

Case #1: Cài Đặt Falcon Sensor

Tổng quan

CrowdStrike Falcon Sensor là một thành phần quan trọng của nền tảng Falcon, nó cung cấp bảo vệ endpoint tiên tiến thông qua giám sát thời gian thực, phân tích hành vi và threat intelligence tích hợp. Thiết kế lightweight, dựa trên nền tảng cloud để đảm bảo rằng các tổ chức có thể duy trì trạng thái bảo vệ mạnh mẽ trong khi giảm thiểu độ phức tạp trong vận hành.

Yêu cầu của khách hàng

- Sensor có thể tiêu tốn tài nguyên hệ thống, dẫn đến hiệu suất giảm trên các endpoint, đặc biệt là trên phần cứng cũ không ?
- Có thể gặp phải những thách thức về khả năng tương thích với các ứng dụng hoặc hệ thống hiện có, dẫn đến gián đoạn trong hoạt động của doanh nghiệp.
- Sensor thu thập và truyền dữ liệu, điều này có thể gây ra lo ngại về quyền riêng tư dữ liệu và việc tuân thủ các quy định (ví dụ: GDPR, HIPAA).

Giải pháp

- Sensor CrowdStrike Falcon là một giải pháp bảo vệ đầu cuối dựa trên đám mây. Nó cung cấp các tính năng và lợi ích sau:
 - Sensor được thiết kế nhẹ và hiệu quả, giảm thiểu tác động đến hiệu suất trên các thiết bị đầu cuối trong khi vẫn đảm bảo an ninh vững chắc.
 - Hỗ trợ nhiều hệ điều hành, bao gồm Windows, macOS và Linux.
 - Sensor Falcon không quét nội dung của các tệp dữ liệu, tin nhắn email hoặc cuộc trò chuyện, cũng như không ghi lại nội dung của các trang web được xem.
 - Dễ dàng triển khai và quản lý, cho phép các tổ chức thực hiện các biện pháp bảo mật mà không cần khởi động lại hay gián đoạn công việc của khách hàng.

Lợi ích & Giá trị

- **Tăng cường Tư thế Bảo mật:** Cung cấp cho các tổ chức khả năng phát hiện, ngăn chặn và phản ứng hiệu quả với các mối đe dọa mạng tinh vi.
- **Giảm Độ Phức Tạp:** Đơn giản hóa việc quản lý bảo mật đầu cuối thông qua một nền tảng thống nhất tích hợp các khả năng phòng ngừa, phát hiện và phản ứng.
- **Khả Năng Mở Rộng:** Dễ dàng mở rộng để đáp ứng nhu cầu của các tổ chức đang phát triển mà không cần đầu tư hạ tầng lớn.

Case #1: Cài Đặt Falcon Sensor

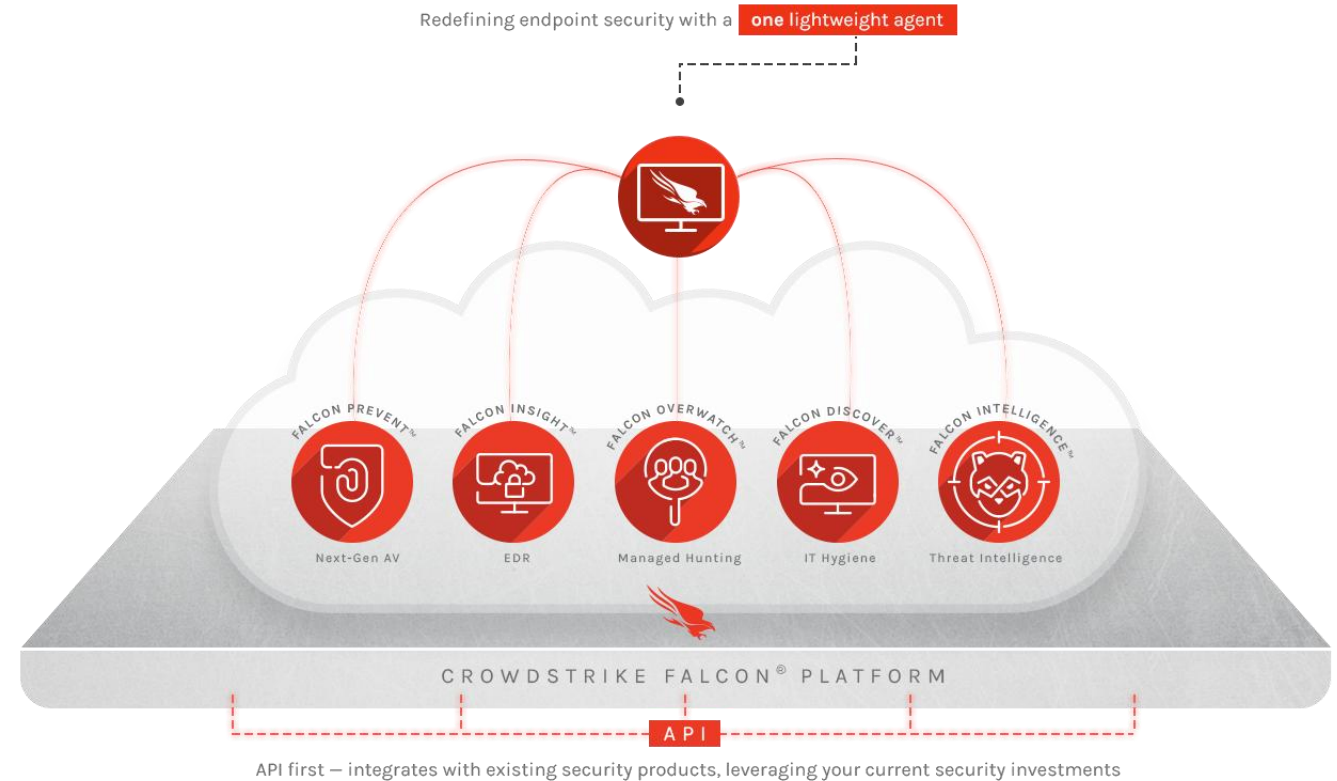
Công nghệ sử dụng

Phần mềm:

- Gói cài đặt Falcon Sensor
- Hỗ trợ nhiều OS khác nhau (Windows, Mac, Linux)
- GPO (On-Demand)

Giá trị đem đến cho khách hàng

- **Tích hợp Nhiều Chức Năng Bảo Mật:** Kết hợp các chức năng bảo mật như antivirus, EDR, XDR và Threat Intelligence vào một giải pháp duy nhất, giúp đơn giản hóa quản lý bảo mật.
- **Sử Dụng Phân Tích Hành Vi Nâng Cao:** Phát hiện các hoạt động đáng ngờ trong những event bình thường, nâng cao khả năng phát hiện các mối đe dọa chưa biết và các cuộc tấn công zero-day.
- **Cung Cấp Tầm Nhìn Chi Tiết về Hoạt Động của Endpoint:** Cho phép các đội ngũ bảo mật thực hiện các cuộc điều tra kỹ lưỡng và thu thập thông tin về các lỗ hổng tiềm ẩn.
- **Thiết Kế Lightweight:** Đảm bảo hiệu suất endpoint vẫn tối ưu trong khi duy trì các biện pháp bảo mật vững chắc.



Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

Nếu bạn chỉ có một số ít các Endpoint cần cài đặt, việc thực hiện cài đặt thủ công có thể là lựa chọn tốt nhất.

Windows:

1. Yêu cầu

- **Services:**
 - + LMHosts (Optional for TCP/IP NetBIOS Helper)
 - + Network Store Interface (NSI)
 - + Windows Base Filtering Engine (BFE)
 - + Windows Power Service

Trên Windows Server 2016, 2019, and 2022, Windows Defender được bật theo mặc định. Để sử dụng tính năng Quarantine của Falcon's Next-Gen Antivirus, bạn phải vô hiệu hóa Windows Defender.

- **Network:**
 - + Falcon sensor yêu cầu TLS 1.2 để giao tiếp với CrowdStrike Cloud. Những giao thức khác, bao gồm SSL hoặc phiên bản trước của TLS sẽ không được hỗ trợ.
 - + Host phải kết nối với CrowdStrike Cloud trên port 443 trong suốt quá trình cài đặt. Nếu môi trường của bạn giới hạn truy cập Internet, hãy cho phép truy cập tới IP và FQDNs của CrowdStrike Cloud .

Cloud domains for US-1

```
ts01-b.cloudsink.net
lfodown01-b.cloudsink.net
lfoup01-b.cloudsink.net
https://falcon.crowdstrike.com
https://assets.falcon.crowdstrike.com
https://assets-public.falcon.crowdstrike.com
https://api.crowdstrike.com
https://firehose.crowdstrike.com
```

CrowdStrike cloud US-2 domains

```
ts01-gyr-maverick.cloudsink.net
lfodown01-gyr-maverick.cloudsink.net
lfoup01-gyr-maverick.cloudsink.net
https://falcon.us-2.crowdstrike.com
https://assets.falcon.us-2.crowdstrike.com
https://assets-public.falcon.us-2.crowdstrike.com
https://api.us-2.crowdstrike.com
https://firehose.us-2.crowdstrike.com
```

CrowdStrike cloud EU-1 domains

```
ts01-lanner-lion.cloudsink.net
lfodown01-lanner-lion.cloudsink.net
lfoup01-lanner-lion.cloudsink.net
https://falcon.eu-1.crowdstrike.com
https://assets.falcon.eu-1.crowdstrike.com
https://assets-public.falcon.eu-1.crowdstrike.com
https://api.eu-1.crowdstrike.com
https://firehose.eu-1.crowdstrike.com
```

Case #1: Cài Đặt Falcon Sensor

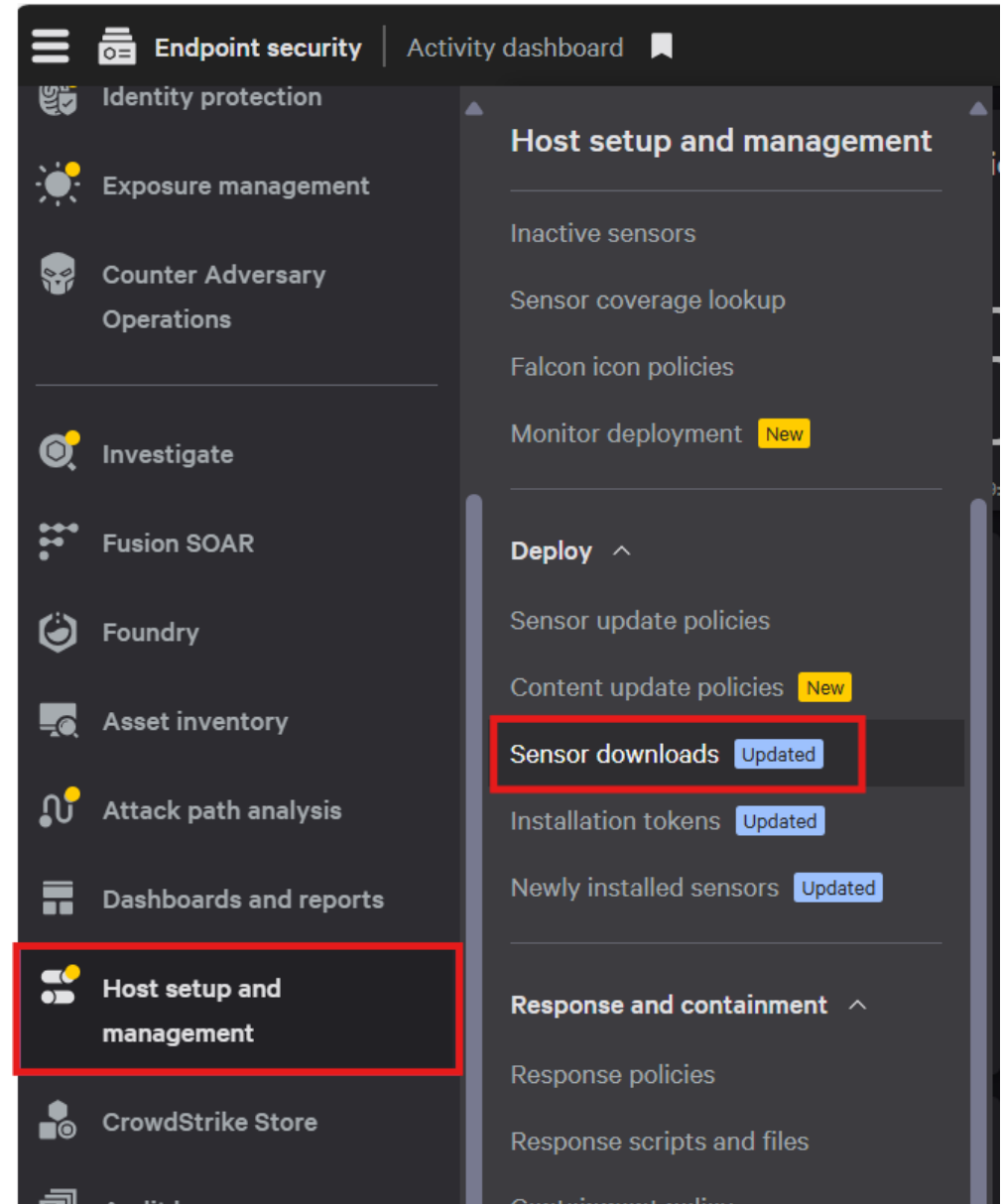
Cài Đặt Falcon Sensor Thủ Công

Nếu bạn chỉ có một số ít các Endpoint cần cài đặt, việc thực hiện cài đặt thủ công có thể là lựa chọn tốt nhất.

Windows:

2. Trên Download gói cài đặt Sensor tại **Host setup and management > Deploy > Sensor downloads > Windows**

- File tải về sẽ có tên: FalconSensor_Windows.exe

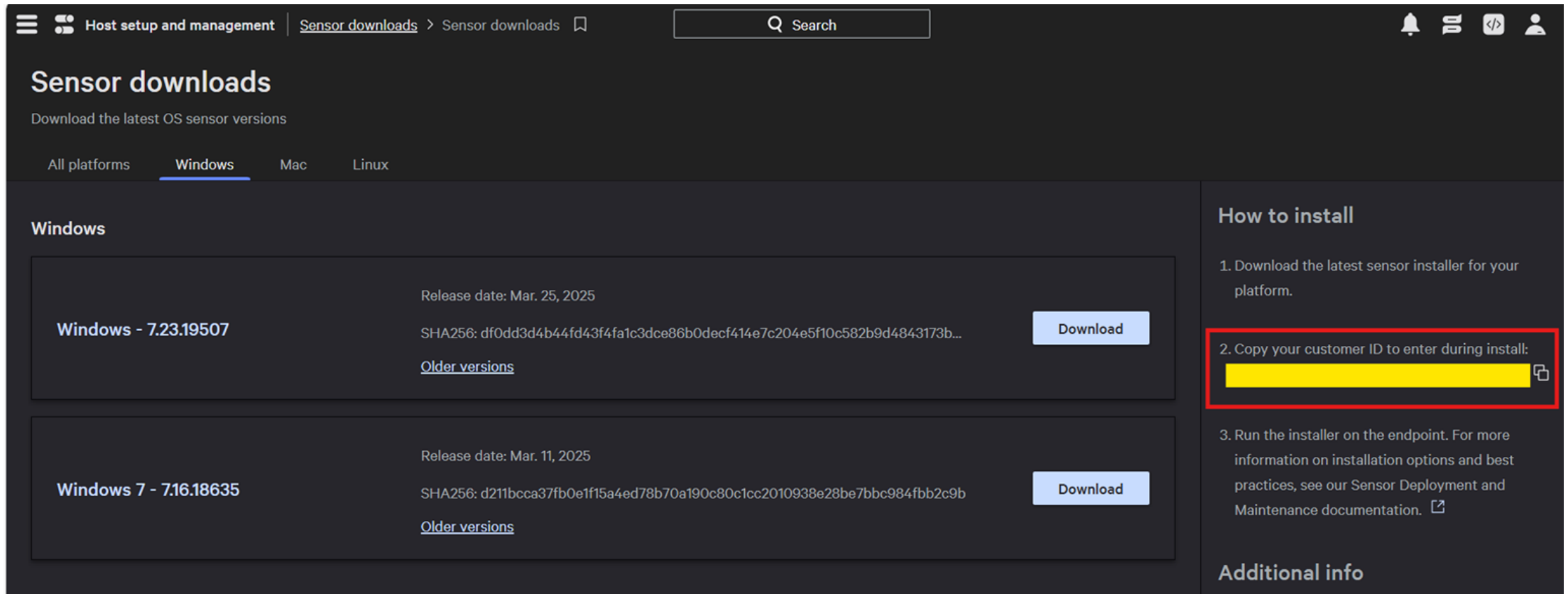


Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

3. Copy customer ID checksum (CCID) của bạn tại **Host setup and management > Deploy > Sensor downloads**.

Nếu bạn là người dung trial, bỏ qua bước này.



The screenshot shows the 'Sensor downloads' page in a dark theme. The breadcrumb navigation is 'Host setup and management > Sensor downloads > Sensor downloads'. The page title is 'Sensor downloads' with the subtitle 'Download the latest OS sensor versions'. There are tabs for 'All platforms', 'Windows', 'Mac', and 'Linux'. The 'Windows' tab is selected. Two sensor versions are listed:

Version	Release date	SHA256	Action
Windows - 7.23.19507	Mar. 25, 2025	df0dd3d4b44fd43f4fa1c3dce86b0decf414e7c204e5f10c582b9d4843173b...	Download
Windows 7 - 7.16.18635	Mar. 11, 2025	d211bccca37fb0e1f15a4ed78b70a190c80c1cc2010938e28be7bbc984fbb2c9b	Download

Each version has a link for 'Older versions'. On the right side, there is a 'How to install' section with three steps:

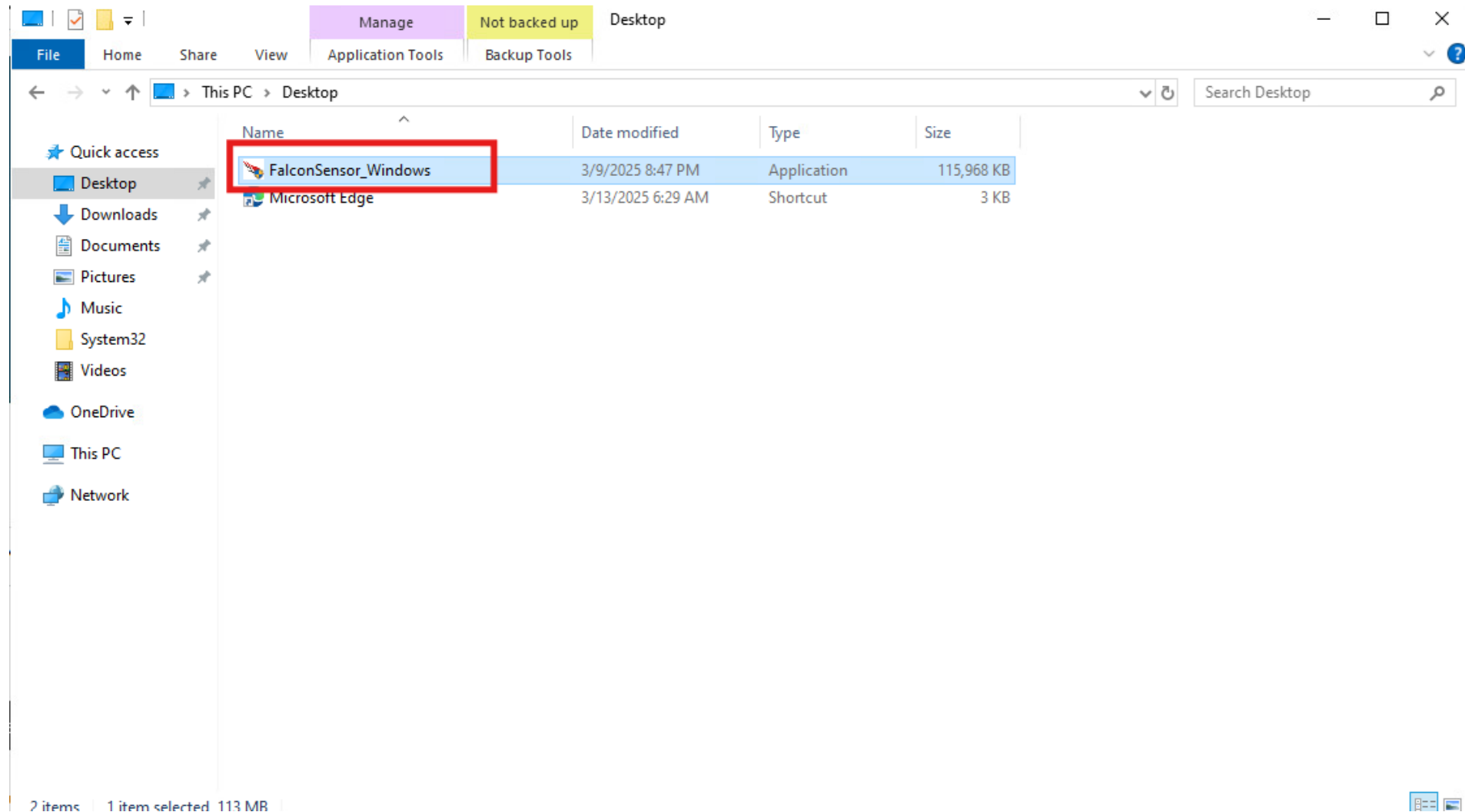
- Download the latest sensor installer for your platform.
- Copy your customer ID to enter during install: (highlighted in yellow and red in the image)
- Run the installer on the endpoint. For more information on installation options and best practices, see our Sensor Deployment and Maintenance documentation.

Below the instructions is an 'Additional info' section.

Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

4. Copy file cài sensor vào endpoint và chạy file cài đặt.



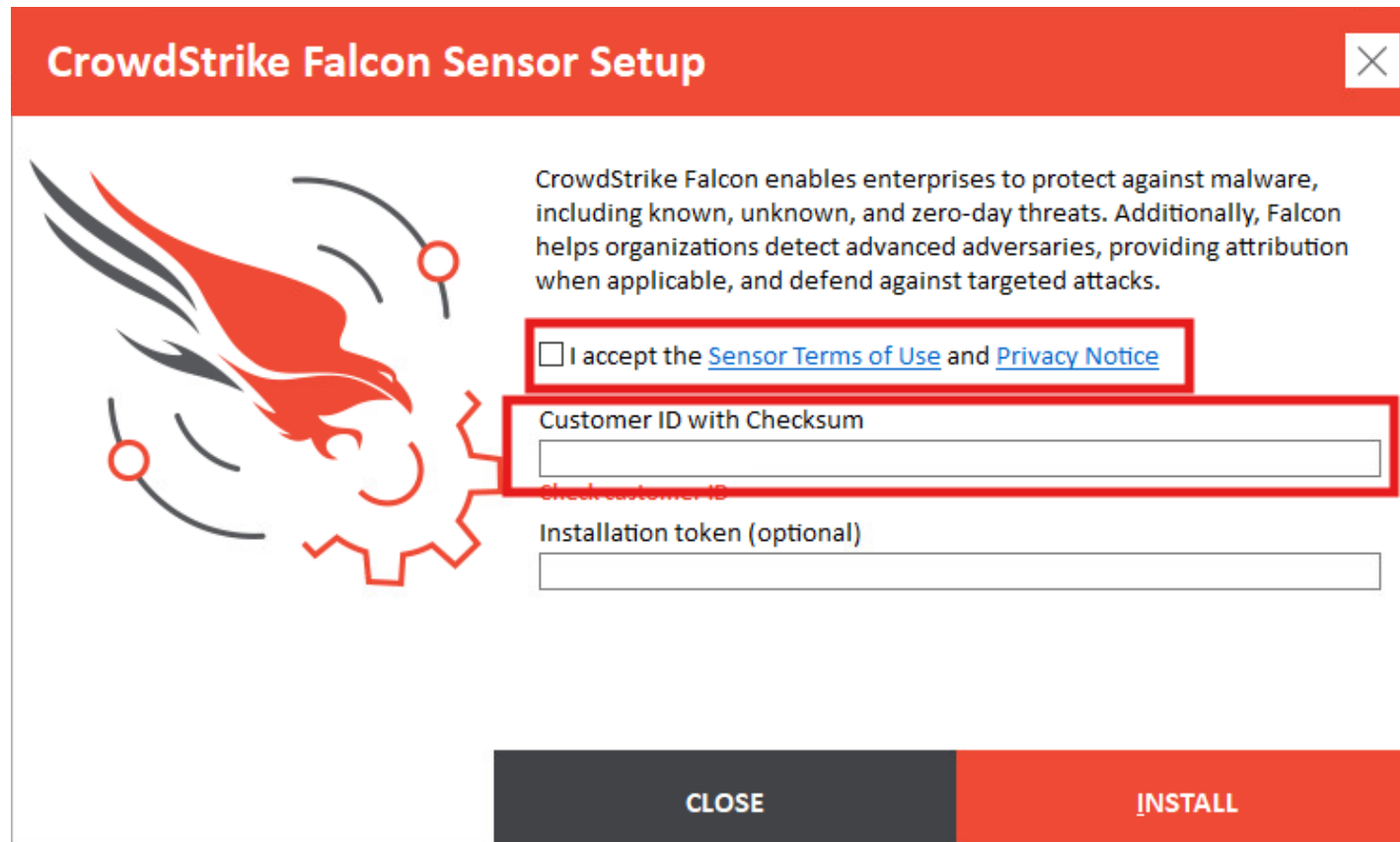
Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

5. Chấp nhận các điều khoản và điền customer ID checksum đã copy vào > Chọn Install.

Nếu bạn là người dùng trial, bỏ qua bước này.

Nếu OS của endpoint xuất hiện thông báo cấp phép cho việc cài đặt, chọn **Yes**.



CrowdStrike Falcon Sensor Setup

CrowdStrike Falcon enables enterprises to protect against malware, including known, unknown, and zero-day threats. Additionally, Falcon helps organizations detect advanced adversaries, providing attribution when applicable, and defend against targeted attacks.

I accept the [Sensor Terms of Use](#) and [Privacy Notice](#)

Customer ID with Checksum

Check customer ID

Installation token (optional)

CLOSE INSTALL

Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

6. Xác nhận Falcon Sensor cài đặt thành công.

Sử dụng lệnh “`sc.exe query csagent`” để kiểm tra trạng thái của Sensor

```
Command Prompt
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Test1>sc.exe query csagent

SERVICE_NAME: csagent
        TYPE               : 2  FILE_SYSTEM_DRIVER
        STATE                : 4  RUNNING
                          (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

C:\Users\Test1>
```

Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

1. Yêu cầu

- System:

- + Falcon Sensor hỗ trợ các phiên bản MacOS 13, 14 và 15.
- + Cài đặt Falcon sensor cho Mac yêu cầu quyền administrator, hay còn gọi là quyền nâng cao.
- + Apple yêu cầu các phần mở rộng hệ thống phải được phê duyệt trước khi có thể được load. Falcon Sensor cho Mac yêu cầu các quyền bổ sung sau trên mỗi host:

- Full Disk Access (FDA) cho Falcon
- Falcon system extension
- Falcon network filter extension

macOS version	Minimum sensor version	Falcon end-of-support date
macOS Sequoia 15	All supported sensor versions Intel CPUs and Apple silicon native support included	December 31, 2027
macOS Sonoma 14	All supported sensor versions Intel CPUs and Apple silicon native support included	December 31, 2026
macOS Ventura 13	All supported sensor versions Intel CPUs and Apple silicon native support included	December 31, 2025

Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

1. Yêu cầu

- Network:

- + Falcon sensor yêu cầu TLS 1.2 để giao tiếp với CrowdStrike Cloud. Những giao thức khác, bao gồm SSL hoặc phiên bản trước của TLS sẽ không được hỗ trợ.
- + Host phải kết nối với CrowdStrike Cloud trên port 443 trong suốt quá trình cài đặt. Nếu môi trường của bạn giới hạn truy cập Internet, hãy cho phép truy cập tới IP và FQDNs của CrowdStrike Cloud.
- + Disable deep packet inspection (hay được gọi là "HTTPS interception," "TLS interception," hoặc "SSL inspection"). Các yếu tố ảnh hưởng phổ biến với certificate pinning cho CrowdStrike Cloud bao gồm hệ thống antivirus, firewall, hoặc proxy.

Cloud domains for US-1

```
ts01-b.cloudsink.net
lfodown01-b.cloudsink.net
lfoup01-b.cloudsink.net
https://falcon.crowdstrike.com
https://assets.falcon.crowdstrike.com
https://assets-public.falcon.crowdstrike.com
https://api.crowdstrike.com
https://firehose.crowdstrike.com
```

CrowdStrike cloud US-2 domains

```
ts01-gyr-maverick.cloudsink.net
lfodown01-gyr-maverick.cloudsink.net
lfoup01-gyr-maverick.cloudsink.net
https://falcon.us-2.crowdstrike.com
https://assets.falcon.us-2.crowdstrike.com
https://assets-public.falcon.us-2.crowdstrike.com
https://api.us-2.crowdstrike.com
https://firehose.us-2.crowdstrike.com
```

CrowdStrike cloud EU-1 domains

```
ts01-lanner-lion.cloudsink.net
lfodown01-lanner-lion.cloudsink.net
lfoup01-lanner-lion.cloudsink.net
https://falcon.eu-1.crowdstrike.com
https://assets.falcon.eu-1.crowdstrike.com
https://assets-public.falcon.eu-1.crowdstrike.com
https://api.eu-1.crowdstrike.com
https://firehose.eu-1.crowdstrike.com
```

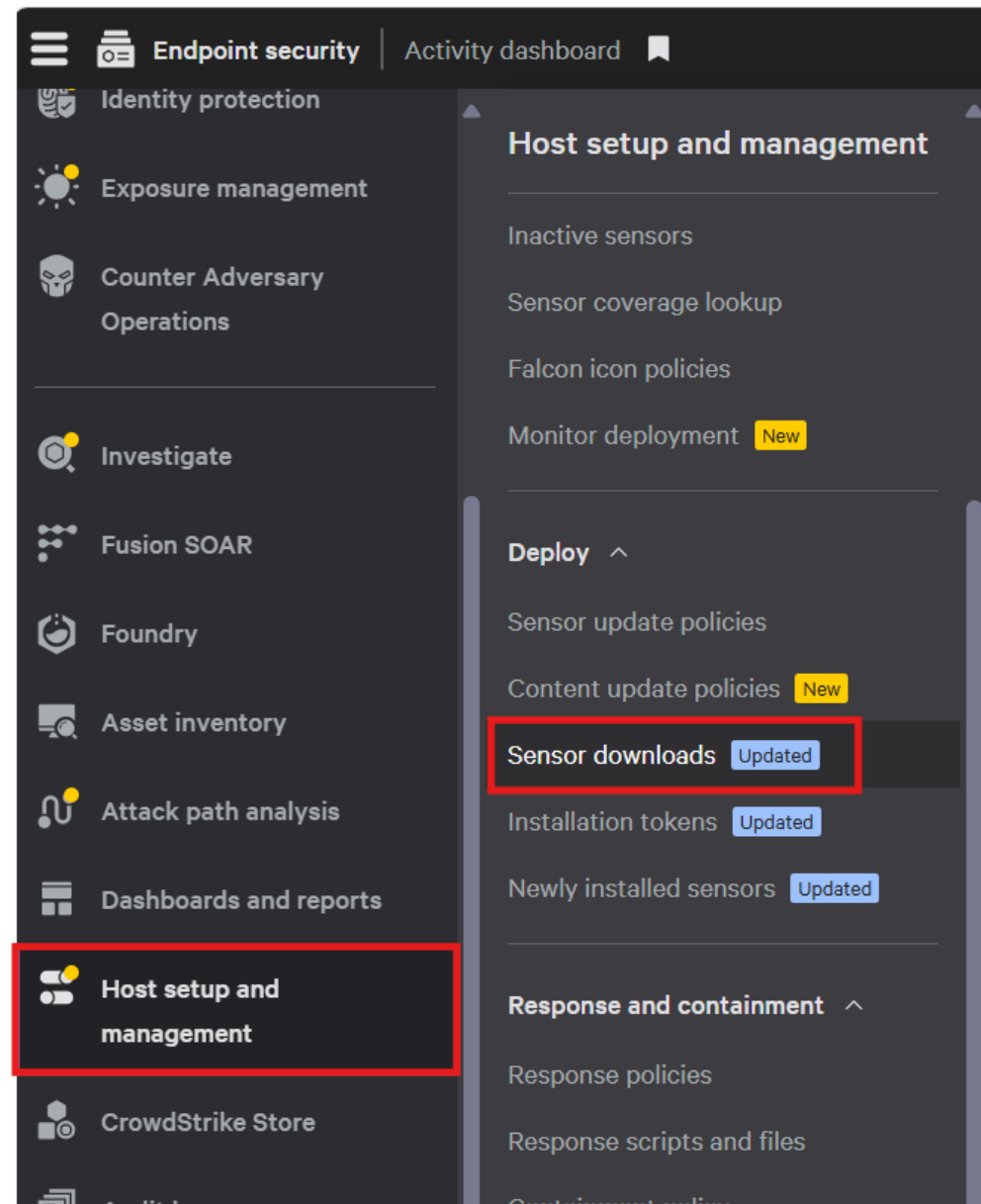
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

2. Tải bộ cài Sensor tại **Host setup and management > Deploy > Sensor downloads >**

MacOS



Case #2: Cài Đặt Falcon Sensor

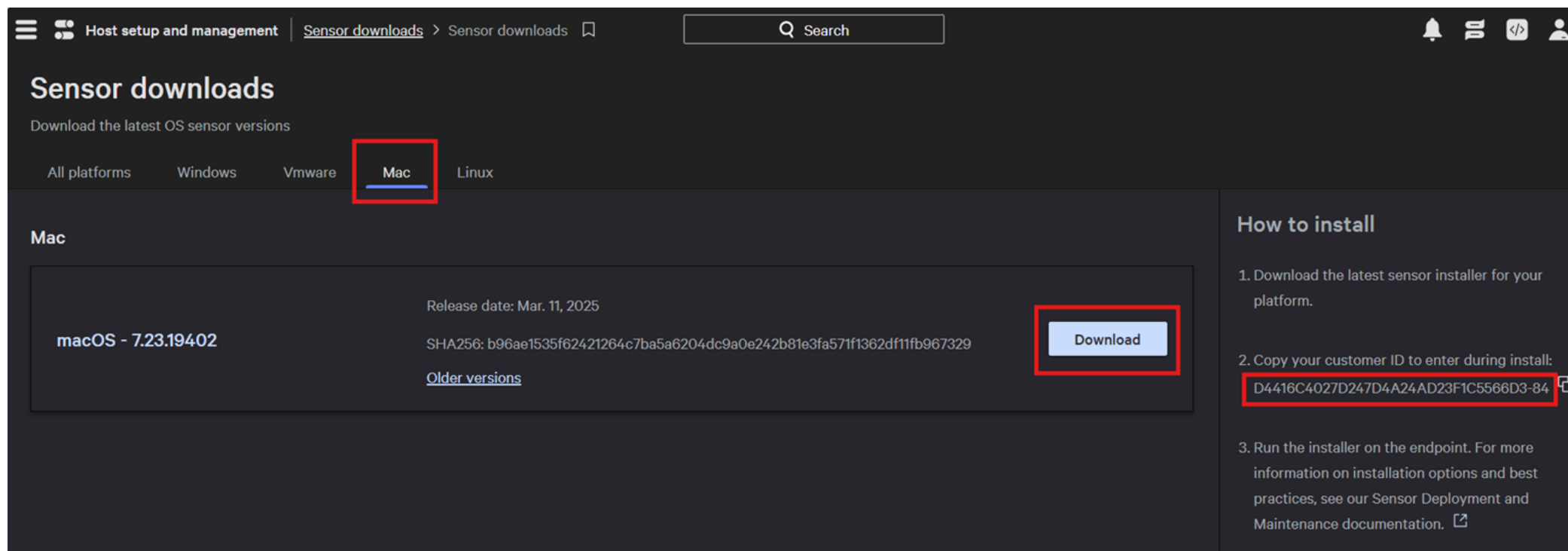
Cài Đặt Falcon Sensor Thủ Công

MacOS:

2. Tải bộ cài Sensor tại **Host setup and management > Deploy > Sensor downloads >**

MacOS

- Copy Customer ID Checksum (CID) của bạn tại trang Sensor Downloads.



The screenshot shows the 'Sensor downloads' page in a dark-themed interface. The breadcrumb navigation is 'Host setup and management > Sensor downloads > Sensor downloads'. The page title is 'Sensor downloads' with the subtitle 'Download the latest OS sensor versions'. There are tabs for 'All platforms', 'Windows', 'Vmware', 'Mac', and 'Linux', with 'Mac' selected and highlighted by a red box. Below the tabs, the 'Mac' section displays the version 'macOS - 7.23.19402', the release date 'Mar. 11, 2025', and the SHA256 checksum 'b96ae1535f62421264c7ba5a6204dc9a0e242b81e3fa571f1362df11fb967329'. A 'Download' button is highlighted with a red box. To the right, the 'How to install' section lists three steps: 1. Download the latest sensor installer for your platform. 2. Copy your customer ID to enter during install: `D4416C4027D247D4A24AD23F1C5566D3-84` (highlighted with a red box). 3. Run the installer on the endpoint. For more information on installation options and best practices, see our Sensor Deployment and Maintenance documentation.

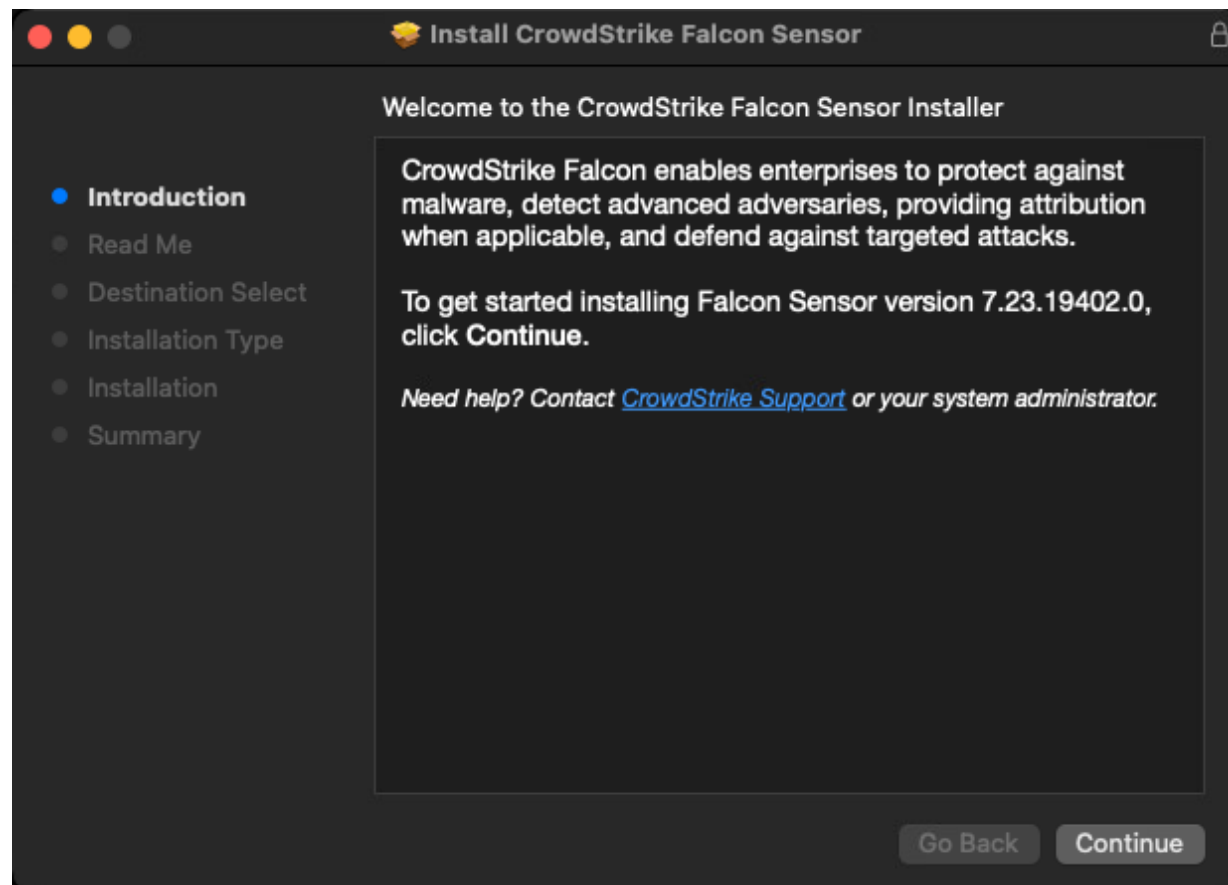
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

3. Double-click để mở file .pkg đã download.

Khi bộ cài cho Falcon Sensor cho Mac chạy > Click **Continue**

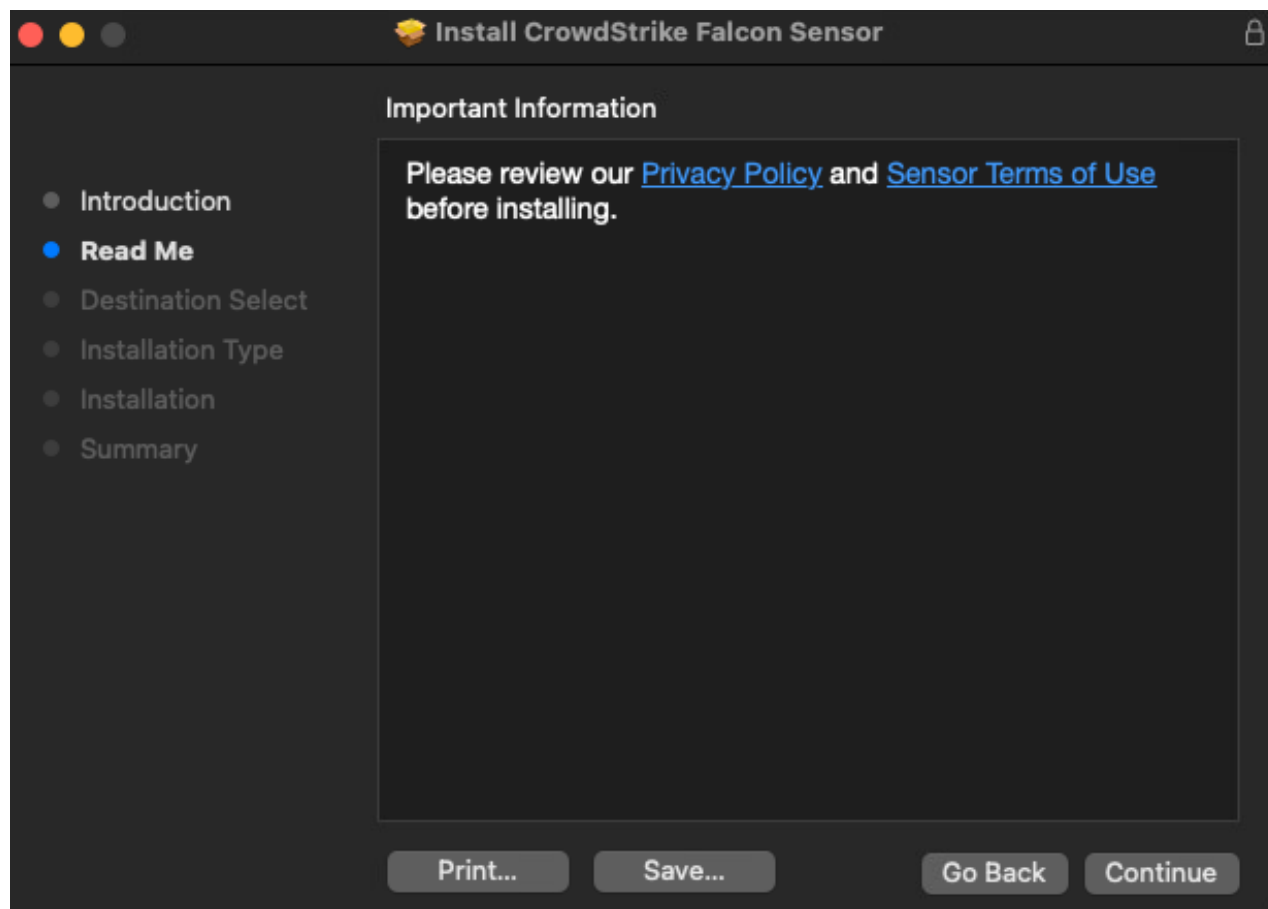


Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

4. Đánh giá Chính sách quyền riêng tư và điều khoản sử dụng và chọn **Continue**



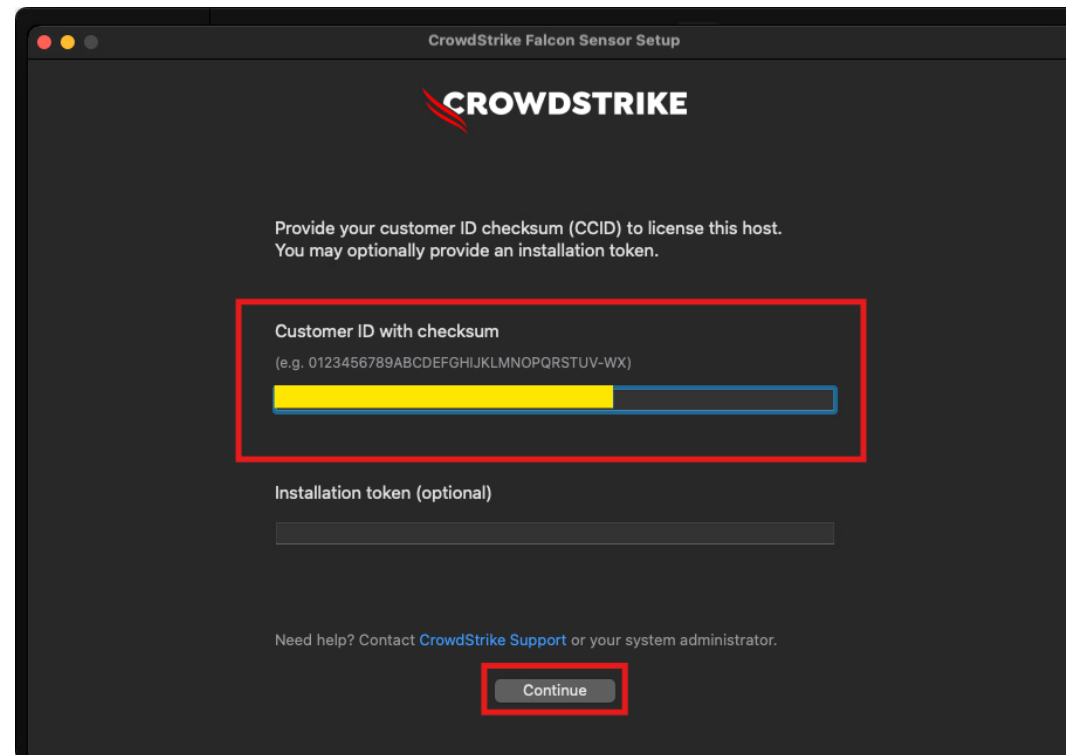
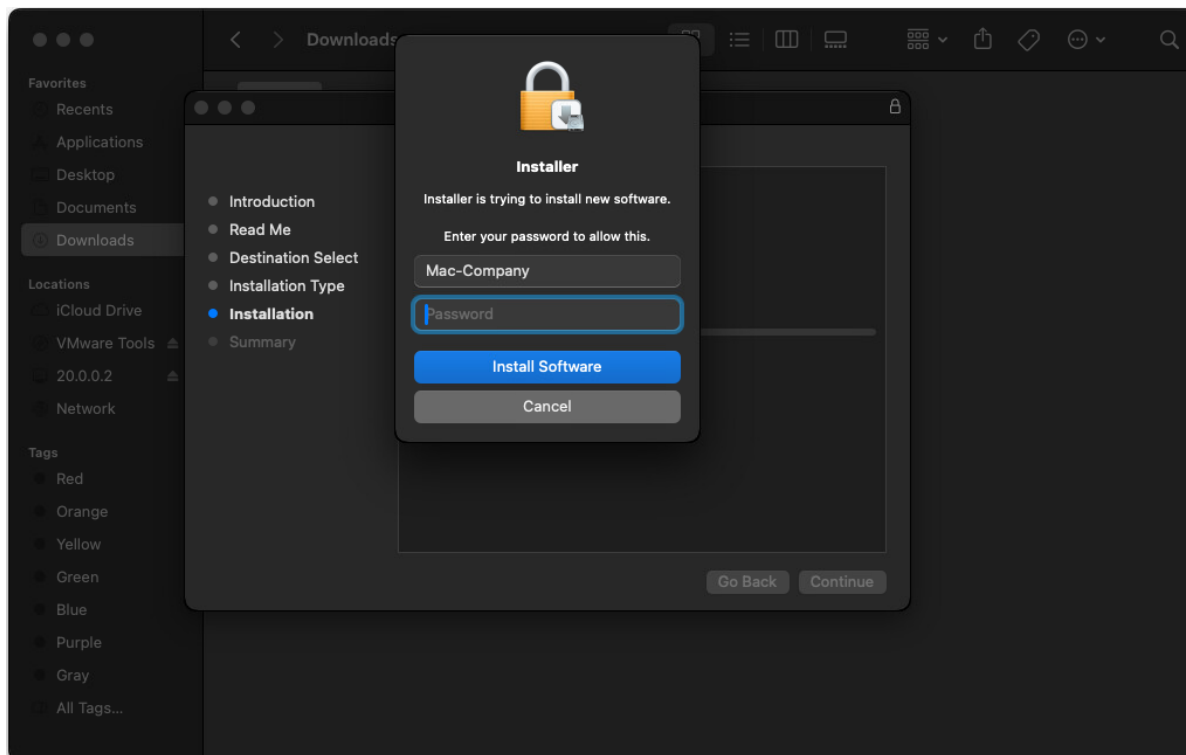
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

5. Khi một cửa sổ hiện ra, đăng nhập bằng tài khoản với quyền administrative và chọn **Install Software**.

Trong cửa sổ cài đặt, điền customer ID checksum (CCID) của bạn > Chọn **Continue**.

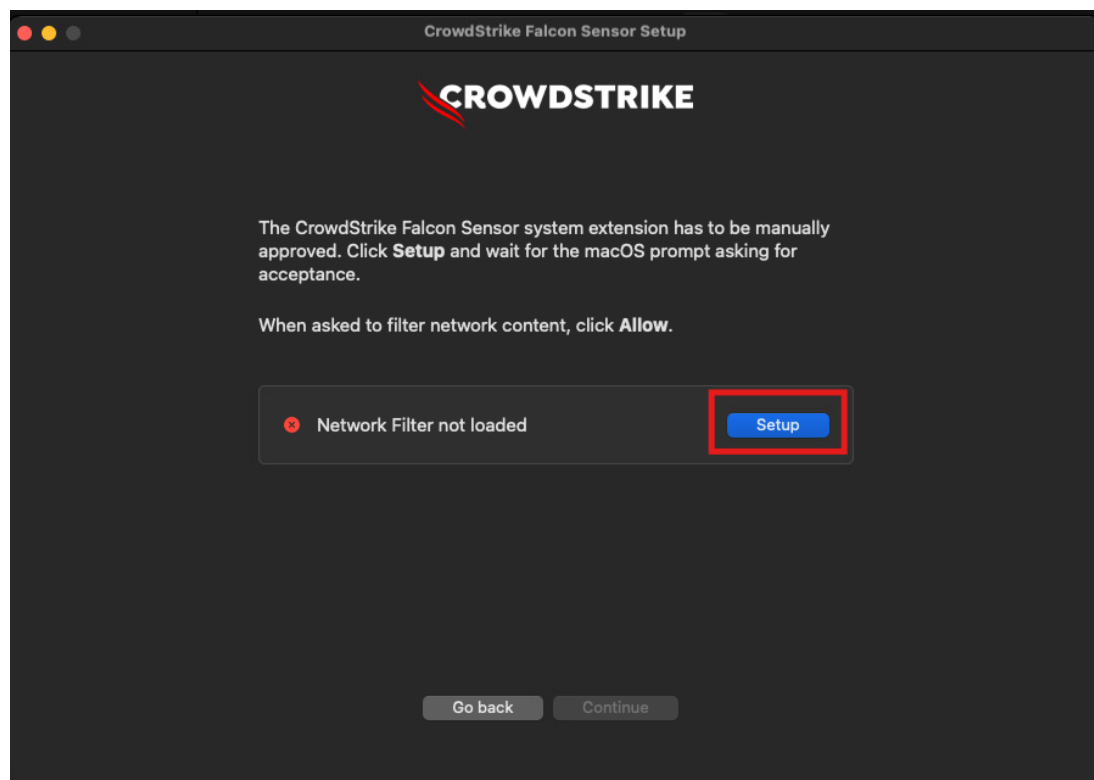


Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

6. Click **Setup** và khi có bảng thông báo hiện lên, click **Allow** để cho phép **network content filtering** > Chọn **Continue**.



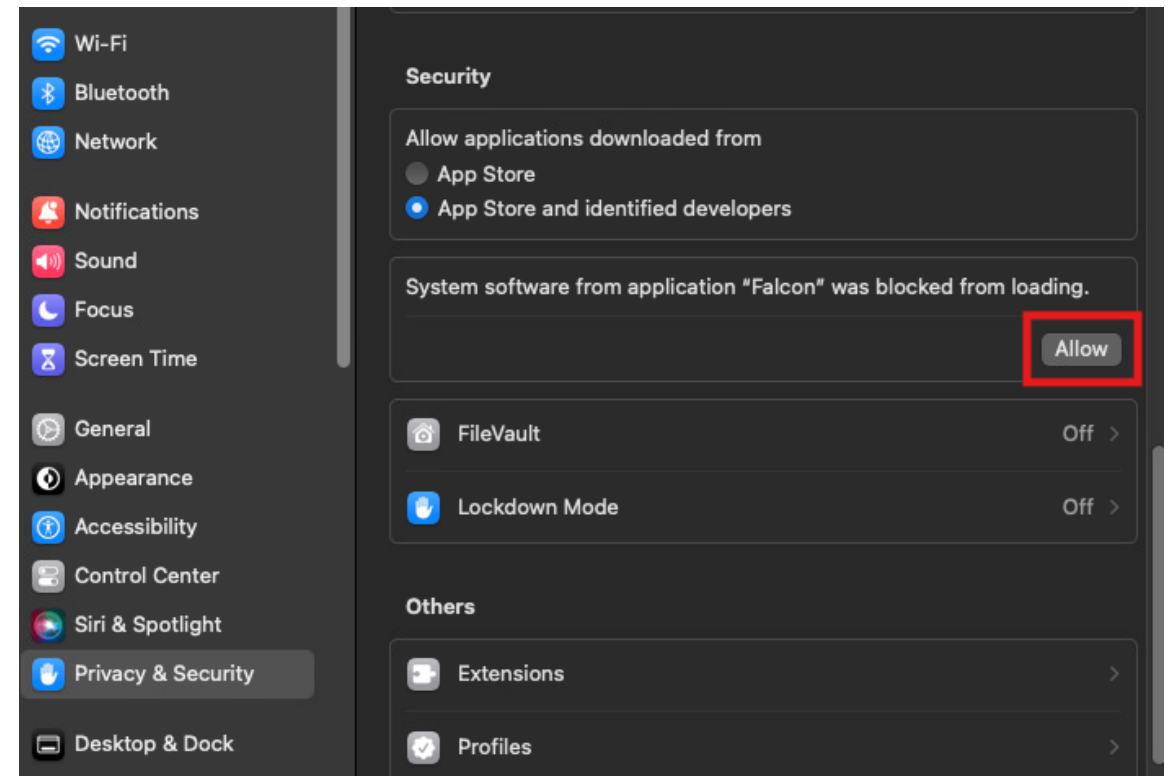
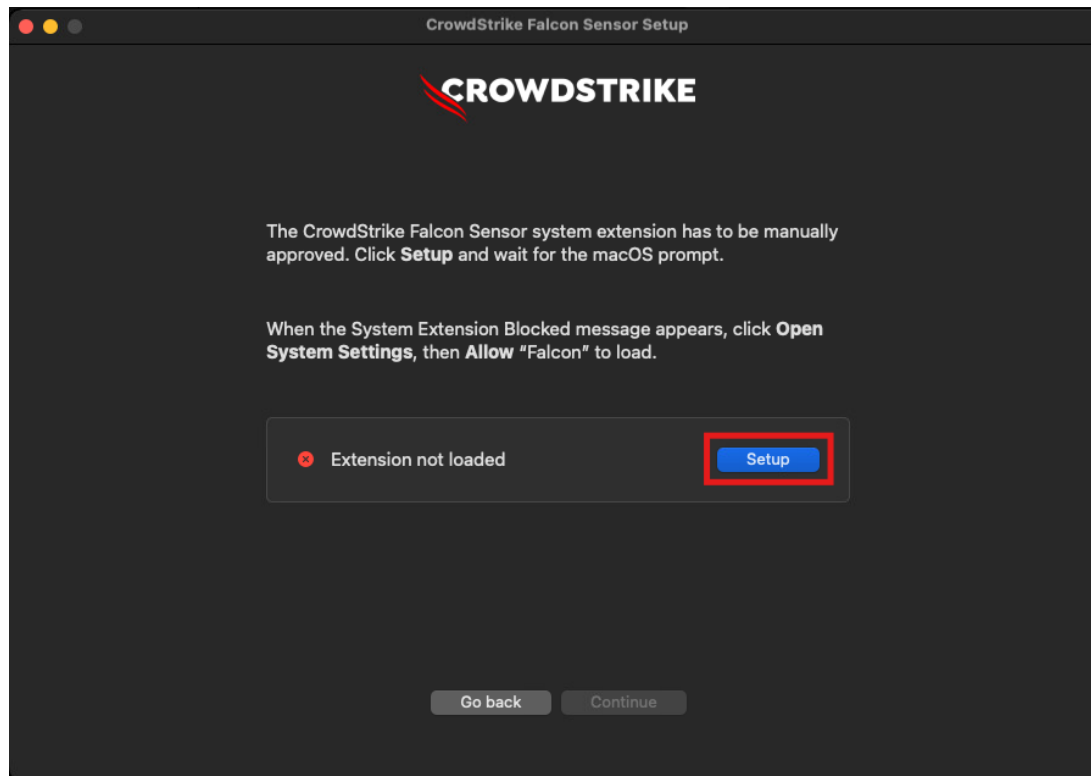
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

7. Click **Setup** và khi có bảng thông báo hiện lên, click **Open System Settings**. Trong Security section, click **Allow** để cho phép **system extension access**.

Khi có bảng thông báo hiện lên, đăng nhập bằng user có quyền quản trị và click **Modify Settings** > Chọn **Continue**.



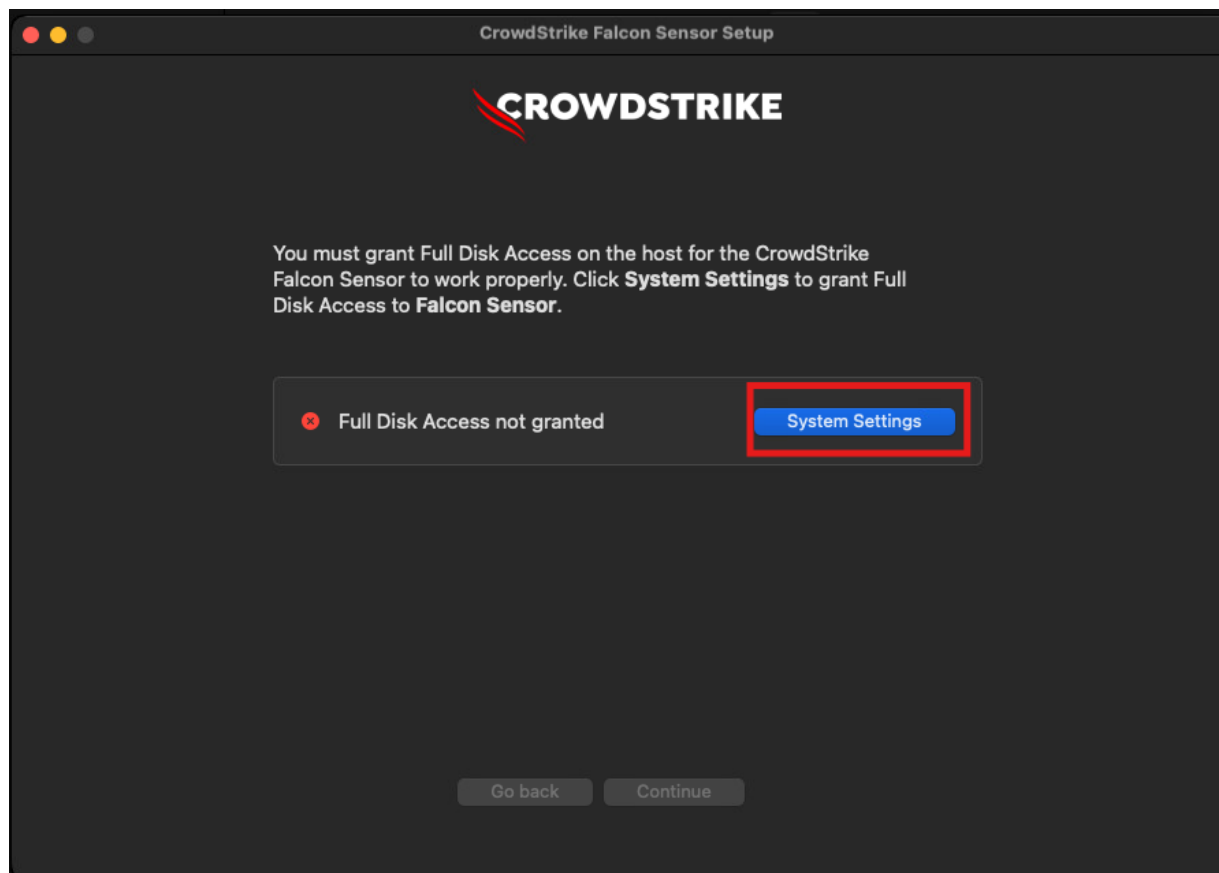
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

8. Click **System Settings** trong cửa sổ cài đặt.

Tại MacOS **Privacy & Security** > Chọn **Full Disk Access**.



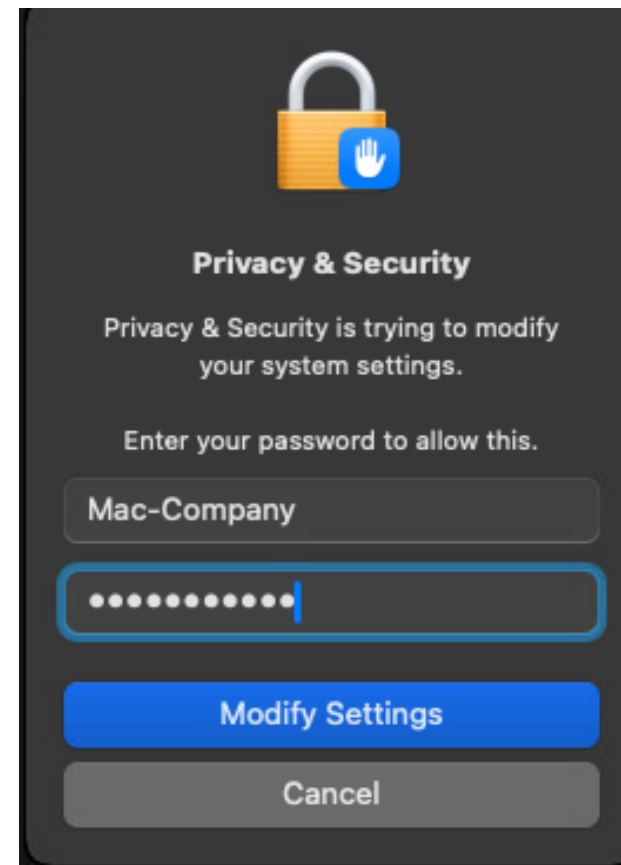
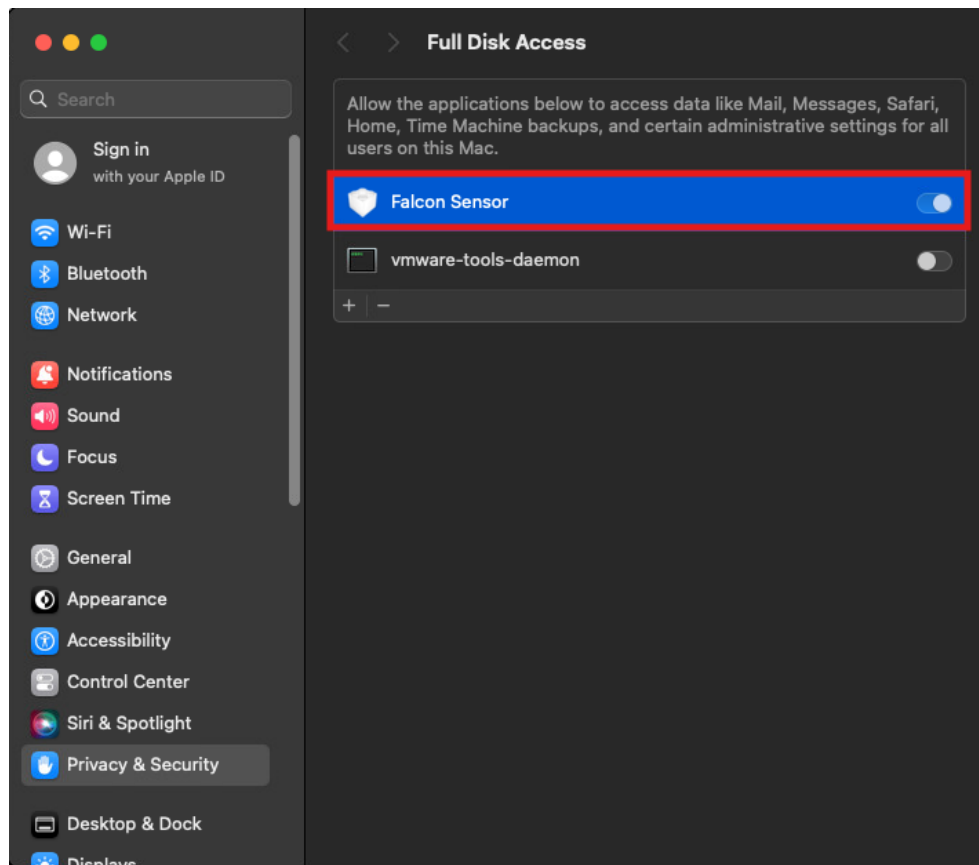
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

9. Trong **Full Disk Access** section, cho phép Falcon Sensor quyền **Full Disk Access**.

Khi có bảng thông báo hiện lên, đăng nhập bằng user có quyền quản trị và click **Modify Settings** > Chọn **Continue**.



Case #2: Cài Đặt Falcon Sensor

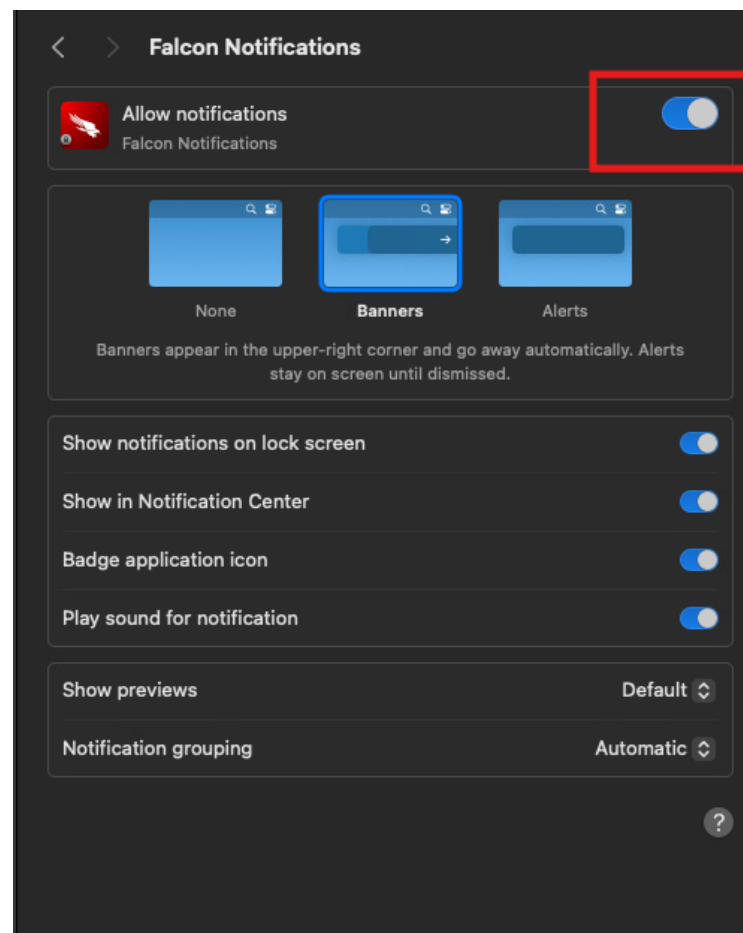
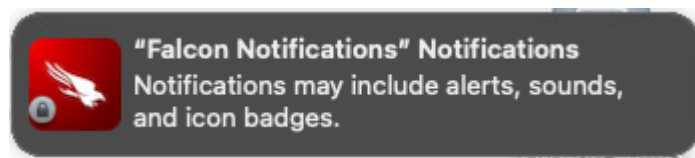
Cài Đặt Falcon Sensor Thủ Công

MacOS:

10. Click vào thông báo Falcon notifications.

Ngoài ra, bạn có thể nhấp vào Notifications trong thanh bên của cửa sổ System Settings trên macOS. Trong phần Application Notifications, tìm Falcon Notifications.

Kích hoạt để cho phép thông báo từ Falcon.

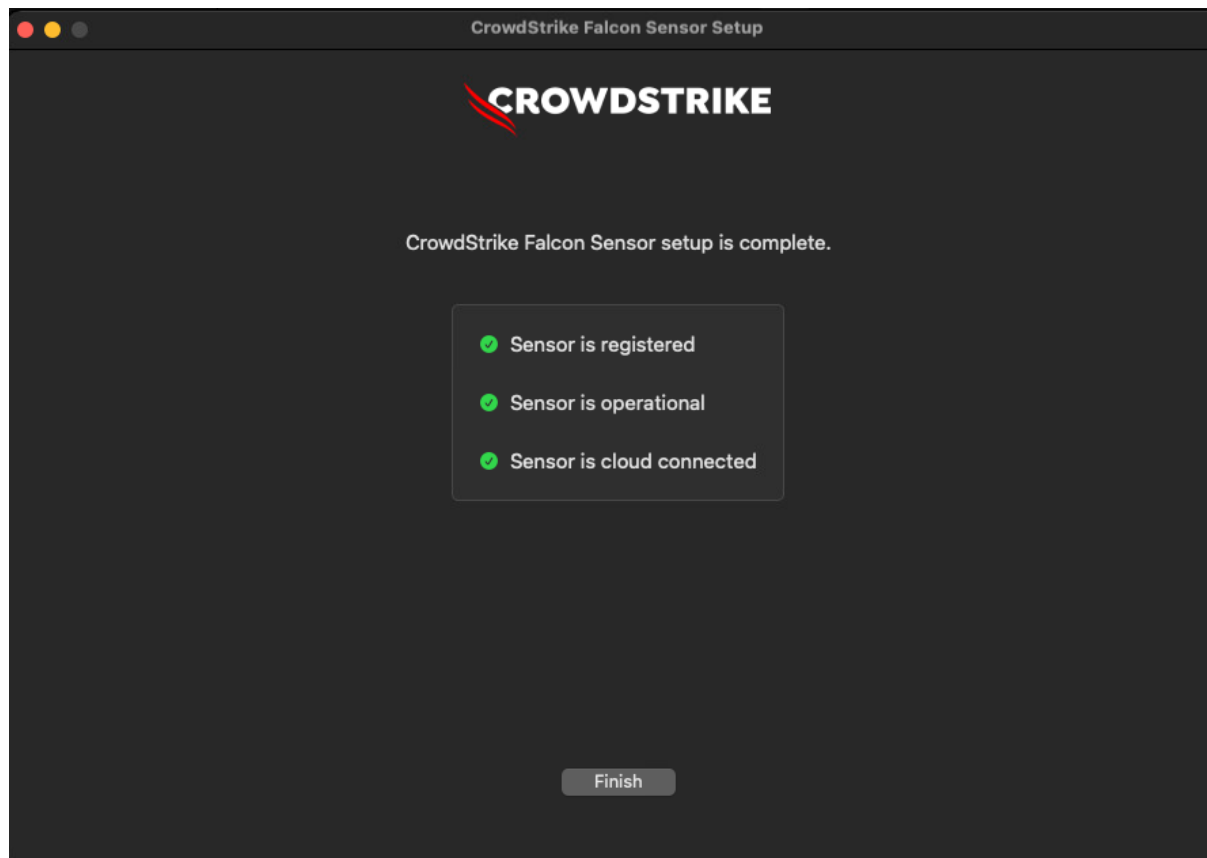


Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

11. Một cài đặt hoàn chỉnh với ba dấu tích màu xanh. Dấu tích màu xanh cho biết cảm biến đã được cài đặt thành công, đã đăng ký, hoạt động và kết nối với CrowdStrike Cloud.



Case #2: Quản Lý Host

Tổng quan

Xem thông tin quan trọng về các host của khách hàng và quản lý chúng bằng cách thực hiện các hành động như thêm hoặc xóa Grouping tags, cập nhật trạng thái cách ly, kích hoạt hoặc vô hiệu hóa các detection.

Yêu cầu:

- **Subscription:** Host management bao gồm trong tất cả các subscription.
- **Default roles:** Quản lý host groups có thể được thực hiện bởi các default roles
- Những default roles có thể thấy host management section và quản lý các host group:
 - + **Falcon Administrator**
 - + **Endpoint Manager**
- Những default roles có thể thấy host management nhưng không thể quản lý host groups:
 - + **Prevention Policy Manager**
 - + **Falcon Analyst**
 - + **Help Desk Analyst**

Case #2: Quản Lý Host

Thông tin tổng quan của host

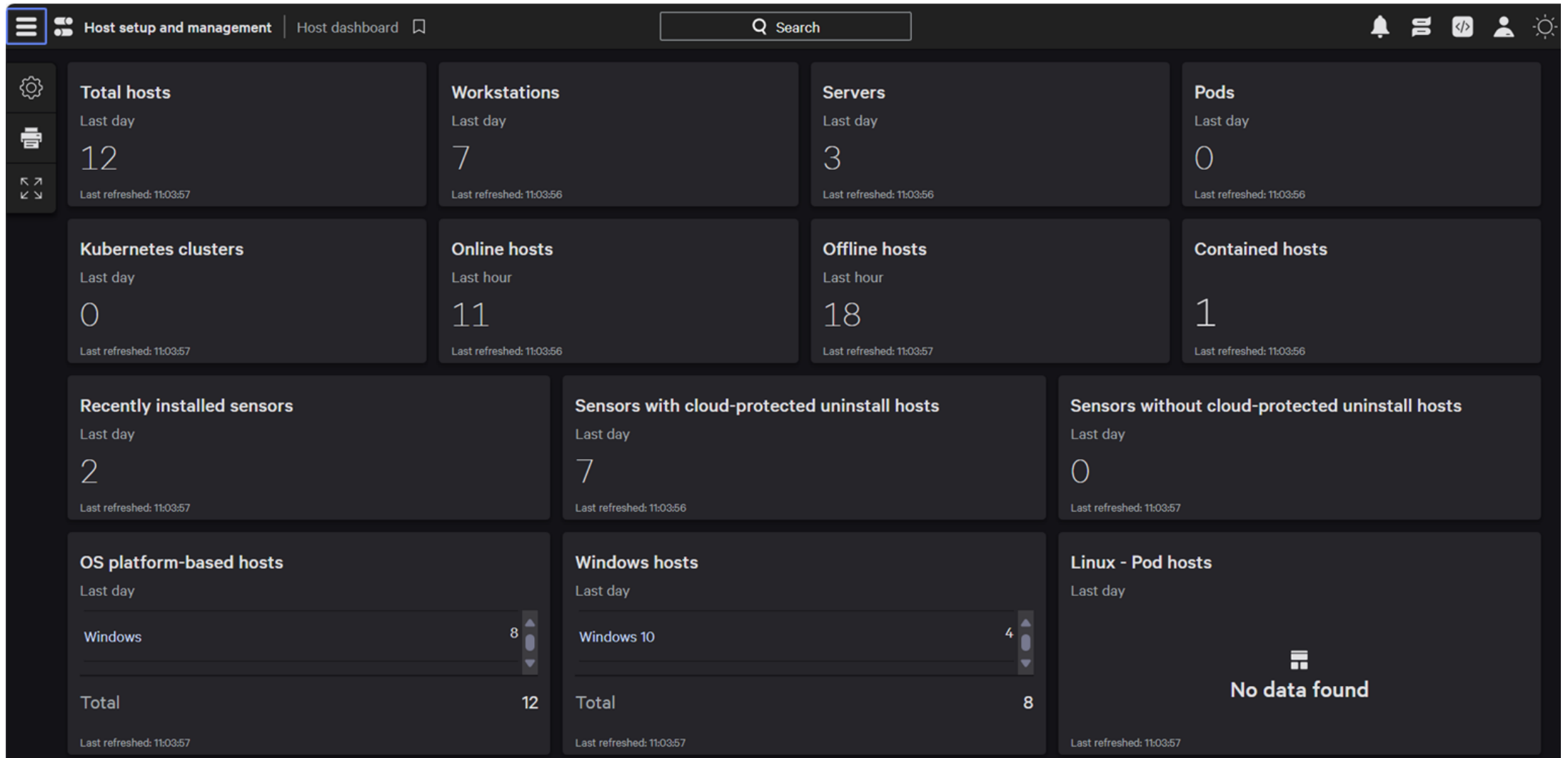
1. **Bảng tổng quan của host** hiển thị thông tin chi tiết về các host của khách hàng như là số lượng host theo loại host, số lượng host online hoặc offline, số lượng host trên mỗi nền tảng và hệ điều hành,.... Bảng điều khiển cũng hiển thị thông tin tổng quan cấp độ cao về pod cho các cloud container được bảo mật bằng Falcon Container Sensor Linux.

The screenshot displays the 'Host setup and management' dashboard. The left sidebar contains a navigation menu with items like Identity protection, Exposure management, Counter Adversary Operations, Investigate, Fusion SOAR, Foundry, Asset inventory, Attack path analysis, and Dashboards and reports. The 'Host setup and management' item is highlighted with a red box. The main content area shows a 'Host dashboard' menu with 'Host dashboard' highlighted by a red box. Below this are sections for 'Host management' (Updated), 'Host groups', 'Content update states' (New), 'Host retention policies' (New), 'Zero trust assessment', 'Sensor health', 'Inactive sensors', 'Sensor coverage lookup', 'Falcon icon policies', and 'Monitor deployment' (New). The dashboard also features several summary cards: 'Servers' (3), 'Offline hosts' (18), 'Sensors with cloud-protected uninstall hosts' (7), and 'Windows hosts'. The top navigation bar includes 'Host setup and management', 'Host dashboard', and a search bar.

Case #2: Quản Lý Host

Thông tin tổng quan của host

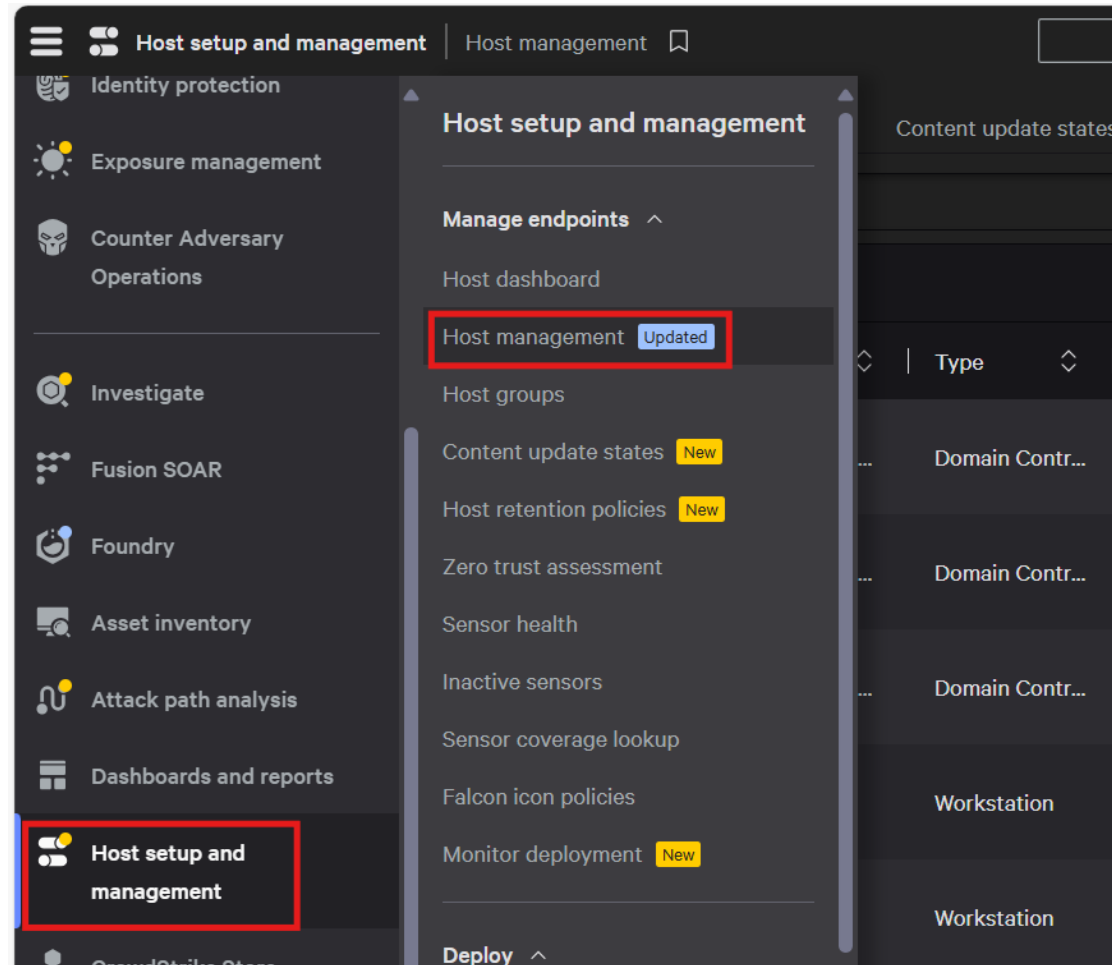
2. Ví dụ về Host dashboard



Case #2: Quản Lý Host

Trang Host Management

1. Trên trang **Host Management**, xem thông tin về mỗi host bao gồm OS, loại host, prevention policy được áp dụng tới host, trạng thái cách ly của host và phiên bản của sensor.



Case #2: Quản Lý Host

Trang Host Management

2. Từ trang **Host Management**, có thể xem prevention policy nào được áp dụng cho một host. Cột Prevention Policy có thể có các giá trị sau:

- "No Policy" - Nếu host vừa được cài đặt Falcon Sensor và Falcon Cloud vẫn chưa đánh giá chính sách nào là phù hợp, hoặc host không còn hoạt động.
- "{Policy Name}" & "{Applied Date}" – Tên của policy đã được đẩy xuống host và thời gian mà host nhận được policy.
- "{Policy Name}" & "Changes pending" - Tên của policy sẽ được đẩy xuống host.
- "Policy Deleted" & "Changes pending" – Host có một policy đã bị xóa và Falcon Cloud vẫn chưa xác định policy mới nào mà Sensor nên nhận. Trong thời gian chuyển tiếp này, host sẽ tiếp tục sử dụng policy đã được áp dụng trước đó trong khi chờ nhận policy mới từ Falcon Cloud.

Prevention po...	Sensor updat...	Content upda...	Host retentio...	
Mar. 11, 202...	Mar. 11, 202...	Mar. 11, 202...	Mar. 11, 202...	•
Prevention po... Changes pen...	Uninstall Policy Apr. 2, 2025...	Default (all) Mar. 10, 202...	Default Policy... Mar. 10, 202...	•
Default (Wind... Apr. 2, 2025...	Default (Wind... Apr. 2, 2025...	Default (all) Apr. 2, 2025...	Default Policy... Apr. 2, 2025...	•
Default (Wind... Mar. 7, 2025...	Default (Wind... Mar. 7, 2025...	Default (all) Mar. 7, 2025...	Default Policy... Mar. 7, 2025...	•
Default (Wind... Mar. 11, 202...	Default (Wind... Mar. 11, 202...	Default (all) Mar. 11, 202...	Default Policy... Mar. 11, 202...	•
Malware Prev... Mar. 12, 202...	Default (Wind... Mar. 10, 202...	Default (all) Mar. 10, 202...	Default Policy... Mar. 10, 202...	•
Malware Prev... Mar. 3, 2025...	Policy deleted Changes pen...	Default (all) Mar. 3, 2025...	Default Policy... Mar. 3, 2025...	•

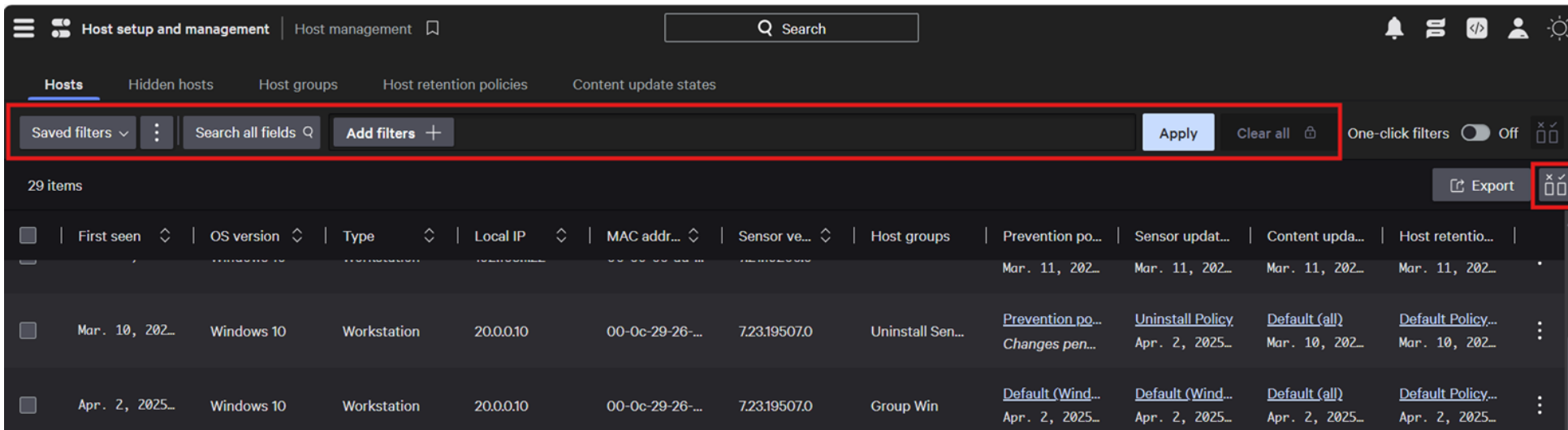
Case #2: Quản Lý Host

Trang Host Management

3. Trang **Host Management** có thể lọc, tìm kiếm, và tùy chỉnh các cột giúp tìm kiếm và quản lý host tốt hơn.

Sử dụng thanh lọc ở trên cùng để tìm kiếm một host cụ thể, hoặc nhấp vào các bộ lọc mặc định để xem nhiều mục tiêu hơn.

Để chọn các cột hiển thị trong bảng Host Management, nhấp vào biểu tượng , sau đó chọn các cột mong muốn.



The screenshot displays the Host Management interface with a search bar and filter controls highlighted by a red box. The interface includes a search bar, a filter bar with 'Saved filters', 'Search all fields', and 'Add filters' buttons, and an 'Apply' button. Below the filter bar, there are 'One-click filters' and 'Export' buttons. The main table shows a list of hosts with columns for 'First seen', 'OS version', 'Type', 'Local IP', 'MAC address', 'Sensor version', 'Host groups', 'Prevention policies', 'Sensor updates', 'Content updates', and 'Host retention policies'. The table contains 29 items.

	First seen	OS version	Type	Local IP	MAC address	Sensor version	Host groups	Prevention policies	Sensor updates	Content updates	Host retention policies
	Mar. 11, 202...	Windows 10	Workstation	20.0.0.10	00-0c-29-26-...	7.23.19507.0	Uninstall Sen...	Prevention po... Changes pen...	Uninstall Policy Apr. 2, 2025...	Default (all) Mar. 10, 202...	Default Policy... Mar. 10, 202...
	Apr. 2, 2025...	Windows 10	Workstation	20.0.0.10	00-0c-29-26-...	7.23.19507.0	Group Win	Default (Wind... Apr. 2, 2025...	Default (Wind... Apr. 2, 2025...	Default (all) Apr. 2, 2025...	Default Policy... Apr. 2, 2025...

Case #2: Quản Lý Host

Trang Host Management

4. Ví dụ bảng Host management

The screenshot shows the 'Host management' page with a table of 29 items. The table columns are: Hostname, Last seen, First seen, OS version, Type, Local IP, MAC address, Sensor version, Host groups, Prevention policy, and Sensor update. A yellow vertical bar highlights the MAC address column.

Hostname	Last seen	First seen	OS version	Type	Local IP	MAC address	Sensor version	Host groups	Prevention policy	Sensor update
AD2	Mar. 12, 202...	Mar. 12, 202...	Windows Ser...	Domain Contr...	10.22.0.102	-ad-...	7.21.19205.0		Default (Wind...	Default (Wind...
DC-1	Apr. 3, 2025...	Mar. 12, 202...	Windows Ser...	Domain Contr...	20.0.0.2	-53-...	7.22.19409.0	Lab_Server_G...	Prevention po...	Test
DC-2	Apr. 3, 2025...	Mar. 27, 202...	Windows Ser...	Domain Contr...	20.0.0.3	-ad-...	7.22.19409.0	Lab_Server_G...	Prevention po...	Test
DESKTOP-5E...	Mar. 3, 2025...	Feb. 28, 202...	Windows 10	Workstation	192.168.4.135	-a5-...	7.21.19205.0		Default (Wind...	Default (Wind...
DESKTOP-DO...	Mar. 23, 202...	Mar. 17, 202...	Windows 10	Workstation	192.168.64.1	-c0-...	7.22.19406.0	Group Win, La...	Prevention po...	Default (Wind...

Case #2: Quản Lý Host

Trang Host Management

5. Xem bảng tổng quan host

Để mở bảng tổng quan host, chọn vào một host trong list.

Lưu ý: Thông tin hiển thị trên bảng tổng quan host thay đổi tùy theo gói đăng ký sản phẩm Falcon và user role của bạn.

Thông tin trạng thái của host và các liên kết nhanh để thực hiện các hành động khác nhau có sẵn ở trên cùng của bảng:

- Xem trạng thái trực tuyến hiện tại của host:
 - + **Online** (blue): Host đã được nhìn thấy gần đây, và chúng tôi tự tin rằng nó hiện đang trực tuyến..
 - + **Offline** (gray): Host chưa được nhìn thấy trong một thời gian, và chúng tôi tự tin rằng nó hiện đang ngoại tuyến.
 - + **Unknown** (amber): Host chưa được nhìn thấy gần đây, và chúng tôi không tự tin về trạng thái hiện tại của nó.
- Kết nối với host và thực hiện các hành động phản ứng theo thời gian thực
- Vô hiệu hóa hoặc kích hoạt lại các detection trên host
- Xem và thay đổi trạng thái cách ly của host
- Xóa host
- Lấy mã host maintenance token để gỡ cài đặt sensor

The screenshot displays the 'Host information' page for host 'DC-1'. The 'Host info' section is highlighted with a red box, showing the 'Host status' as 'Online' with a blue dot. The 'Actions' menu is also highlighted with a red box, listing various actions such as 'Network contain host', 'Lift file system containment', 'Host timeline', 'Disable detections', 'Asset details', 'Asset graph', 'Host search', 'Add grouping tags', and 'Remove grouping tags'. The page also shows 'Network containment status' as 'Normal', 'File system containment status' as 'Normal', and 'First seen' as 'Mar. 12, 2025 09:34:32'. Other details include 'Serial number' (VMware-56 4d 8d 91 fe 23 86 e3-1...), 'Local IP' (20.0.0.2), and 'Default gateway IP'.

Case #3: Quản Lý Nhóm Host

Tổng quan

Các nhóm host cho phép gán các thiết lập policy, nâng cấp Sensor, tùy chỉnh đường dẫn tệp ngoại lệ và nhiều hơn nữa. Các host có thể thuộc nhiều nhóm khác nhau, giúp điều chỉnh policy và các thiết lập cấu hình khác theo nhu cầu của môi trường khách hàng.

Phân loại:

Có hai loại nhóm host: **dynamic** và **static**. Loại nhóm được chọn khi bạn tạo nhóm host và không thể thay đổi sau đó.

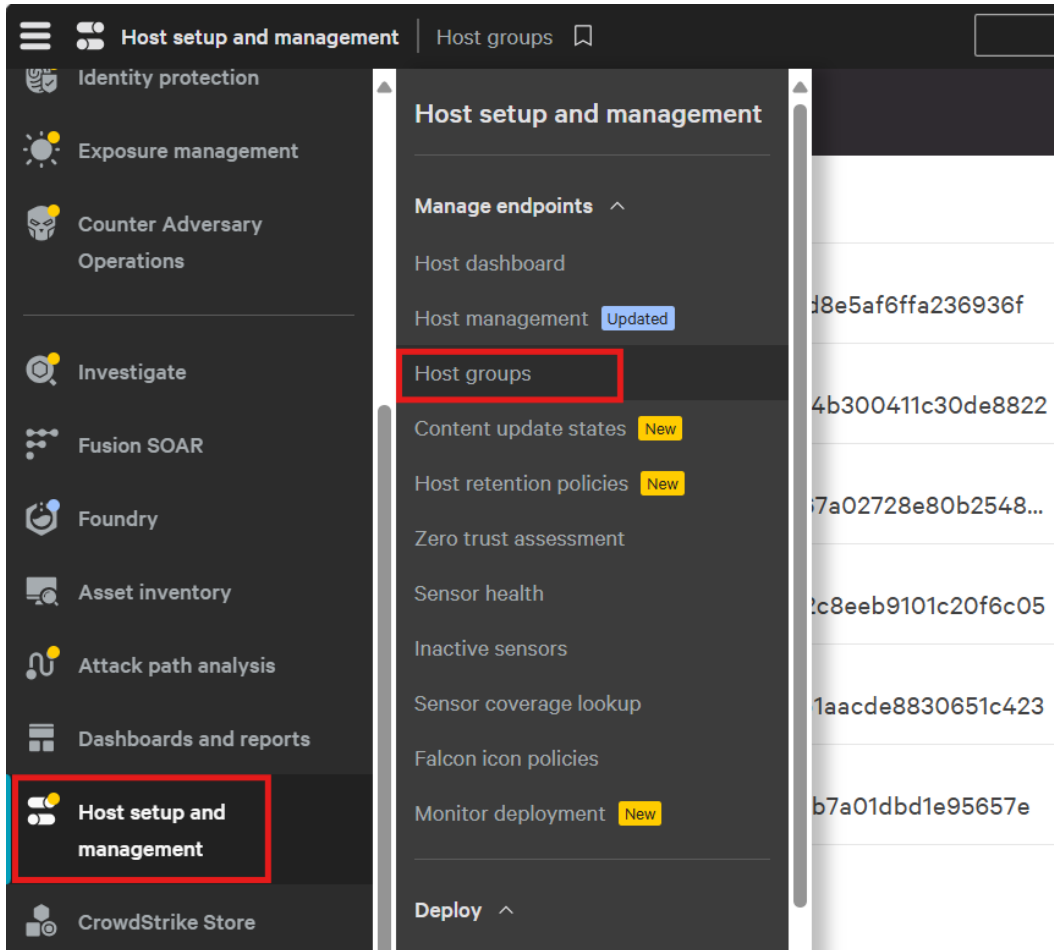
- Nhóm host dynamic sẽ trống sau khi tạo. Để thêm host, định nghĩa bộ lọc dựa trên các thuộc tính như thẻ nhóm, dải IP/CIDR, phiên bản hệ điều hành, OU Active Directory, hoặc tiền tố/hậu tố của tên host. Khi có các host phù hợp với quy tắc đã thiết lập từ trước, chúng sẽ tự động được thêm vào nhóm. Khi có một host không còn phù hợp với quy tắc đã thiết lập, nó sẽ tự động bị xóa. Chúng tôi khuyên bạn nên sử dụng nhóm host dynamic trong hầu hết các trường hợp.
- Nhóm host static được định nghĩa thủ công. Nhóm host static phù hợp cho các host trong môi trường tĩnh, chẳng hạn như QA hoặc cho mục đích thử nghiệm, hoặc khi bộ lọc nhóm host dynamic không đủ. Khi tạo một nhóm host static, bạn phải chọn cách thêm host bằng hostname hoặc host ID (còn gọi là agent ID). Bạn có thể thêm host vào nhóm host static bằng bất kỳ phương pháp nào sau đây:
 - Bằng cách chọn host thông qua sử dụng bộ lọc trong Falcon console
 - Bằng cách nhập thủ công host trong Falcon console
 - Bằng cách tải lên một tệp văn bản chứa danh sách các host

Case #3: Quản Lý Nhóm Host

Tạo một nhóm host

1. Điều hướng tới **Host setup and management > Manage endpoints > Host groups**.

Chọn **Add New Group**.



GROUP TYPE	CREATED BY	
Dynamic	[REDACTED]	
Dynamic	[REDACTED]	
Static by hostname	[REDACTED]	
Static by hostname	[REDACTED]	
Static by host ID	[REDACTED]	
Static by host ID	[REDACTED]	

Case #3: Quản Lý Nhóm Host

Tạo một nhóm host

2. Điền tên, mô tả

- Chọn **group type**: **Dynamic**, **Static theo host ID** hoặc **Static theo hostname**.
- Chọn **ADD GROUP**

New Group Details

NAME
Windows Group

DESCRIPTION

Group Type

One type per group, and type can't be switched later. [About host groups](#)

Dynamic
Create a rule to automatically add and remove hosts based on filters

Static by host ID
Add or remove hosts based on host ID

Static by hostname
Add or remove hosts based on hostname

CANCEL ADD GROUP

Case #3: Quản Lý Nhóm Host

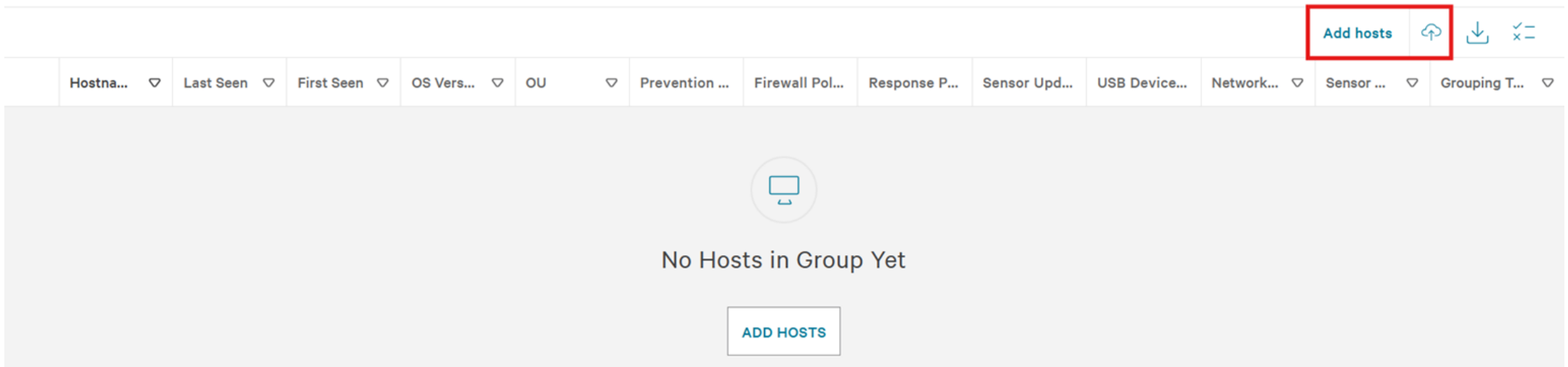
Tạo một nhóm host

3. Gán các host vào một nhóm host

- Gán các host vào một nhóm static

- + Bạn có thể gán host vào nhóm static bằng cách chọn host hiện có trong console hoặc tải lên danh sách host ID hoặc hostname.
- + Khi tải lên các host bằng hostname, Falcon kiểm tra xem hostname tải lên có khớp với các host hiện có trong Falcon console hay không. Nếu bạn muốn thêm host vào nhóm trước khi triển khai Sensor, bạn có thể tắt tính năng xác nhận tính hợp lệ của host.
- + **Note:** Bạn có thể gán tới 1,000 host vào một nhóm static cùng lúc.
- + Tại trang của nhóm static group > Chọn **Add hosts** nếu chọn host có sẵn trong Falcon console hoặc **Upload Hosts** nếu muốn tải lên danh sách host thủ công.

Hosts currently targeted by this group



The screenshot shows the Falcon console interface for a static group. At the top right, there is a toolbar with four icons: 'Add hosts' (highlighted with a red box), a refresh icon, a download icon, and a close icon. Below the toolbar is a table header with columns: Hostna..., Last Seen, First Seen, OS Vers..., OU, Prevention..., Firewall Pol..., Response P..., Sensor Upd..., USB Device..., Network..., Sensor..., and Grouping T... The main content area is a large grey box with a computer icon and the text 'No Hosts in Group Yet'. At the bottom center of this box is a button labeled 'ADD HOSTS'.

Case #3: Quản Lý Nhóm Host

Tạo một nhóm host

3. Gán các host vào một nhóm host

- Gán các host vào một nhóm static

+ Chọn các host trong Falcon console:

- Chọn vào checkbox kế bên mỗi host muốn gán vào nhóm. Chọn bộ lọc để thu hẹp lại danh sách các host được hiển thị.
- Chọn **Add** để gán các host đã chọn vào nhóm.
- Chọn **Add hosts** trong bảng hộp thoại để thêm host.
- Chọn **Done** ở góc phải để hoàn thành việc gán host vào group.

The screenshot shows the Falcon console interface for host management. At the top, there's a search bar and a notification area. Below that, a message says "Select hosts to add to 'Windows Group'. Use filters to help you find them." A button labeled "0 hosts in Windows Group" and a "DONE" button are visible. A filter bar shows "14 Hosts found". The main table lists hosts with columns for Platform, OS Version, OU, Site, Type, Network Containment, and Grouping Tags. Below the table, a summary bar shows "Selected 4 of 14 hosts" and an "Add" button. The table below shows the selected hosts:

Platform	OS Version	OU	Site	Type	Network Containment	Grouping Tags
Windows	9 Windows 10	5 N/A	12 N/A	10 Workstation	8 Status	N/A 14
Linux	3 Ubuntu 22.04	3 Domain Controllers	2 Default-First-Site-Name	4 Server	4 Normal 14	
Mac	2 Windows Server 2022	3 Sequoia (15) Sonoma (14)		2 Domain Controller		

Hostname	Last Seen	First Seen	OS Version	Prevention Poli...	Firewall Policy	Response Policy	Sensor Update...	Network Co...	Sensor Ver...	Grouping Tags
<input type="checkbox"/> DC-1	Apr. 4, 2025 0...	Mar. 12, 2025 0...	Windows Serv...	Prevention pol... Mar. 27, 2025 1...	Default (Windo... Mar. 12, 2025 0...	Response_Poli... Mar. 27, 2025 1...	Test Mar. 28, 2025 ...	Normal	7.22.19409.0	
<input type="checkbox"/> DC-2	Apr. 4, 2025 0...	Mar. 27, 2025 1...	Windows Serv...	Prevention pol... Mar. 27, 2025 1...	Default (Windo... Mar. 27, 2025 1...	Response_Poli... Mar. 27, 2025 1...	Test Mar. 28, 2025 ...	Normal	7.22.19409.0	
<input checked="" type="checkbox"/> DESKTOP-DO9...	Mar. 23, 2025 ...	Mar. 17, 2025 1...	Windows 10	Prevention pol... Mar. 17, 2025 1...	FW_Policies fo... Mar. 22, 2025 1...	Response_Poli... Mar. 17, 2025 1...	Default (Windo... Mar. 17, 2025 1...	Normal	7.22.19406.0	
<input checked="" type="checkbox"/> DESKTOP-K80...	Apr. 2, 2025 11...	Mar. 10, 2025 1...	Windows 10	Prevention pol... Changes pendi...	FW_Policies fo... Apr. 2, 2025 12...	Default (Windo... Mar. 10, 2025 1...	Uninstall Policy Apr. 2, 2025 12...	Normal	7.23.19507.0	
<input checked="" type="checkbox"/> DESKTOP-K80...	Apr. 4, 2025 0...	Apr. 2, 2025 15...	Windows 10	Default (Windo... Apr. 2, 2025 15...	Default (Windo... Apr. 2, 2025 15...	Default (Windo... Apr. 2, 2025 15...	Default (Windo... Apr. 2, 2025 15...	Normal	7.23.19507.0	

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

Tổng quan

CrowdStrike Falcon sử dụng nhiều phương pháp khác nhau để phát hiện cả các mối đe dọa đã biết và chưa biết. Điều này giúp đảm bảo việc phát hiện và ngăn chặn các cuộc tấn công ở nhiều giai đoạn, và cũng là lý do tại sao việc kích hoạt tất cả các chính sách ngăn chặn được khuyến nghị là rất quan trọng.

Chính Sách Ngăn chặn

- Sử dụng Prevention Policies để quản lý hoạt động sẽ kích hoạt các phát hiện và ngăn chặn trên các host của bạn, mà bạn sẽ theo dõi trong trang Activity. Các chính sách được gán cho các host trong nhóm host. Tùy theo nền tảng mà các thiết lập ngăn chặn sẽ khác nhau.
- Bạn có thể có tối đa 100 chính sách tùy chỉnh.

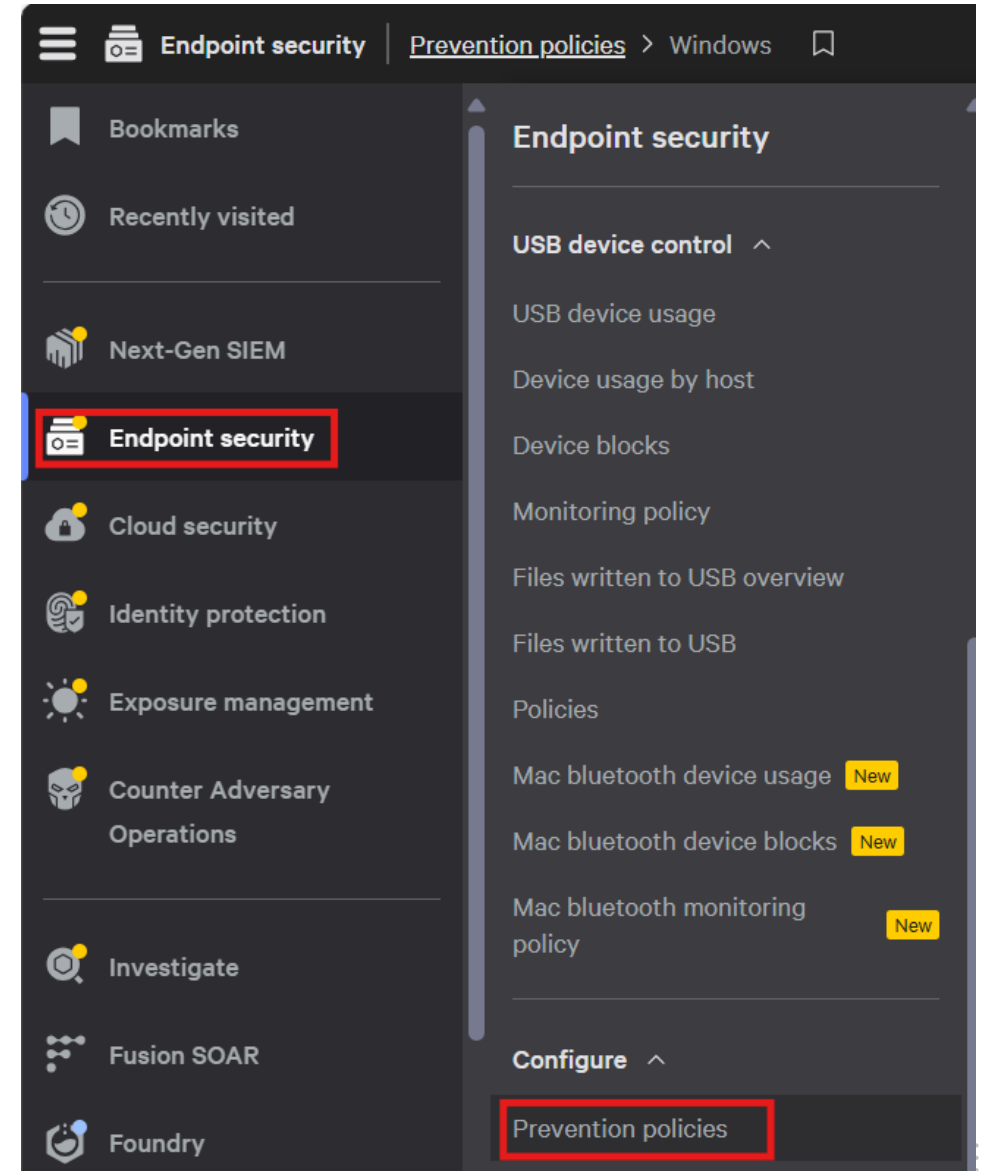
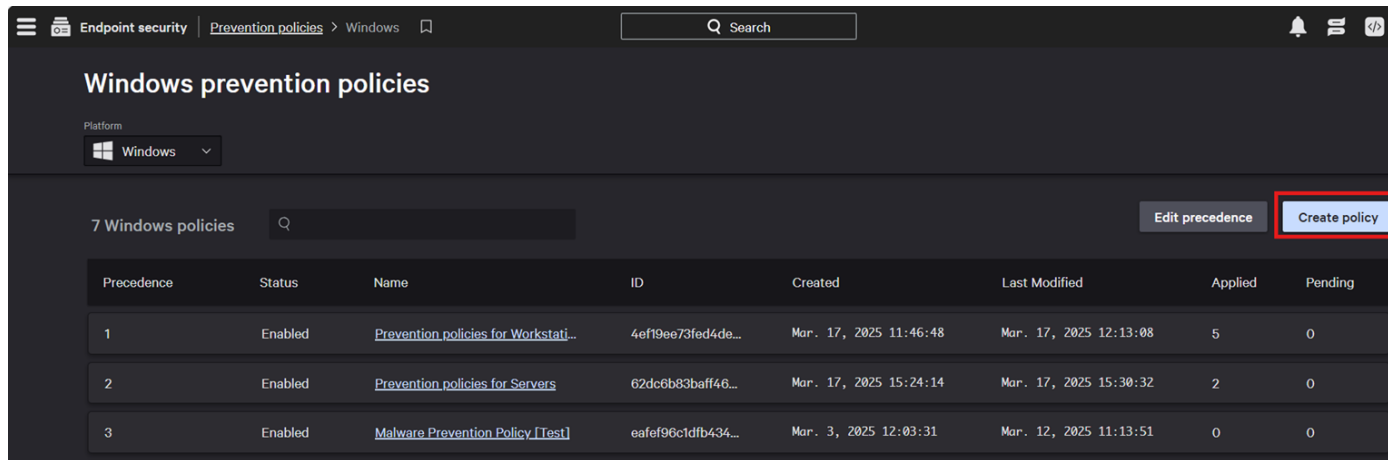
Thiết Lập Chính Sách Ngăn Chặn

- Kiểm tra tất cả các chính sách đã thay đổi trong môi trường thử nghiệm trước và sau đó triển khai các thay đổi vào môi trường chính theo từng giai đoạn. Bạn có thể phân loại các phát hiện và điều chỉnh cài đặt khi cần thiết để thấy ít kết quả dương tính giả hơn, sử dụng quản lý IOC, ML và IOA exclusion.
- Đối với các khách hàng mới, chúng tôi khuyên bạn nên áp dụng phương pháp ba giai đoạn để cấu hình các chính sách ngăn chặn.

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

1. Tạo chính sách

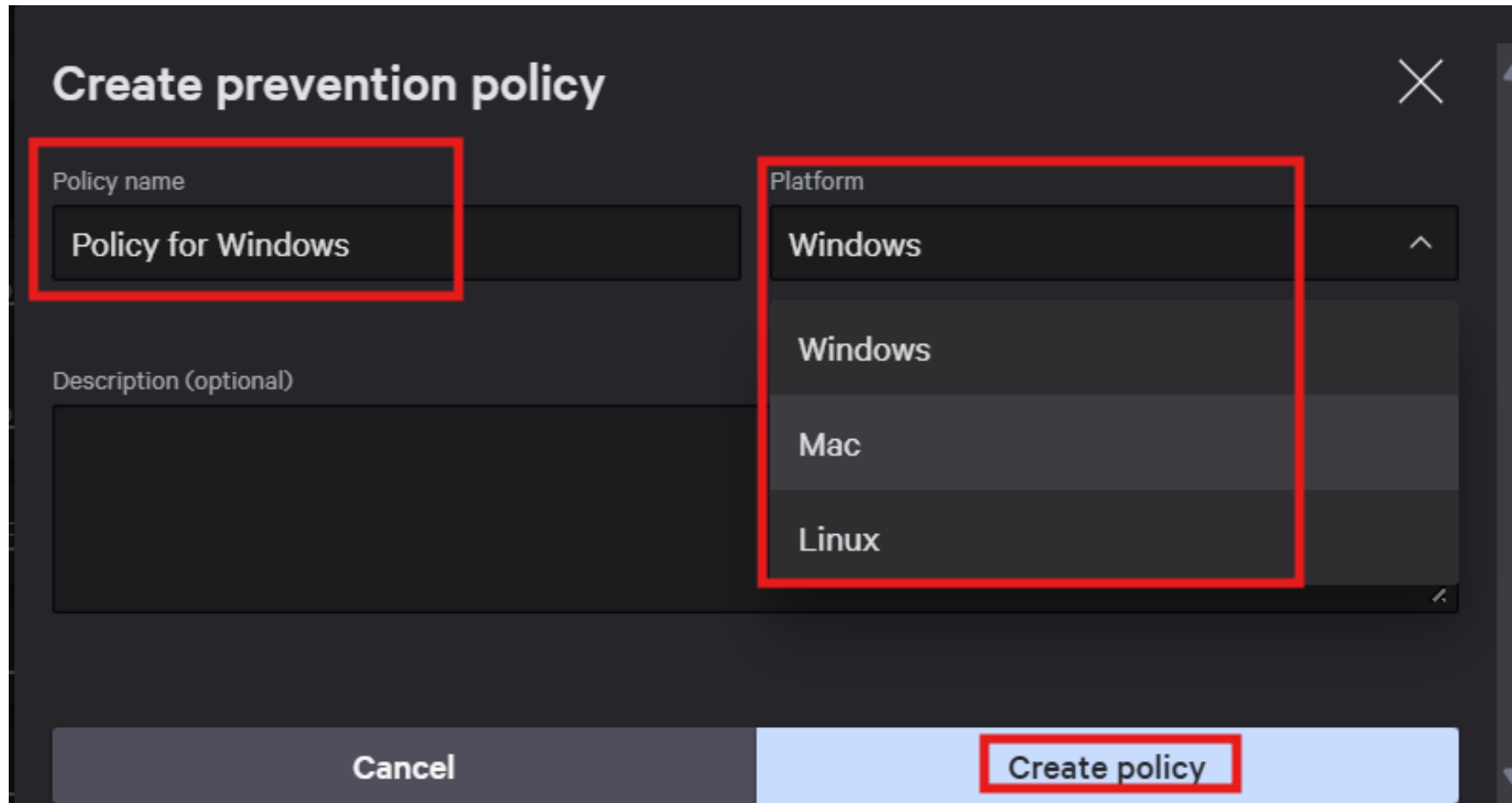
- Di chuyển tới Endpoint security > Configure > Prevention policies.
- Chọn Create policy.



Case #4: Chính Sách Phát Hiện và Ngăn Chặn

1. Tạo chính sách

- Điền các thông tin về **platform**, **policy name**, và **description**.
- Chọn **Create Policy**



The screenshot shows a dark-themed dialog box titled "Create prevention policy" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Policy name:** A text input field containing "Policy for Windows".
- Platform:** A dropdown menu with "Windows" selected. The dropdown is open, showing a list of options: "Windows", "Mac", and "Linux".
- Description (optional):** A large empty text area for entering a description.
- Buttons:** At the bottom, there are two buttons: "Cancel" on the left and "Create policy" on the right. The "Create policy" button is highlighted with a red border.

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

1. Tạo chính sách

- **Enable** hoặc **disable** các thiết lập ngăn chặn trong tab **Settings**.
- Để lưu các thiết lập ngăn chặn, chọn **Save**, sau đó chọn **Confirm**.
- Để bật chính sách, chọn **Enable policy**.

The screenshot displays the 'Policy for Windows' configuration page in the Microsoft Defender for Endpoint console. The policy is currently 'Disabled'. The 'Settings' tab is selected, showing a list of settings. Three settings are checked: 'End user notifications', 'Unknown executable analysis', and 'Unknown detection-related executable anal...'. The 'Save' button is highlighted with a red box. A tooltip for 'Interpreter-only visibility' is visible on the right side of the screen.

Setting Name	Required setting is OFF	Compare
Sensor capabilities		
End user notifications	<input checked="" type="checkbox"/>	
Unknown executable analysis	<input checked="" type="checkbox"/>	
Unknown detection-related executable anal...	<input checked="" type="checkbox"/>	

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

2. Gán chính sách ngăn chặn vào một group host

- Đi đến tab **Assigned Host Groups**.
- Chọn **Assign host groups to policy**

The screenshot displays the 'Policy for Windows' configuration page in the Microsoft Defender console. The page is currently in a 'Disabled' state. The 'Assigned host groups' tab is highlighted with a red box. Below the tab, a message states 'No host groups assigned yet' with a large minus sign icon. A button labeled 'Assign host groups to policy' is also highlighted with a red box. The page includes a search bar, navigation tabs (Settings, Assigned host groups, Assigned custom IOAs, Audit log), and a table with columns for Name and Hosts. The table is currently empty.

Name	Hosts
------	-------

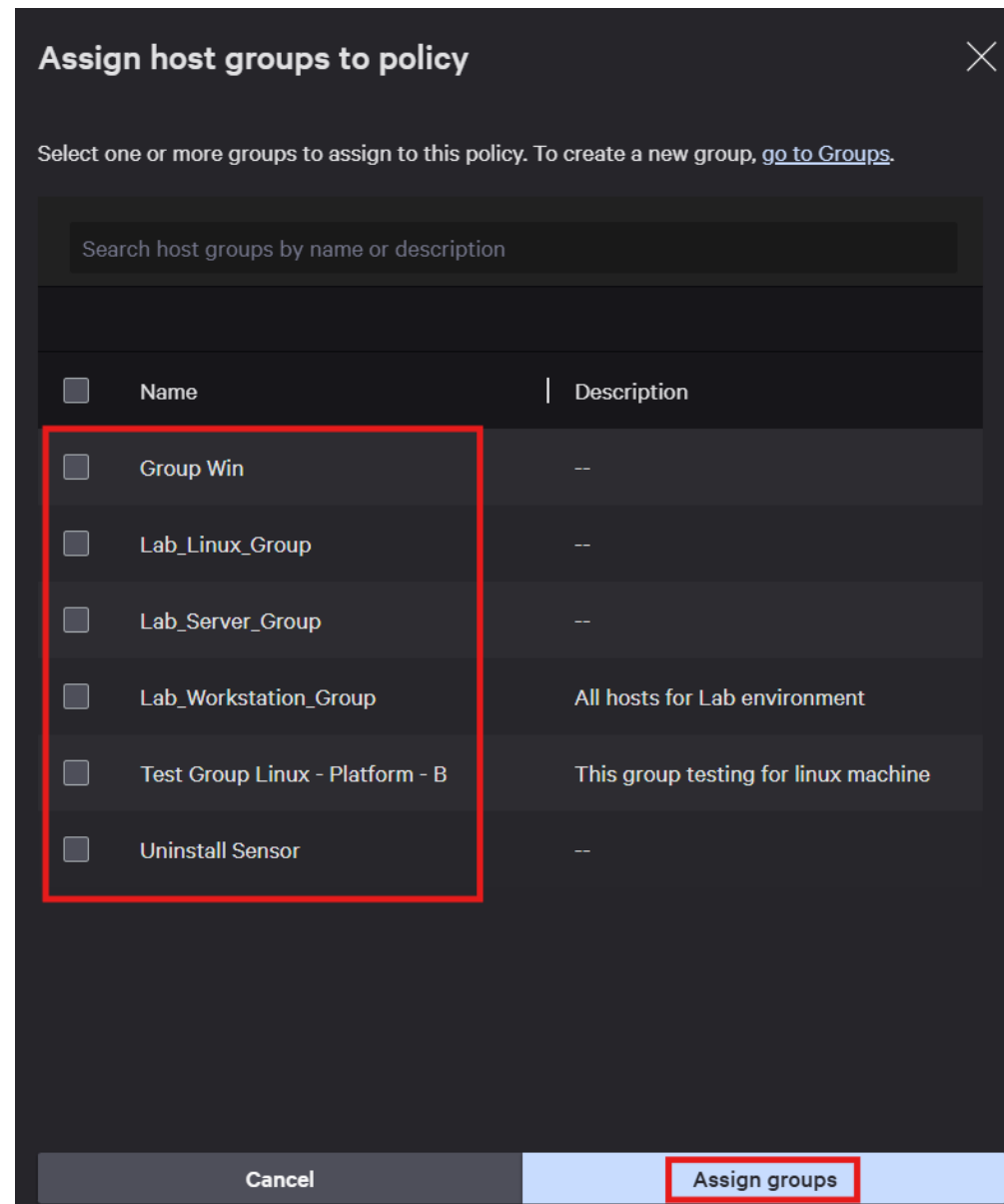
Platform: Windows
Policy ID: e3f1622a440548a5aac0a8bb778468e8
Precedence: 7 of 8
Created: Apr. 4, 2025 15:..
Last modified: Apr. 4, 2025 15:..

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

2. Gán chính sách ngăn chặn vào một group host

- Chọn một hoặc nhiều group host.
- Chọn **Assign groups**.

Sau khi bạn gán một group host cho một chính sách, group host đó sẽ không còn xuất hiện trong danh sách các group có sẵn.



Case #4: Chính Sách Phát Hiện và Ngăn Chặn

3. Chính sách ưu tiên

- Xác định các thiết lập cấu hình của chính sách nào được áp dụng cho một host khi host đó là thành viên của nhiều chính sách ngăn chặn. Việc định nghĩa các chính sách với các mức ưu tiên khác nhau để giải quyết xung đột. Khi gặp xung đột, cloud sẽ tự động áp dụng chính sách có mức ưu tiên cao hơn (1 cao hơn 2, 2 cao hơn 3, v.v.).
- Nếu một host không thuộc bất kỳ nhóm nào, hoặc các nhóm mà nó thuộc không có chính sách nào được gán, host đó sẽ tự động được gán cho chính sách mặc định.
- Chọn **Edit precedence**
- Kéo thả để sắp xếp lại các chính sách
- Chọn **Save**

The screenshot shows the 'Windows prevention policies' page in the Endpoint security console. It features a search bar, a 'Platform' dropdown set to 'Windows', and a table of 8 policies. The 'Edit precedence' button is highlighted with a red box.

Precedence	Status	Name	ID	Created	Last Modified	Applied	Pending
1	Enabled	Prevention policies for Workstati...	4ef19ee73fed4de...	Mar. 17, 2025 11:46:48	Mar. 17, 2025 12:13:08	5	0
2	Enabled	Prevention policies for Servers	62dc6b83baff46...	Mar. 17, 2025 15:24:14	Mar. 17, 2025 15:30:32	2	0
3	Enabled	Malware Prevention Policy [Test]	eafef96c1dfb434...	Mar. 3, 2025 12:03:31	Mar. 12, 2025 11:13:51	0	0

This close-up view shows the 'Precedence' column of the policy list. Each item has a set of up and down arrows to its left, which are highlighted by a red box, indicating that the policies can be reordered by dragging.

Precedence	Status	Name
1	Enabled	Prevention policies for Workstati...
2	Enabled	Prevention policies for Servers
3	Enabled	Malware Prevention Policy [Test]

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

- Các chiến thuật playbook tiêu chuẩn cho kẻ thù tận dụng việc nâng quyền và đánh cắp thông tin đăng nhập. Những chiến thuật này cho phép di chuyển ngang hàng, khai thác hoặc xâm nhập vào các hệ thống trong môi trường của bạn. Do đó, việc có cái nhìn tổng quan về các hoạt động qua tất cả các giai đoạn tấn công là rất quan trọng. Chỉ bật 8 trong số 10 tùy chọn chính sách không có nghĩa là bạn được bảo vệ 80%. Nếu các cài đặt cần thiết để phát hiện một cuộc tấn công độc hại cụ thể trong môi trường của bạn bị tắt, bạn vẫn có thể bị kẻ tấn công xâm nhập 100%.
- Chọn tab **Settings** để thiết lập cấu hình cho Prevention Policies.

The screenshot displays the 'Policy for Windows' configuration page in the Microsoft Defender for Endpoint console. The page is titled 'Policy for Windows' and shows the policy is currently 'Enabled'. Below the title, there are tabs for 'Settings', 'Assigned host groups', 'Assigned custom IOAs', and 'Audit log'. The 'Settings' tab is selected and highlighted with a red box. The settings list includes:

Setting Name	Status
End user notifications	Off
Unknown executable analysis	Off
Unknown detection-related executable anal...	Off
Sensor tamper prevention	Off

Additional information shown includes the platform 'Windows', policy ID 'e3f1622a440548a5a...', precedence '7 of 8', and creation date 'Apr. 4, 2025 15:...'.

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

- Chọn vào một cài đặt để xem mô tả, yêu cầu và chính sách khuyến nghị ba giai đoạn.

The screenshot displays the Microsoft Defender console interface. The breadcrumb navigation shows: Endpoint security > Prevention policies > Windows > Policy for Windows. The 'Settings' tab is active, showing a list of sensor capabilities. The 'End user notifications' setting is highlighted with a red box. To the right, a detailed configuration panel for this setting is shown, including a description and a table of recommendations.

Setting Name | * Required setting is OFF | Compare

Sensor capabilities

- End user notifications
- Unknown executable analysis
- Unknown detection-related executable anal...
- Sensor tamper prevention

Sensor visibility | Enhanced visibility

- Additional user mode data visibility
- Interpreter-only visibility
- System management engine visibility
- Script-based execution visibility
- HTTP visibility and detection

End user notifications

Show a pop-up notification to the end user when the Falcon sensor blocks, kills, or quarantines. These messages also show up in the Windows Event Viewer under Applications and Service Logs.

Windows prevention policy setting recommendations - three-phase view

Type	Category	Setting	Phase 1 - For rapid deployment with pre-existing AV	Phase Interi prote level
Sensor Capabilities	-	End User Notifications	Customer preference	Custo prefer

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

- Bạn có thể so sánh chính sách này với các chính sách khác. Di chuyển tới **Compare > Chọn policies** bạn muốn so sánh > Chọn **Compare**.
- CrowdStrike cung cấp 3 policy ứng với 3 giai đoạn giúp người dùng có thể dễ dàng so sánh

Setting Name	*	Preve... X	Compare v
Sensor capabilities			Search policies
End user notifications	<input checked="" type="checkbox"/>	=	<input checked="" type="checkbox"/> Prevention policies for Workstati...
Unknown executable analysis	<input checked="" type="checkbox"/>	=	<input type="checkbox"/> Prevention policies for Servers
Unknown detection-related executable anal...	<input checked="" type="checkbox"/>	=	<input type="checkbox"/> Malware Prevention Policy [Test]
Sensor tamper prevention	<input type="checkbox"/>	≠	<input type="checkbox"/> Phase 3 - optimal protection
Sensor visibility Enhanced visibility			<input type="checkbox"/> Phase 2 - interim protection
Additional user mode data visibility	<input checked="" type="checkbox"/>	=	<input type="checkbox"/> Phase 1 - initial deployment
			<input type="checkbox"/> Default (Windows)

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

- Xác định mức độ **Machine Learning** cho các chính sách Machine Learning trong tổ chức của bạn.

Level	Description
Disabled	Disable all detections or preventions.
Cautious	Detect or prevent only when our machine learning system has high confidence that something is malicious.
Moderate	Detect or prevent when our machine learning system has moderate confidence that something is malicious. We recommend this setting for most use cases. This setting also detects and prevents activity that would be detected or prevented by Cautious .
Aggressive	Detect or prevent when our machine learning system has low confidence that something is malicious. This setting also detects and prevents activity that would be detected or prevented by Moderate and Cautious .
Extra Aggressive	Detect or prevent when our machine learning system has the lowest confidence that something is malicious. This setting also detects and prevents activity that would be detected or prevented by Aggressive , Moderate , and Cautious .

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

- Cách tiếp cận ba giai đoạn trong triển khai các thiết lập chính sách ngăn chặn, cung cấp một lộ trình có cấu trúc từ việc triển khai ban đầu đến việc thực hiện đầy đủ các best practice của chúng tôi. Nếu khách hàng đang sử dụng các bộ phần mềm diệt virus hoặc HIPS, hãy bắt đầu với **giai đoạn 1** để giảm thiểu xung đột có thể xảy ra. Nếu không sử dụng phần mềm diệt virus hoặc HIPS, hãy bắt đầu với **giai đoạn 2**. Sử dụng quy trình kiểm soát thay đổi để tiến hành cập nhật các host sang giai đoạn tiếp theo, điều chỉnh các **exclude**, **quản lý IOC** và **các quy tắc IOA tùy chỉnh** để tinh chỉnh cấu hình và giảm thiểu các cảnh báo giả trong môi trường khách hàng.
- Thông thường, không nên mất quá 45 ngày để hoàn tất việc triển khai cảm biến đến tất cả các endpoint đủ điều kiện và chuyển sang cài đặt giai đoạn 2. Không nên mất quá 90 ngày sau khi triển khai để áp dụng cài đặt giai đoạn 3 cho tất cả các host.

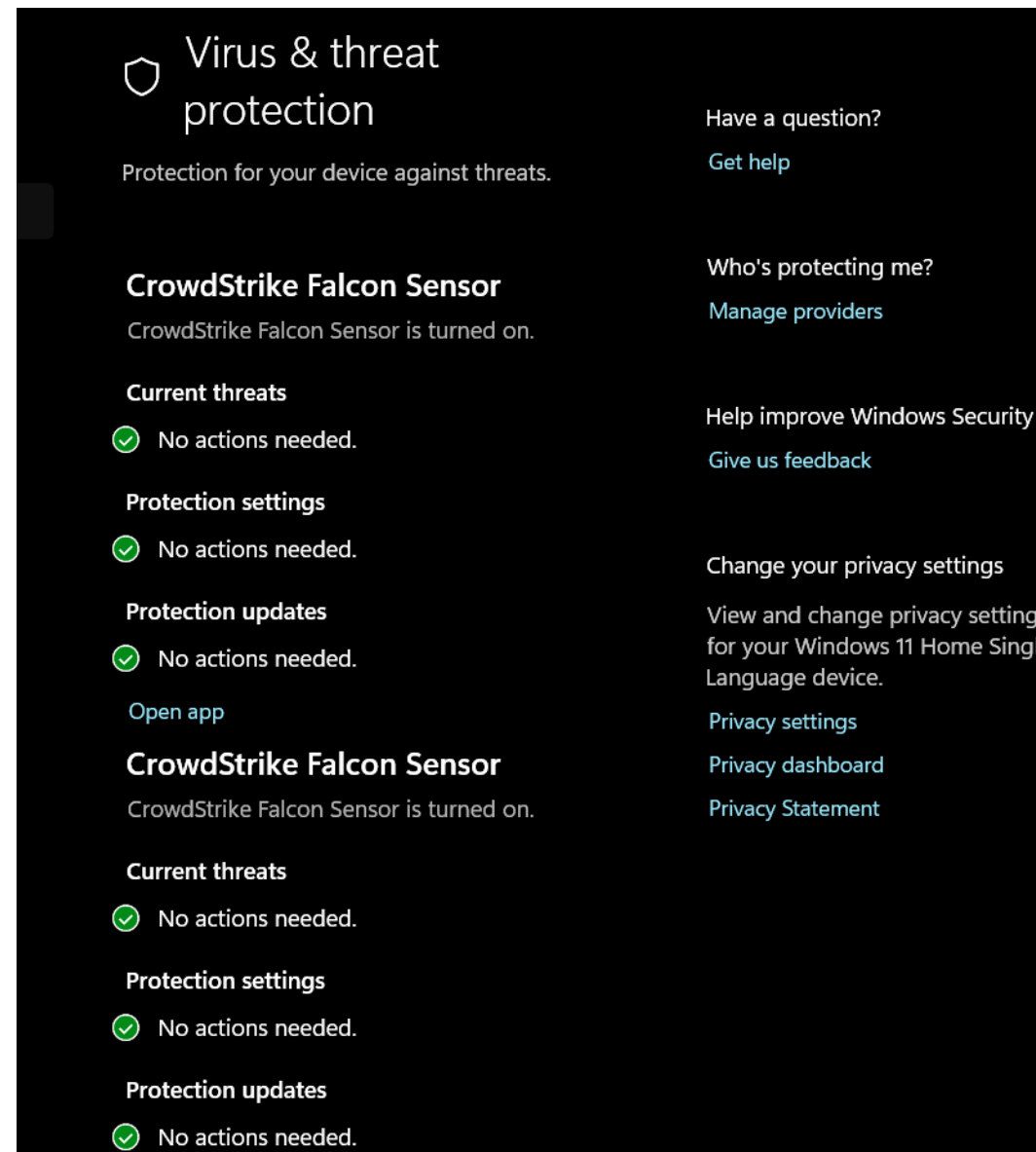
Lưu ý: Đối với triển khai lần đầu hoặc triển khai trong môi trường nhiều ứng dụng nhạy cảm, khuyến nghị sử dụng chính sách giai đoạn 1 (Chỉ phát hiện) hoặc 2 (Bảo vệ tối thiểu) để theo dõi và tránh xung đột với các ứng dụng ngay khi vừa triển khai

Phase 1 - For rapid deployment with pre-existing AV	Phase 2 - Interim protection level	Phase 3 - Optimal protection
--	---	-------------------------------------

Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

Sau khi policy được đẩy thành công, kiểm tra trên Windows Defender sẽ thấy đã bị thay thế bởi **CrowdStrike Falcon Sensor**



Case #5: Endpoint Monitoring

Theo dõi các phát hiện

1. Tổng quan

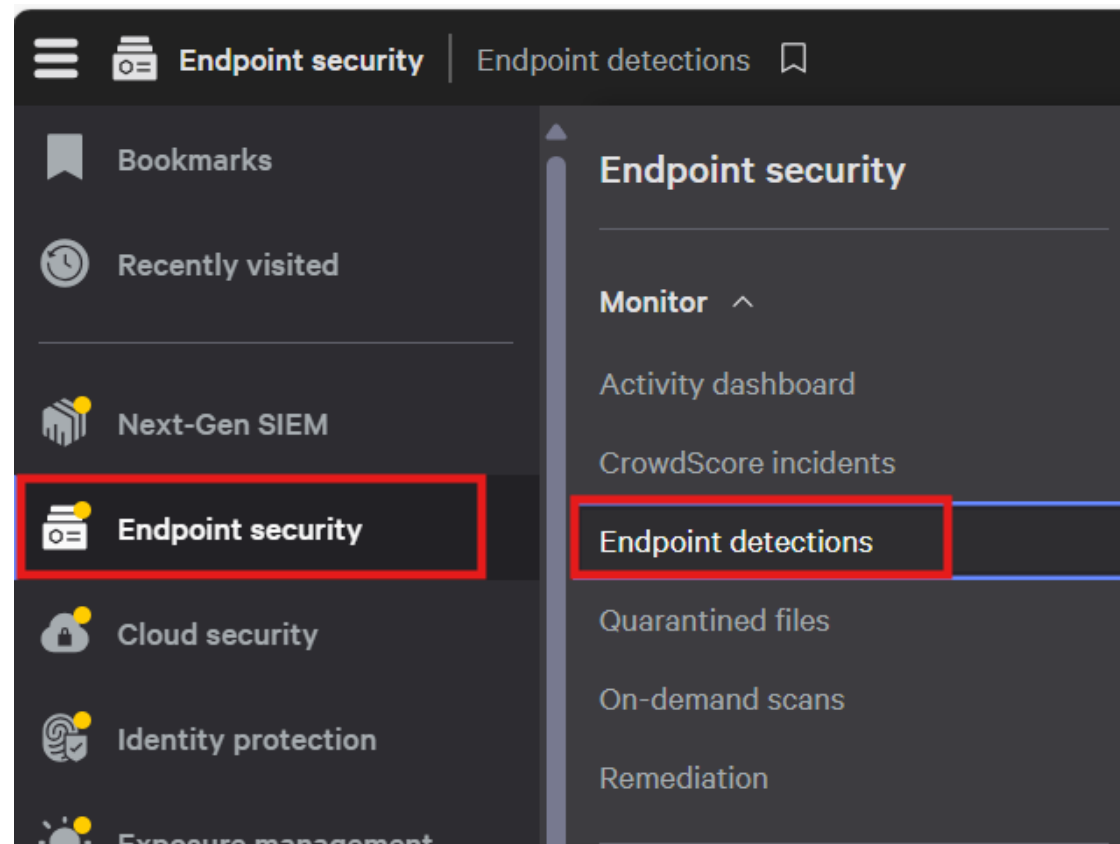
Giám sát các phát hiện từ endpoint để hiểu hoạt động đang diễn ra trong môi trường. Xem thông tin chi tiết về các process, tệp, hành vi nghi ngờ và kết quả quét theo yêu cầu.

2. Hiểu về các phát hiện trên endpoint

The Falcon console provides cung cấp thông tin về các tệp và hành vi nghi ngờ dưới dạng các phát hiện riêng lẻ. Các phát hiện này có thể cảnh báo về nhiều hoạt động đang diễn ra trên các máy tính, từ sự hiện diện của một file độc hại dưới dạng **dấu hiệu xâm nhập (IOC)** đến một tập hợp tinh vi của các hành vi nghi ngờ dưới dạng **dấu hiệu tấn công (IOA)**.

3. Làm việc qua phát hiện endpoint

Đối với các phát hiện từ endpoint trên các máy Windows, macOS và Linux, Falcon cung cấp thông tin trong **Endpoint security > Monitor > Endpoint detections**.



Case #5: Endpoint Monitoring

Theo dõi các phát hiện

3. Làm việc qua phát hiện endpoint

- **Lọc, sắp xếp và nhóm các phát hiện:** Theo mặc định, tất cả các phát hiện đều được hiển thị và được sắp xếp theo thời gian, từ mới nhất đến cũ nhất. Thu hẹp và tinh chỉnh hiển thị theo ý của bạn bằng cách lọc, sắp xếp, và nhóm các phát hiện.
- Hiển thị hoặc ẩn các cột trong bảng bằng cách nhấp vào **Configure table columns**.

The screenshot displays the 'Endpoint security' dashboard with 'Endpoint detections' selected. The interface shows 85 results. A red box highlights the filter bar containing: 'Search detections', 'Severity', 'Time', 'Status', 'Tactic', 'Technique', 'Tags', 'Host', 'Add/remove filters', and 'Clear all'. Another red box highlights the 'Group by' dropdown menu. A third red box highlights the 'Sort by Time: Newest to oldest' dropdown menu. Below these, a table of detection results is visible, with columns for Severity, Detect time, Process on host, Tactic via tech..., Triggering file, Hostname, User name, Assigned to, and Resolution. The first row shows a 'High' severity detection on 'Apr. 12, 2025' at '18:21:47' involving 'vmtoolsd.exe on DESTOP-WI...' with tactic 'Defense E...' and user 'User'.

Case #5: Endpoint Monitoring

Theo dõi các phát hiện

3. Làm việc qua phát hiện endpoint

- **Xem thêm chi tiết về một phát hiện:** Nhấp vào một phát hiện để xem bảng quy trình và thông tin tóm tắt của phát hiện đó. Trong bảng tóm tắt, xem thêm thông tin về phát hiện. Các thông tin hiển thị thay đổi theo loại phát hiện và tùy vào gói đăng ký Falcon

Apr. 12, 2025 18:21:47

vmtoolsd.exe on DESTOP-WIN10-B by User Investigate Actions

Edit status Network contain Cannot connect to host

No notes from OverWatch

No related adversaries

Status

Process

Workflows 1

Hash

File

[See full detection](#)

Process actions

Network operations 5

Disk operations 31

DNS requests 1

Registry operations 1

Case #5: Endpoint Monitoring

Theo dõi các phát hiện

3. Làm việc qua phát hiện endpoint

- Xem thêm chi tiết về một phát hiện:
 - + Trong chế độ xem tóm tắt, nhấp vào "See full detection" để xem tất cả thông tin chi tiết về phát hiện. Xem thêm chi tiết phát hiện qua nhiều chế độ xem:
 - **Details:** Thông tin chi tiết hơn về phát hiện. Chế độ xem này cũng bao gồm một nhật ký trạng thái cho phát hiện.
 - **Process table:** Một chế độ xem bảng về các quy trình liên quan đến phát hiện, với quy trình liên quan đầu tiên được hiển thị ở đầu bảng. Tinh chỉnh chế độ xem bằng cách hiển thị và ẩn các lớp. Bạn có thể hiển thị và ẩn chú thích và bảng tóm tắt.
 - **Process tree:** Một chế độ xem đồ thị về các quy trình liên quan đến phát hiện. Mỗi nút trong cây quy trình đại diện cho một quy trình. Di chuột qua hoặc nhấp vào một nút để xem thêm chi tiết. Tinh chỉnh chế độ xem bằng cách hiển thị và ẩn các lớp. Bạn có thể hiển thị và ẩn chú thích và bảng tóm tắt.
 - **Events timeline:** Một danh sách tất cả các sự kiện liên quan theo thứ tự thời gian.

The screenshot displays an endpoint monitoring interface. At the top, there is a search bar and navigation tabs: "Details", "Process table", "Process tree", "Process graph", and "Events timeline". The "Process tree" tab is selected, showing a hierarchical view of processes. The root process is "WannaCry.exe" (PID 12104), which is highlighted with a red circle. Below it, several other processes are listed, including "RedEye.exe" and "runonce.exe". The "Details" tab is also visible, showing information for "WannaCry.exe", including a "Detection - critical" status, "Execution details", "Host name", "User name" (TECH\Administ...), "Local process ID" (12104), and the "Command line" (C:\Users\Administrator\TECH\Downloads\The-MALWARE-Repo-master\Ransomware\WannaCry.exe /r).