Configure and Manage Exclusions in Cisco Secure Endpoint Connector

Contents

Introduction

This document describes how to create the exclusion for the different engines on the Cisco Secure Endpoint console.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Modify and apply an exclusion list to a policy in the Secure Endpoint console
- Windows CSIDL convention

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Endpoint console 5.4.20211013
- Secure Endpoint User Guide revision Oct 15, 2021

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Secure Endpoint workflow

In a high level of operations the Cisco Secure Endpoint processes a file Secure Hash Algorithm (SHA) in this order through the main components of the connector:

- Exclusions
- Tetra Engine
- Application control (Allow list / Blocklist)
- SHA Engine
- Exploit prevention (Exprev) / Malicious Activity Protection (MAP) / System Process Protection / Network engine (Device Flow Correlation)

Note: Exclusion or Allow/Blocklist creation depends on which engine detected the file.

Cisco Maintained Exclusions

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the Secure Endpoint Connector and antivirus, and security products, or other software.

These exclusion sets contain different types of exclusions to ensure proper operation.

You can track the changes performed to these exclusions in the article Cisco-Maintained Exclusion List Changes for Cisco Secure Endpoint Console.

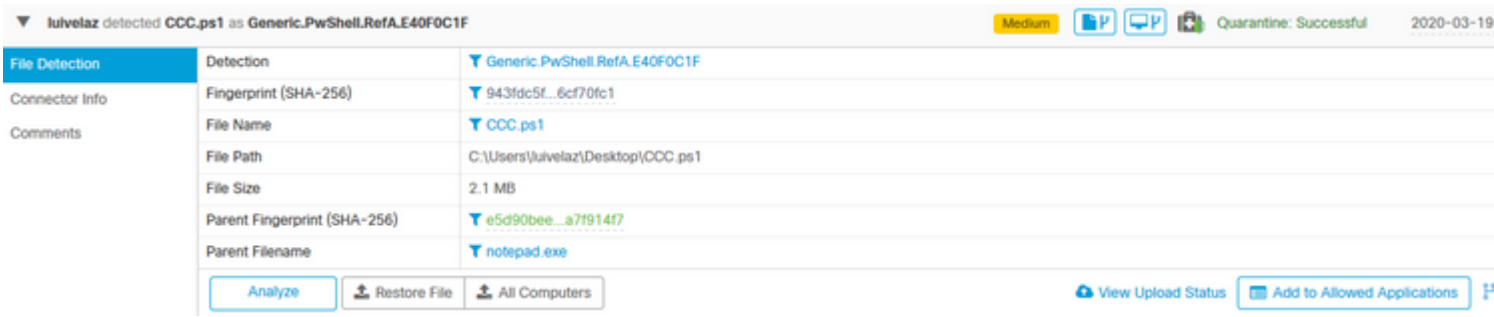
Custom Exclusions

Secure Endpoint engine

File Scan (CPU usage / File detections) by Tetra & SHA engine:

Use these types of exclusions to avoid detection/quarantine of a file or to mitigate Secure Endpoint high CPU.

The event on the Secure Endpoint console is as shown in the image.



Note: CSIDL can be used for exclusions, please refer to this Microsoft document for more information on CSIDL.

Path Exclusion

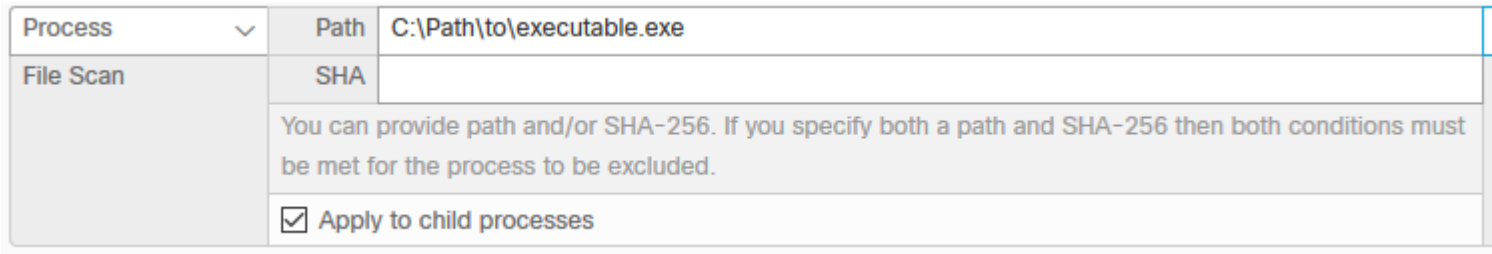
Wildcard Exclusion

Note: Option **Apply to all drive letters** is used to also apply the exclusion to drives [A-Z] attached to the system.

File Extension Exclusion

Caution: Use this type of exclusion with caution as it excludes all files with the file extension from scans regardless of the path location.

Process: File Scan Exclusion

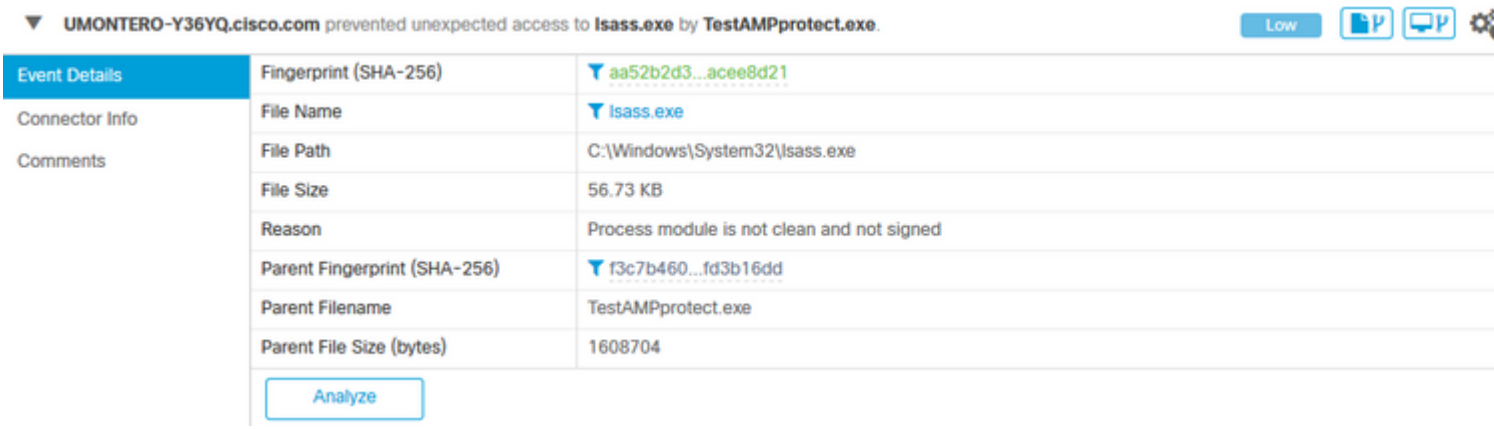


System Process Protection (SPP)

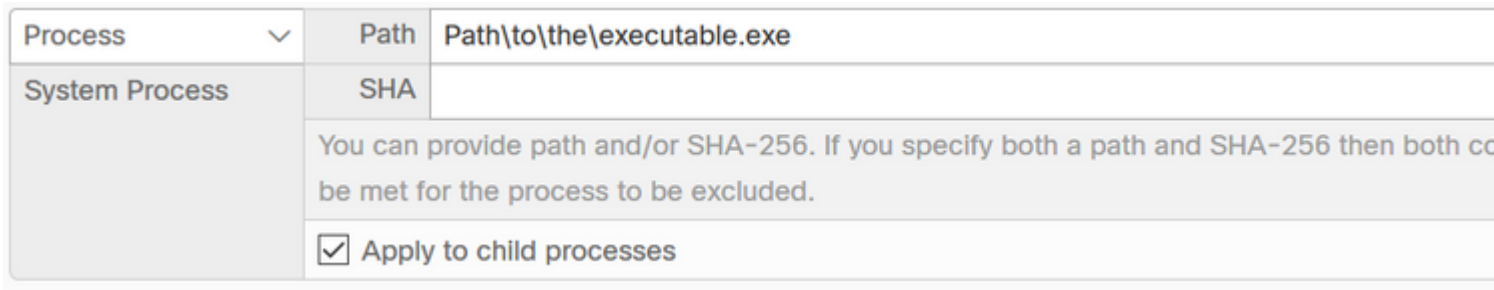
System Process Protection engine is available from connector version 6.0.5 and it protects the next Windows processes:

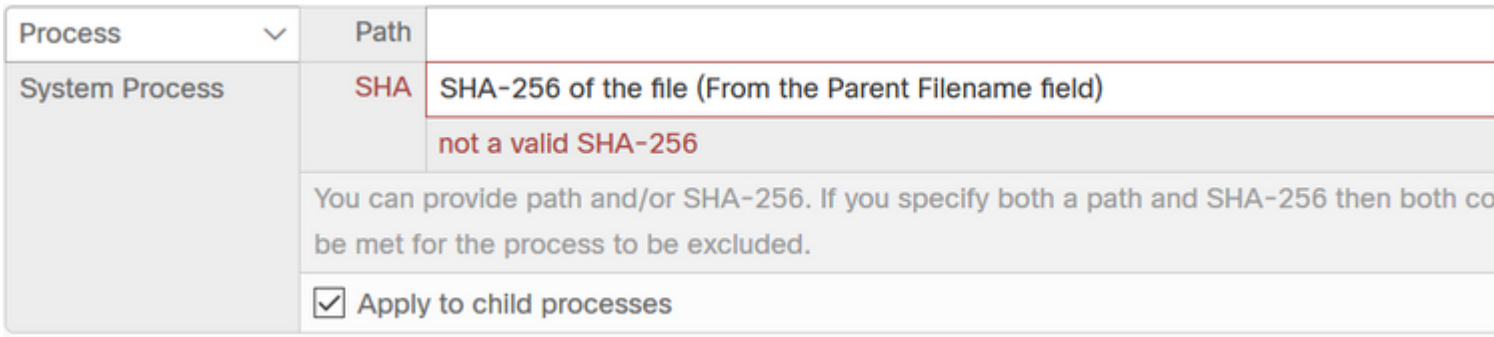
- Session Manager Subsystem (smss.exe)
- Client/Server Runtime Subsystem (csrss.exe)
- Local Security Authority Subsystem (lsass.exe)
- Windows Logon Application (winlogon.exe)
- Windows Start-up Application (wininit.exe)

This image shows an SPP event.



SPP Exclusion

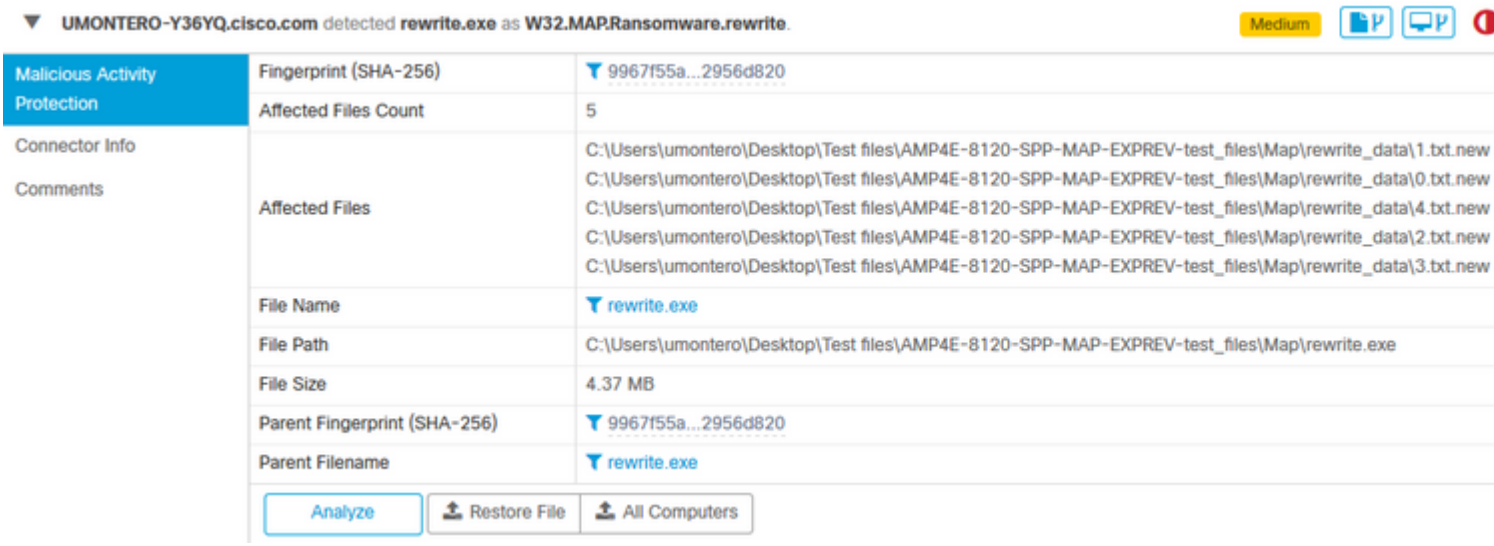




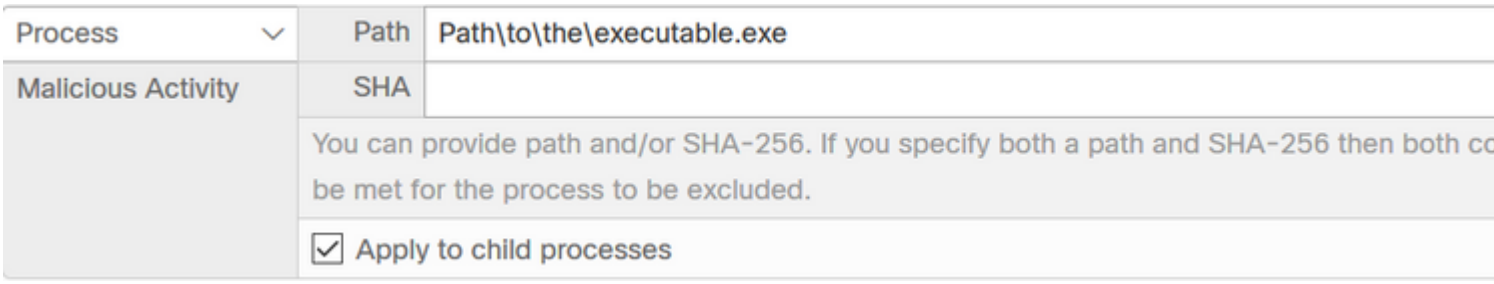
Malicious Activity Protection (MAP)

Malicious Activity Protection (MAP) engine, defends your endpoint from a ransomware attack. It identifies malicious actions or processes when they execute, and protects your data against encryption.

A MAP event is shown in this image.



MAP Exclusion

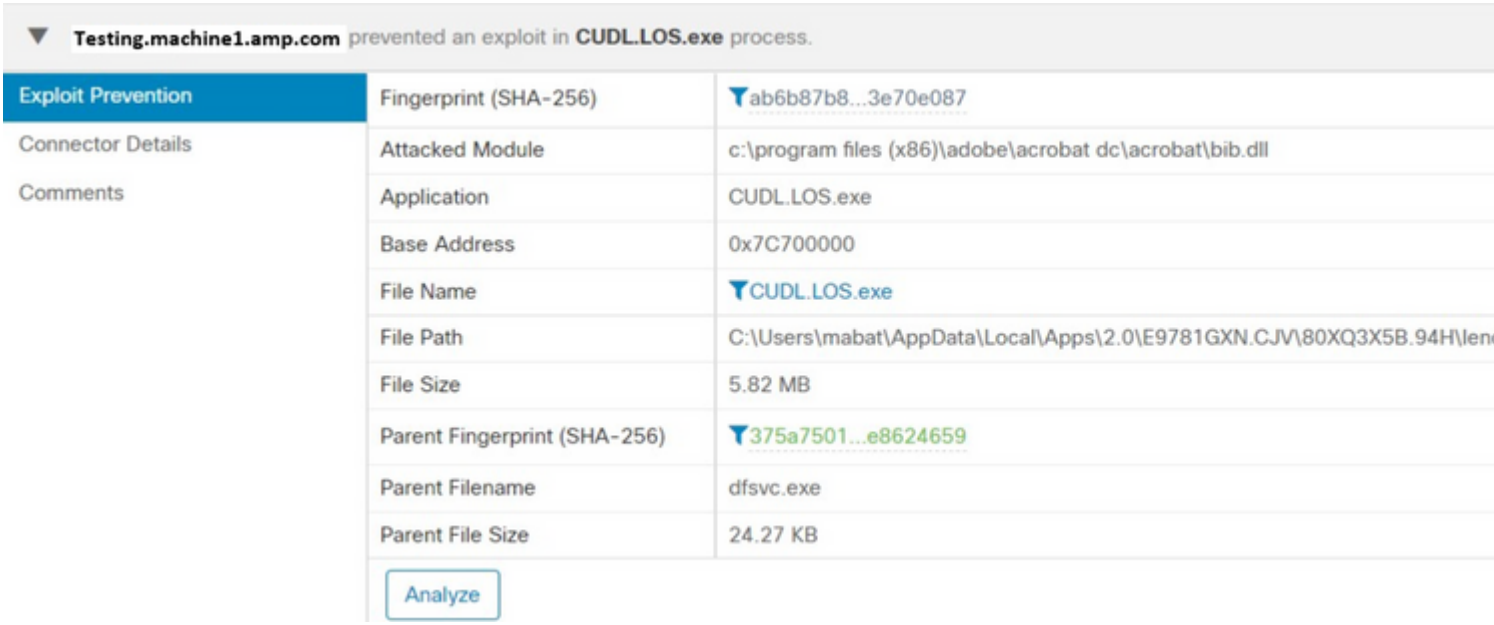


> **Caution**: Use this type of exclusion with caution and after you confirm that the detection is indeed not malicious.

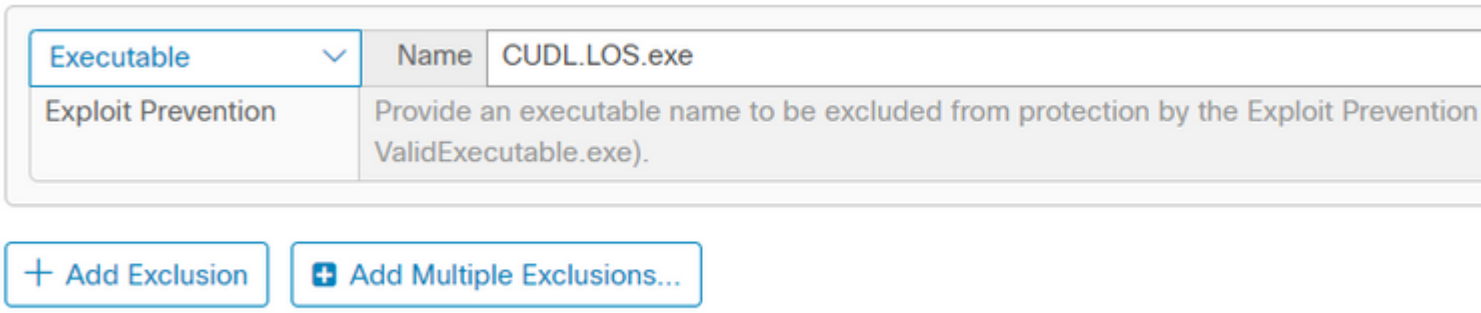
Exploit Prevention (Exprev)

The exploit prevention engine defends your endpoints from memory injection attacks commonly used by malware and other zero-day attacks on unpatched software
vulnerabilities. When it detects an attack against a protected process it will be blocked and generate an event but there will not be a quarantine.

An Exprev event is shown in this image.



Exprev exclusion

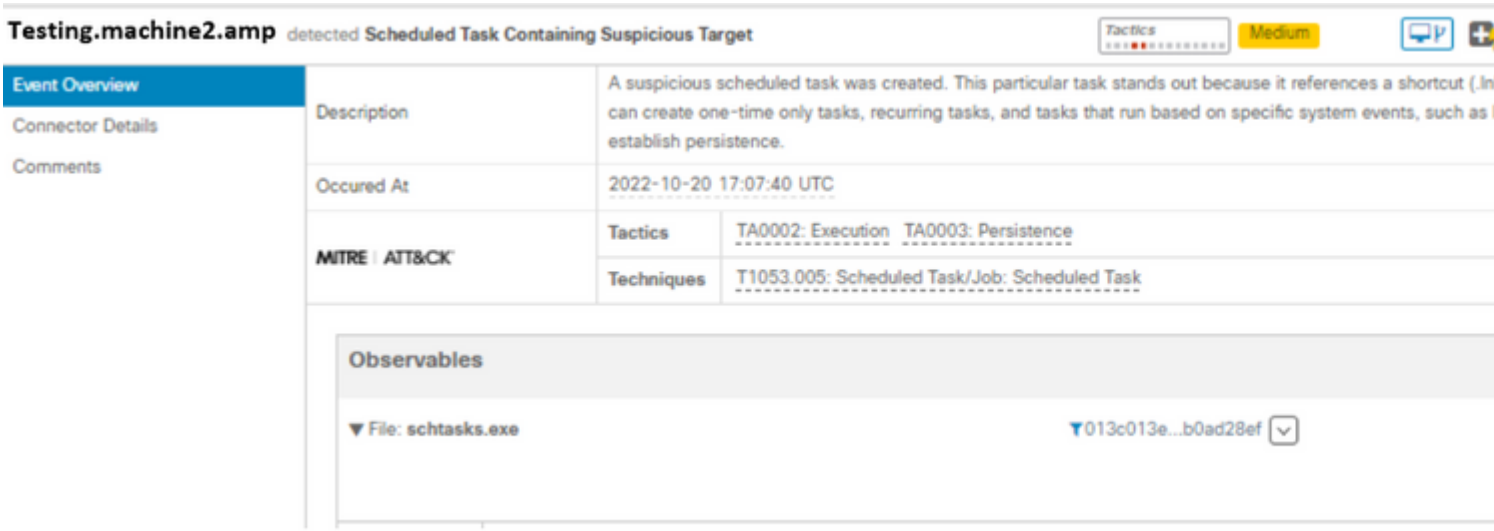


Caution: Use this exclusion whenever you trust the activity on the affected module/application.

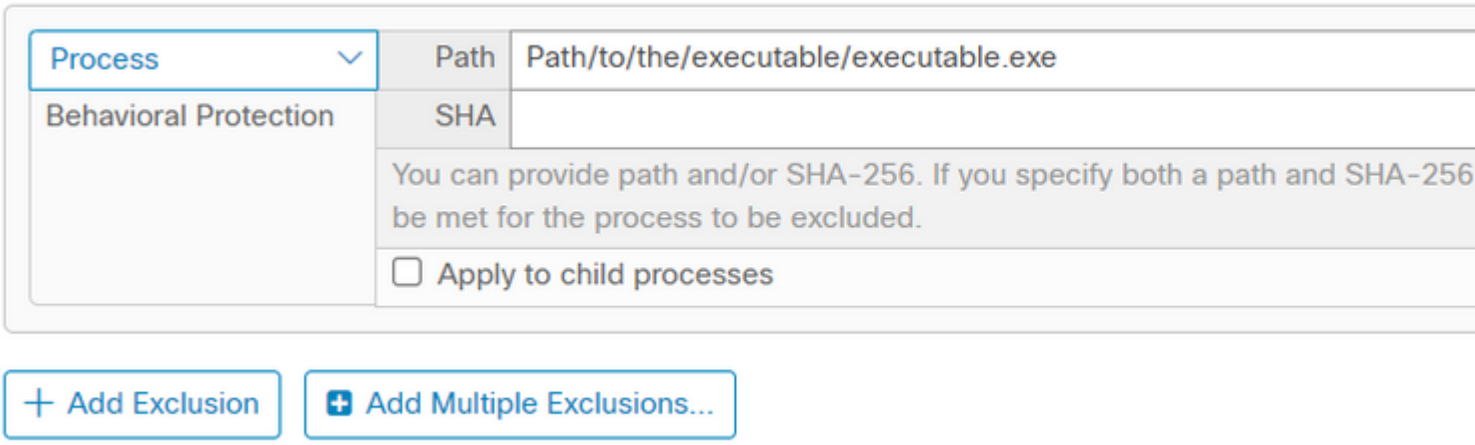
Behavioral Protection (BP)

The behavioral protection engine enhances the ability to detect and stop threats behaviorally. It deepens the ability to detect "living-off-the-land" attacks and provides
faster response to changes in the threat landscape through signature updates.

A BP event is shown in this image.



BP exclusion



Related Information

- **For more information on the policy configuration, navigate to the User Guide**
- **Create Exclusions in Cisco Secure Endpoint Connector video**
- **Technical Support & Documentation - Cisco Systems**