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™ Apex One™ security uses XGen™ threat and malware protection, using a blend of cross generational threat protection techniques, such as machine learning, behavioral analysis and vulnerability protection. 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™ Apex One™ as a Service: Endpoint Sensor gives insight to detections by allowing threat investigators to explore detections and hunt for new threats using EDR investigation functionality.

**KEY FEATURES**

**Integrated workflow:** Threat hunting and detection investigation is performed within the workflow and console of Trend Micro Apex One™ as a Service endpoint protection. 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 Apex One™ server to allow investigators to “sweep” for indicators of compromise (IOCs).

**Server side IOC sweeping:** The Apex One™ as a Service 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 or YARA 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, isolate users, update security, 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. Investigators can view a colour-coded Root Cause Analysis to identify risky or unknown processes and guide in the remediation. Investigators can also access Trend Micro™ Threat Connect™ service to research our database of threat information.

**Immediate response options:** Apex One™ as a Service 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 for investigators to also manually respond while performing an investigation. Endpoints can be isolated, processes can be terminated, and security intelligence can be automatically updated on a per-user or enterprise-wide basis.

**Advanced threat hunting:** Investigators can perform threat hunting based on indicators of attack (IOAs). This allows investigators to develop attack discovery rules or work with the IOAs provided by Trend Micro to hunt for threats.

**Open APIs:** Many customers want to be able to leverage their security operations tools. Apex One™ as a Service has multiple built-in documented APIs that allow the product to work with these tools.

**Sandbox integration:** Security investigators can select objects and manually submit them to Trend Micro sandboxes. Suspicious objects can be sent to our Deep Discovery™ network security sandboxes on-premises, or to Apex One™ Sandbox as a Service subscription option.
HOW IT WORKS

1. Endpoints with Apex One™ as a Service Endpoint Sensor enabled will record system behaviors, user behaviors, and communications.

2. Metadata on the recorded information is sent to the Apex One™ as a Service server.

3. When a detection is made with Apex One™, 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™ as a Service to block similar attacks in the future.

5. Alternately, before a detection, investigators can search for indicators of attack (IOAs) by searching using various parameters or with IOCs and YARA rules.
Protection Points

- Windows®
- Macintosh®
  *Sweeping only

Key Features

- IOC sweeping
- IOA hunting
- Root cause analysis of detection
- Impact analysis of detection
- Instant response
- Open APIs
- Vendor assistance