Trend Micro

WORRY-FREE™ SERVICES ENDPOINT SENSOR

Integrated investigation tool for a complete Endpoint Detection and Response (EDR) add-on for Trend Micro Worry-Free Services

Advanced malware can manifest itself in your enterprise networks, bypassing traditional security technology. It can change and spread through an organization before executing and exploiting your intellectual property. Or it can sit dormant until an opportunity presents itself to steal or ransom data. Fortunately, Trend Micro™ Worry-Free™ Services uses XGen™ threat and malware protection, a blend of cross generational threat protection techniques, such as machine learning and behavioral analysis. Once a detection has been made though, questions remain: What was the root cause? How many endpoints did it spread to? Was it related to other detections picked up by the endpoint protection?

Trend Micro™ Worry-Free™ Services Endpoint Sensor gives insight to detections by allowing threat investigators to explore detections using EDR investigation functionality.

KEY FEATURES

Integrated workflow: Threat detection investigation is performed within the workflow and console of Worry-Free Services. No more moving from one console to another.

Efficient endpoint recording: Endpoint Sensor records and stores information on system behaviors, communications and user behaviors. Metadata on this information is sent to the Worry-Free Services server to allow investigators to "sweep" for indicators of compromise (IOCs)

Server side IOC sweeping: The Worry-Free Services server only stores essential metadata of end user recorded data (or telemetry). This allows investigators to perform multiple searches or "sweeps" of this data without having to query each endpoint individually. In addition, detailed root cause investigations can be made on each endpoint directly.

Flexible searching: Investigators can search (or sweep) with multiple parameters. Searches can be made on parameters such as; specific communications, specific malware, registry activity, account activity, and running processes. Or investigators can search using industry standard OpenIOC rules.

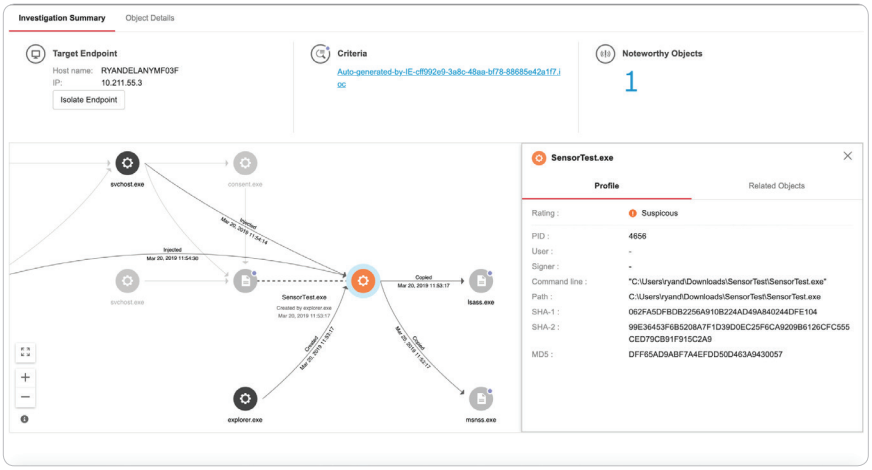
Root cause analysis: Investigators can drill down on an interactive process tree that illustrates the full chain of attack to analyze how the detection arrived, changed, and spread by viewing activities, objects, and processes. Immediate response can be taken to terminate processes and to sweep further.

Vendor intelligence and assistance: Layering in proactive global threat intelligence, the Trend Micro™ Smart Protection Network™ provides clarity and assistance to threat investigators. Endpoint Sensor recognizes known good objects and processes as well as known bad objects and processes. Investigators can view a colour-coded Root Cause Analysis to identify risky or unknown processes and guide in the remediation.

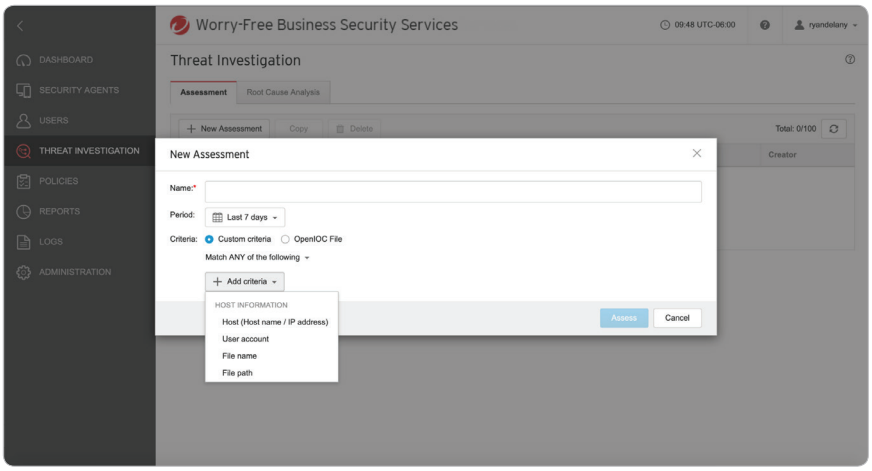
Immediate response options: Worry-Free Services already provides advanced automation to remediate detections. It can automatically isolate, quarantine, block executions, roll back settings (and files, in the case of ransomware), with the option to manually respond while performing an investigation by isolating endpoints.

HOW IT WORKS

1. Endpoints with Worry-Free Services Endpoint Sensor enabled will record system behaviors, user behaviors, and communications.
2. Metadata on the recorded information is sent to the Worry-Free Services server.
3. When a detection is made with Worry-Free Services, investigators can search through the metadata to understand the impact analysis of the detection to understand how far has it spread and who else has been compromised.
4. A full root cause analysis allows investigators to understand the cause of the detection and immediately implement a response that includes remediating affected systems and updating Apex One to block similar attacks in the future.



5. Alternately, before a detection, investigators can search their environment using various parameters or with OpenIOC.



MINIMUM AGENT REQUIREMENTS

Worry-Free Services Endpoint Sensor is available as an optional add-on to Worry-Free Services endpoint protection. Please refer to the system requirements for Worry-Free Services.

Worry-Free Services Endpoint Sensor is supported on the following endpoints with Worry-Free Services:

Windows

- Windows 7 SP1 (6.1)
- Windows 8.1 (6.3)
- Windows 10 (10.0)

Hardware:
2GB minimum RAM, 2GB available disk space (3GB recommended)

Protection Points

- Microsoft® Windows®

Key Features

- IOC sweeping
- Root cause analysis of detection
- Impact analysis of detection
- Instant response

TREND MICRO™

Securing Your Connected World