DATASHEET

Trend Micro™

ENDPOINT SENSOR AS A SERVICE: XDR EDITION

Integrated investigation, detection and response capabilities across email, endpoint, and servers

Effective protection against new and emerging threats is a vital part of any organization's security strategy. Unfortunately, there is no silver bullet when it comes to protecting against threats, and even the most advanced endpoint security solutions can't prevent 100 percent of new threats 100 percent of the time. That's why having tightly-integrated protection and detection capabilities that can help quickly detect, track, and investigate threats—that make it past defenses—is so important to eliminate or minimize the impact.

Stealthy advanced threats can manifest themselves in your enterprise networks by bypassing traditional endpoint, email, and server security technologies. Threats 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, a blend of cross generational 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 far did it spread? Was it related to other detections picked up by the endpoint or email protection?

Trend Micro™ Endpoint Sensor as a Service: XDR Edition gives insight to detections by allowing threat investigators to use investigation functionality to explore detections and hunt for new threats across endpoints, emails, and servers.

KEY FEATURES

Integrated workflow: Threat hunting and detection investigation is performed within the workflow and console of Apex One and shows investigations across connected emails and servers. 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 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 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. Endpoints can be isolated, processes can be terminated, and security intelligence can be automatically updated on a per-user or enterprise-wide basis.

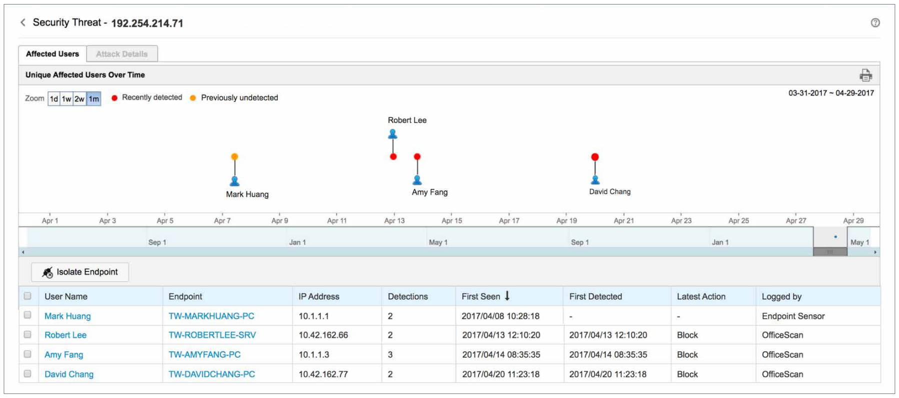
Advanced threat hunting: Threat hunting, based on indicators of attack (IoAs), allows investigators to develop attack discovery rules or work with the IoAs provided by Trend Micro to hunt for threats.

Open APIs: Many customers want to be able to leverage their security operations tools. Apex One has multiple built-in documented application programming interfaces (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 Trend Micro™ Deep Discovery™ network security sandboxes on-premises, or to Trend Micro Apex One™ Sandbox as a Service subscription option.

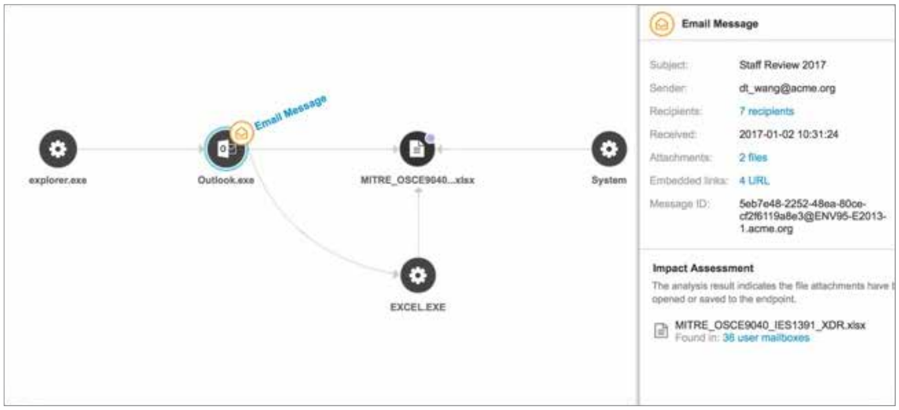
HOW IT WORKS

1. Endpoints with Trend Micro™ Apex One Endpoint Sensor enabled, and emails with Trend Micro™ Cloud App Security, will record system behaviors, user behaviors, and communications.
2. Activity and detection data from these servers, endpoints, and emails is sent to the Trend Micro™ XDR data lake.
3. When a detection is made, investigators can search through the data to understand the impact analysis of the detection to understand how far has it spread and who else has been compromised.



□	User Name	Endpoint	IP Address	Detections	First Seen ↓	First Detected	Latest Action	Logged by
□	Mark Huang	TW-MARKHUANG-PC	10.1.1.1	2	2017/04/08 10:28:18	-	-	Endpoint Sensor
□	Robert Lee	TW-ROBERTLEE-SRV	10.42.162.66	2	2017/04/13 12:10:20	2017/04/13 12:10:20	Block	OfficeScan
□	Amy Fang	TW-AMYFANG-PC	10.1.1.3	3	2017/04/14 08:35:35	2017/04/14 08:35:35	Block	OfficeScan
□	David Chang	TW-DAVIDCHANG-PC	10.42.162.77	2	2017/04/20 11:23:18	2017/04/20 11:23:18	Block	OfficeScan

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 and Cloud App Security to block similar attacks in the future.



Email Message

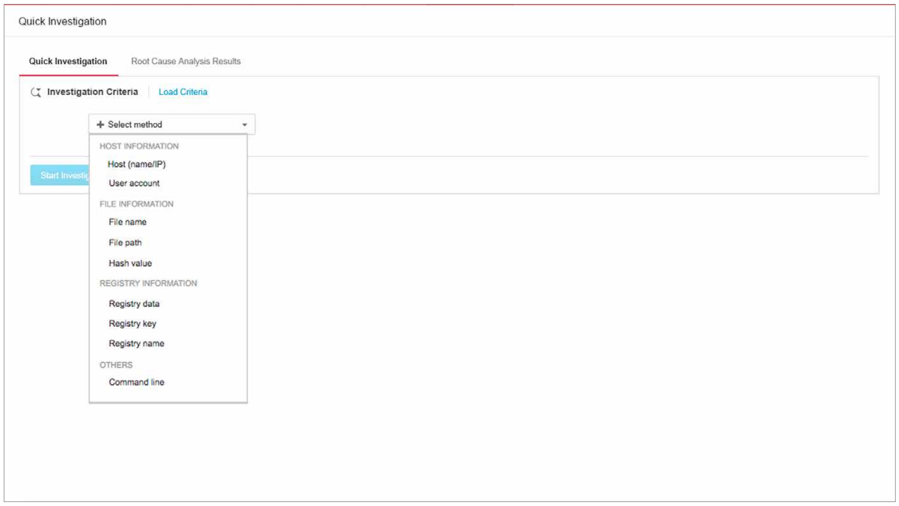
Subject: Staff Review 2017
Sender: dt_wang@acme.org
Recipients: 7 recipients
Received: 2017-01-02 10:31:24
Attachments: 2 files
Embedded links: 4 URL
Message ID: 5eb7e48-2252-48ea-80ce-cf2f6119a8e3@ENV95-E2013-1.acme.org

Impact Assessment

The analysis result indicates the file attachments have b
opened or saved to the endpoint.

MITRE_OSCE9040_IES1391_XDR.xlsx
Found in: 36 user mailboxes

5. Alternately, before a detection, investigators can search for IoAs by using various search parameters or with IoCs and YARA rules.



MINIMUM AGENT REQUIREMENTS

Apex One Endpoint Sensor is available as an optional add-on to Apex One endpoint protection. It is available on-premises along with Apex One or in SaaS along with Trend Micro Apex One™ as a Service. Please refer to the system requirements for Apex One.

Apex One Endpoint Sensor is supported on the following endpoints with Apex One:

Windows

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

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

Mac

- macOS™ Mojave 10.14
- macOS™ High Sierra 10.13
- macOS™ Sierra 10.12
- OS X™ El Capitan 10.11
- OS X™ Yosemite 10.10 or later
- OS X™ Mavericks 10.9.5 or later

Hardware: Intel Core™ processor, 512 MB RAM minimum, 300 MB minimum disk space

Protection Points

- Microsoft® 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

TREND MICRO™

Securing Your Connected World

For details about what personal information we collect and why, please see our Privacy Notice on our website at: https://www.trendmicro.com/privacy