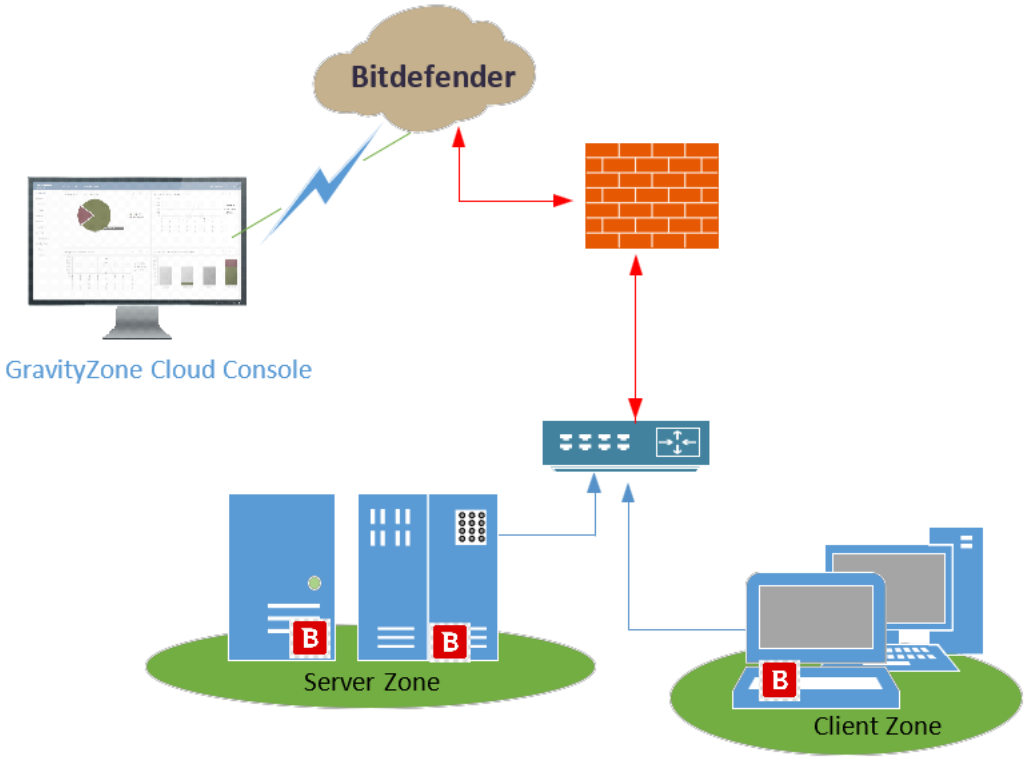
I. Kiến trúc GravityZone Cloud



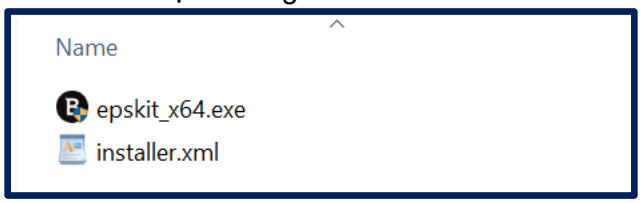
Bao gồm:

- GravityZone Console Cloud: [Bitdefender GravityZone]
- Các agent cài trên các máy trạm bên trong Doanh Nghiệp

II. CÁC BƯỚC CÀI ĐẶT VÀ KIỂM TRA ĐỐI VỚI NGƯỜI DÙNG ĐẦU CUỐI

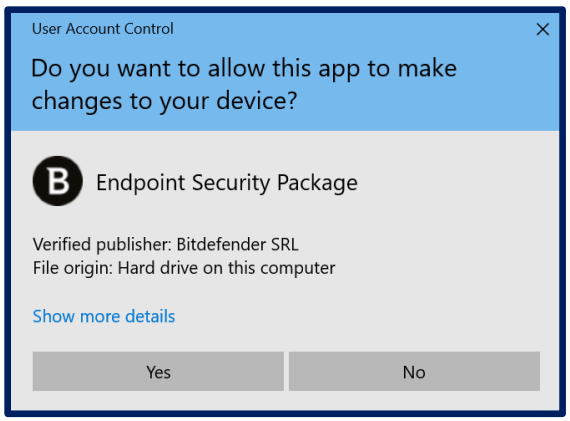
1. Tải gói cài đặt qua link Google Drive tương ứng cho win 32 bit hay 64 bit (không phân biệt win 7,10,11)
2. Cài đặt cho win 10/11

- Tải bản cài đặt về và giải nén

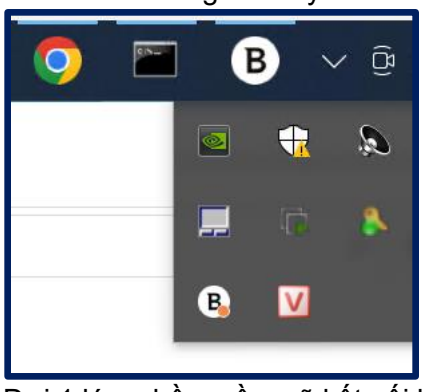


***Lưu ý: file exe và file installer.xml phải trong cùng 1 thư mục

- Thực hiện chạy file exe



- Yes và đợi thực hiện cài, trong quá trình cài Bit sẽ yêu cầu gỡ các phần mềm diệt virus free hay có phí tương ứng để tiếp tục cài.
- Sau khi cài xong sẽ thấy icon trên máy



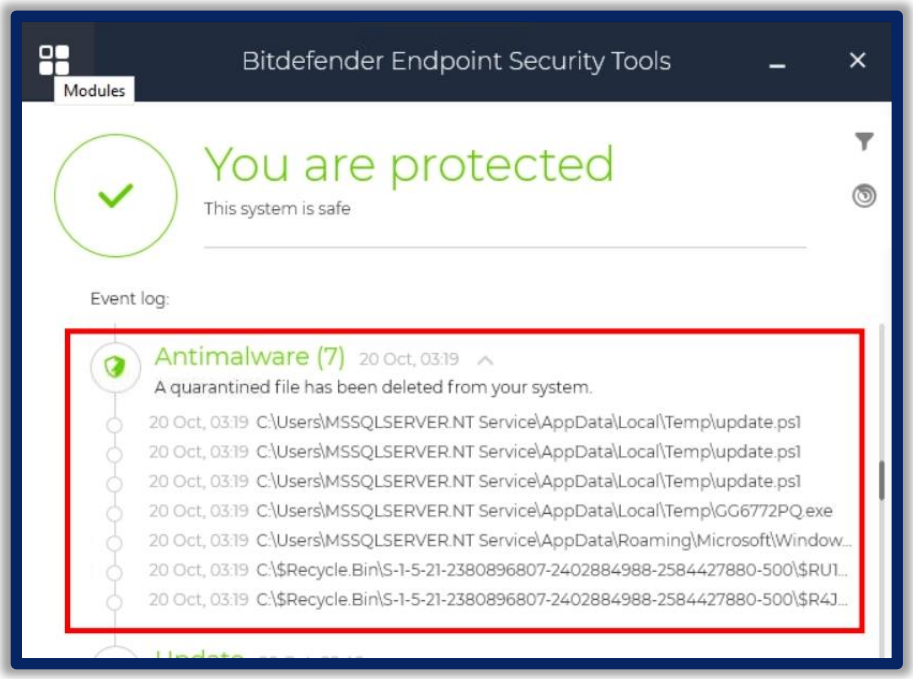
- Đợi 1 lúc, phần mềm sẽ kết nối lên Cloud Console và hiển thị trang tháy sau:

*** Do yêu cầu full scan > thực hiện full scan hoặc scan vào giờ thấp điểm.

- Trạng thái hoàn thiện như sau:

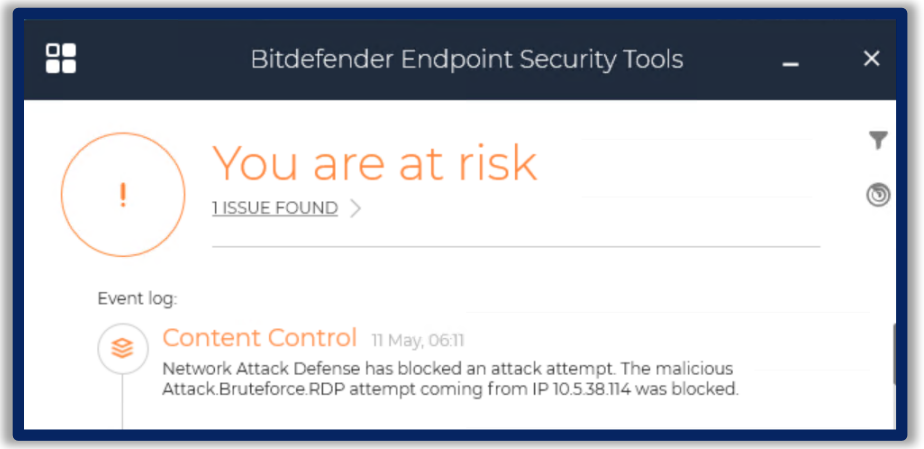
*** Hệ thống an toàn

- Các trường hợp phần mềm chặn và bảo vệ máy tính cho User như sau:

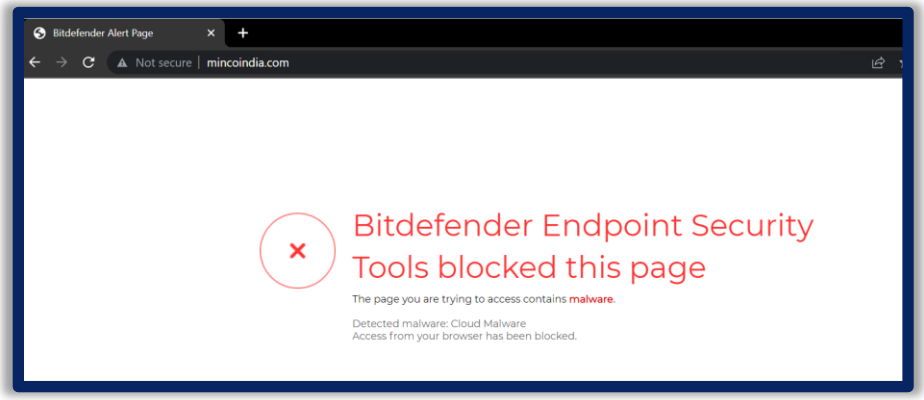


*** Ngăn chặn các file nhiễm mã độc và cách ly

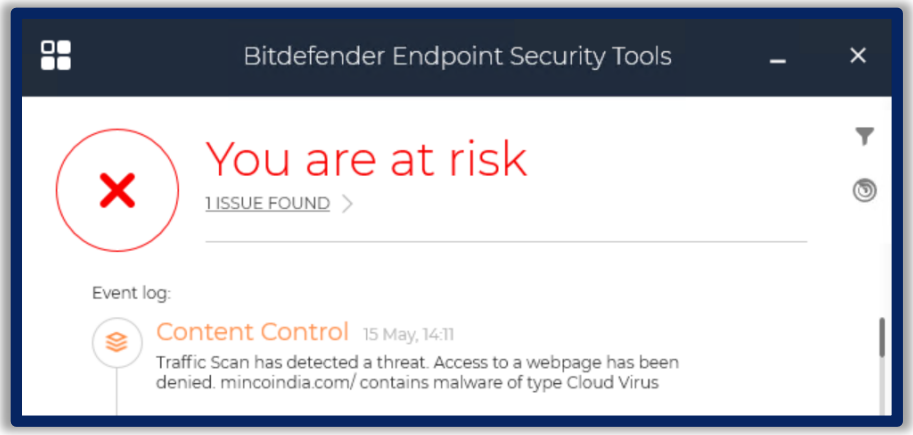
*** Ngăn chặn các hành vi tấn công lớp mạng, scan port



*** Ngăn chặn hành vi tấn công lớp mạng, Bruteforce



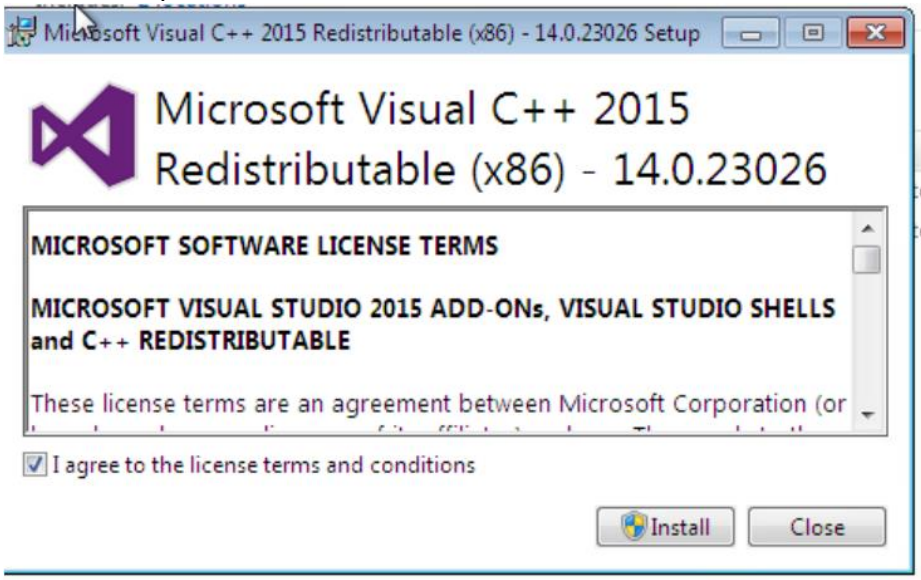
*** Ngăn chặn truy cập vào các trang web độc hại

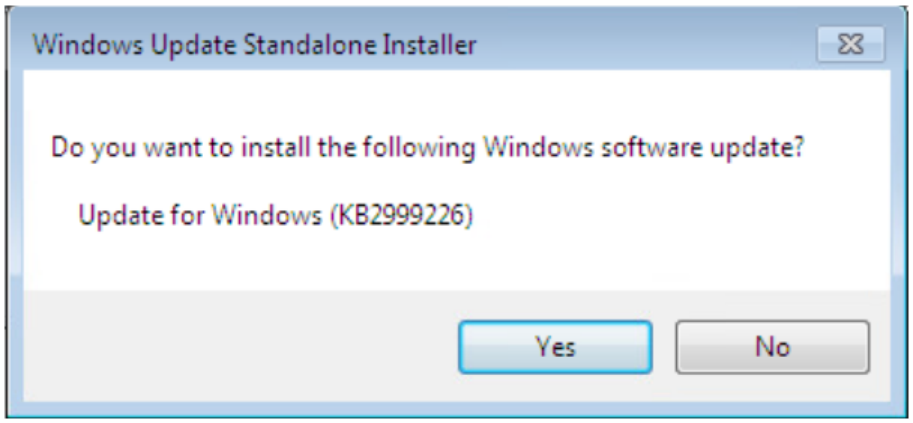


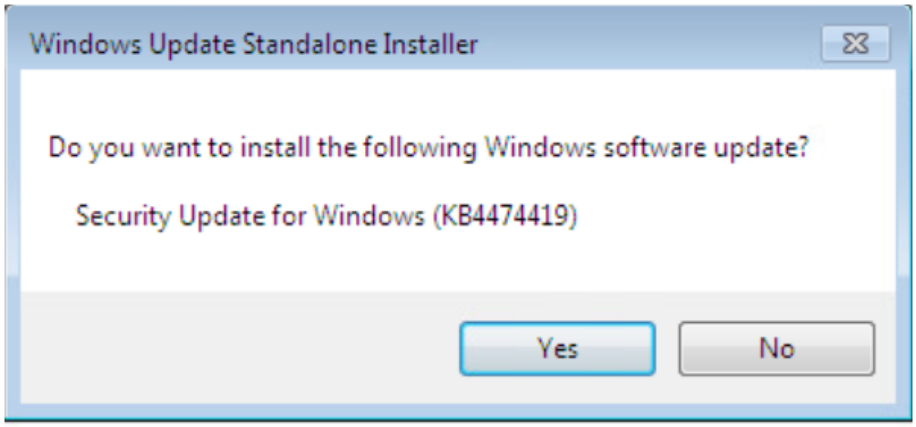
*** Ngăn chặn tải các phần mềm, mã độc từ internet

3. Cài đặt cho win 7

- Win 7 cần cập nhật Patch và Certificate
- Link down các cập nhật (theo phiên bản win): https://drive.google.com/drive/folders/11ZFwu95E0uRFqnDp6sA49iy0NTiRQA0H?usp=drive_link
- Link down các Certificate https://drive.google.com/drive/folders/1sORQFVvGbL_i-d525eyVM8Xoemy27hz7?usp=drive_link
- Thực hiện update theo thứ tự các file

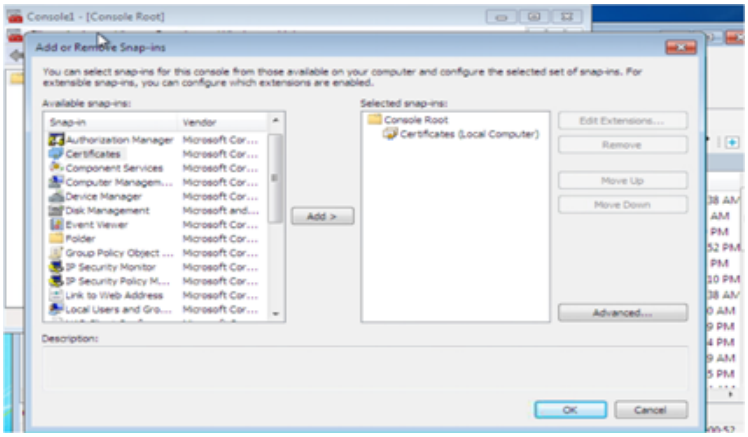


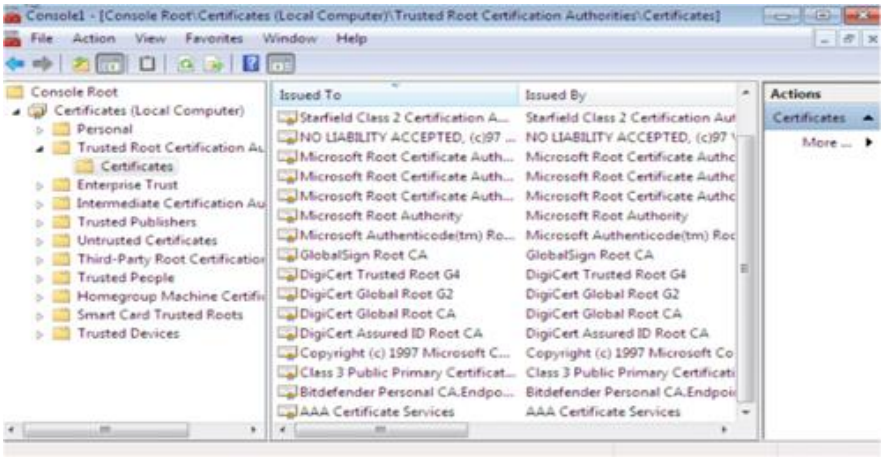




*** Nếu bước cài đặt file đầu tiên vc_redist bị lỗi thì nhưng cài đặt, vì đây là lỗi dịch vụ trên win7 không thể khắc phục

- Tiếp theo cập nhật Certificate cho Win 7
- Sau khi down các Certificate > vào Search > mmc > Add or Remove Snap-ins > Certificate > personal > Trusted Root Certification Auth > Certificates > Click phải > Import > Chọn các Certificate lúc nãy



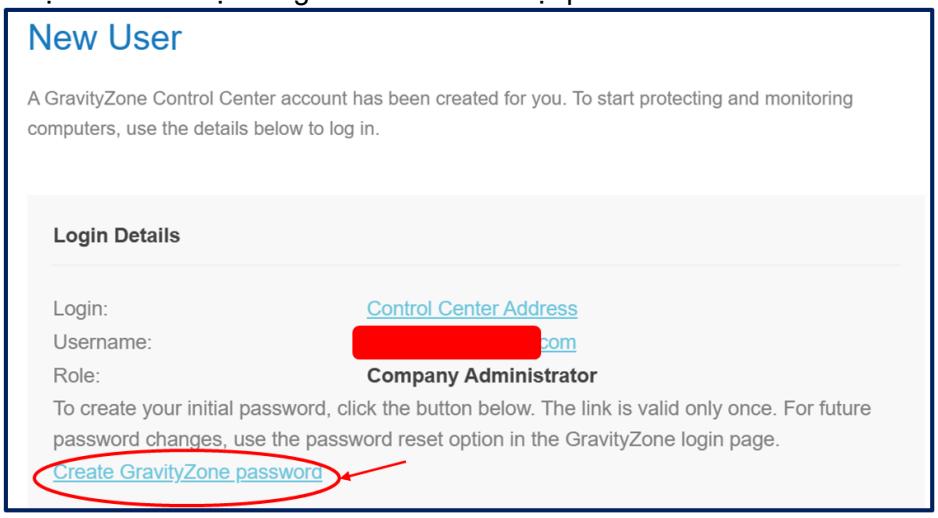


- Sau khi import xong > chạy lại file cài đặt và tiến hành cài tương tự Win 10/11
- Kiểm tra trạng thái như Win 10/11

III. CÁC BƯỚC QUẢN TRỊ DÀNH CHO ADMIN

1. Login vào GravityZone Console

- Nhận email từ hệ thống > tiến hành cài đặt password & 2FA



New User

A GravityZone Control Center account has been created for you. To start protecting and monitoring computers, use the details below to log in.

Login Details

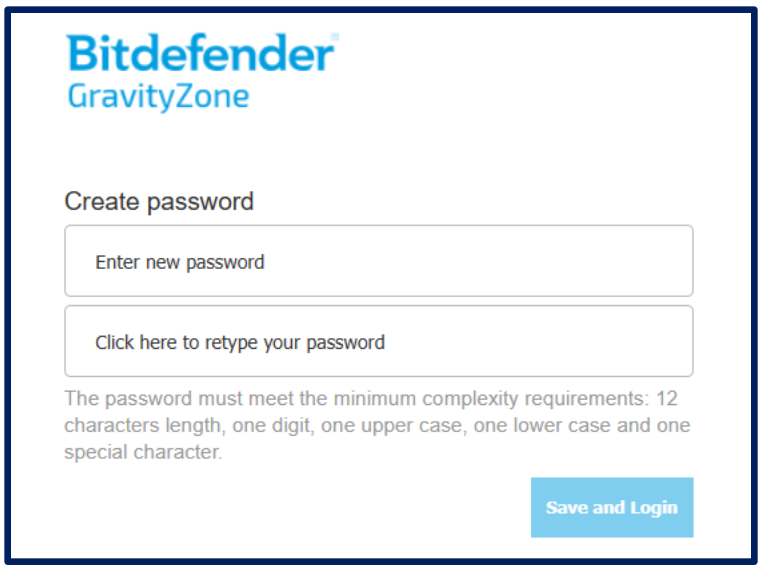
Login: Control Center Address

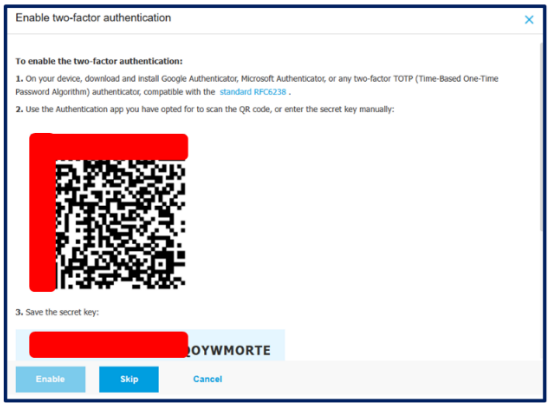
Username: [redacted]com

Role: **Company Administrator**

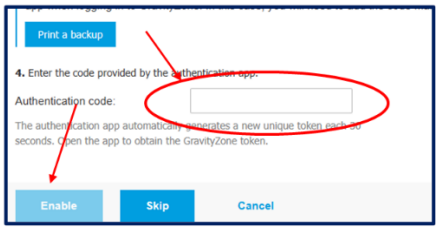
To create your initial password, click the button below. The link is valid only once. For future password changes, use the password reset option in the GravityZone login page.

Create GravityZone password

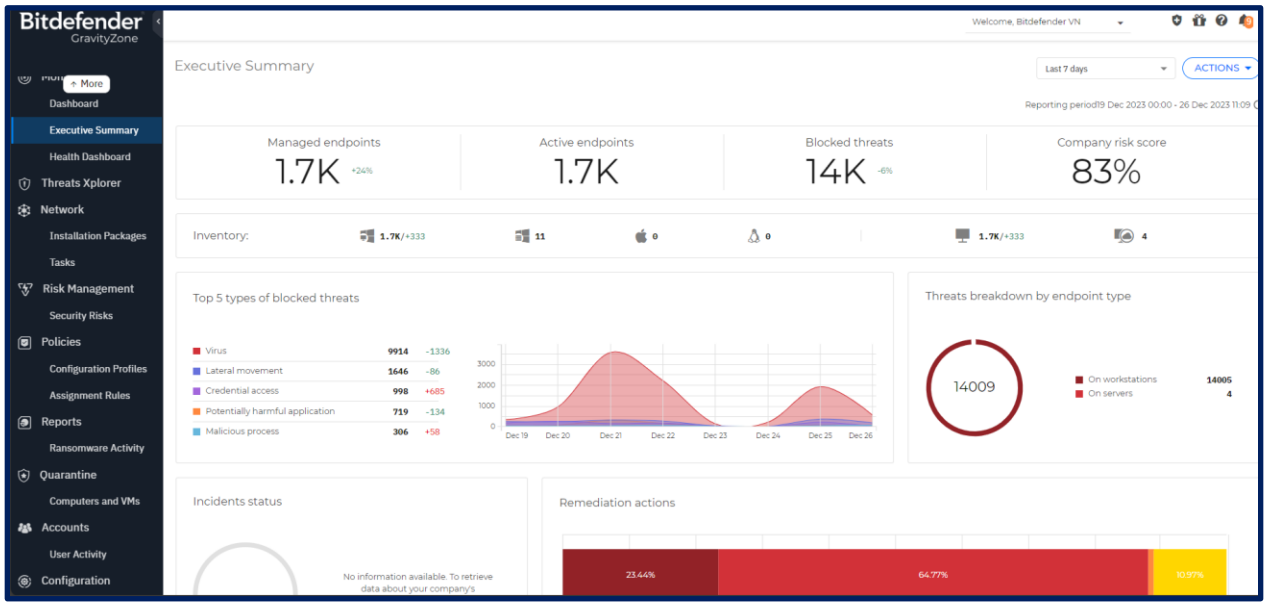




Sử dụng GG authen trên điện thoại
Sau khi scan QR code nhập mã số trên Apps để kích hoạt

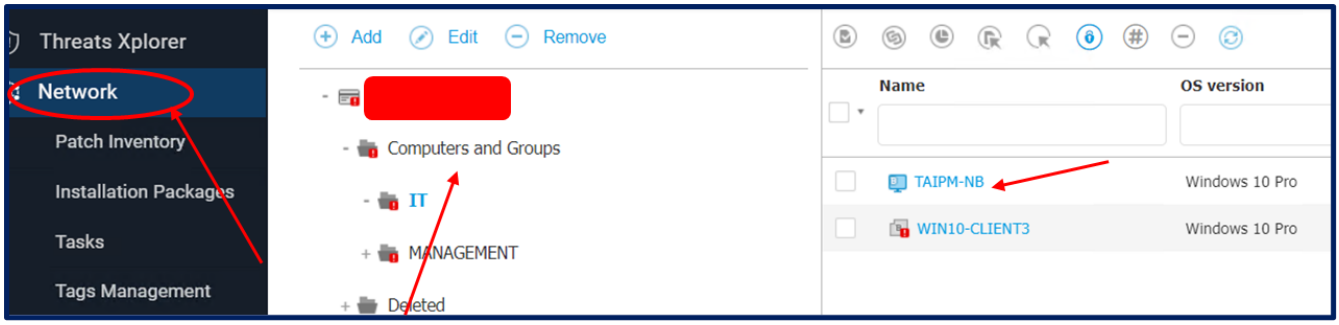


- Giao diện sau khi đăng nhập

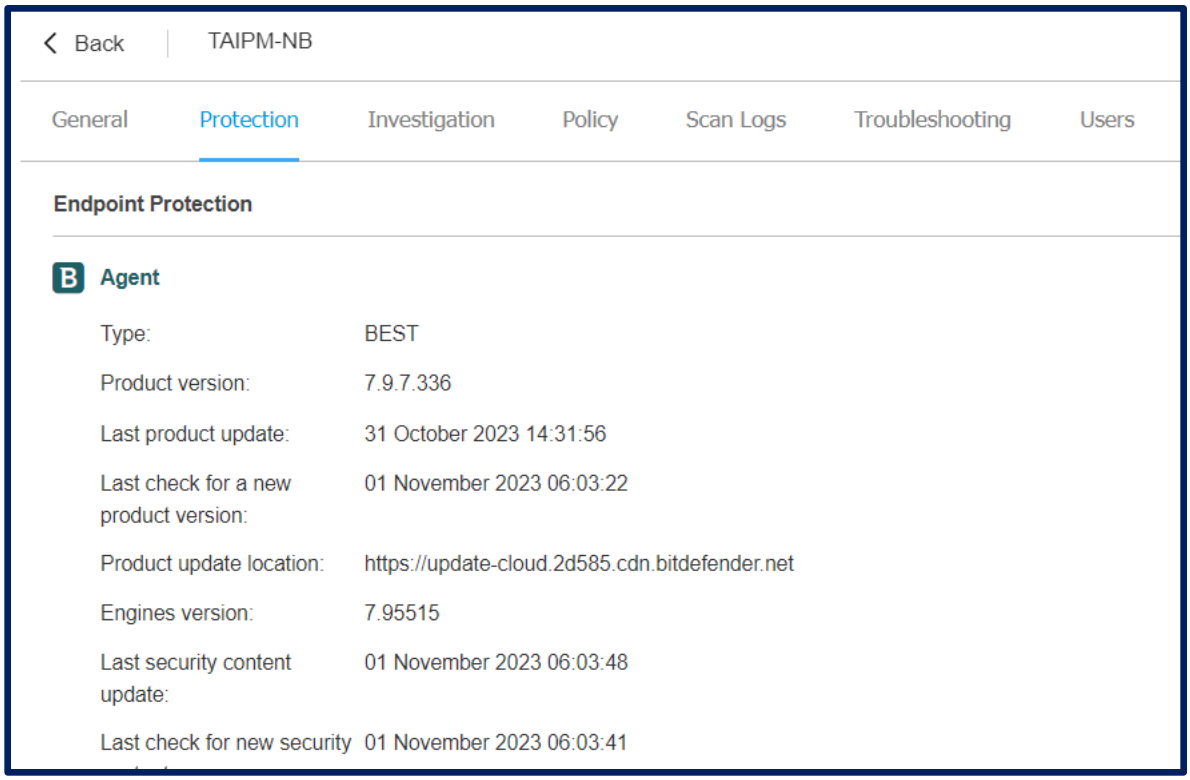


2. Kiểm tra số lượng máy đã được cài đặt

- Vào Network > Sổ xuống Group mình quản trị

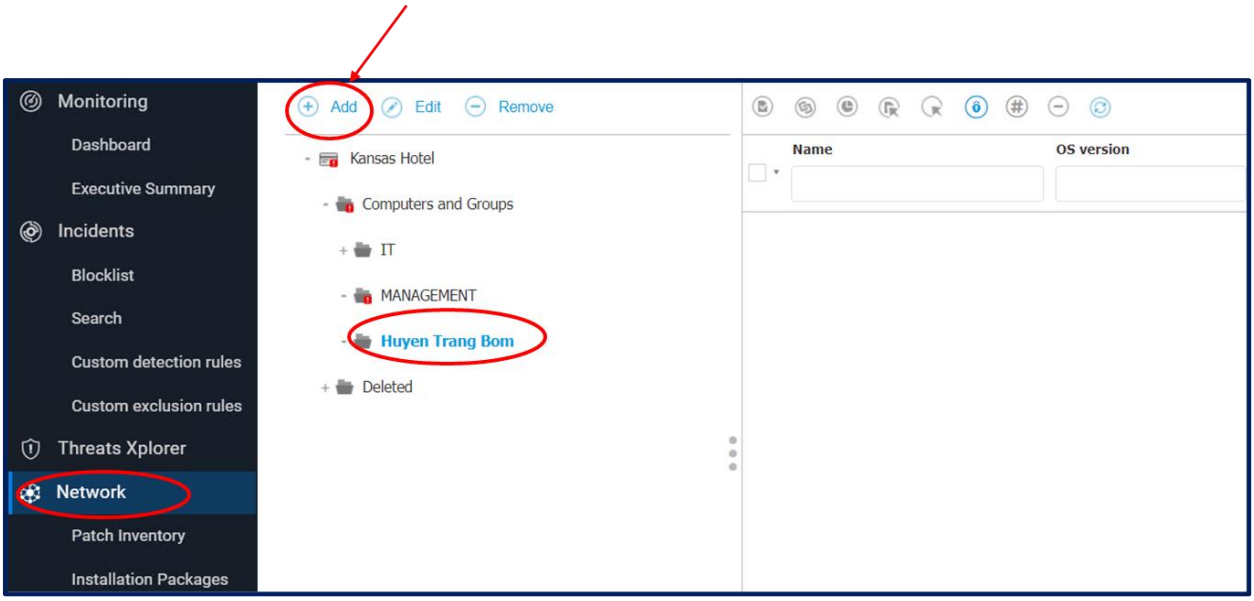


- Xem trạng thái của từng máy > chọn vào máy đó > Tab Protection



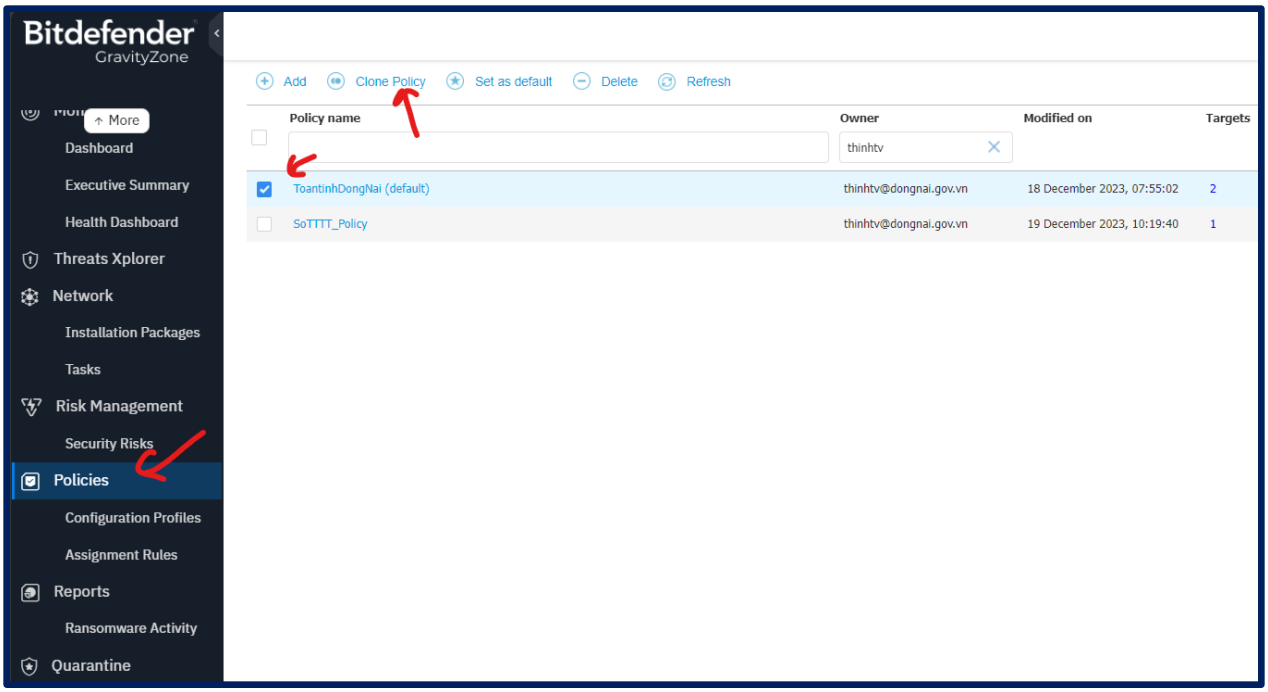
3. Tạo thêm Group để quản trị

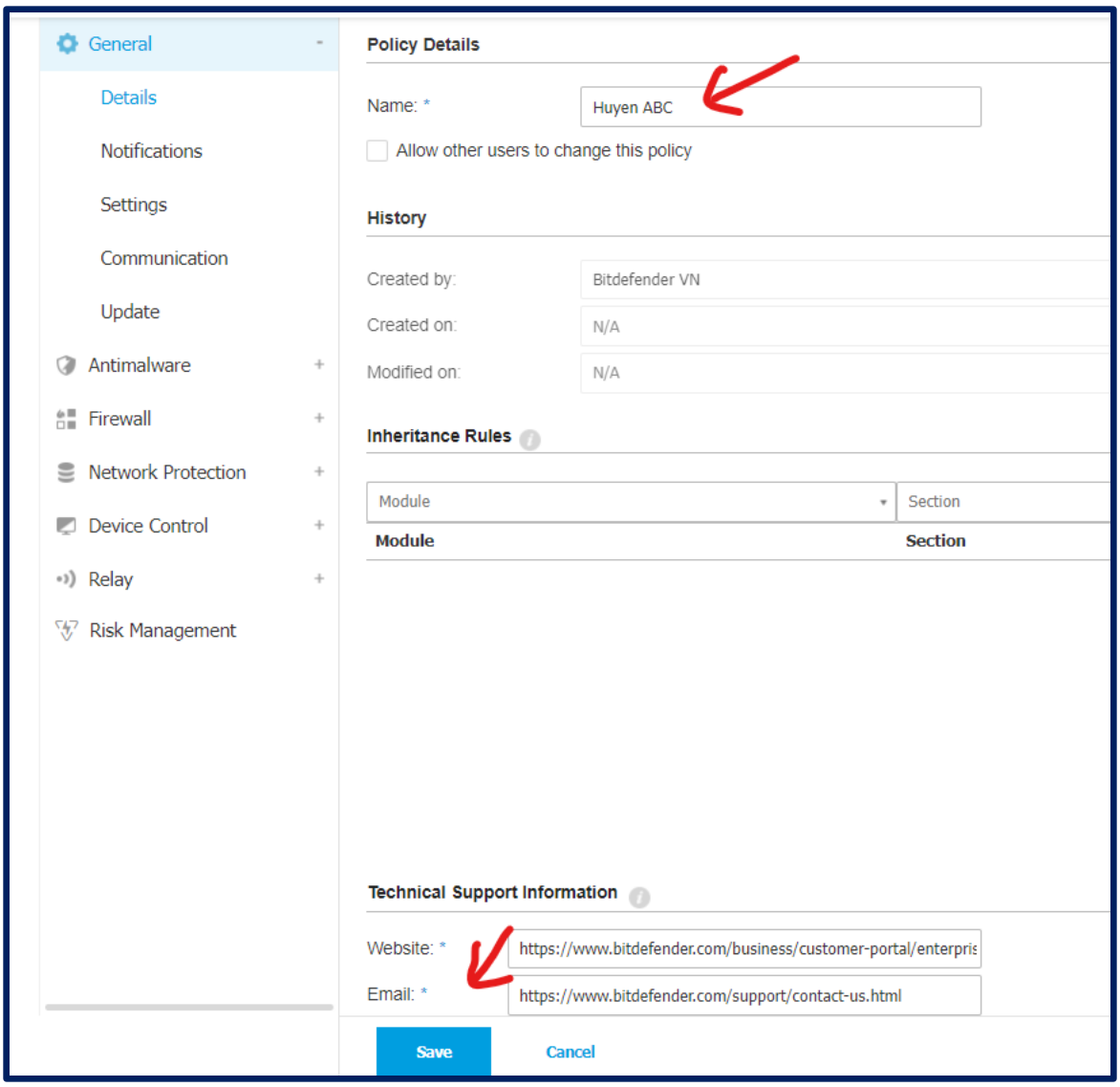
- Vào Tab Network > Chọn Group muốn tạo group con > phía bên trên góc trái có nút Add > Nhập tên group



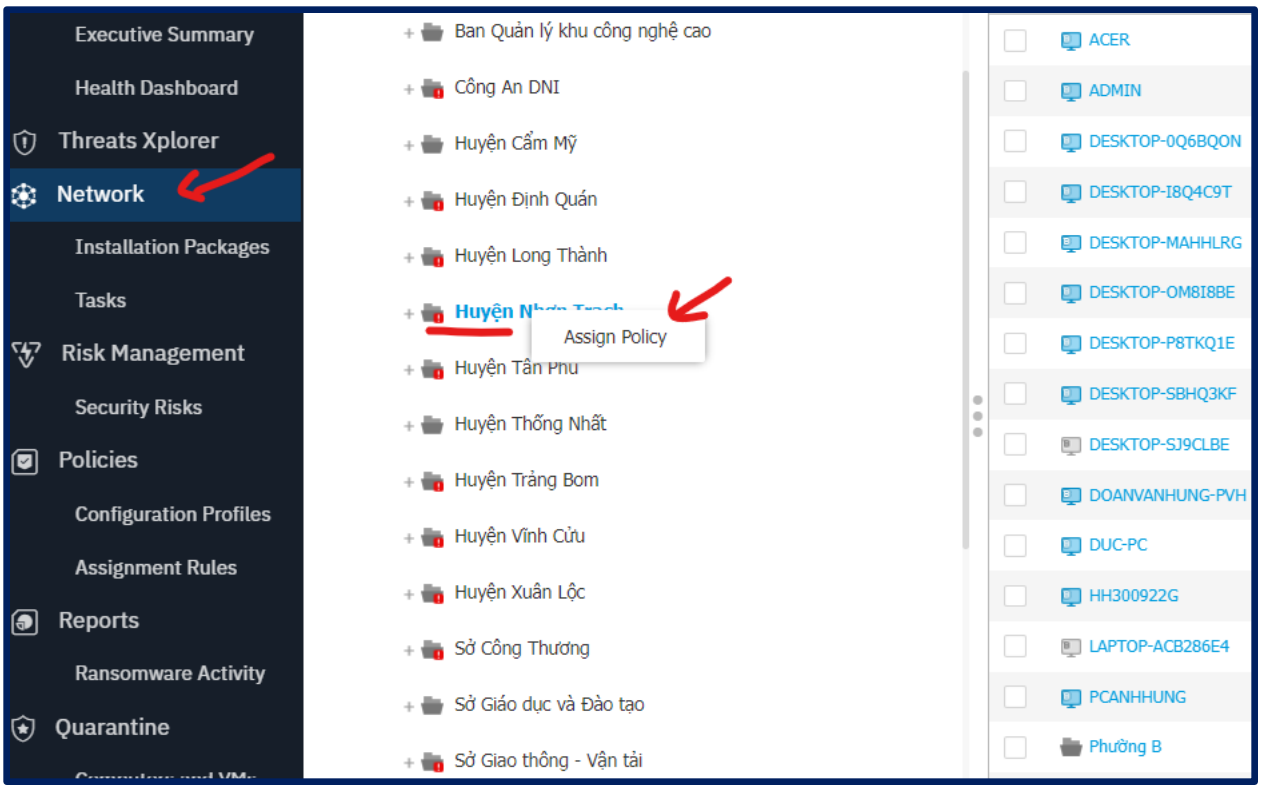
4. Tạo policy cho Đơn vị để tùy chỉnh các module, cài đặt

- Vào tab Policy trên GZ Console > Chọn Policy ToantinhDongNai(default) > clone đặt tên > Save

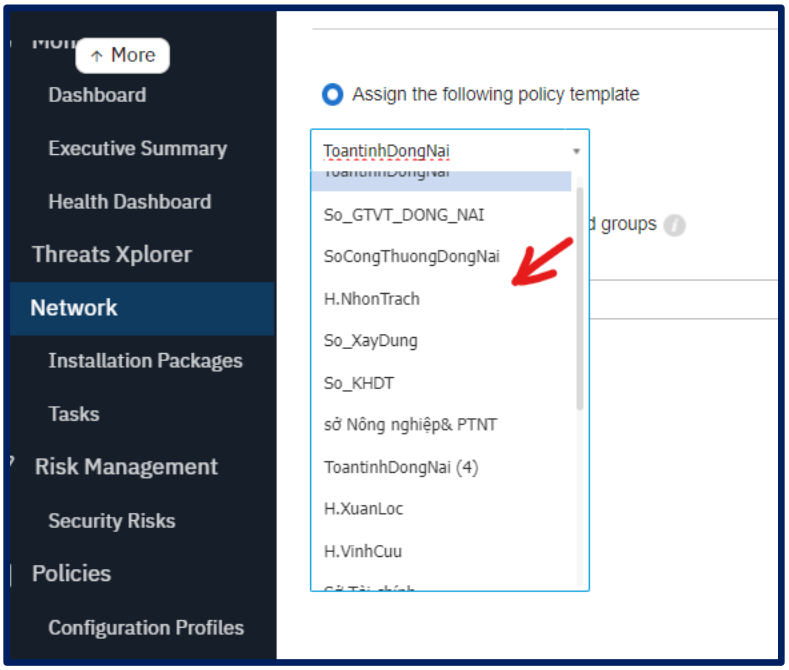




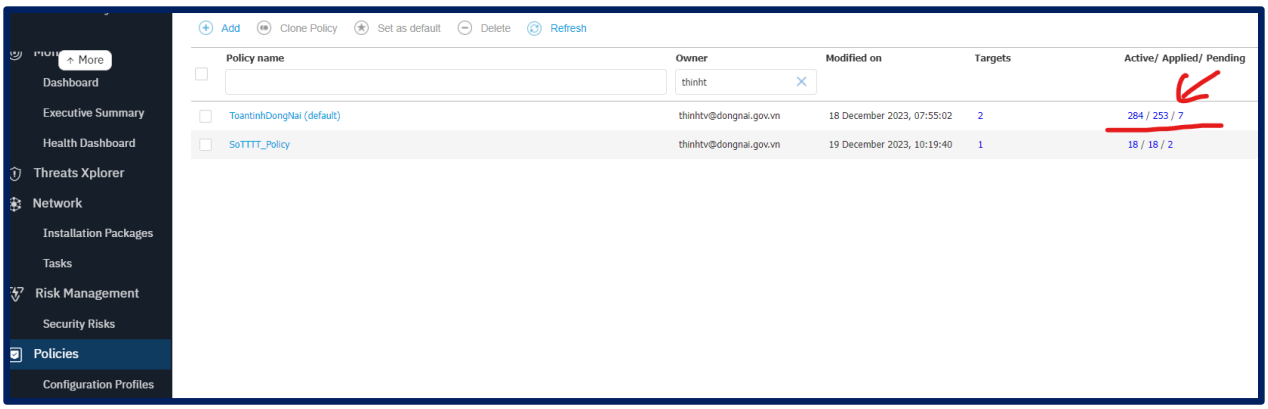
- Apply cho toàn group của đơn vị, vào Network Tab > chọn Group > click phải chuột > apply Policy



- Chọn Policy Name tương ứng và Finish

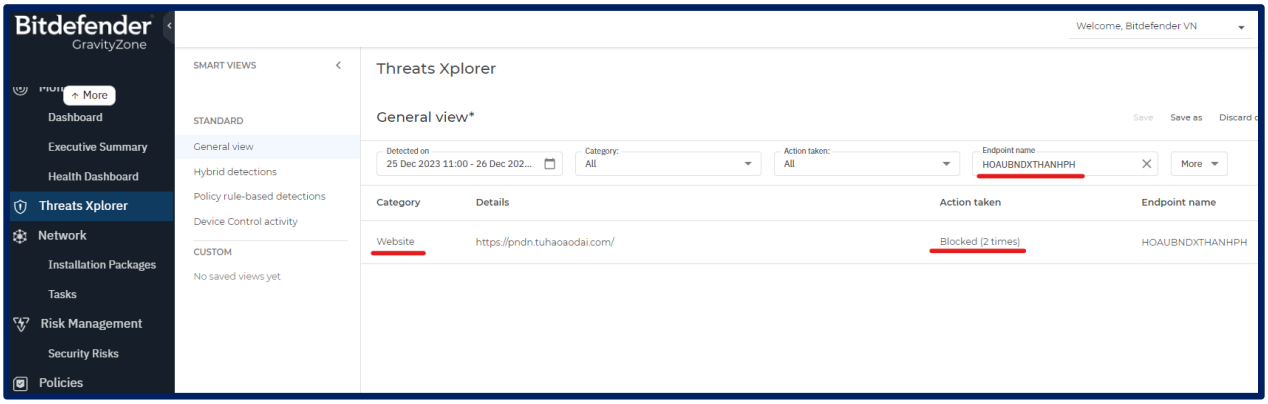


- Sau khi apply xong, vào lại Tab Policy để thấy số lượng máy được gán policy



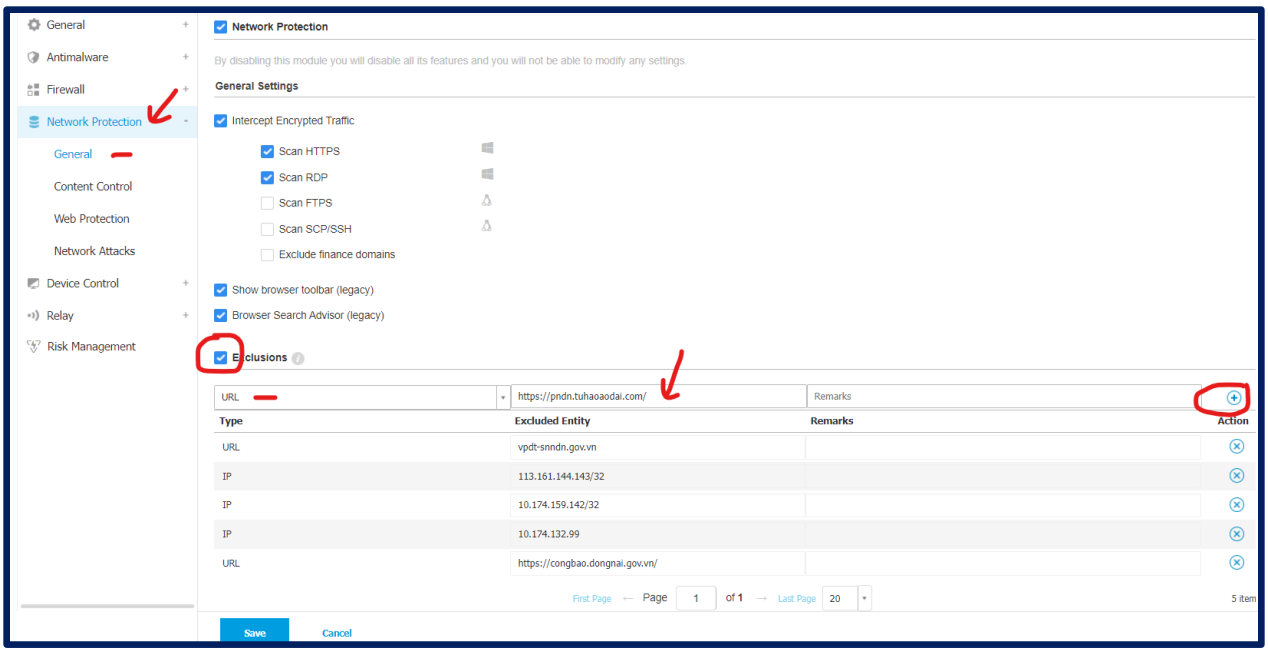
5. Add loại trừ cho các trường hợp các trang web bị chặn

- Vào Threat Xplorer > Search Endpoint Name (Máy mà User phản ánh)



*** Category Website và Action Blocked là trang web đó bị chặn

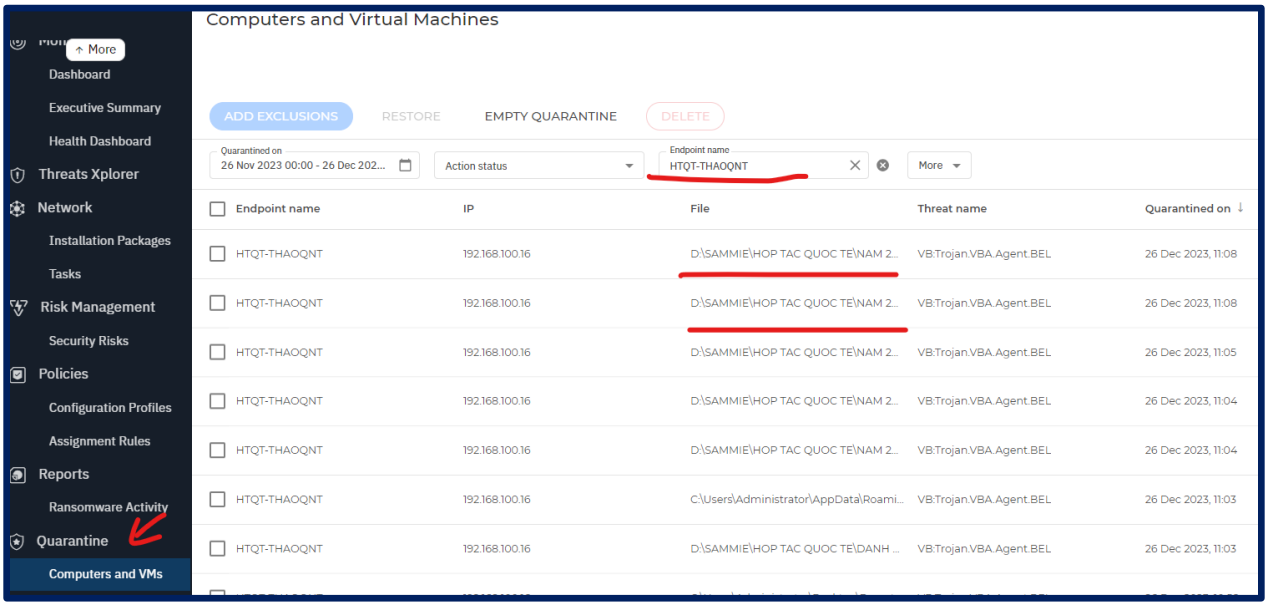
- Copy thông tin URL detail: https://pndn.tuhaoaodai.com/
- Vào Policy name đã apply cho Group > Network Protection > General > tích chọn Exclusion



***Add Type URL và link vừa copy > + Add và Save lại

6. Add loại trừ cho file, phần mềm, folder

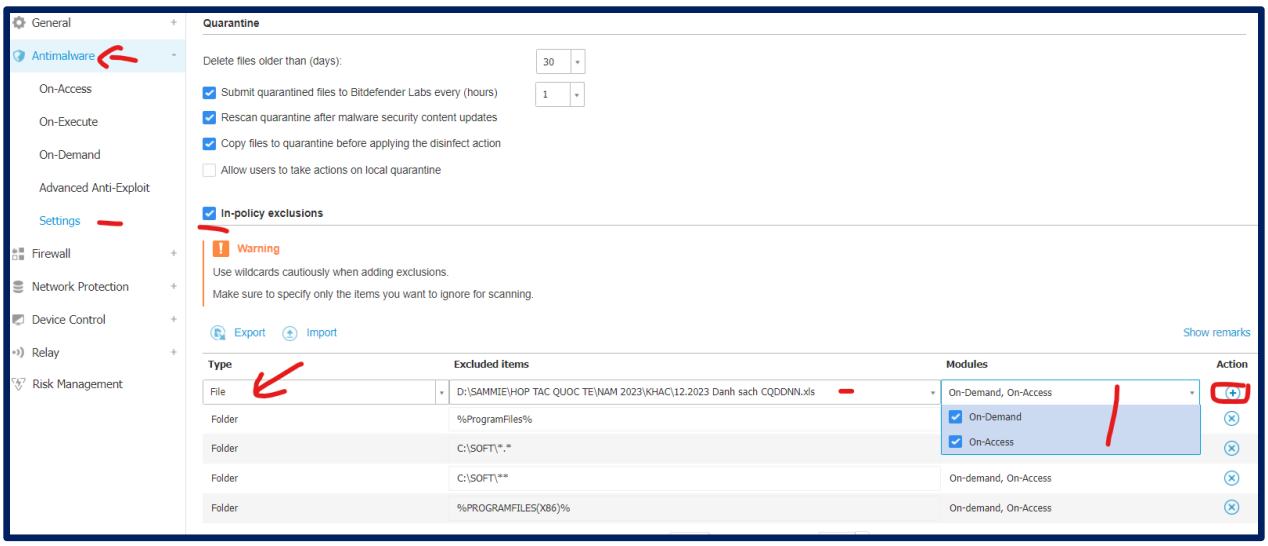
- Vào Tab Quarantine > Search Endpoint Name (Máy yêu cầu khôi phục file).
- **Lưu ý trước khi khôi phục phải add loại trừ vì khôi phục lại vẫn bị quét tiếp.**



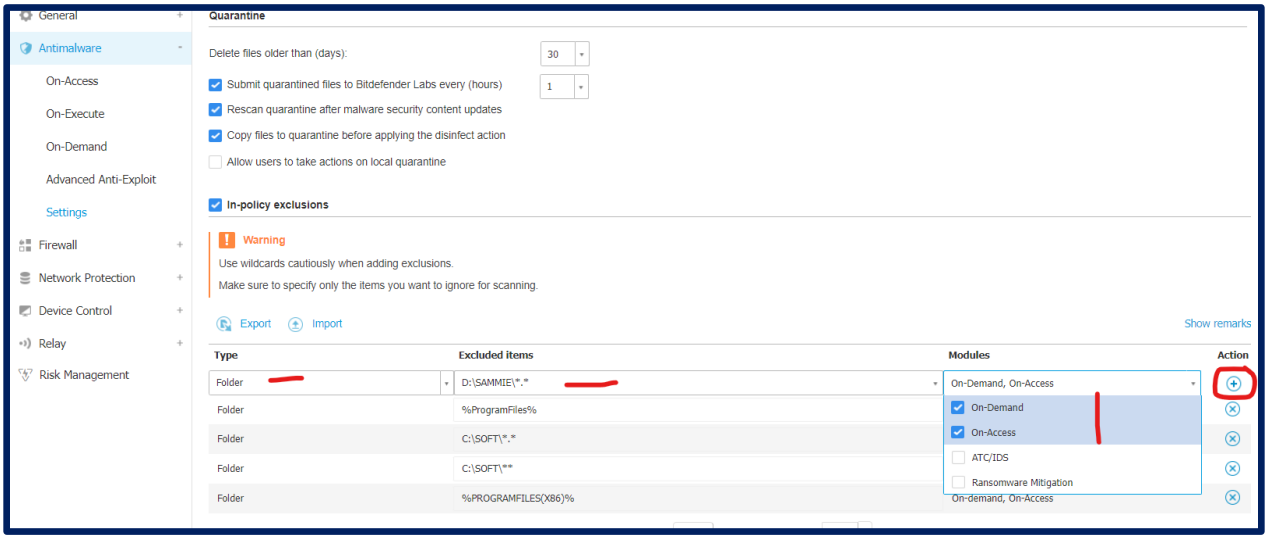
*** Copy đường dẫn chi tiết file D:\SAMMIE\HOP TAC QUOC TE\NAM 2023\KHAC\12.2023 Danh sach CQDDNN.xls

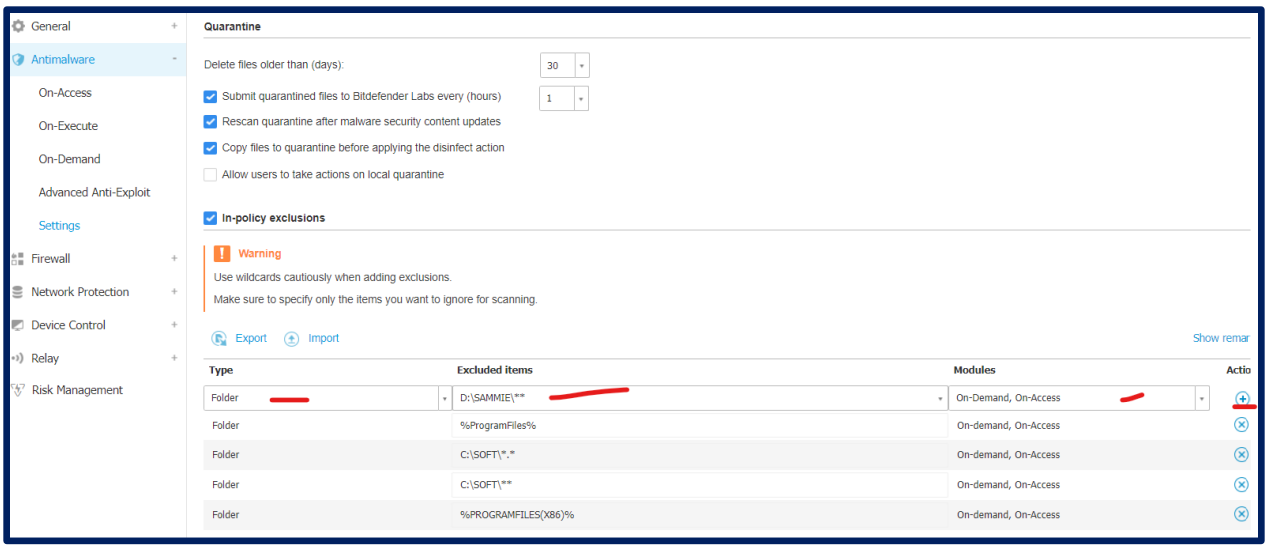
- Vào Policy mà máy này đang được apply > Antimalware > Setting > In-policy exclusions

PA1: Chọn add loại trừ type File thì add toàn bộ đường dẫn chi tiết và module loại trừ là On-demand & On-Access. Không chọn ATC và Ransomware



PA2: Add loại trừ cả Folder để cho các file khác nếu có nhiễm trong folder đó được loại trừ luôn.

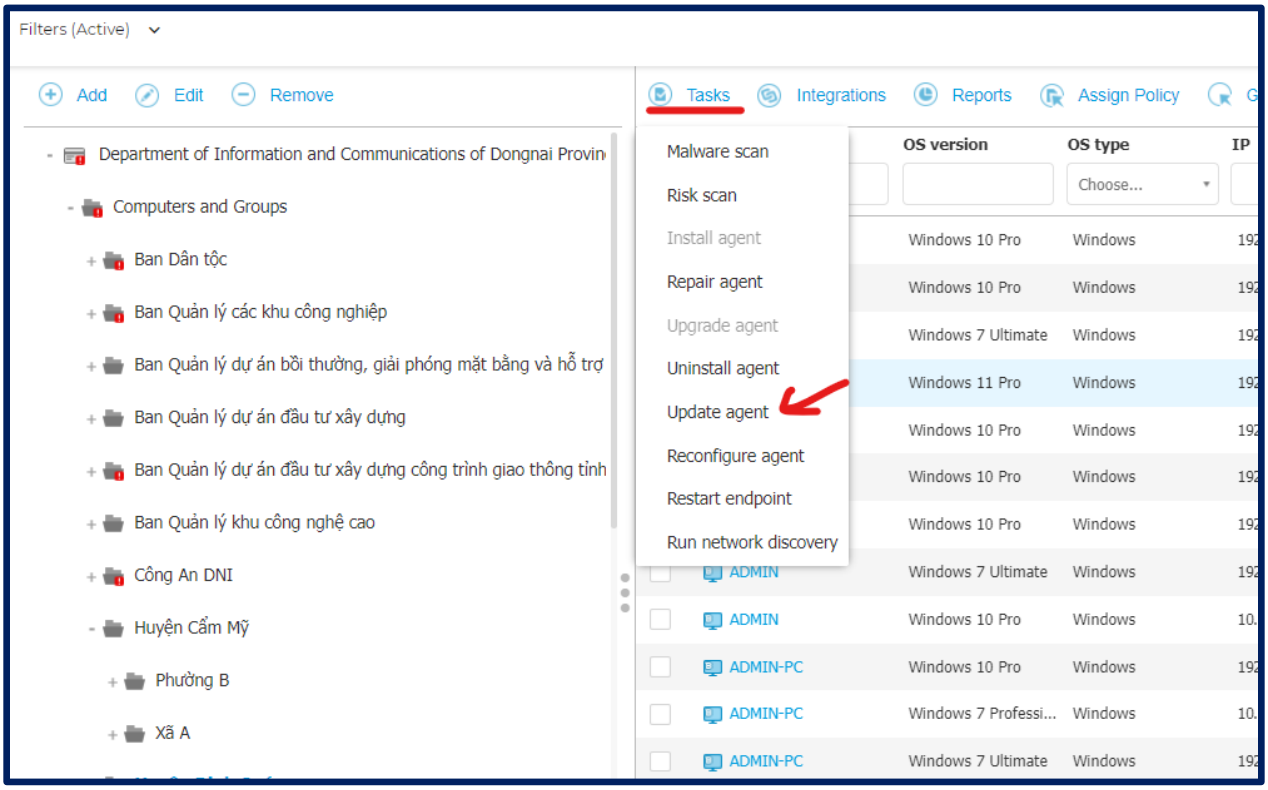




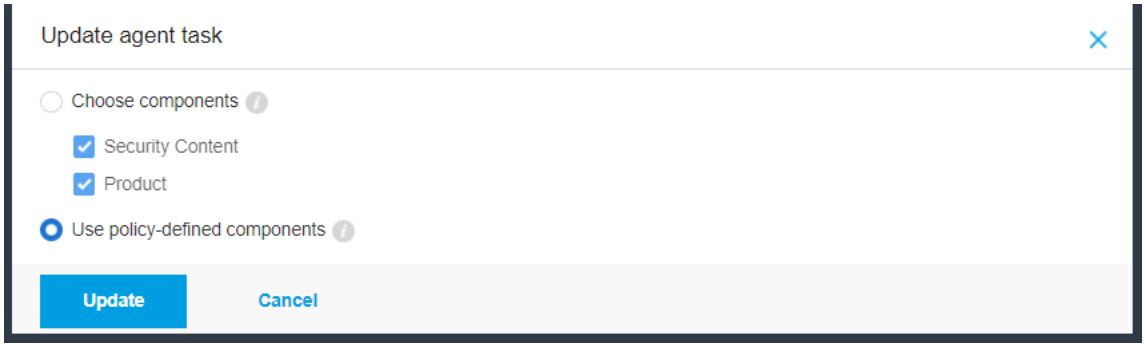
*** Để loại trừ Folder cần 02 excluded là D:\SAMMIE*.* là loại trừ tất các file trong folder SAMMIE

D:\SAMMIE** là lại trừ tất cả file và folder con trong folder SAMMIE này

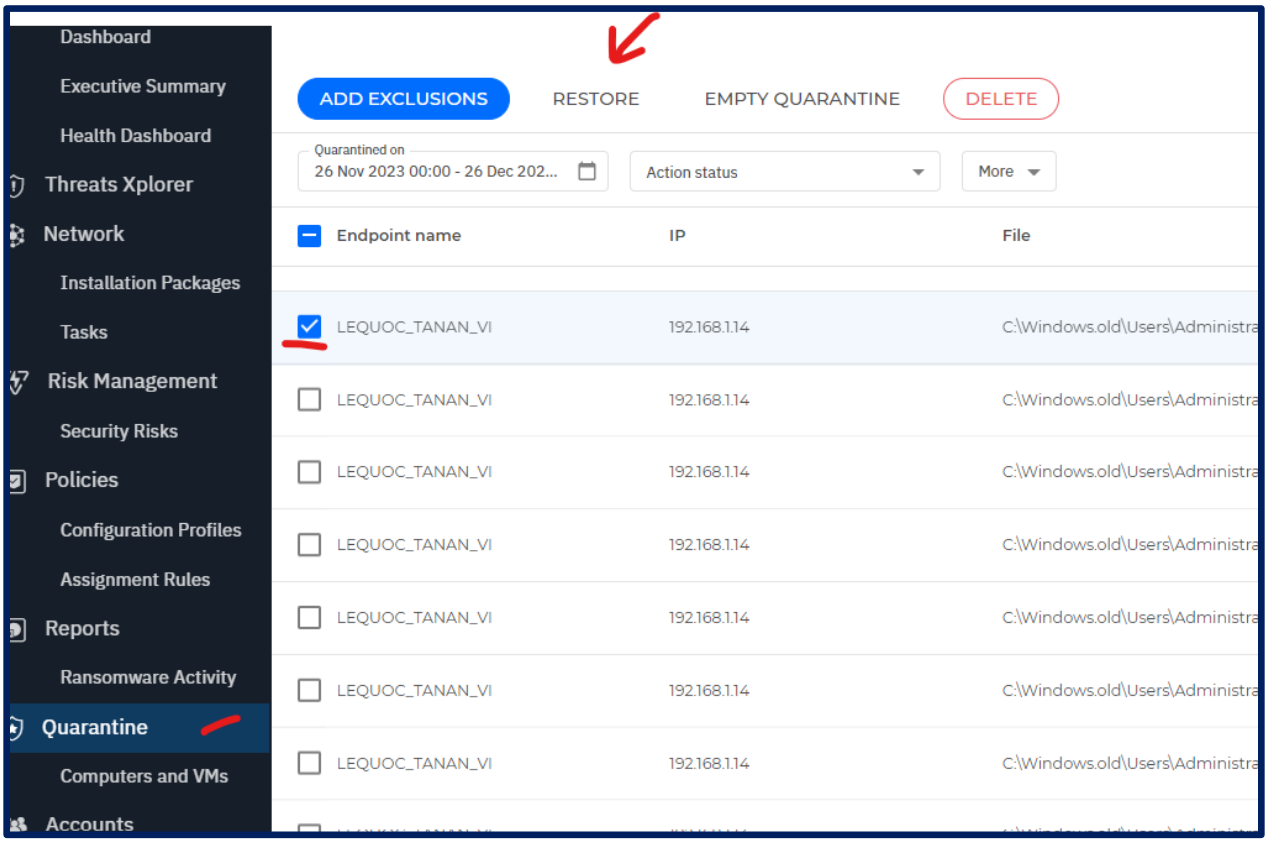
- Sau khi loại trừ và Save Policy, vào máy yêu cầu loại trừ > update agent để cập nhật policy tức thì
- Chọn Máy > Task > Update agent



- Chọn Update policy

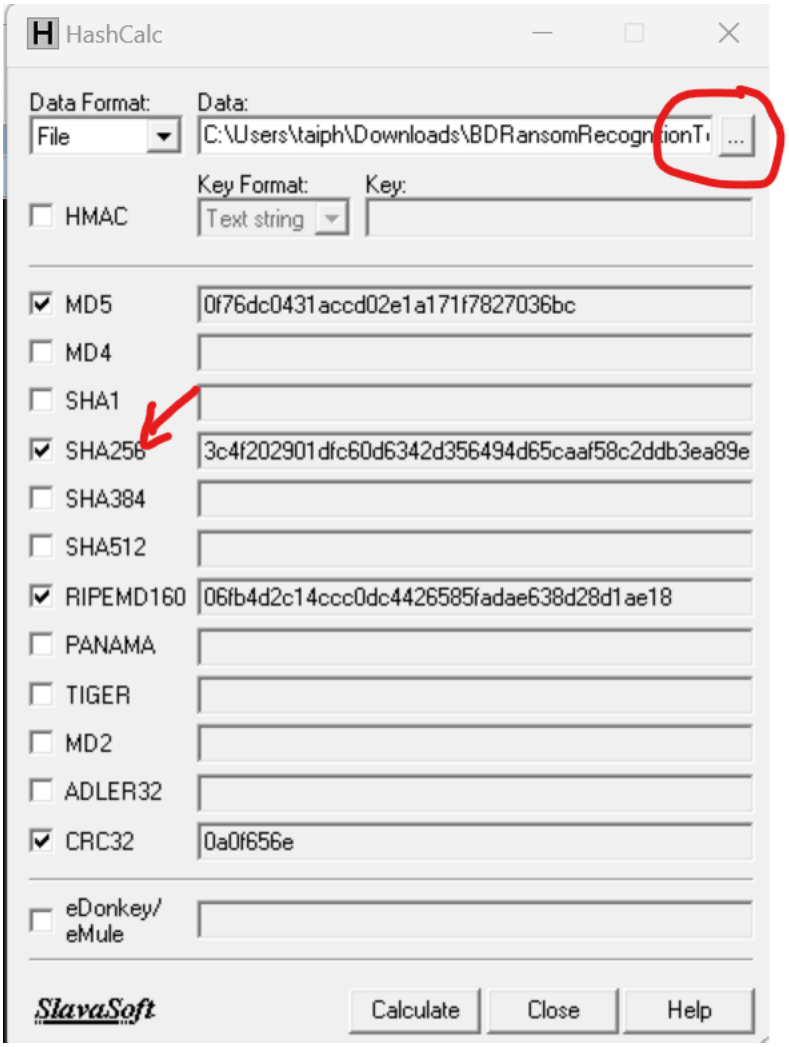


- Sau khi Endpoint được update xong , quay lại Tab Quarantine > chọn file của Endpoint mới loại trừ > restore

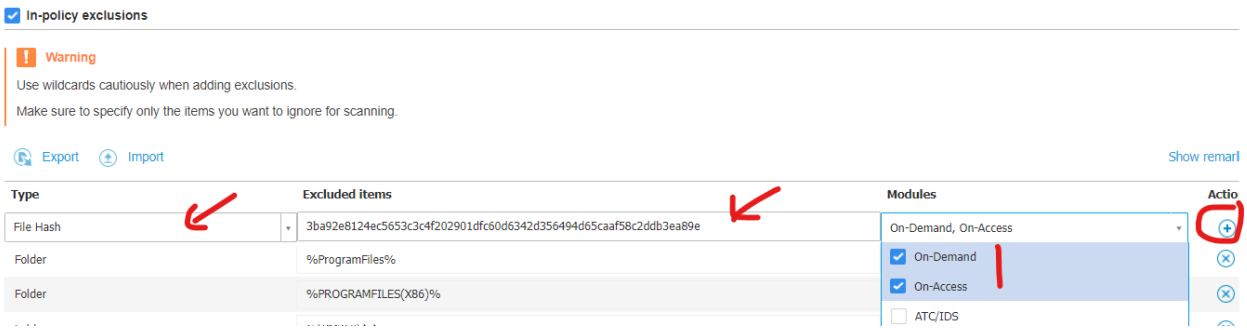


7. Add loại trừ cho file nằm ở vị trí bất kỳ trên máy (dùng File Hash)

- Download Hashcal để tính ra giá trị SHA256 Hash
  https://download.com.vn/hashcalc-21854
- Trỏ đến file exe cần loại trừ và enable SHA256



- Vào policy > Antimalware > setting > in-policy exclusion > Type: File Hash



**Lưu ý chỉ loại trừ 02 Module On-Demand và On-Access