

# Trellix Endpoint Security (HX) Integration Guide

FireEye HX Endpoint Security (now Trellix) is an advanced EDR (Endpoint Detection and Response) platform that provides real-time threat detection, live response capabilities, forensic data acquisition, and automated containment across enterprise endpoints. Integrating FireEye HX with GreyMatter creates a force-multiplying effect by correlating HX's granular endpoint telemetry with broader network and security data sources, enabling unified threat detection workflows that accelerate investigation timelines and orchestrate coordinated response actions across the entire security stack.

## Deployment Type

This integration supports **on-premises** through Port 3000 and **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please check your organization's compatibility before continuing.

## Required Information and Setup

To integrate GreyMatter with Trellix Endpoint Security (HX), collect the following details:

- API base URL
- Username
- Password

See instructions below to gather the required information.

### Create User with Required Permissions

Create a user in Trellix with at least one “api\_x” user role privilege based on the features you want to use in GreyMatter. See the permissions table below for specifics.

## Permissions and Functionality

### Permissions

GreyMatter Capability	Action(s)	Required Permission
Detect	GET_DETECTION_RECORDS	minimum: api_analyst
Respond	ISOLATE_HOST	mininum: api_admin
	UNISOLATE_HOST	mininum: api_admin

### Respond

Playbook Name	Description	Required Input Variables
Isolate Host	Isolates host. There is generally some delay in the actual isolation. However, once initiated by the Trellix	Source host or Host ID

# Trellix Endpoint Security (HX) Integration Guide

	<p>platform, the isolation completes unless host power is turned off (edge case). Follow these steps in that case:</p> <ol style="list-style-type: none"> <li>1. Check Containment state of the input host.</li> <li>2. If NOT “Contained” or “Containing,” create a request to isolate the specified host.</li> <li>3. Programmatically approve the request containment of host.</li> </ol>	
Unisolate Host	<p>Unisolates host. There is generally some delay in the actual unisolation. However, once initiated by the Trellix platform, the unisolation completes unless host power is turned off (edge case). Follow these steps in that case:</p> <ol style="list-style-type: none"> <li>1. Check Containment state of the input host.</li> <li>2. If NOT “Normal” or “Uncontaining,” unisolate the host.</li> </ol>	Source host or Host ID

## Detect

Trellix Endpoint Security (HX) supports **Detection at Source**.

**Note** and **State Syncing** are *not* supported for **Vendor-Authored detections**.

**Disclaimer:** All customer data is classified and handled as ‘Confidential’ (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.