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

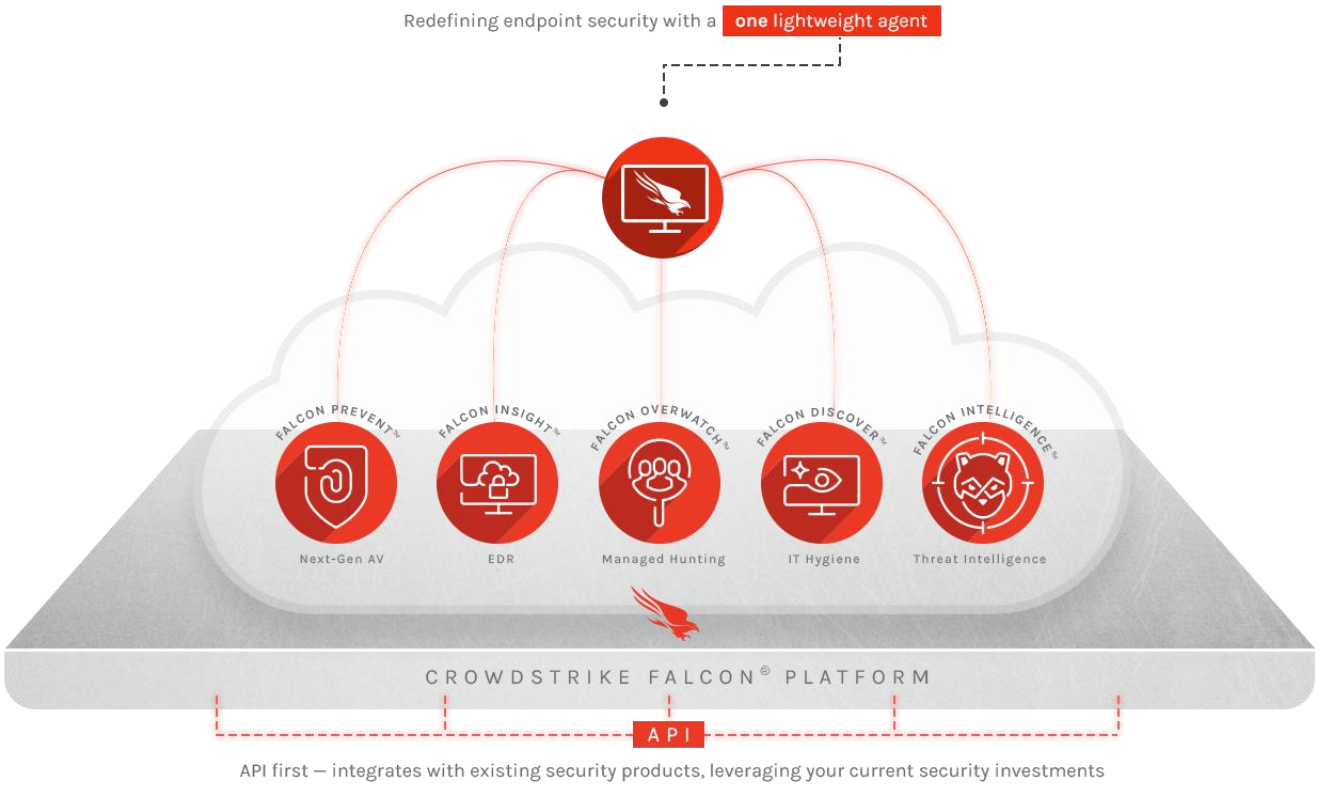
Công nghệ sử dụng

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

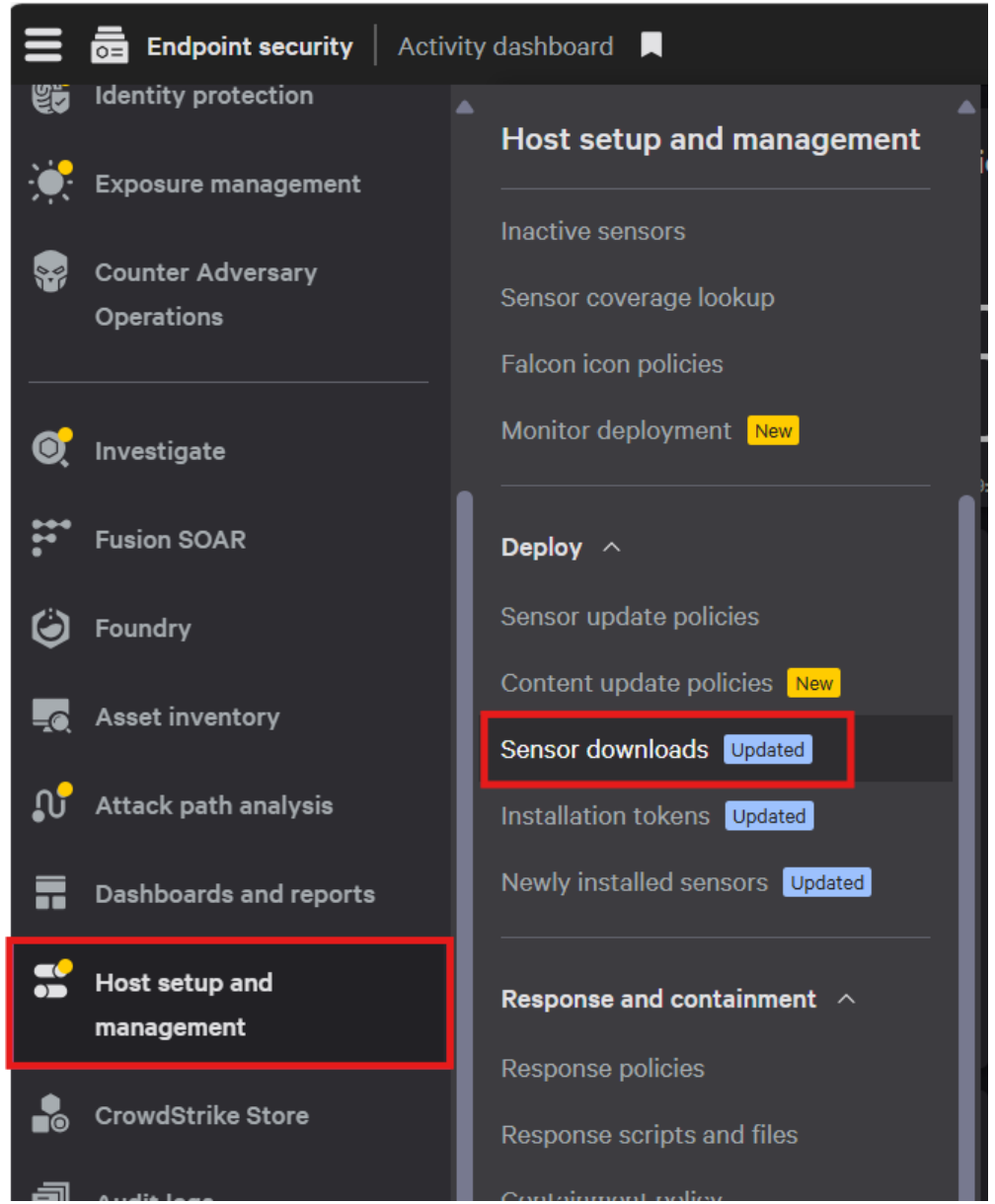
Cài Đặt Falcon Sensor Thủ Công

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

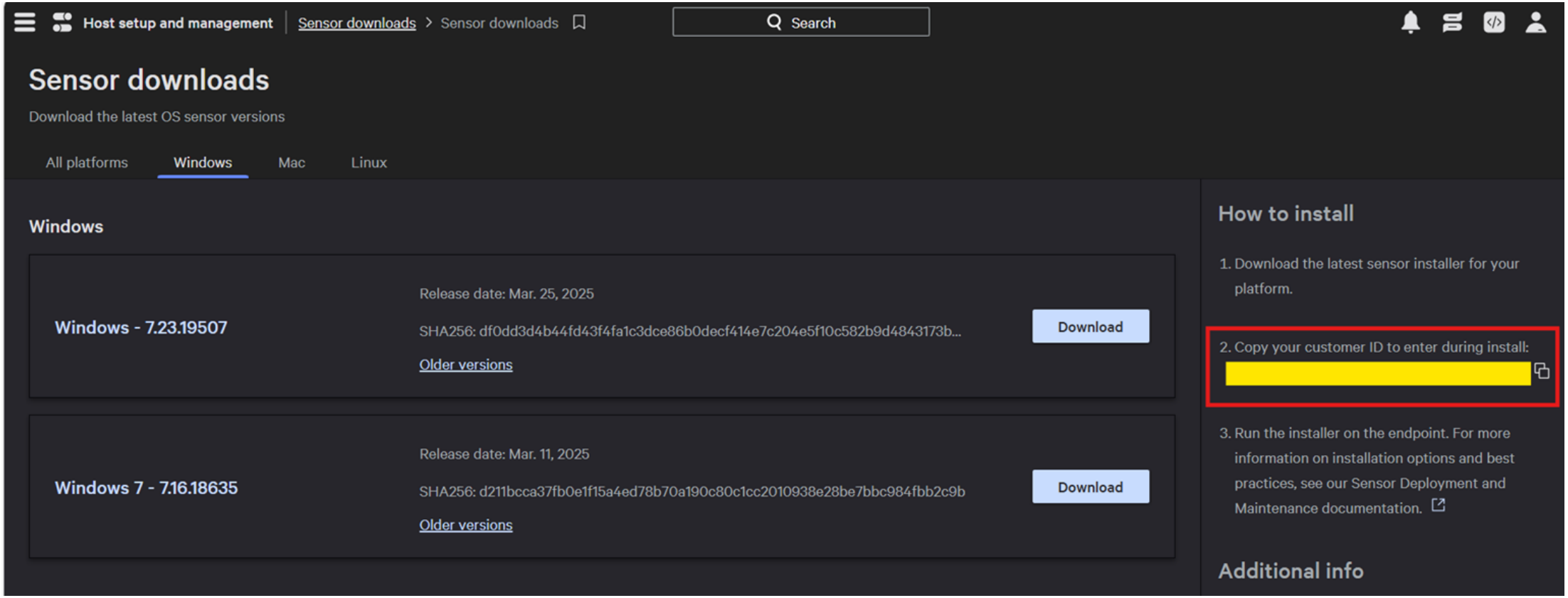


Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

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

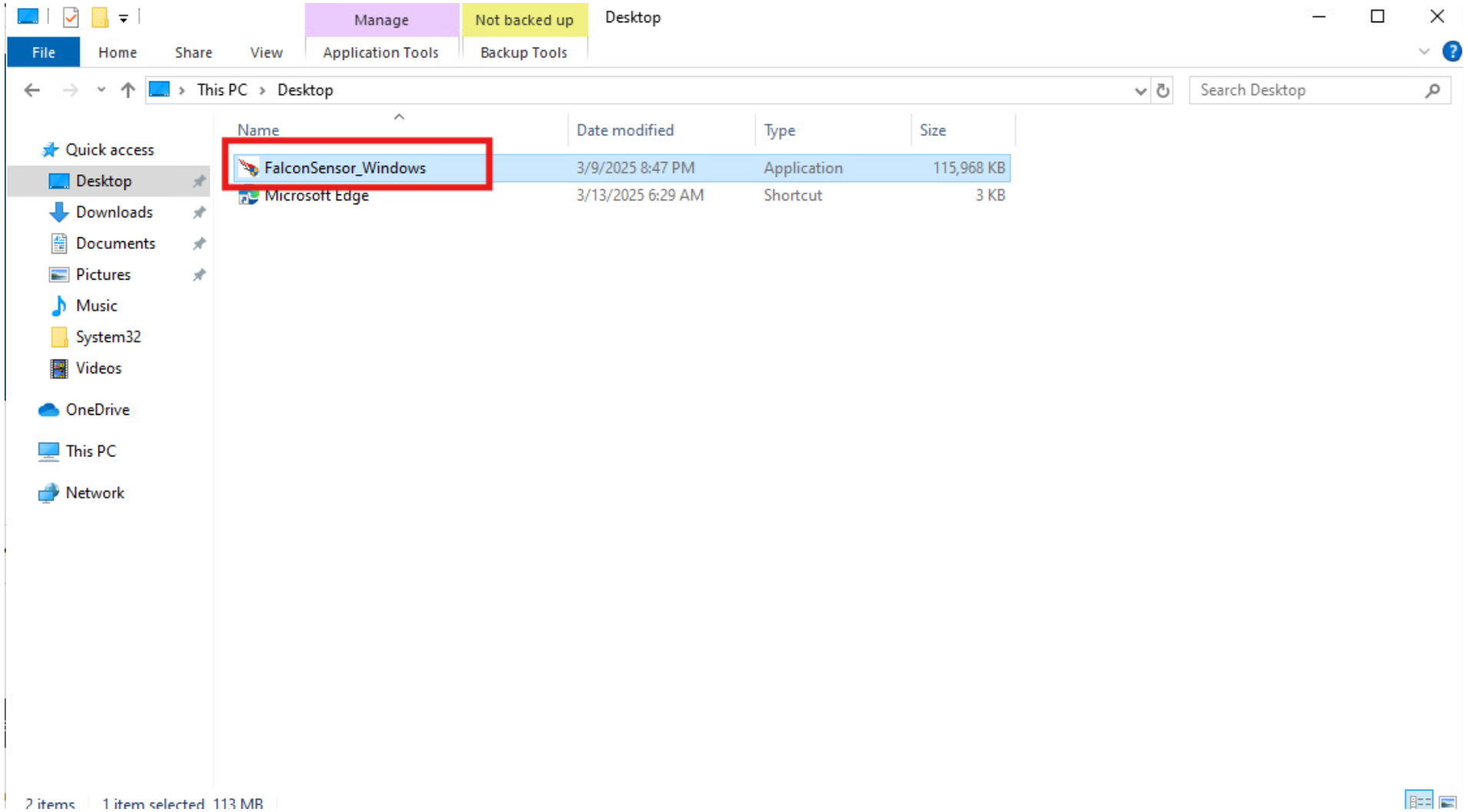
Nếu bạn là người dung trial, bỏ qua bước này.



Case #1: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

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



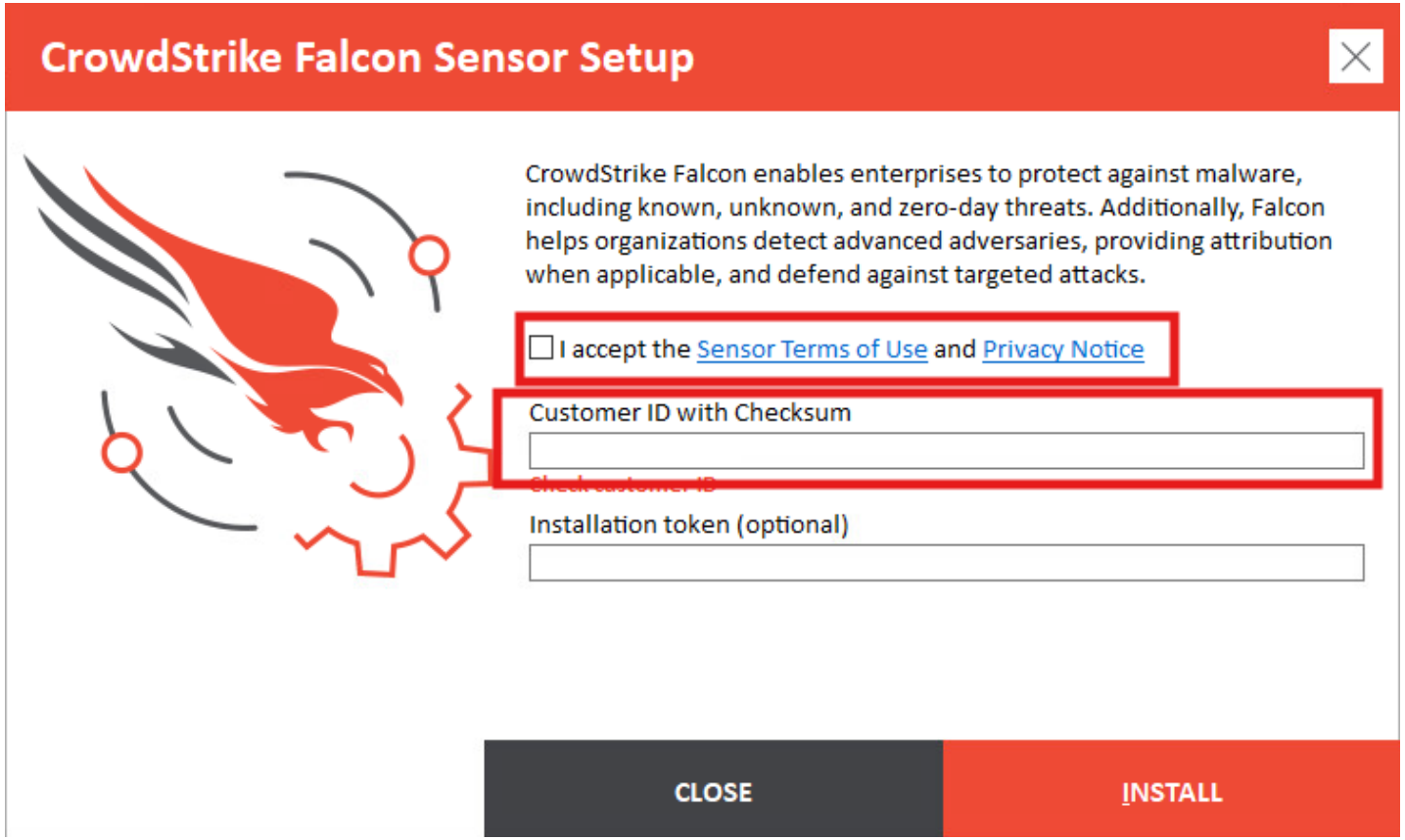
Case #1: Cài Đặt Falcon Sensor

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 dung trial, bỏ qua bước này.

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

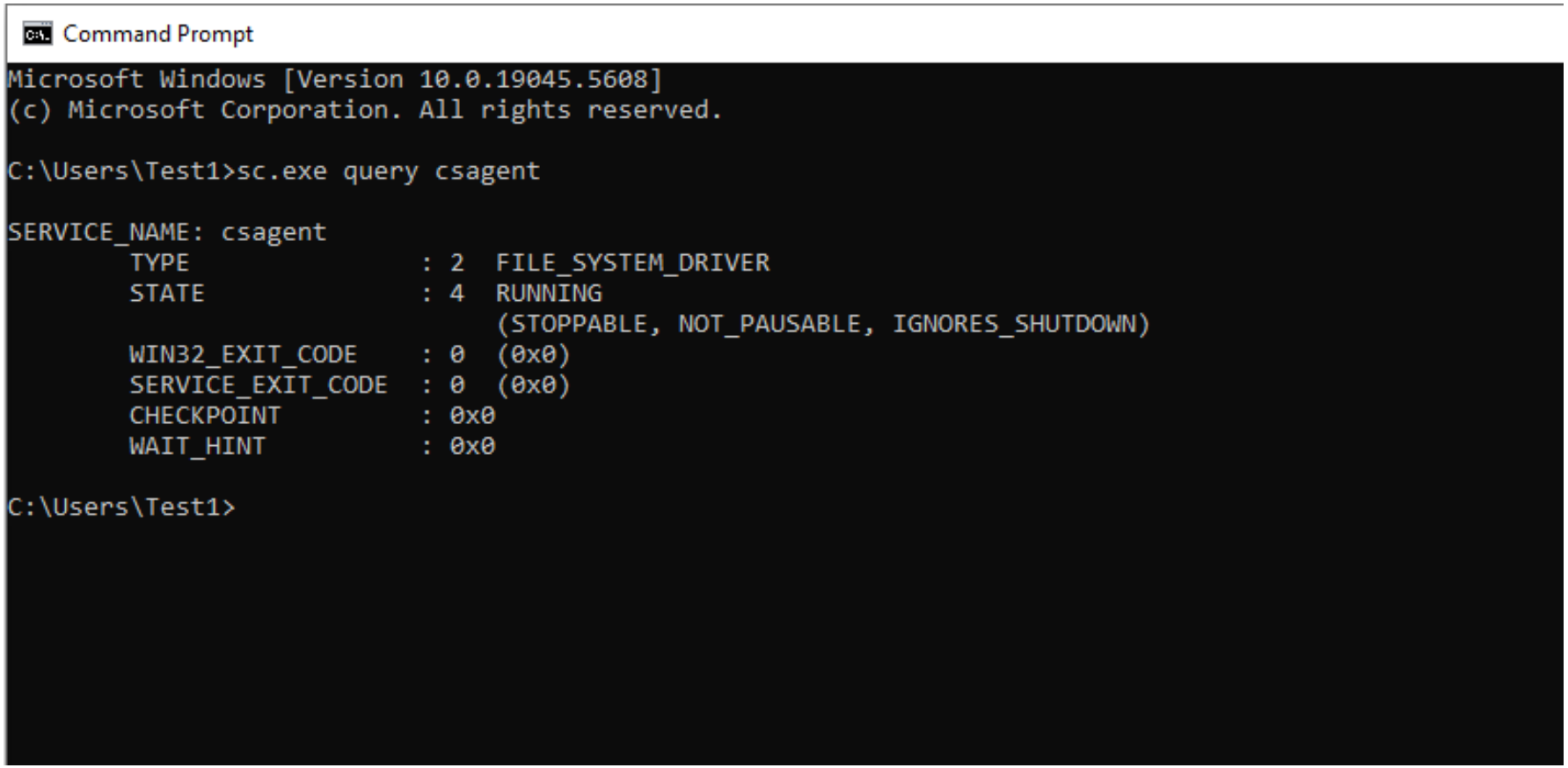


Case #1: Cài Đặt Falcon Sensor

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



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

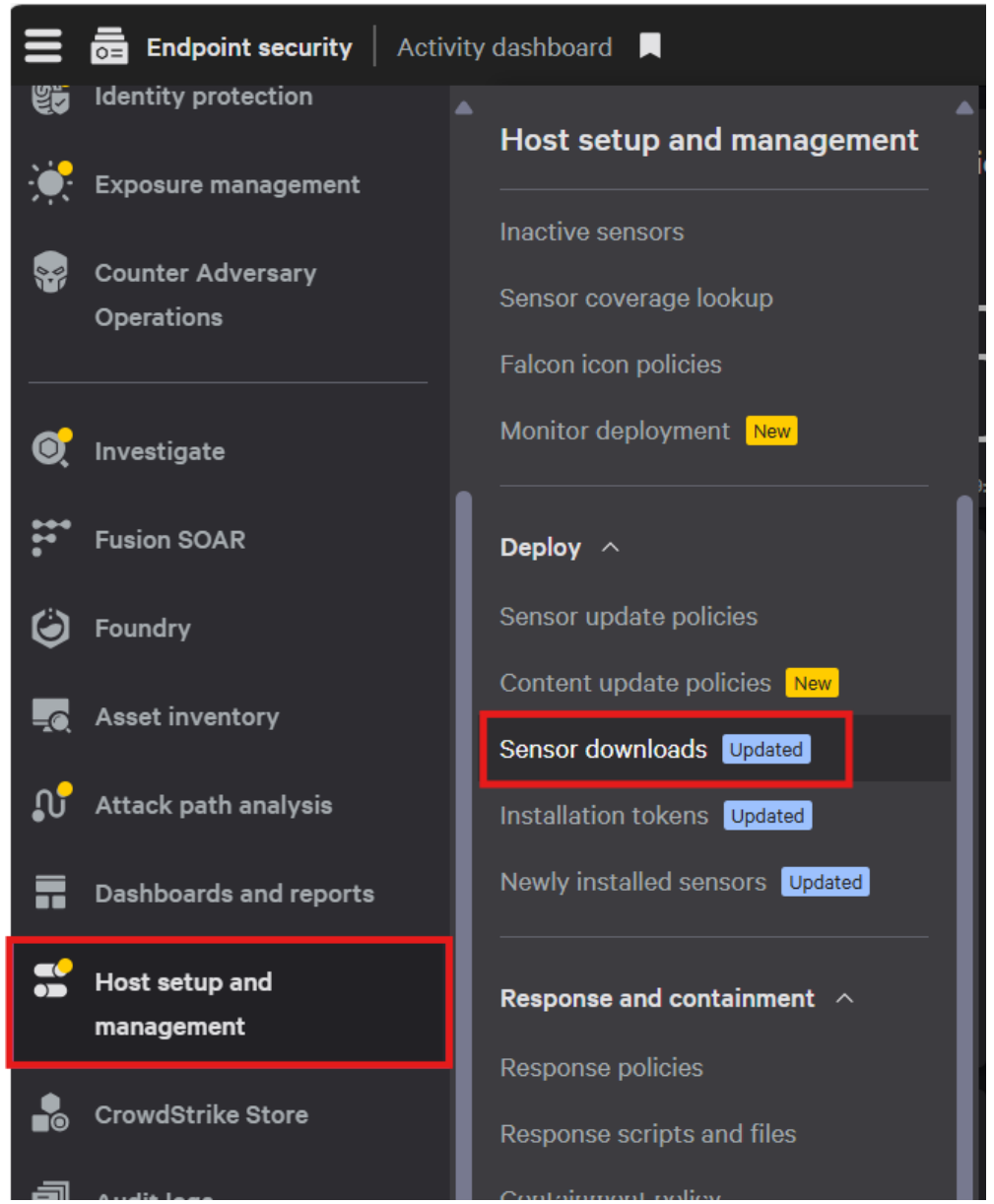
```
ts01-lanner-lion.cloudsink.net
lfodown01-lanner-lion.cloudsink.net
lfoup01-lanner-lion.cloudsink.net
https://falcon.eu-1.crowdstrike.com
https://assets.falcon.eu-1.crowdstrike.com
https://assets-public.falcon.eu-1.crowdstrike.com
https://api.eu-1.crowdstrike.com
https://firehose.eu-1.crowdstrike.com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

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

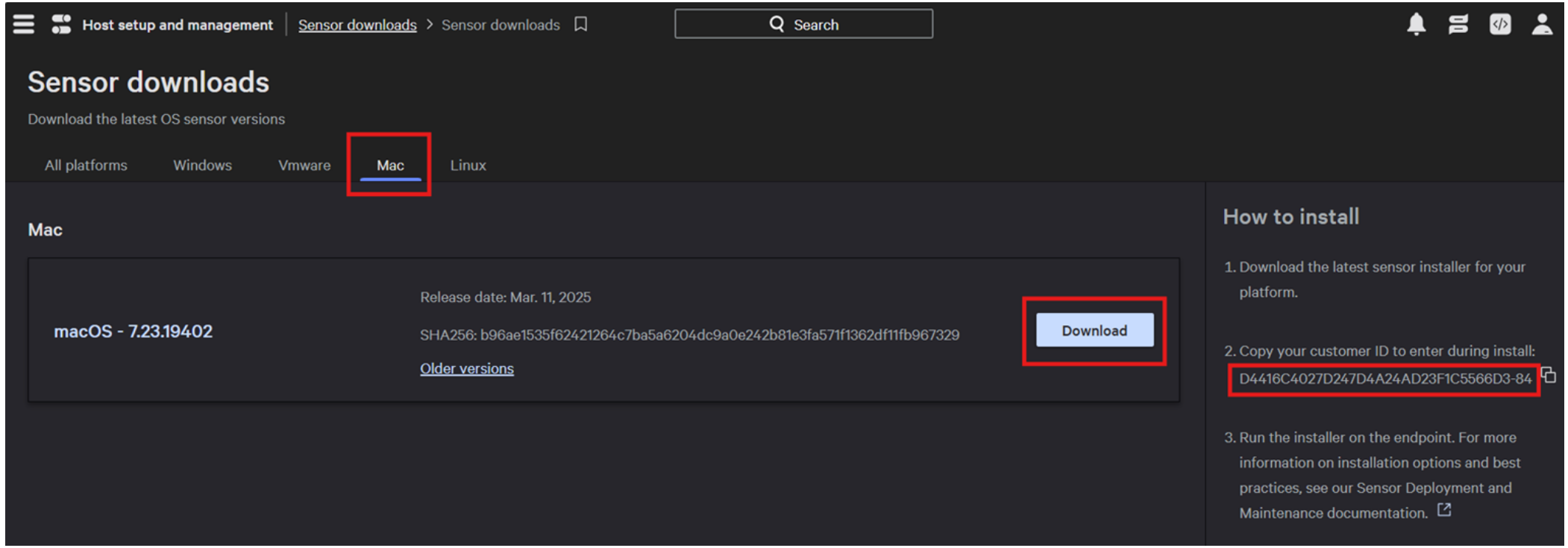
Cài Đặt Falcon Sensor Thủ Công

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.



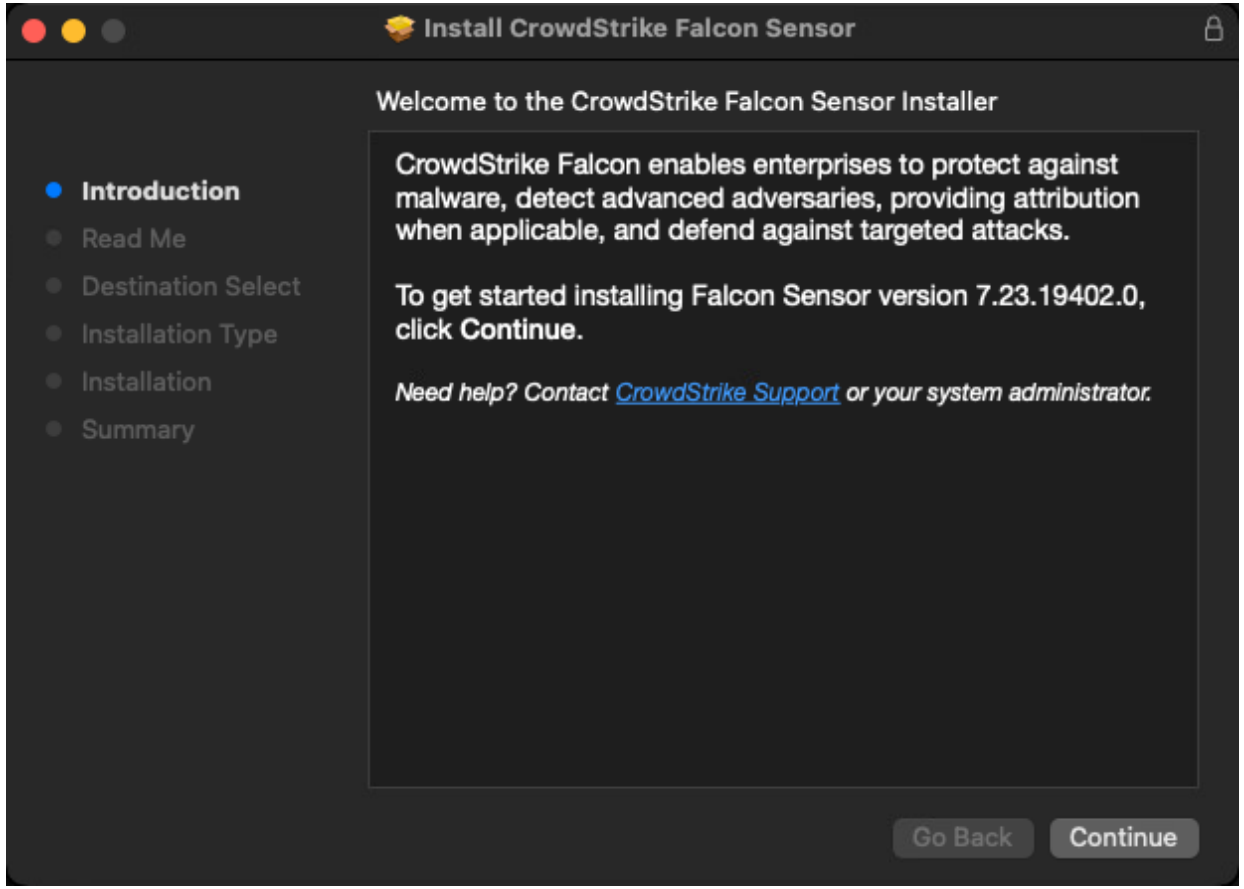
Case #2: Cài Đặt Falcon Sensor

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**

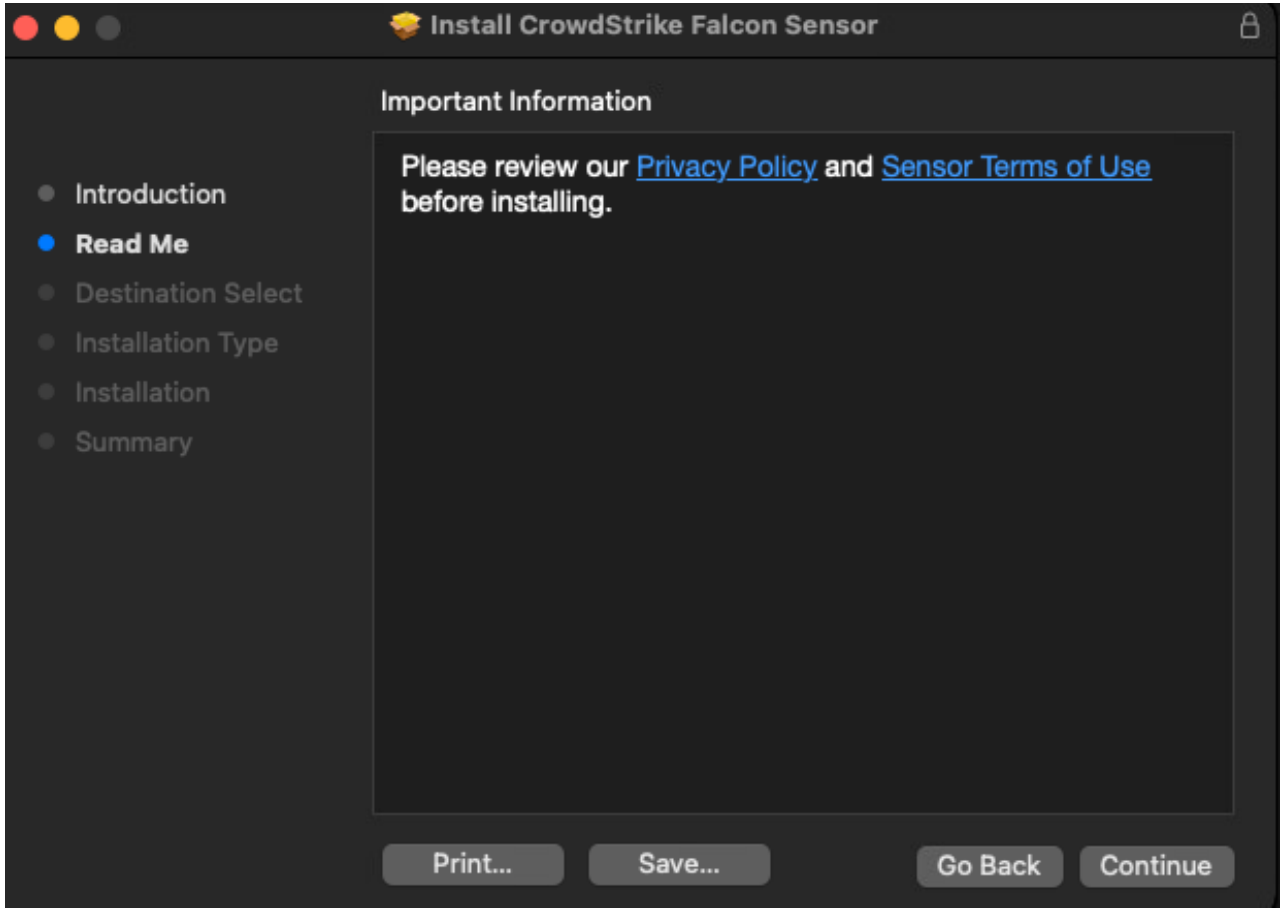


Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

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



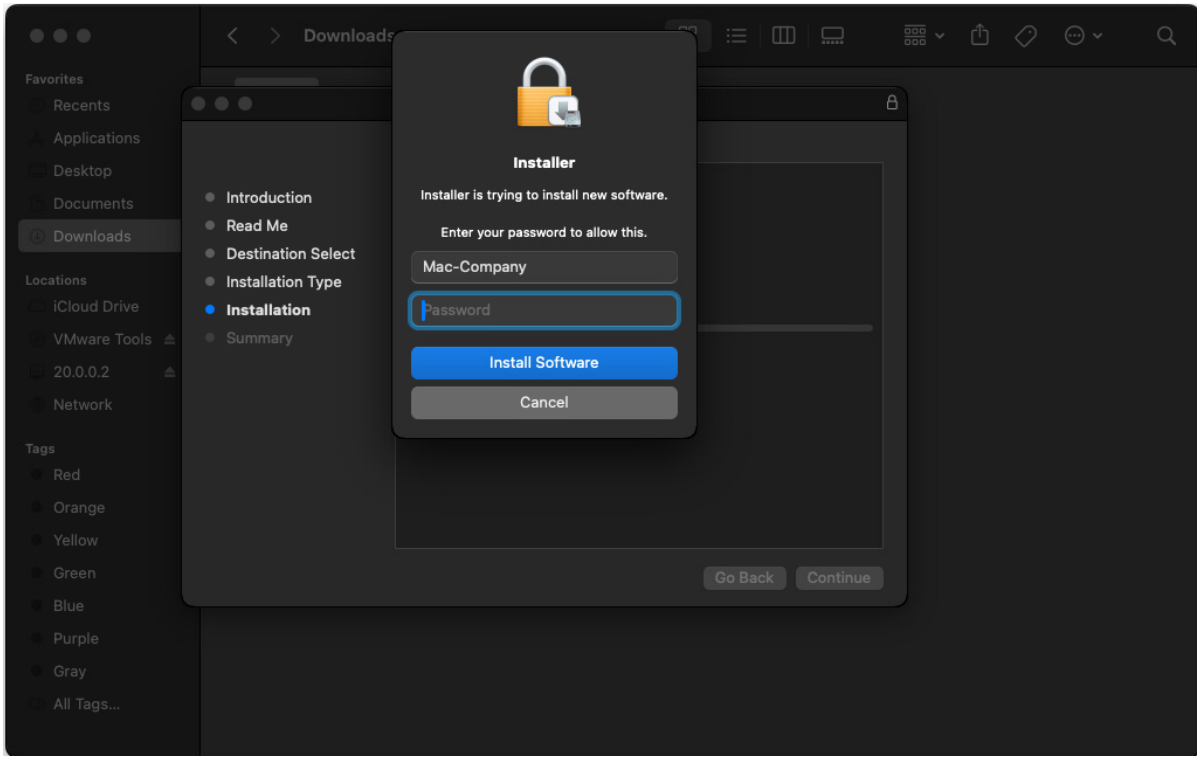
Case #2: Cài Đặt Falcon Sensor

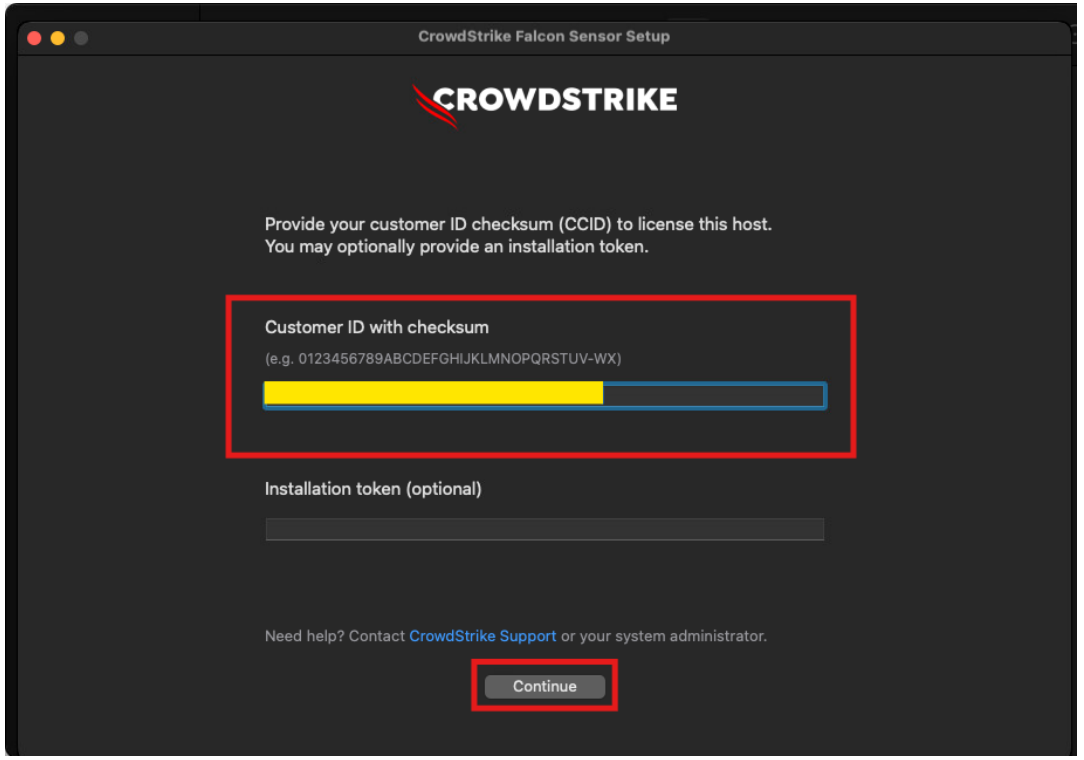
Cài Đặt Falcon Sensor Thủ Công

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**.



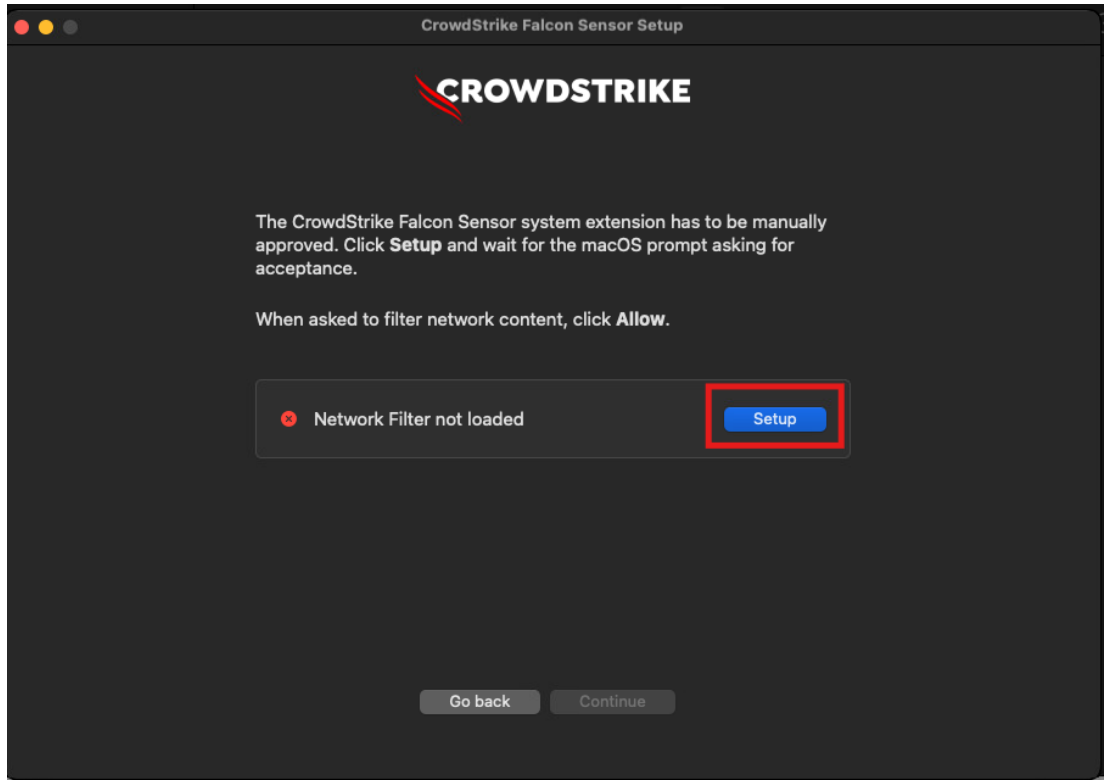


Case #2: Cài Đặt Falcon Sensor

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**.



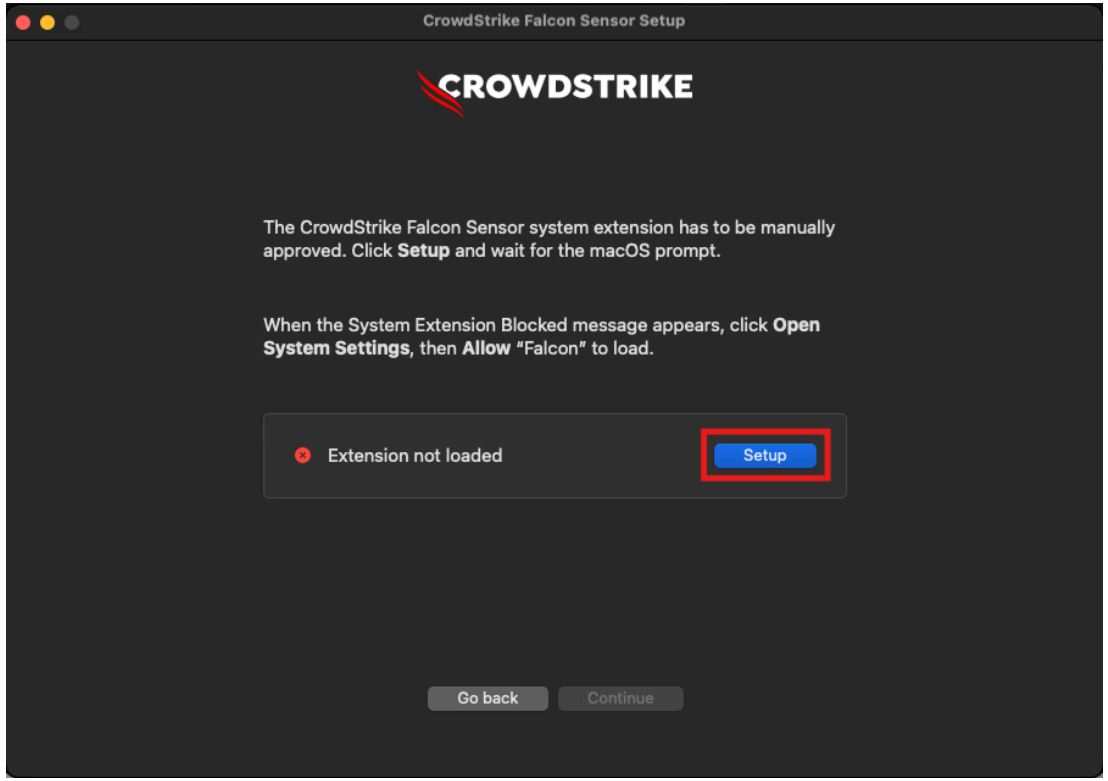
Case #2: Cài Đặt Falcon Sensor

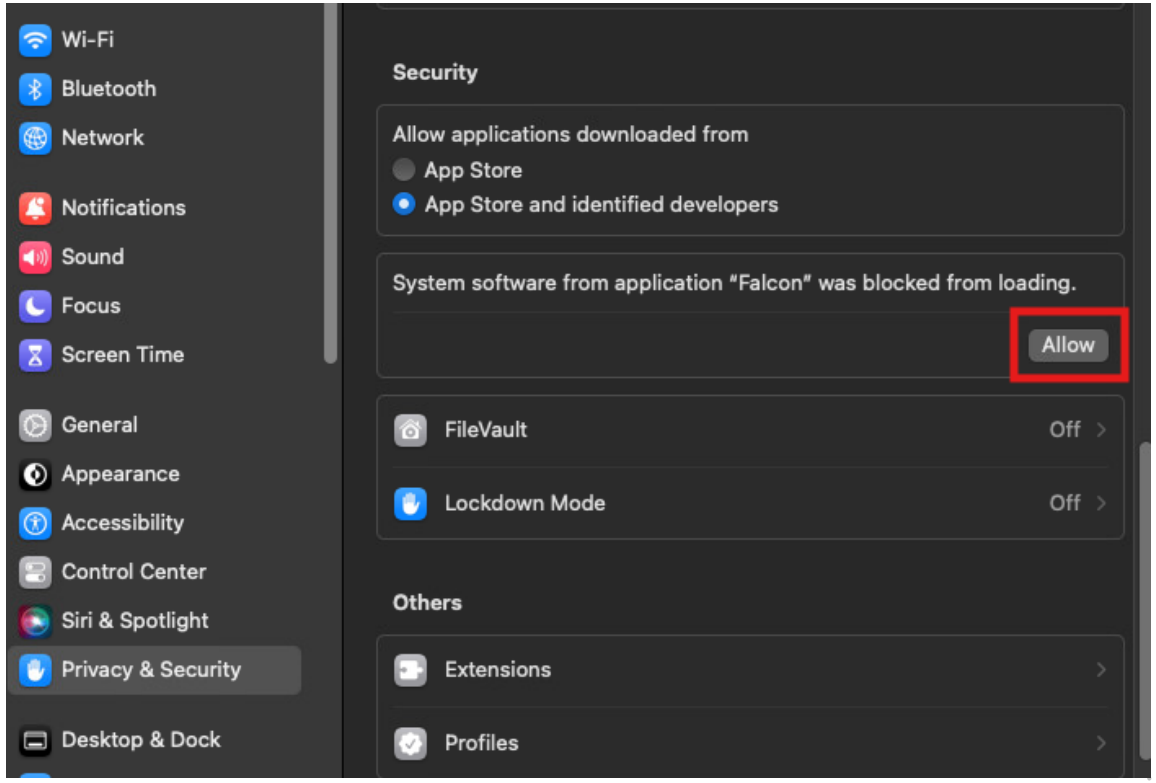
Cài Đặt Falcon Sensor Thủ Công

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**.





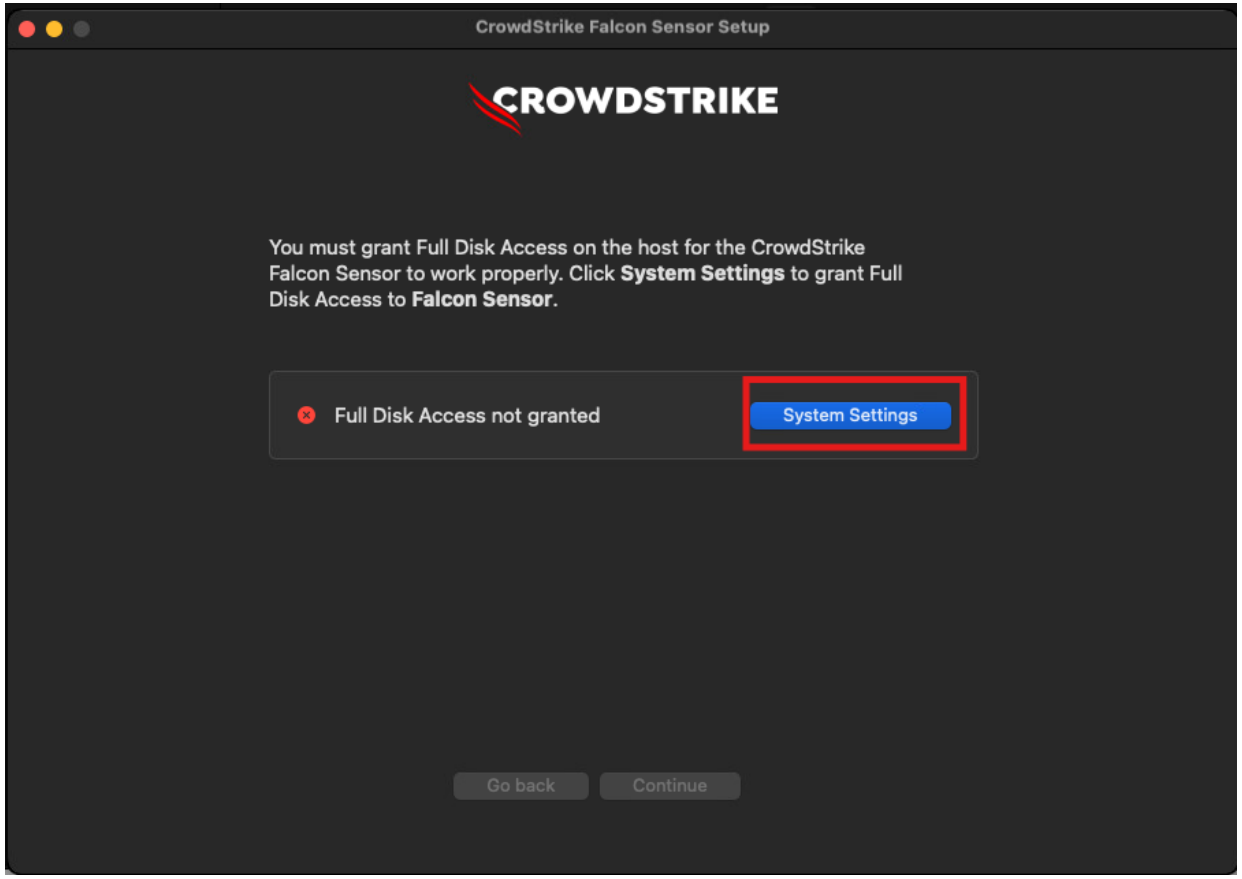
Case #2: Cài Đặt Falcon Sensor

Cài Đặt Falcon Sensor Thủ Công

MacOS:

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

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



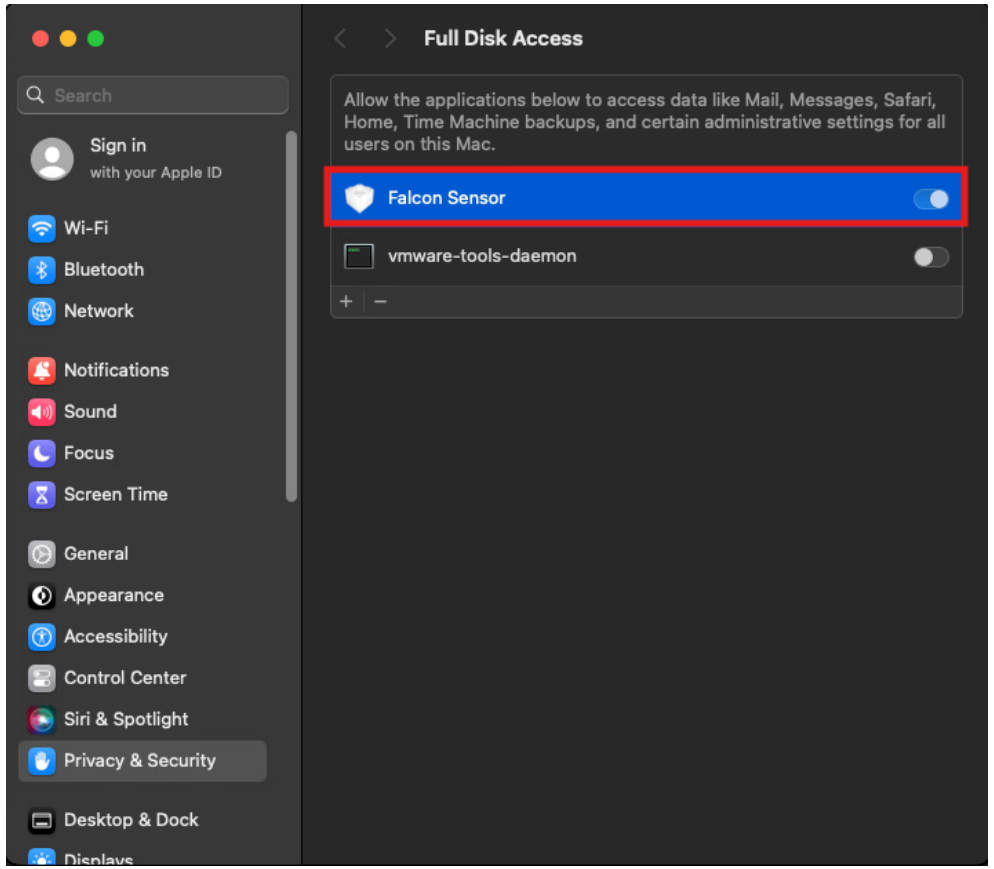
Case #2: Cài Đặt Falcon Sensor

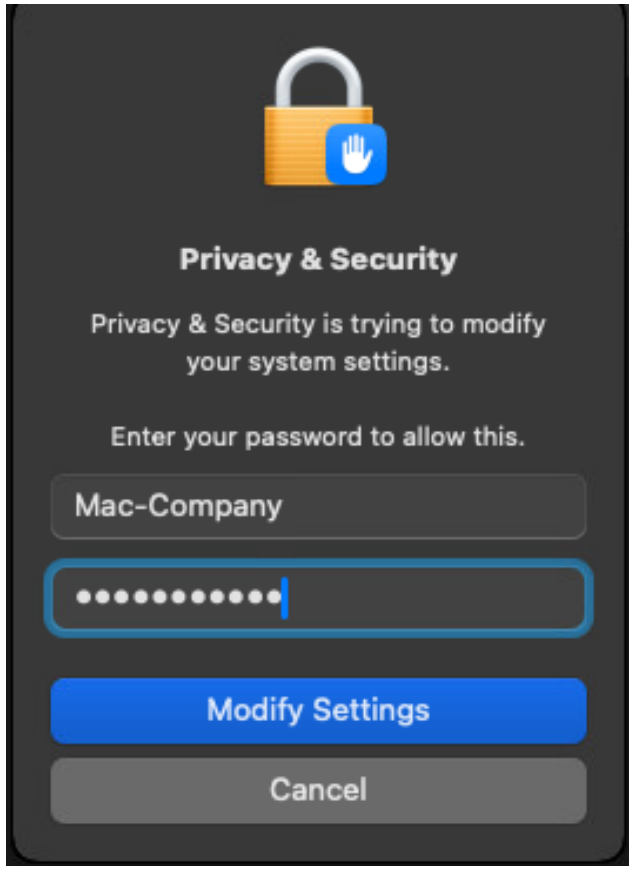
Cài Đặt Falcon Sensor Thủ Công

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

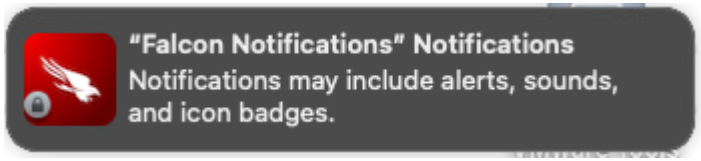
Cài Đặt Falcon Sensor Thủ Công

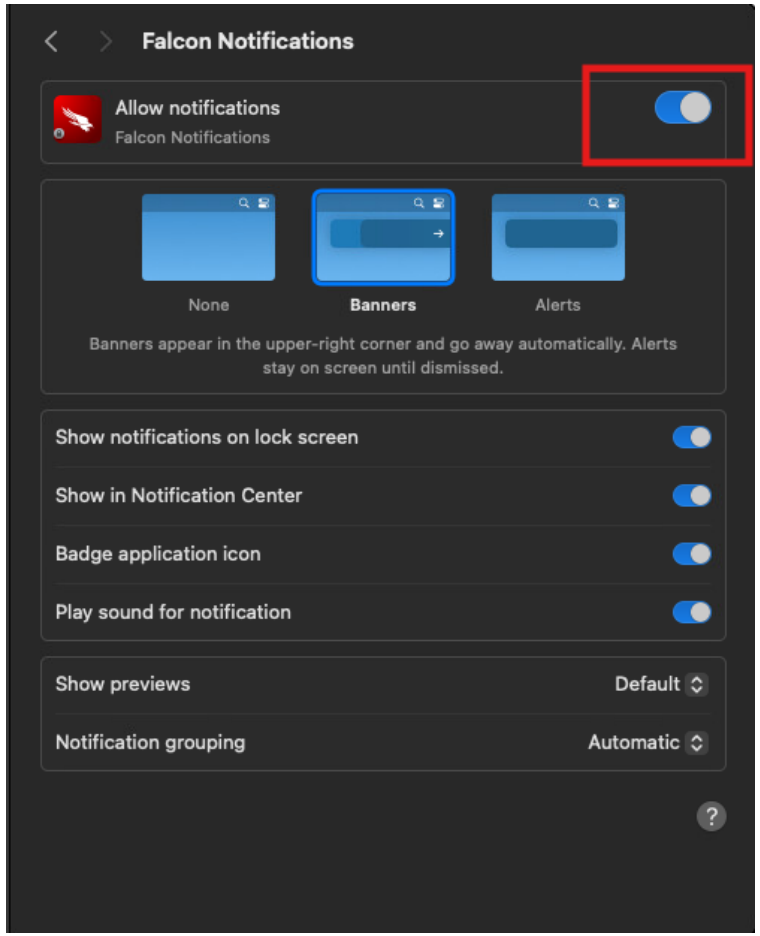
MacOS:

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.

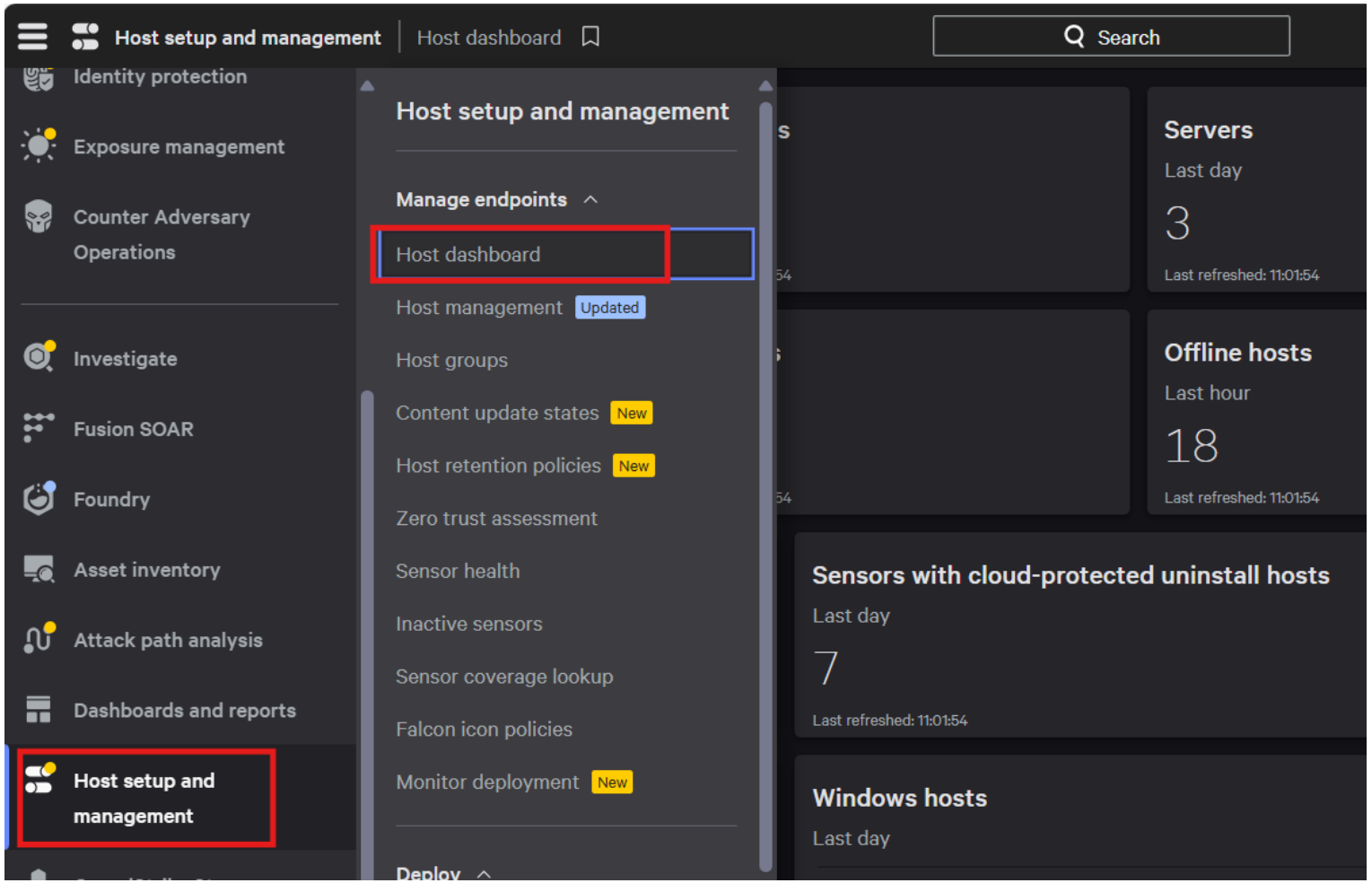
Yêu cầu:

- **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

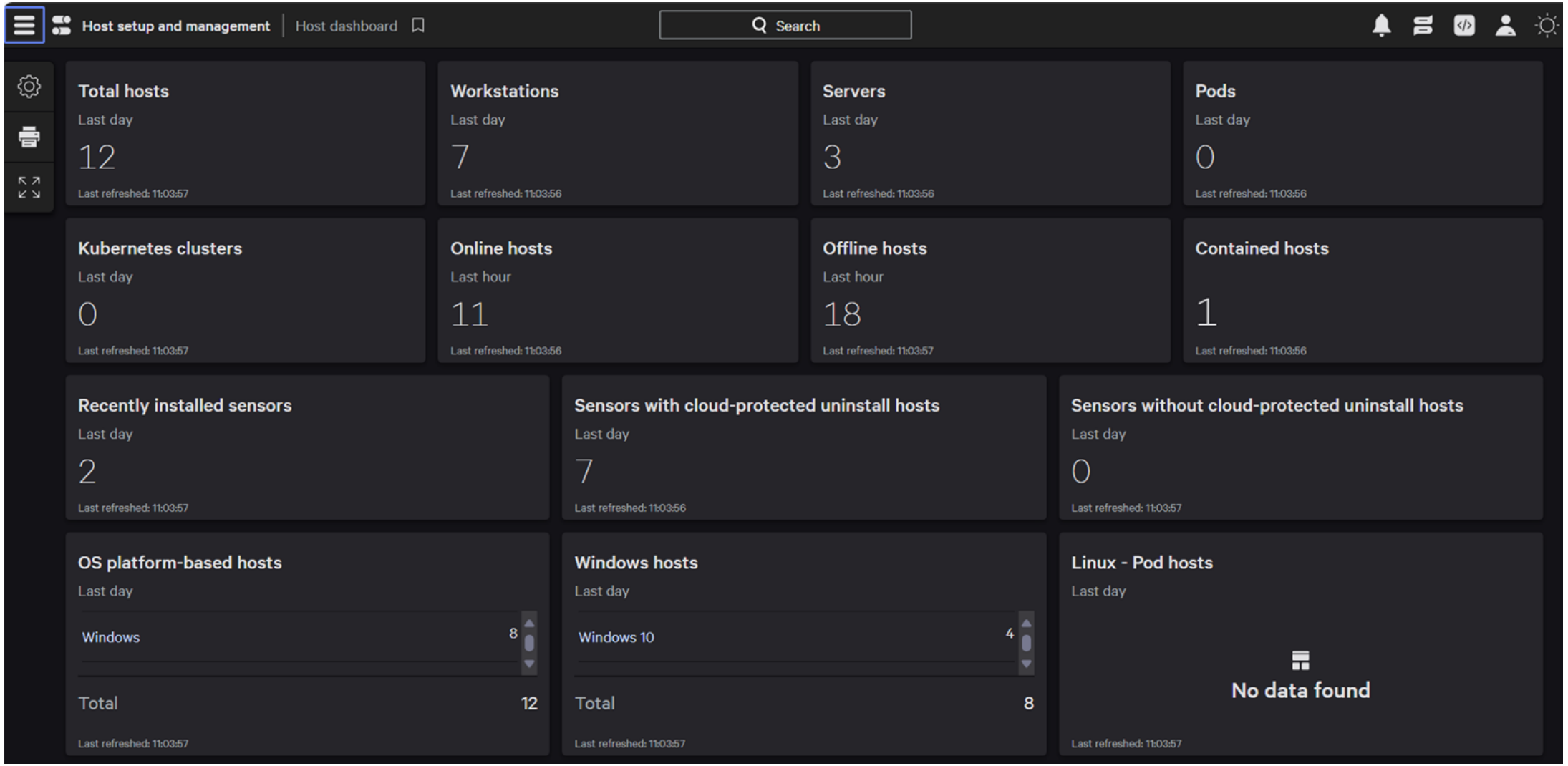
1. Bảng tổng quan của host hiển thị thông tin chi tiết về các host của khách hàng như là số lượng host theo loại host, số lượng host online hoặc offline, số lượng host trên mỗi nền tảng và hệ điều hành,.... Bảng điều khiển cũng hiển thị thông tin tổng quan cấp độ cao về pod cho các cloud container được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



Case #2: Quản Lý Host

Thông tin tổng quan của host

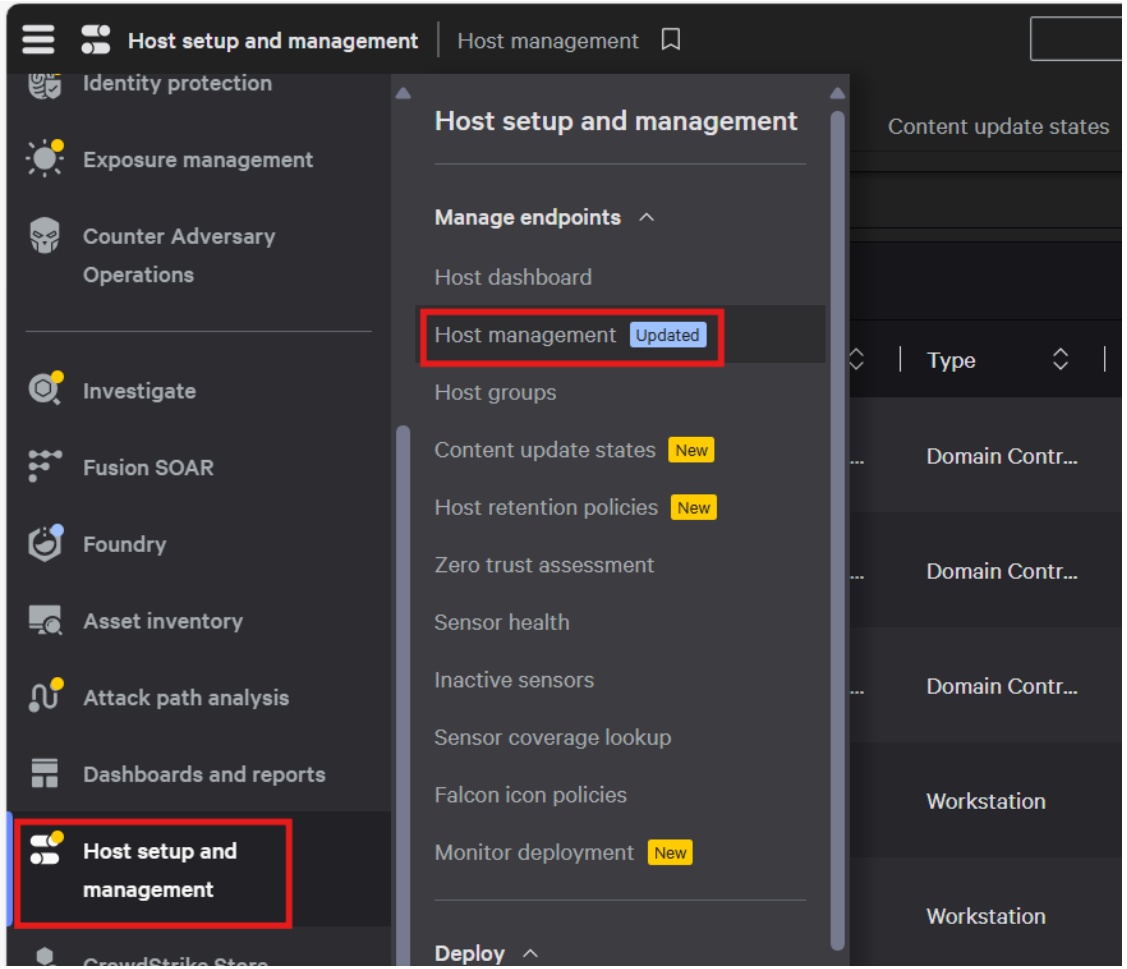
2. Ví dụ về **Host dashboard**



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.

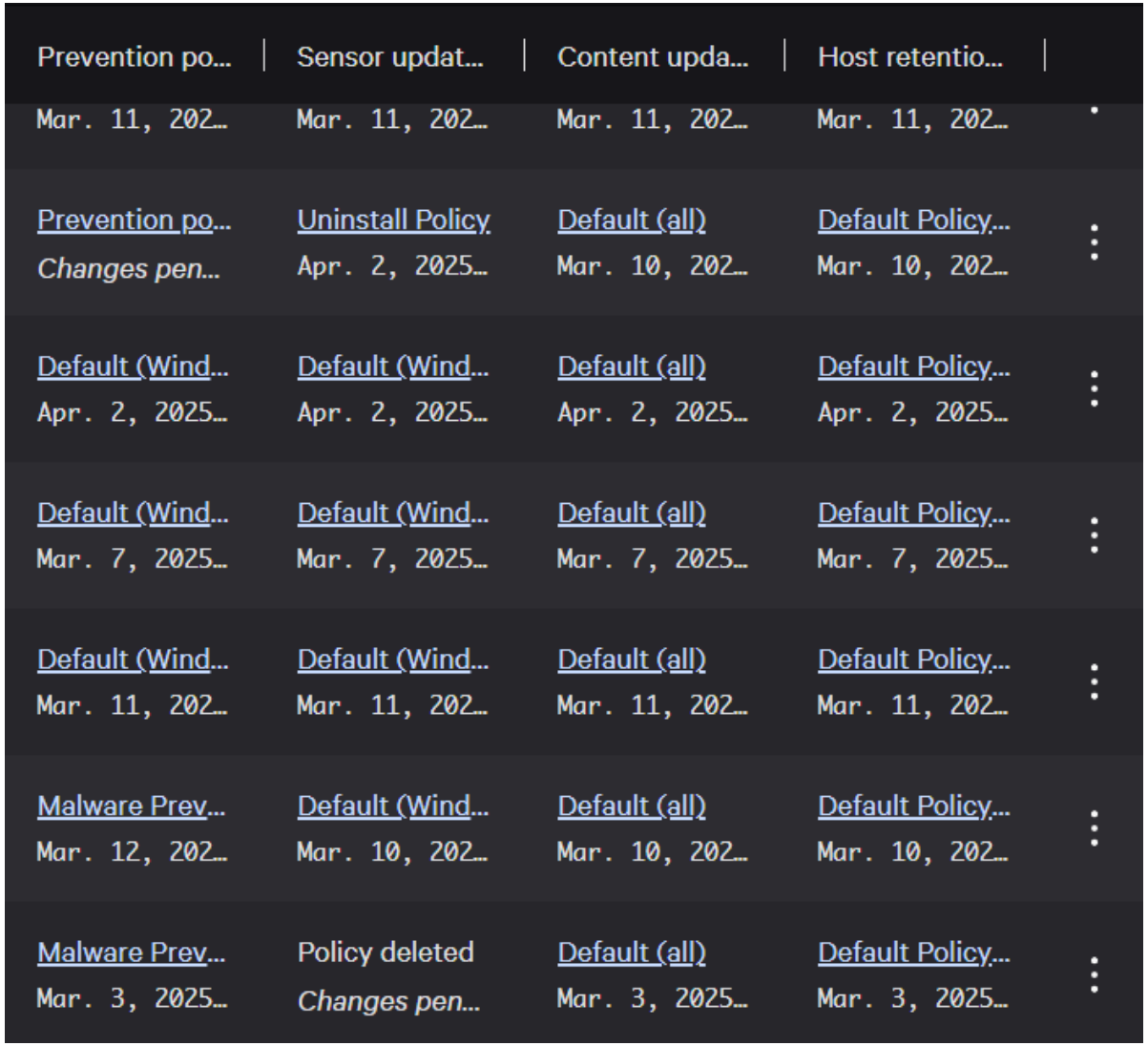


Case #2: Quản Lý Host

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.



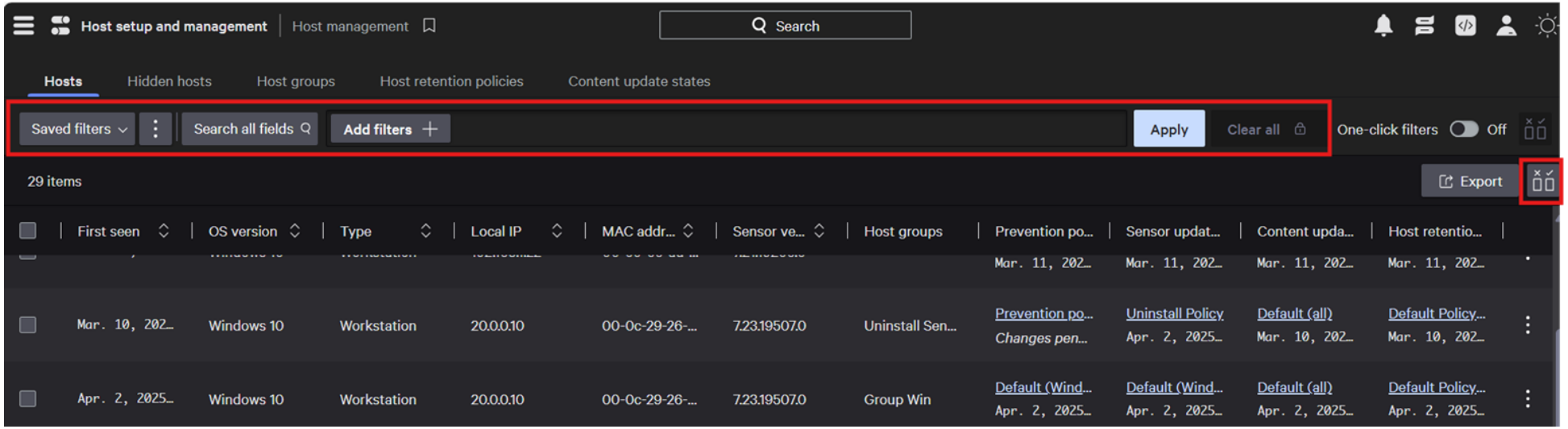
Case #2: Quản Lý Host

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.

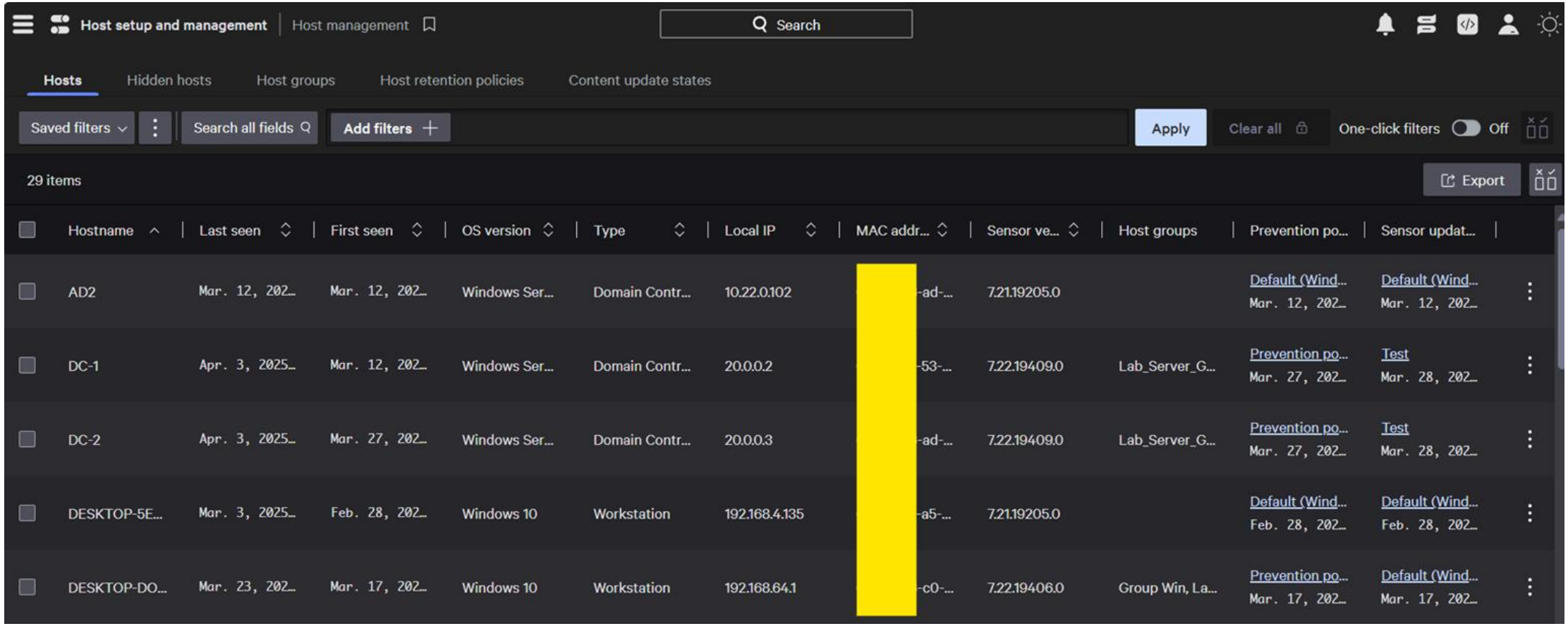
Để chọn các cột hiển thị trong bảng Host Management, nhấp vào biểu tượng , sau đó chọn các cột mong muốn.



Case #2: Quản Lý Host

Trang Host Management

4. Ví dụ bảng **Host management**



Case #2: Quản Lý Host

Trang Host Management

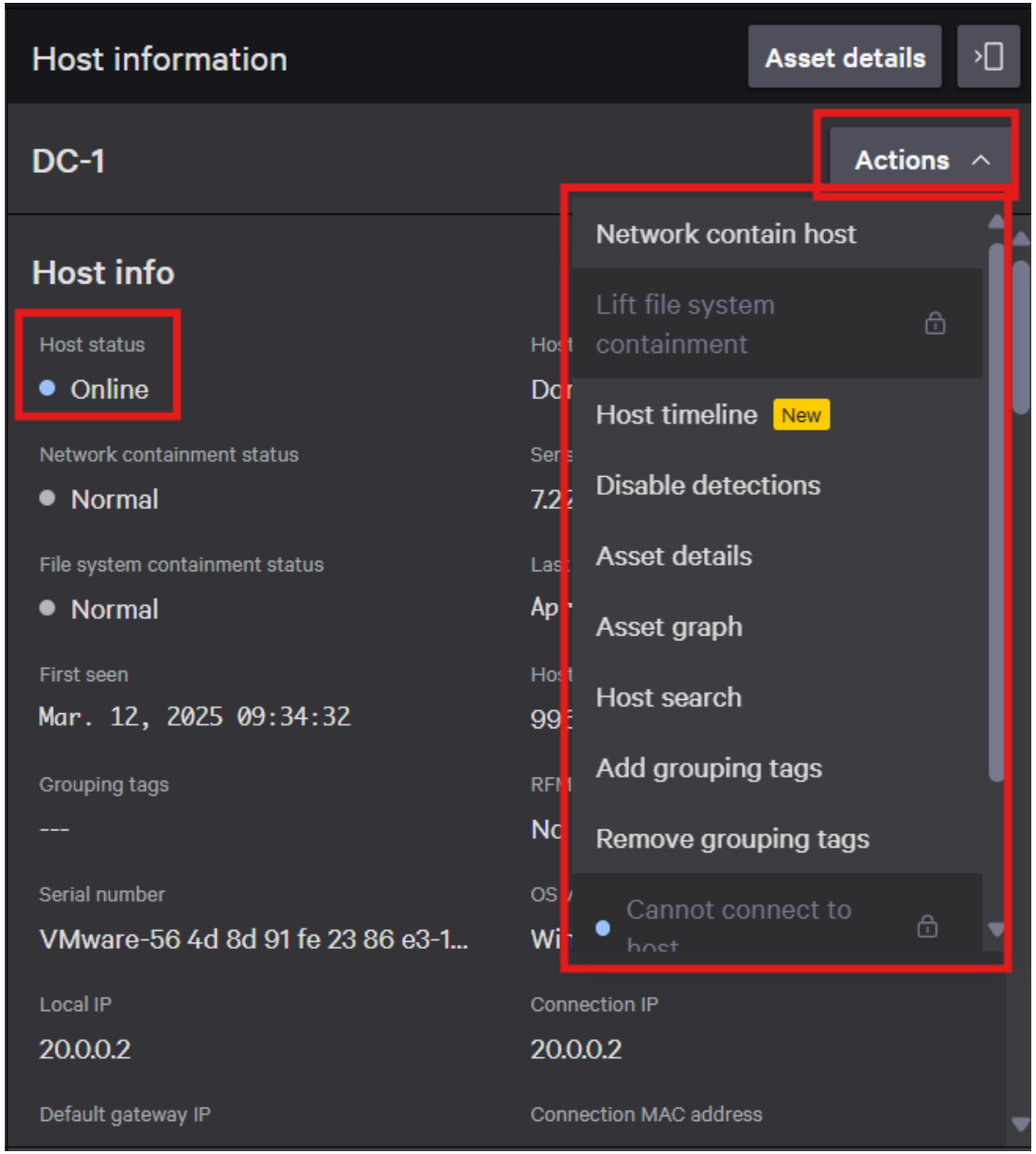
5. Xem **bảng tổng quan host**

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



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.

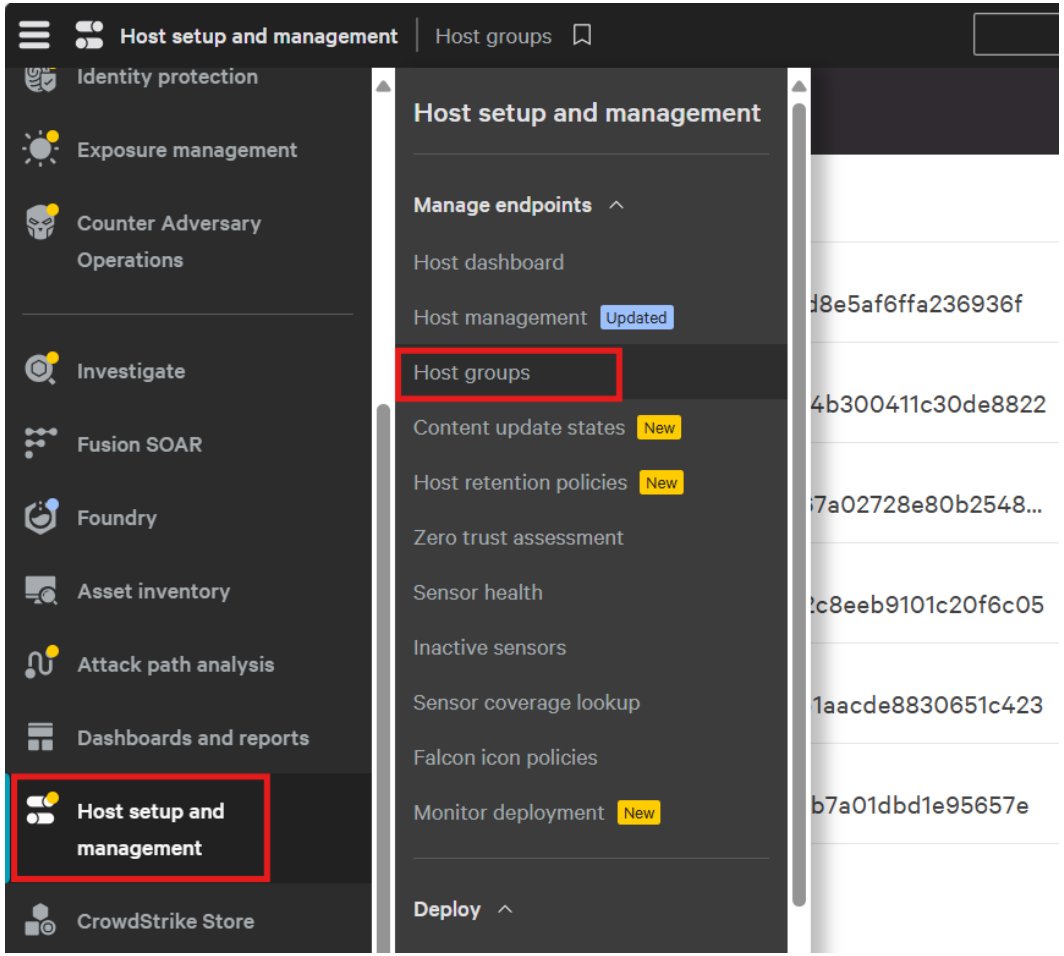
- Nhóm host dynamic sẽ trống sau khi tạo. Để thêm host, định nghĩa bộ lọc dựa trên các thuộc tính như thẻ nhóm, dải IP/CIDR, phiên bản hệ điều hành, OU Active Directory, hoặc tiền tố/hậu tố của tên host. Khi có các host phù hợp với quy tắc đã thiết lập từ trước, chúng sẽ tự động được thêm vào nhóm. Khi 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

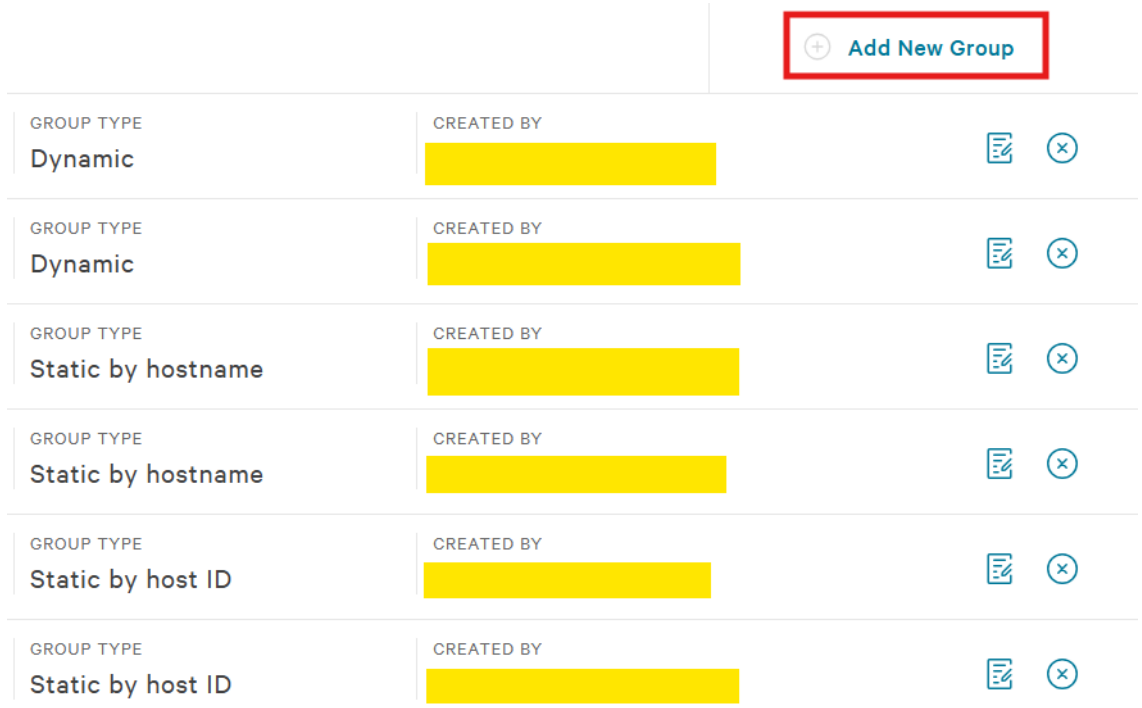
Case #3: Quản Lý Nhóm Host

Tạo một nhóm host

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

Chọn **Add New Group**.





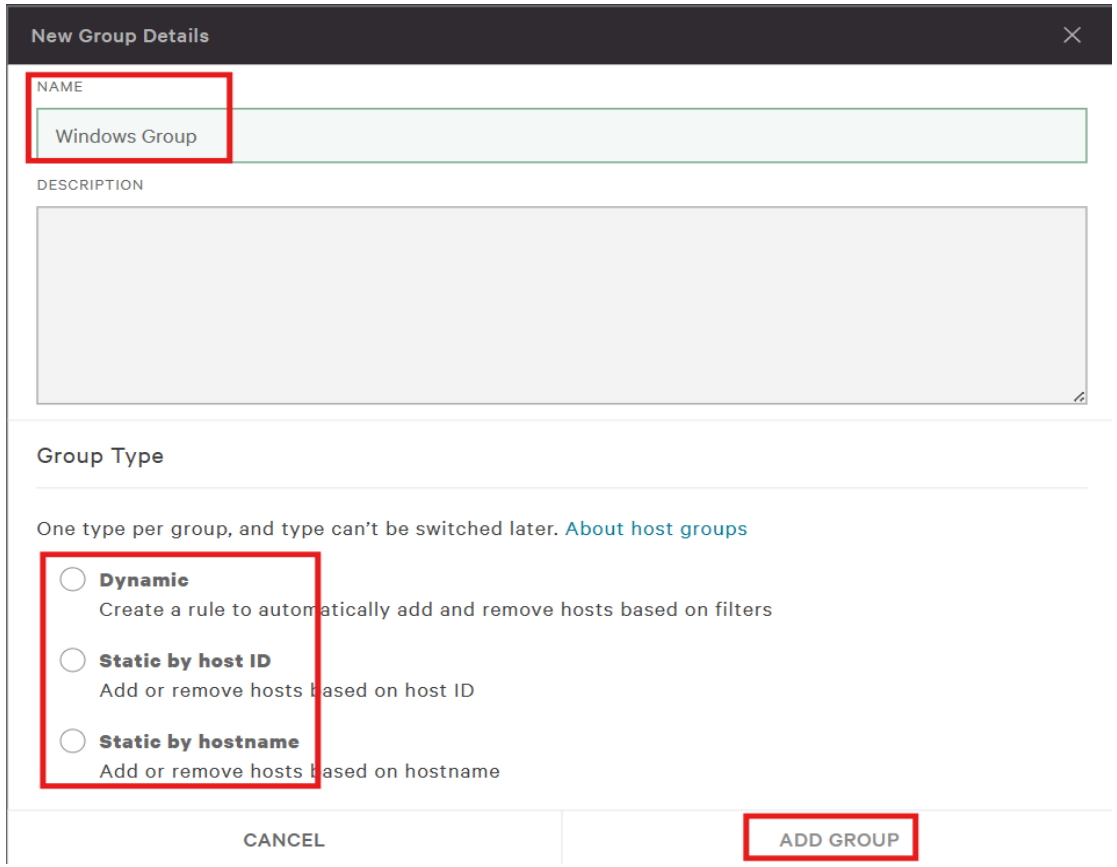
Case #3: Quản Lý Nhóm Host

Tạo một nhóm host

2. Điền tên, mô tả

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

- Chọn **ADD GROUP**

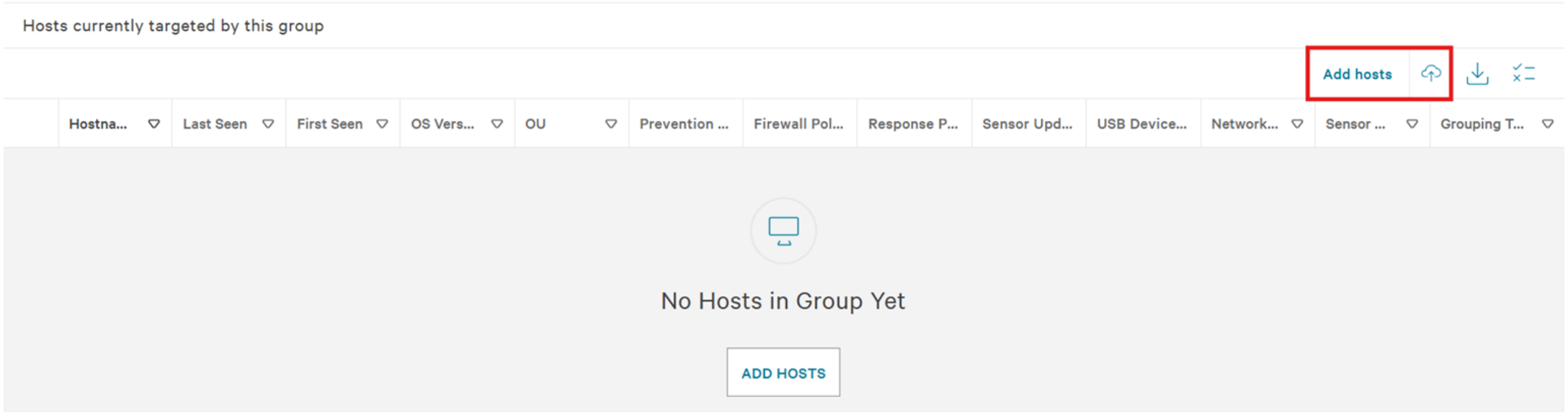


Case #3: Quản Lý Nhóm Host

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.

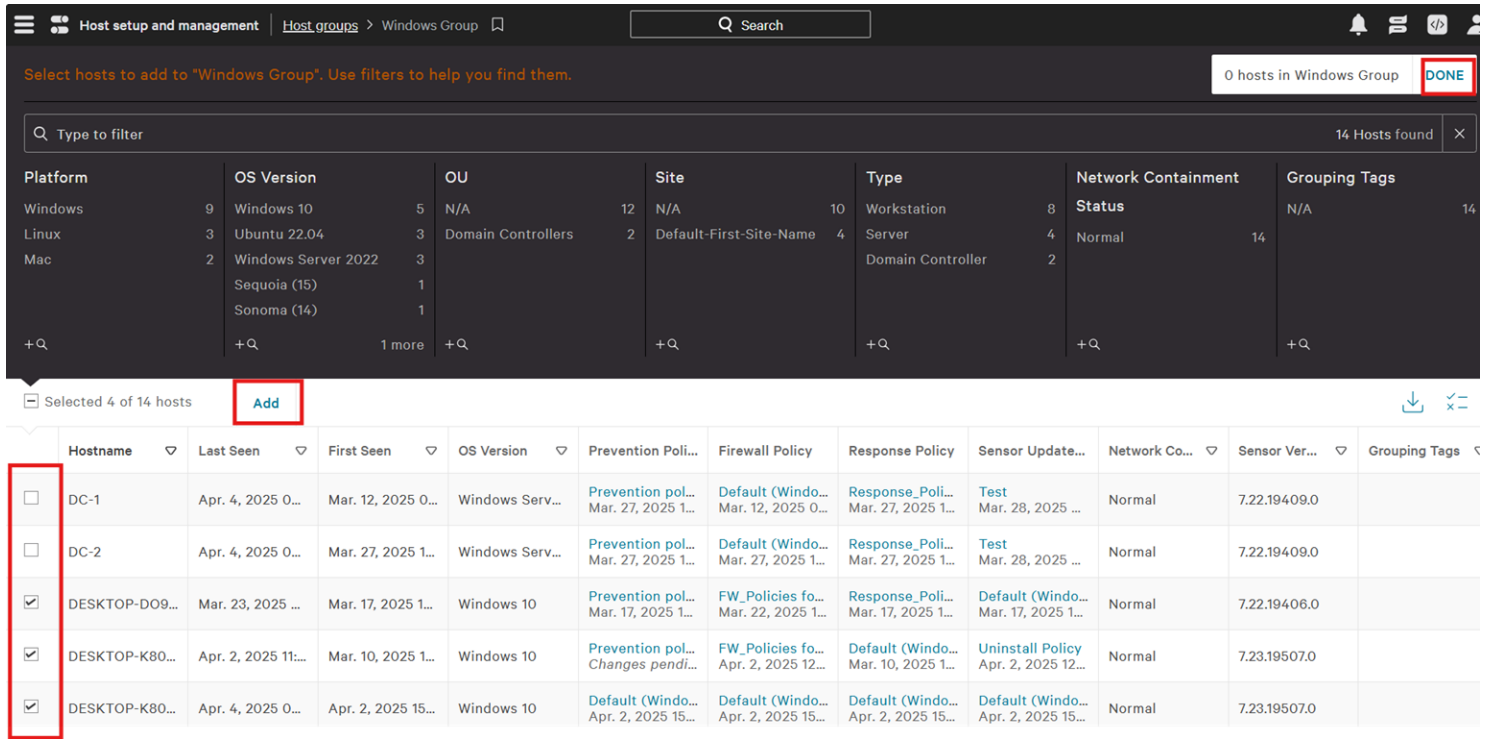


Case #3: Quản Lý Nhóm Host

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.



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.

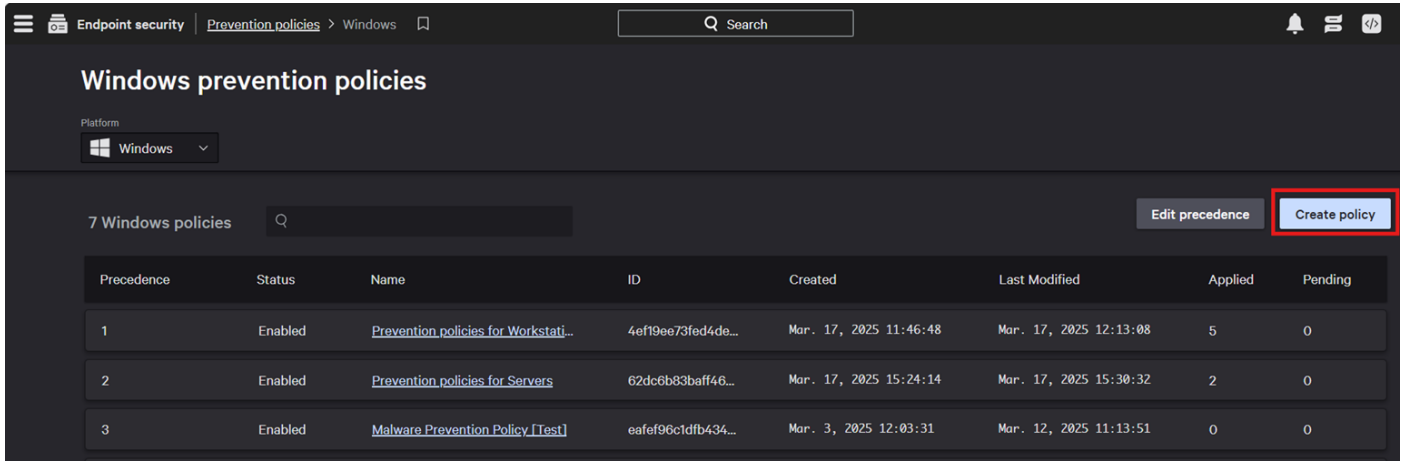
Thiết Lập Chính Sách Ngăn Chặn

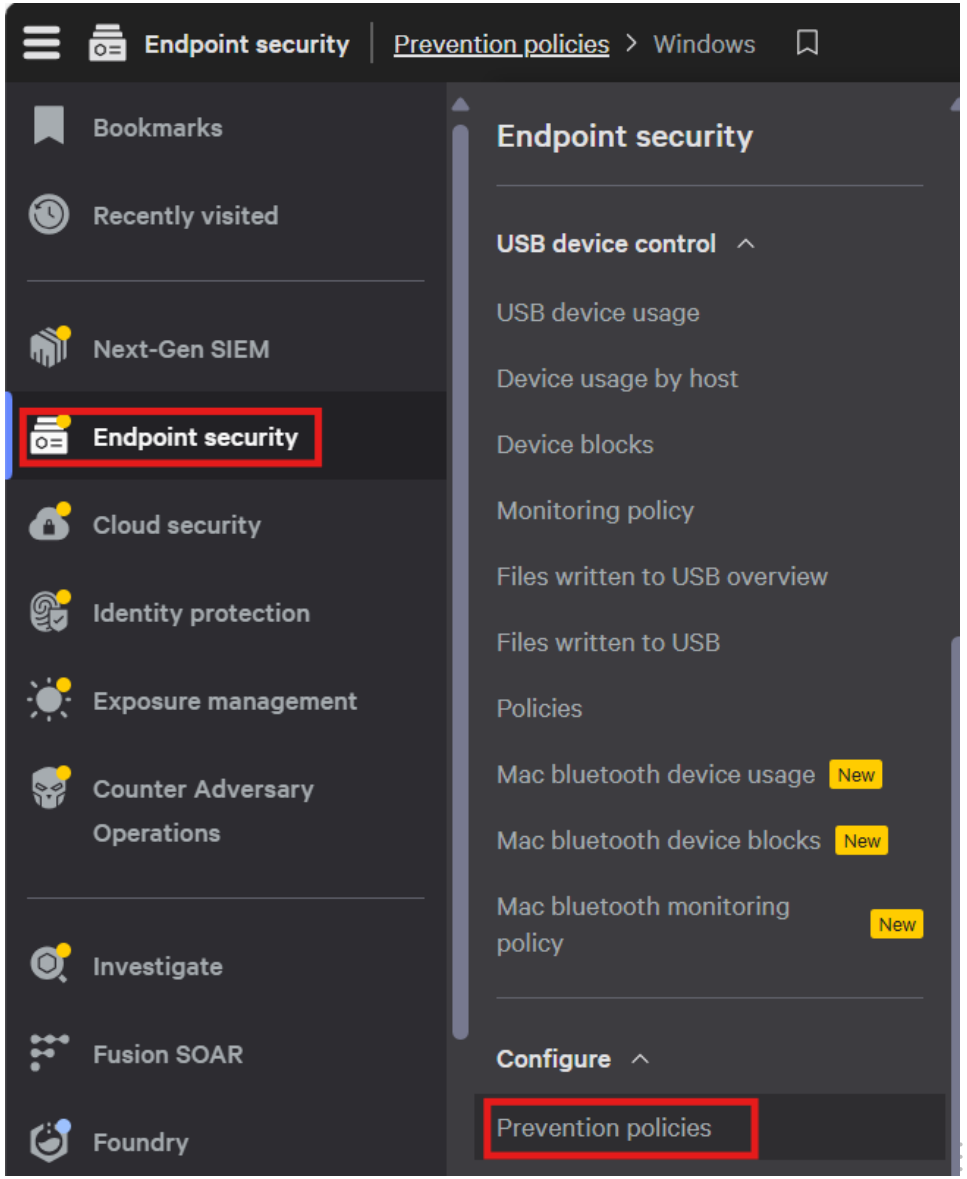
- Kiểm tra tất cả các chính sách đã thay đổi trong môi trường thử nghiệm trước và sau đó triển khai các thay đổi vào môi trường chính theo từng giai đoạn. Bạn có thể phân loại các phát hiện và điều chỉnh cài đặt khi cần thiết để thấy ít kết quả dương tính giả hơn, sử dụng quản lý IOC, ML và IOA exlusion.
- 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.**

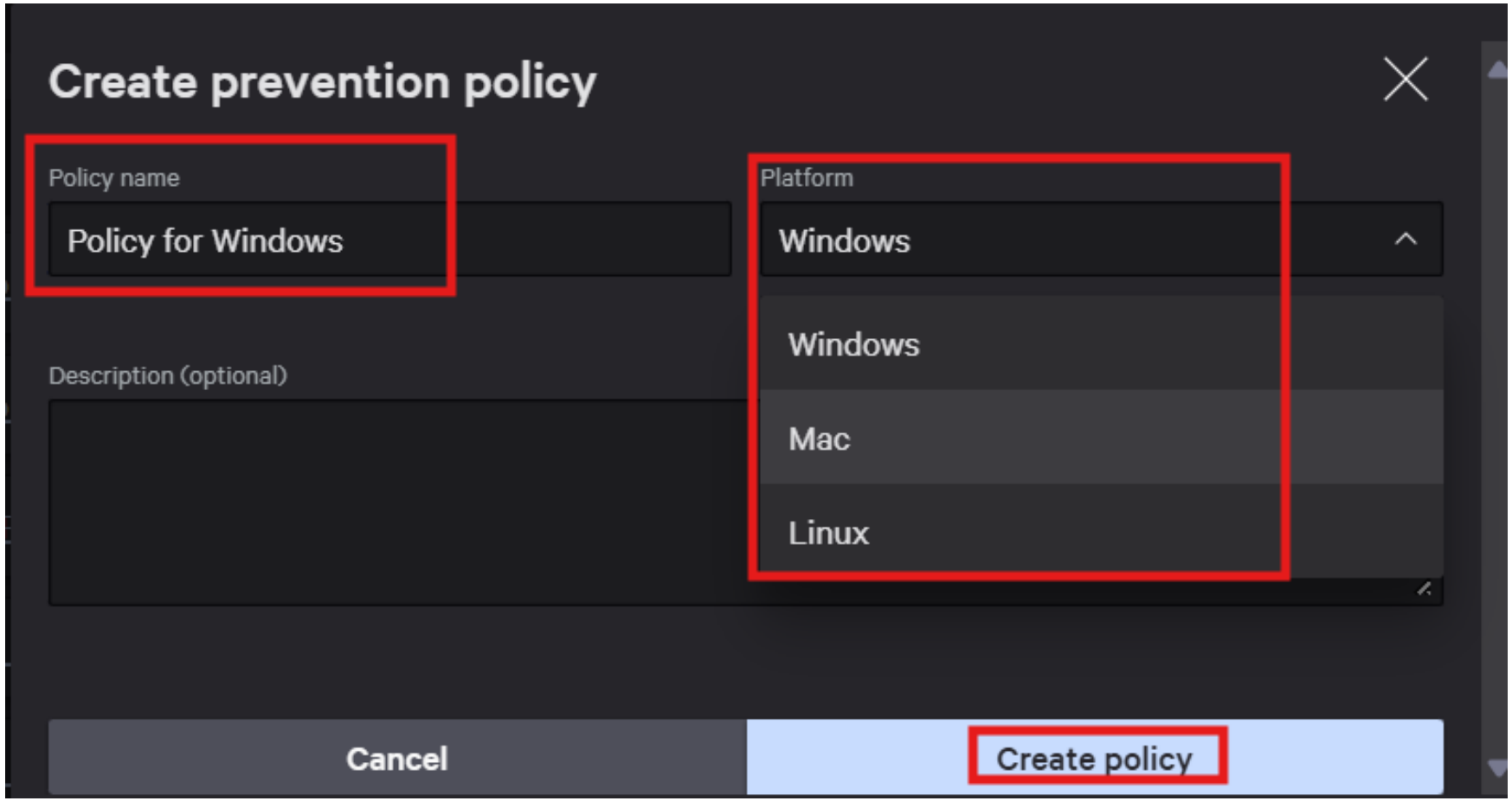




Case #4: Chính Sách Phát Hiện và Ngăn Chặn

1. Tạo chính sách

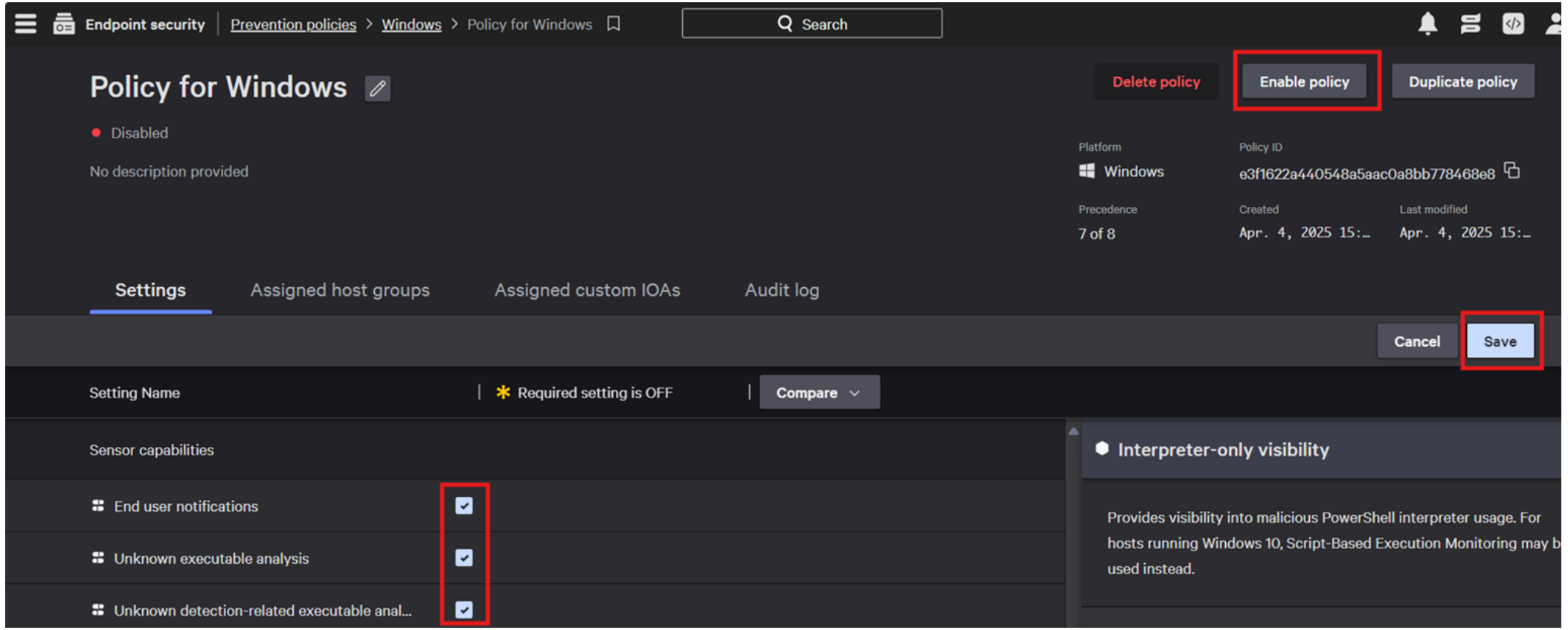
- Điền các thông tin về **platform**, **policy name**, và **description.**
- Chọn **Create Policy**



Case #4: Chính Sách Phát Hiện và Ngăn Chặn

1. Tạo chính sách

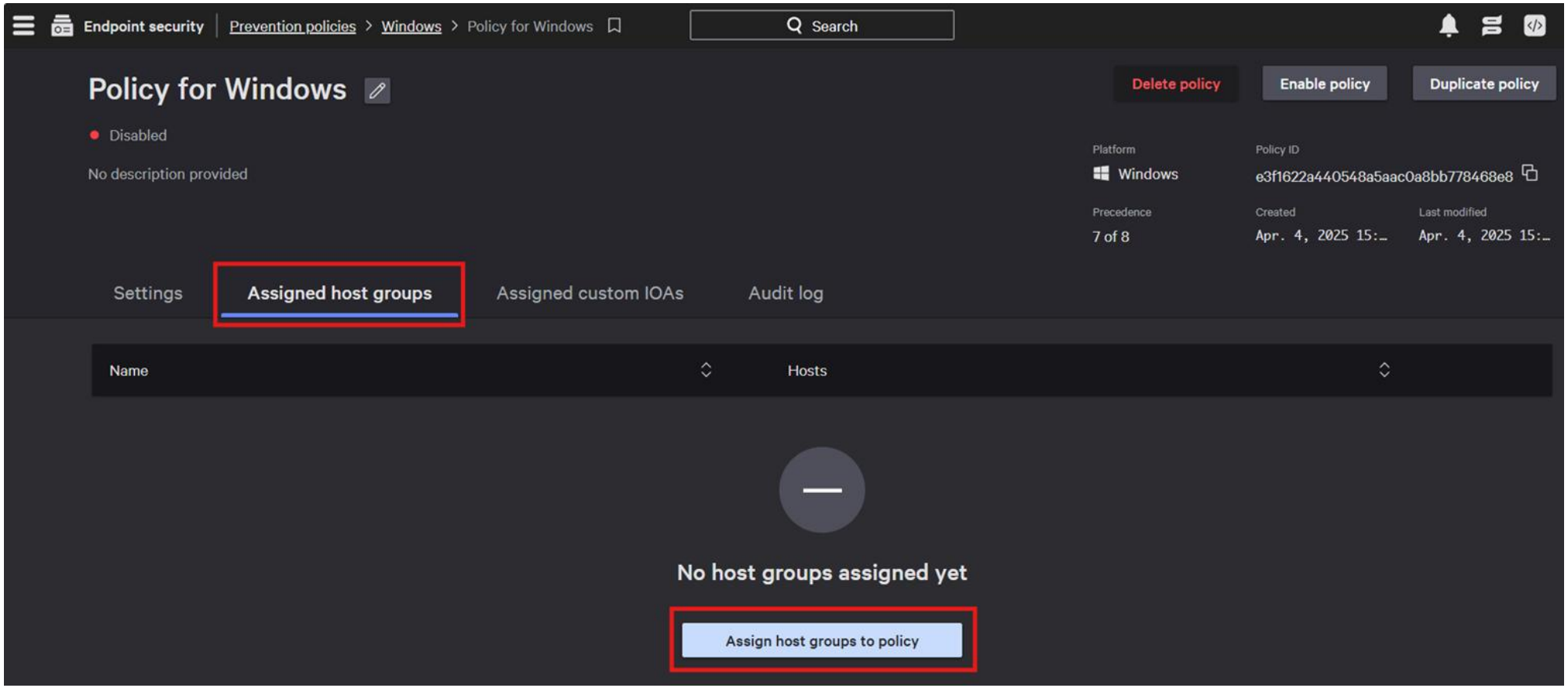
- **Enable** hoặc **disable** các thiết lập ngăn chặn trong tab **Settings**.
- Để lưu các thiết lập ngăn chặn, chọn **Save**, sau đó chọn **Confirm**.
- Để bật chính sách, chọn **Enable policy**.



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**

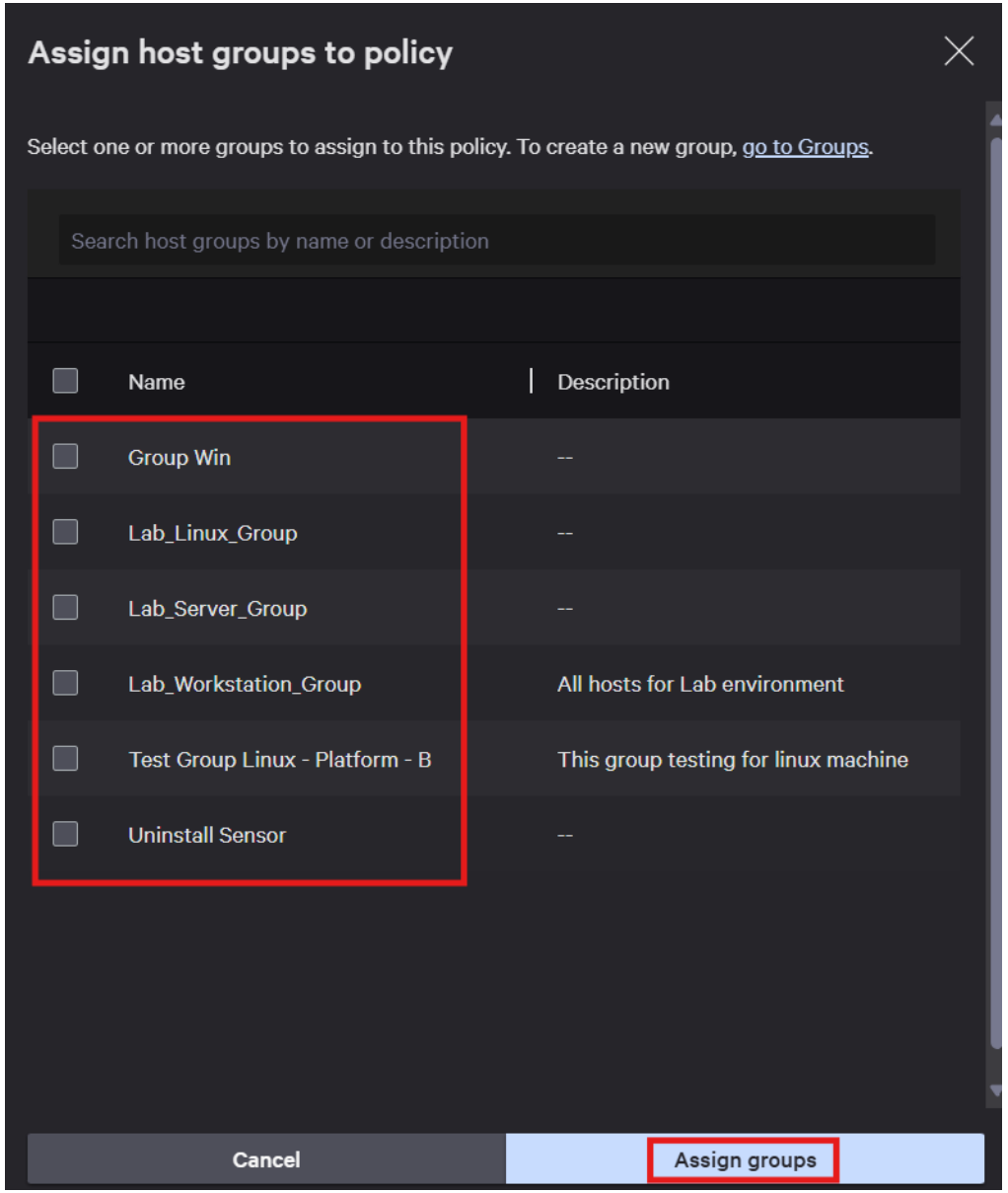


Case #4: Chính Sách Phát Hiện và Ngăn Chặn

2. Gán chính sách ngăn chặn vào một group host

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

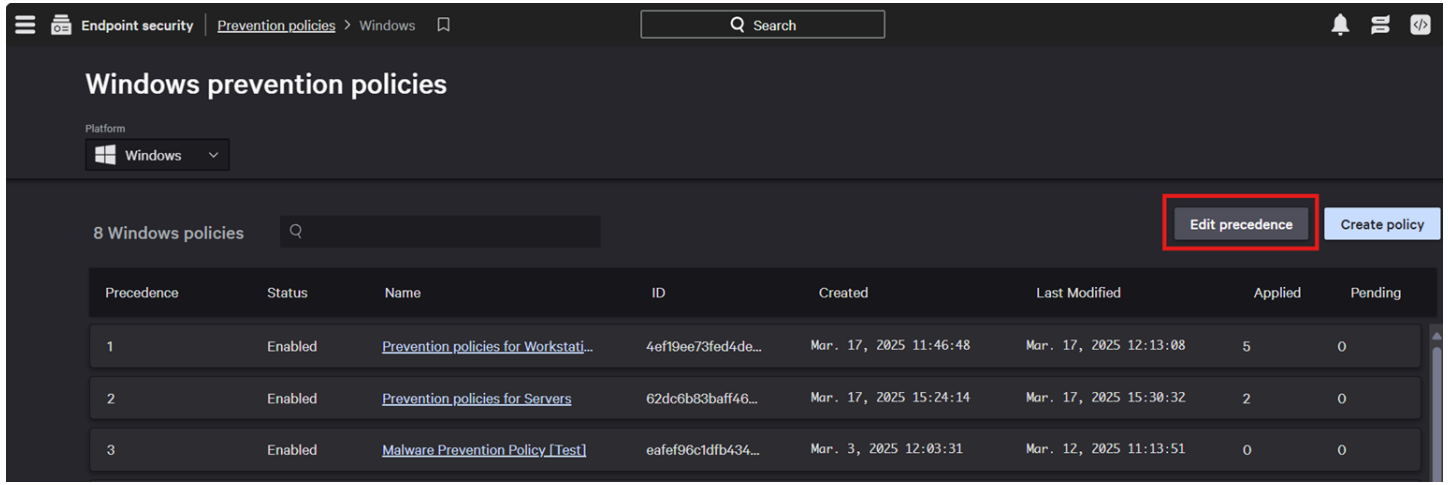
Sau khi bạn gán một group host cho một chính sách, group host đó sẽ không còn xuất hiện trong danh sách các group có sẵn.

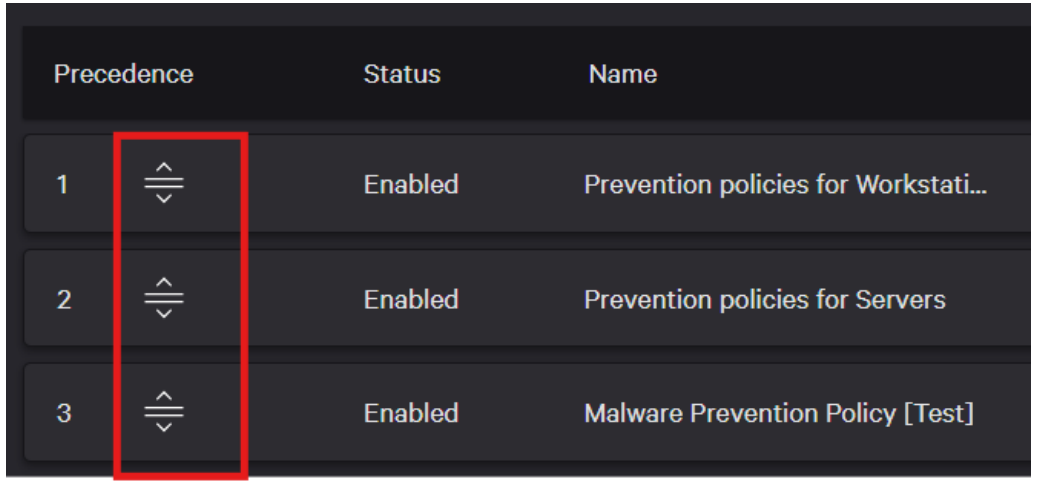


Case #4: Chính Sách Phát Hiện và Ngăn Chặn

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 chinh sách
- Chọn **Save**

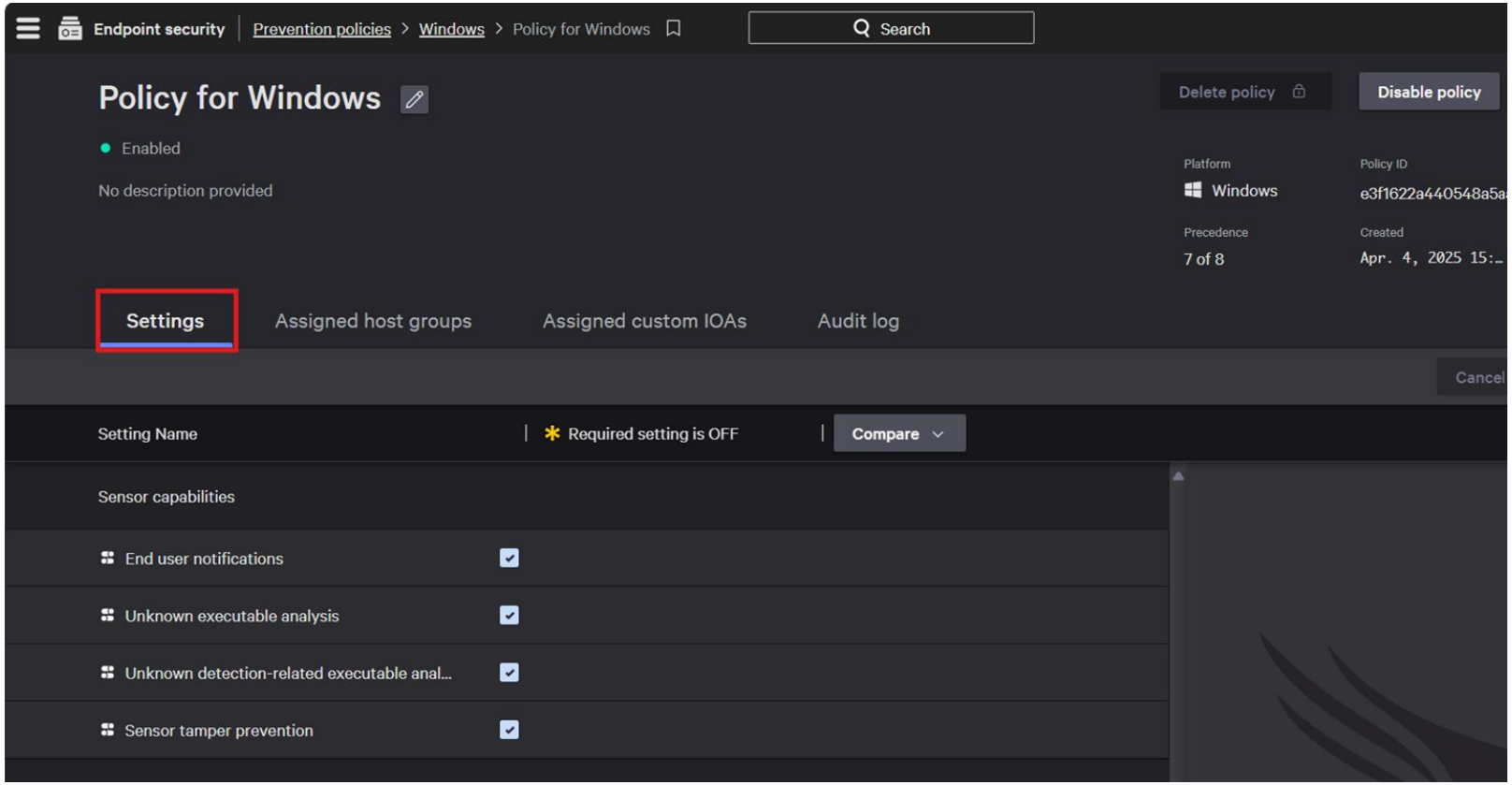




Case #4: Chính Sách Phát Hiện và Ngăn Chặn

4. Các thiết lập chính sách ngăn chặn

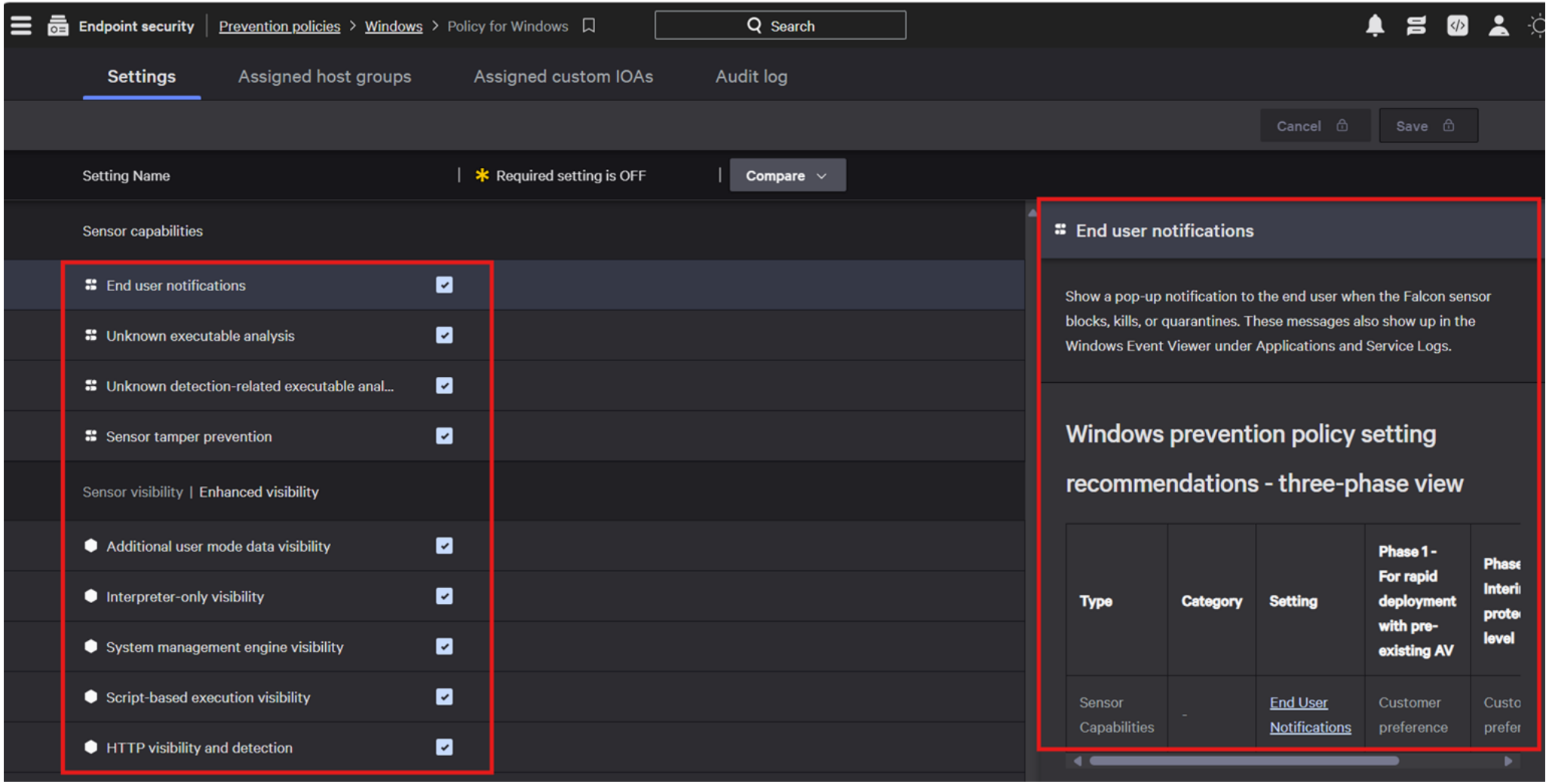
- Các chiến thuật playbook tiêu chuẩn cho kẻ thù tận dụng việc nâng quyền và đánh cắp thông tin đăng nhập. Những chiến thuật này cho phép di chuyển ngang hàng, khai thác hoặc xâm nhập vào các hệ thống trong môi trường của bạn. Do đó, việc có cái nhìn tổng quan về các hoạt động qua tất cả các giai đoạn 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.



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 nghi ba giai đoạn.

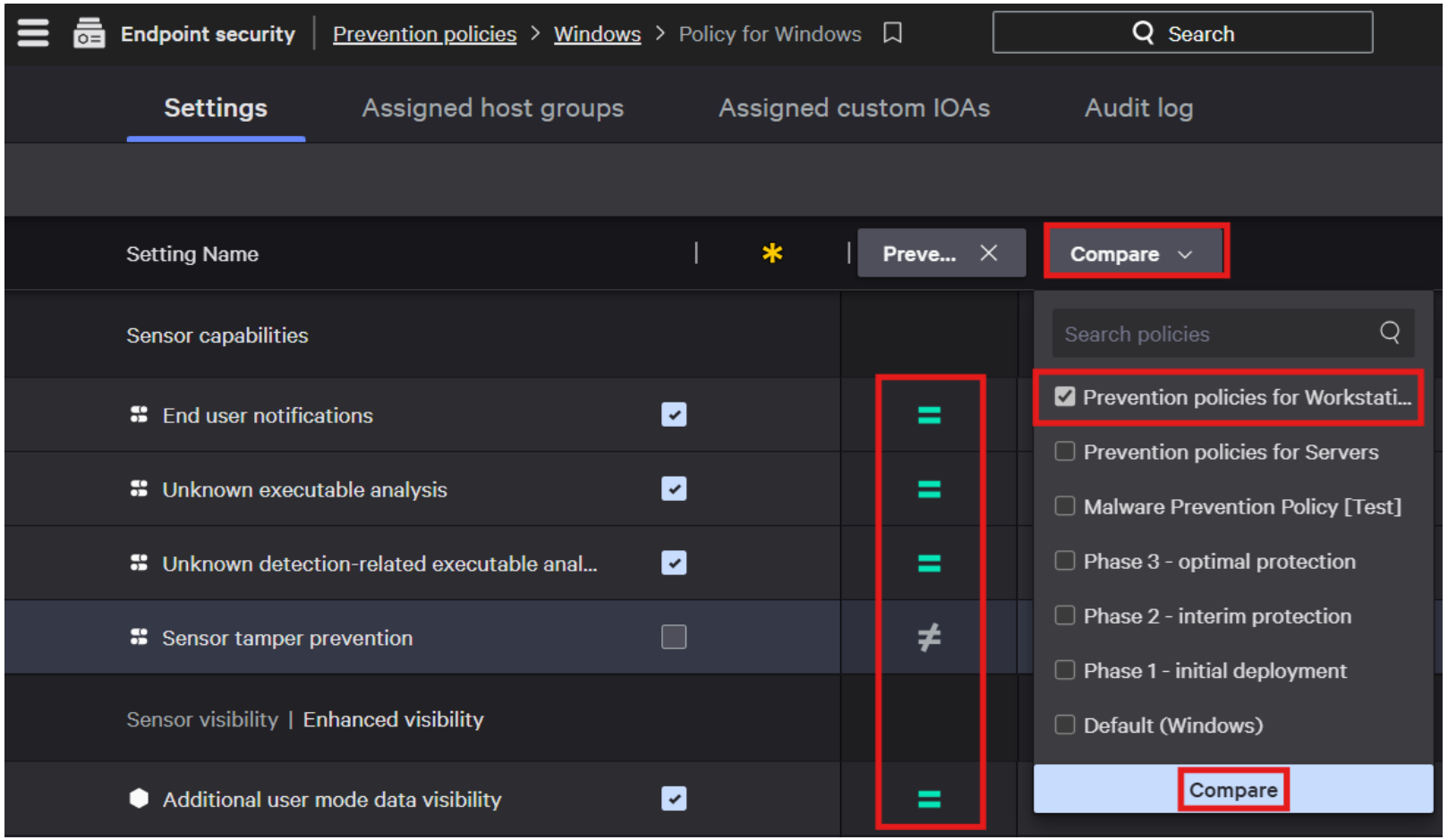


Case #4: Chính Sách Phát Hiện và Ngăn Chặn

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



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.

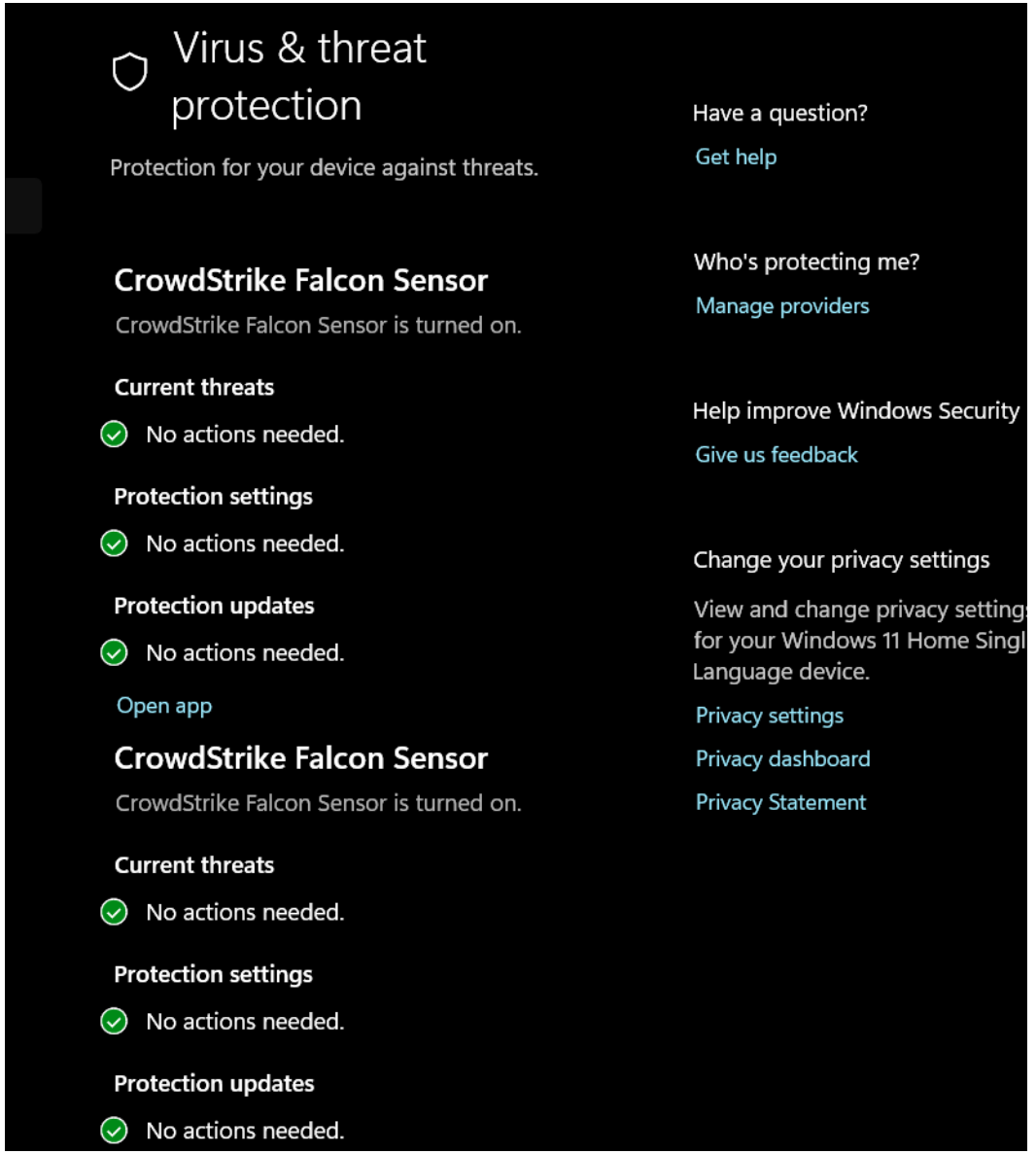
Lưu ý: Đối với triển khai lần đầu hoặc triển khai trong môi trường nhiều ứng dụng nhạy cảm, khuyến nghị sử dụng chính sách giai đoạn 1 (Chỉ phát hiện) hoặc 2 (Bảo vệ tối thiểu) để theo dõi và tránh xung đột với các ứng dụng ngay khi vừa triển khai

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

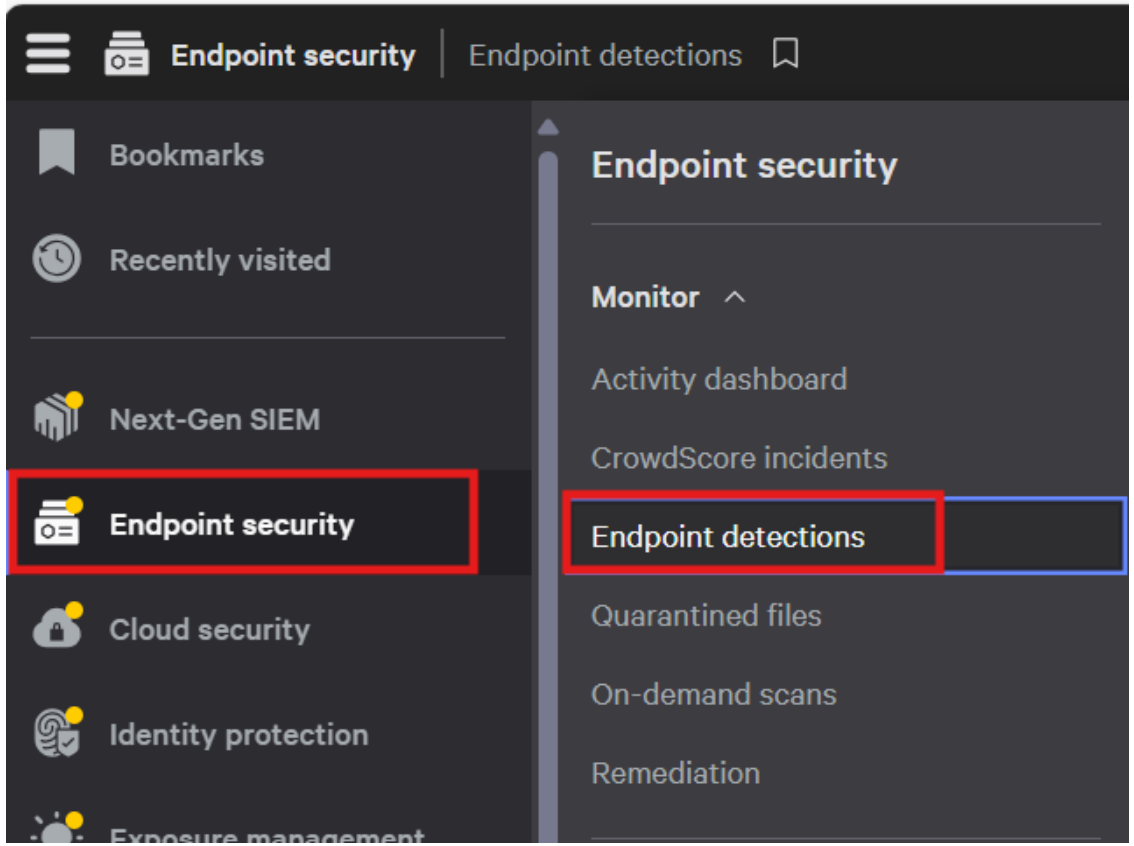
Giám sát các phát hiện từ endpoint để hiểu hoạt động đang diễn ra trong môi trường. Xem thông tin chi tiết về các process, tệp, hành vi nghi ngờ và kết quả quét theo yêu cầu.

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**.

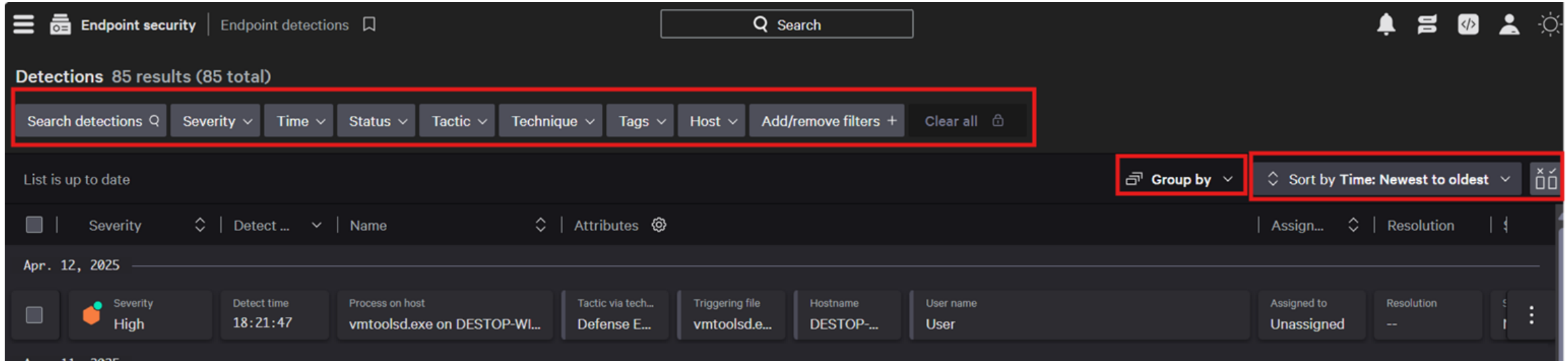


Case #5: Endpoint Monitoring

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**.

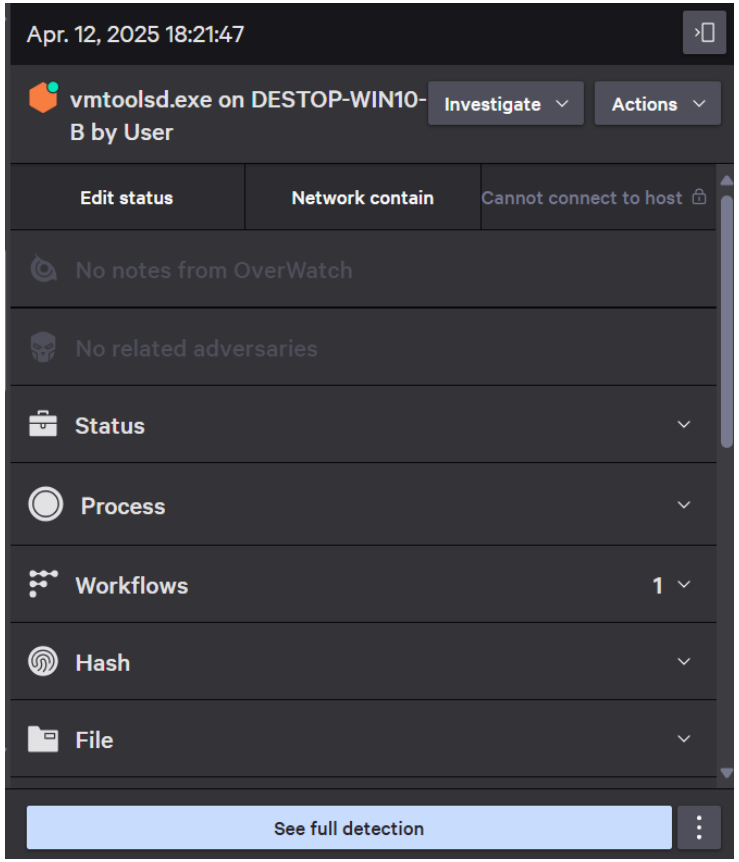


Case #5: Endpoint Monitoring

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



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.