the Trend Vision One™ Product Instance interface. On the left, a navigation sidebar lists categories like Identity Security, Data Security, Endpoint Security, Cloud Security, Network Security, Email and Collaboration Security, Mobile Security, Service Management (selected), Product Instance (highlighted in red), Asset Visibility Management, Asset Group Management, Administration, and Customize your navigation. A notification bar at the bottom left indicates 19 unread items. The main content area displays a table of product instances. The first instance, 'UIT', is selected and shown in more detail. The 'Managed Instance Settings' dialog is open over the table, containing fields for Instance type (set to Standard Endpoint Protection), Display name (empty), Region (Select a region), and Description (empty). Buttons for Save and Cancel are at the bottom right of the dialog. The top right of the screen shows a system tray with a clock, file, settings, and help icons, along with a notification count of 6.

Display name	Status	Instance ID	Instance type
UIT	Connected	000d3a97-97e9-680a-517a-0136cd73e5d8	Standard Endpoint Protection
Cloud Email and Collaboration Protection	Connected	deeee3fa-46c2-4b94-bd88-58b57481614b	Cloud Email and Collaboration Protection

Managed Instance Settings

Instance type:  
Standard Endpoint Protection

Display name:  
Display name

Region:  
Select a region

Description:  
Description

Save Cancel

# CẤU HÌNH VÀ CÀI ĐẶT

## Cài đặt Agent trên Victim

**Bước 2:** Tại Endpoint Security → Endpoint Inventory → Agent Installer → Điền Thông tin → Tải và chạy Image Setup Tool → Tải và chạy Agent.



# CẤU HÌNH VÀ CÀI ĐẶT

The screenshot shows the Trend Vision One™ Endpoint Inventory interface. On the left, a navigation sidebar includes Threat Intelligence, Workflow and Automation, Zero Trust Secure Access, Assessment, Identity Security, Data Security, Endpoint Security (selected), Endpoint Inventory (selected), Endpoint Security Configuration (selected), Cloud Security, and a notification icon with 19 messages. The main area displays the Endpoint Inventory with sections for Available Actions (Sensor disabled), Security Deployment (All managed endpoints), and Endpoint Management (Standard Endpoint Protection). A modal window titled "Agent Installer" is open, showing tabs for "Installer Package" (selected) and "Deployment Script". It contains instructions to save time by configuring default connection and sensor settings, update proxy settings, and set up endpoint security policies. It also provides information on using a software management system to deploy agents. Below the modal, there are two sections: "Standard Endpoint Protection" (User-centric protection with DLP capabilities, Windows OS, 64-bit architecture, and Windows Endpoint Group Manager) and "Server & Workload Protection".

04.

# TRIỂN KHAI



# TRIỂN KHAI

Các kịch bản triển khai:

## a. Bảo vệ URL

- Các tính năng sử dụng: **Web Reputation, URL Filtering**
- Video demo: [https://youtu.be/r\\_rGcdImGSI](https://youtu.be/r_rGcdImGSI)
- Hệ thống sẽ kiểm tra độ uy tín của các URL theo thời gian thực, chặn truy cập vào các trang web được đưa vào blacklist. Người dùng bị cảnh báo và ngăn truy cập.



# TRIỂN KHAI

Các kịch bản triển khai:

b. Phát hiện và ngăn chặn malware có sẵn trên thiết bị  
EndPoint

- Các tính năng sử dụng: **Real-Time Scan**
- Video demo: <https://youtu.be/O0UkCtBXH5s>



# TRIỂN KHAI

Các kịch bản triển khai:

b. Phát hiện và ngăn chặn malware có sẵn trên thiết bị EndPoint

- Khi Apex One agent đã được cài sẵn trên thiết bị endpoint, hệ thống sẽ tự động quét để tìm kiếm malware ẩn hoặc đã tồn tại trước đó. Ngay khi phát hiện, agent sẽ tự động cách ly tập tin, ghi nhận sự kiện và gửi cảnh báo về console quản trị.

# TRIỂN KHAI

Các kịch bản triển khai:

c. Phát hiện và ngăn chặn malware tấn công từ bên ngoài

- Tính năng đã sử dụng: **Real-Time Scan**
- Video demo: <https://youtu.be/SPmQyWSV-S0>



# TRIỂN KHAI

Các kịch bản triển khai:

c. Phát hiện và ngăn chặn malware tấn công từ bên ngoài

- Khi người dùng truy cập một website tải về tệp đính kèm chứa mã độc, Apex One sẽ lập tức ghi nhận hành vi, cách ly file độc hại, gửi cảnh báo về console để ngăn mã độc lây lan trong mạng nội bộ.



# TRIỂN KHAI

Các kịch bản triển khai:

d. Ngăn chặn tấn công từ thiết bị lưu trữ bên ngoài

- Tính năng đã sử dụng: **Real-Time Scan, Device Control**
- Video demo: <https://youtu.be/q7o2BWgUn9o>
- Khi người dùng kết nối USB vào máy tính, Apex One sẽ tự động quét nội dung thiết bị. Khi phát hiện tập tin chứa mã độc, hệ thống sẽ chặn truy cập, cách ly file và cảnh báo ngay lập tức.

# TRIỂN KHAI

Các kịch bản triển khai:

e. Ngăn chặn mất mát dữ liệu

- Tính năng đã sử dụng: **Data Loss Prevention (DLP)**
- Video demo: <https://youtu.be/tMWb0QeAKaQ>
- Khi người dùng gửi dữ liệu nhạy cảm qua email hoặc tải lên web không tin cậy, hệ thống sẽ phát hiện và chặn hành vi đó dựa trên từ khóa, định dạng tệp, hoặc loại dữ liệu đã định nghĩa.



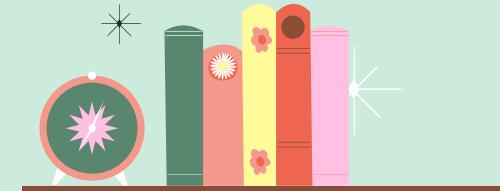
# TRIỂN KHAI

Các kịch bản triển khai:

## f. Phân tích bằng sandbox trong Trend Micro Vision One

- Tính năng đã sử dụng: **Sandbox Analysis**
- Video demo: <https://youtu.be/xK659bB8AfA>
- Người dùng tải file lên Sandbox Analysis để phân tích. Hệ thống sẽ thực thi file trong môi trường ảo, quan sát hành vi. Kết quả phân tích sẽ hiển thị mức độ nguy hiểm, hành vi đáng ngờ và chỉ số tấn công (IOC).

# 05. TỔNG KẾT



# TỔNG KẾT

## a. Ưu điểm

- Tích hợp toàn diện
- Phát hiện nâng cao
- Khả năng quản lý tốt
- Khả năng EDR mạnh
- Hỗ trợ nhiều nền tảng

## b. Nhược điểm

- Chi phí
- Phức tạp khi triển khai ban đầu
- Yêu cầu tài nguyên



# TỔNG KẾT

**Trend Micro Apex One** là giải pháp bảo mật mạnh mẽ dành cho doanh nghiệp, đặc biệt là các tổ chức cần một nền tảng endpoint protection tích hợp cả EPP và EDR. Mặc dù có thể phức tạp và tốn chi phí, nhưng đổi lại, Apex One cung cấp khả năng bảo vệ tối ưu cho các thiết bị bên trong mạng trước các mối đe dọa như hiện nay.



# Thanks!!

