Trend Micro

APEX ONE™ ENDPOINT SENSOR

Integriertes Investigations-Tool für Apex One™, um ein komplettes Endpoint Detection and Response (EDR) durchführen zu können.

Fortgeschrittene Schadsoftware kann sich im Unternehmensnetzwerk festsetzen, indem sie traditionelle Sicherheitstechnologien umgeht. Die Schadsoftware ist in der Lage, sich zu ändern und sich in einer Organisation zu verbreiten, bevor sie ihre Payload ausführt und das geistige Eigentum des Unternehmens kompromittiert. Sie kann auch untätig auf eine Gelegenheit warten, Daten zu stehlen oder Lösegeld zu erpressen. Trend Micro™ Apex One™-Sicherheit unterstützt durch XGen™-Schutz vor Bedrohungen und Schadsoftware, nutzt eine Kombination aus generationsübergreifenden Schutztechniken wie maschinelles Lernen, Verhaltensanalyse und Schwachstellenschutz. Doch sobald eine Schadsoftware entdeckt wird, müssen Fragen beantwortet werden. Was war ihr Ursprung? Auf wie vielen Endpunkten hat sie sich verbreitet? Besteht eine Verbindung zu anderen von der Endpoint-Schutzlösung entdeckten Schädlingen?

Trend Micro™ Apex One™ Endpoint Sensor ermöglicht Einsichten in erkannte Bedrohungen. Es unterstützt Sicherheitsforscher bei der Analyse der Bedrohungen und dabei, mit EDR-Investigationsfunktionen nach neuen Bedrohungen zu suchen.

KERNFÄHIGKEITEN

Integrierter Workflow: Die Jagd nach Bedrohungen und die Untersuchung der Funde werden innerhalb des Workflows und der Konsole des Trend Micro Apex Central durchgeführt. Damit ist der ständige Wechsel von einer Konsole zur anderen Vergangenheit.

Effizientes Erfassen auf Endpunkten: Endpoint Sensor erfasst und speichert Informationen zu Systemverhaltensweisen, Kommunikationen und Nutzerverhalten. Metadaten zu diesen Informationen werden an den Apex One™-Server gesendet, damit Bedrohungsermittler diese nach Indicators of Compromise (IOC) durchforsten können.

IOC-Suche auf dem Server: Der Apex One™ Server speichert nur die wichtigen Metadaten aus den erfassten Endanwenderdaten (Telemetrie). Dies ermöglicht es den Bedrohungsermittlern, mehrere Suchen(Sweeps) in diesen Daten durchzuführen, ohne jeden Endpunkt einzeln abfragen zu müssen. Darüber hinaus können detaillierte Analysen zu den Ursachen an jedem Endpunkt direkt ausgeführt werden.

Flexible Suche: Sicherheitsforscher können ihre Suchläufe mithilfe mehrerer Parameter durchführen. Dazu gehören Parameter wie spezifische Kommunikationen, bestimmte Malware, Registry-Aktivitäten, Kontoaktivitäten und laufende Prozesse. Des Weiteren lassen sich branchenübliche OpenIOC- oder YARA-Regeln für die Suche einsetzen.

Ursachenanalyse (Root Cause Analysis): Forscher können einen interaktiven Prozessbaum, der die gesamte Angriffskette veranschaulicht, aufschlüsseln und auswerten. Über die Ansicht von Aktivitäten, Objekten und Prozessen können sie analysieren, wie die erkannte Bedrohung ankam, geändert und verbreitet wurde. Sofortige Reaktionen lassen sich aufsetzen, um Prozesse zu beenden, befallene Systeme zu isolieren, die Sicherheit zu aktualisieren und weiter zu suchen.

Anbieterwissen und Unterstützung: Das proaktive globale Bedrohungswissen im Trend Micro™ Smart Protection Network™ bietet Sicherheitsforschern Klarheit und Unterstützung. Endpoint Sensor erkennt sowohl bekannte gute Objekte und Prozesse als auch bekannte bösartige. Untersuchungsexperten können sich eine farbcodierte Ursachenanalyse anzeigen lassen, um riskante oder unbekannte Prozesse zu identifizieren und somit Betroffene bei der Wiederherstellung zu unterstützen. Sie können auch auf den Trend Micro™ Threat Connect™-Dienst zugreifen und die Datenbank nach Bedrohungsinformationen durchsuchen.

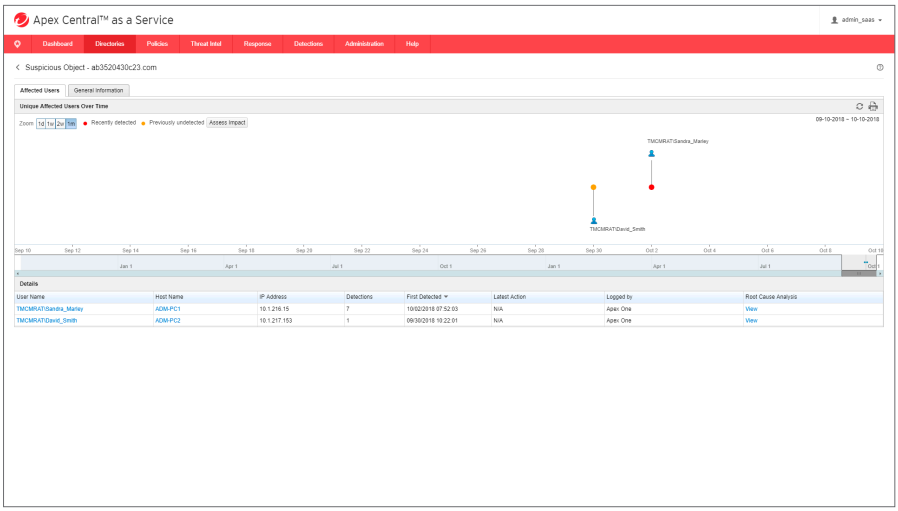
Varianten für sofortige Reaktionen: Apex One™ bietet fortschrittliche Automatisierung für die Wiederherstellung bei erkannter Malware. Der Dienst kann automatisch isolieren, in Quarantäne stellen, die Ausführung blockieren, Einstellungen zurücksetzen (und auch Dateien im Falle von Ransomware). Sicherheitsforscher haben auch die Option, während einer Untersuchung manuell zu reagieren. Endpunkte können isoliert werden, Prozesse terminiert, und Sicherheitswissen kann pro Nutzer oder unternehmensweit automatisch aktualisiert werden.

Fortschrittliche Bedrohungsjagd: Forscher können auf der Basis von Indicators of Attack (IOA) Bedrohungen jagen. Dies ermöglicht es ihnen, Regeln für die Entdeckung von Angriffen zu entwickeln oder mit den von Trend Micro gelieferten IOAs zu arbeiten.

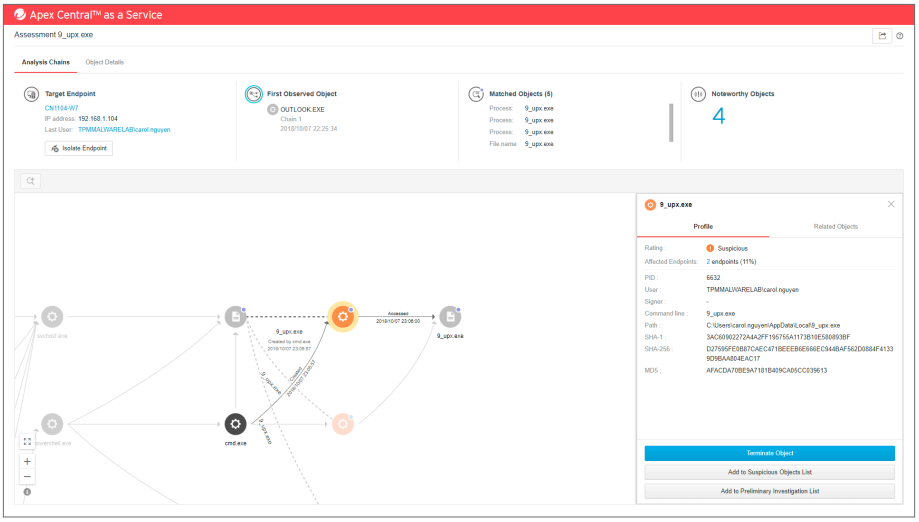
Offene APIs: Viele Kunden wollen ihre vorhandenen Tools aus dem eigenen Sicherheitsbetrieb nutzen. Apex One™ beinhaltet eine dokumentierte API, mit deren Hilfe das Produkt mit diesen bereits vorhandenen Tools zusammenarbeiten kann.

FUNKTIONSWEISE

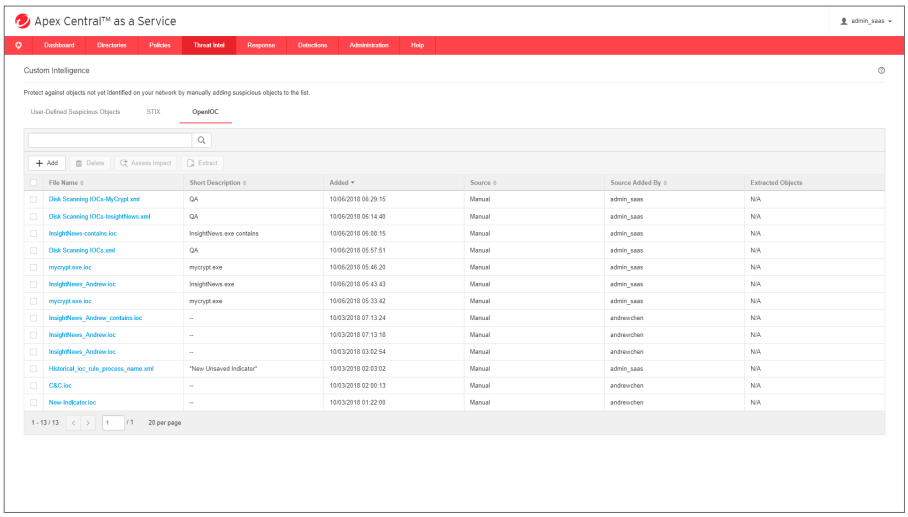
1. Endpunkte mit dem aktivierten Apex One™ Endpoint Sensor zeichnen Systemverhaltensweisen, Nutzerverhalten und Kommunikationen auf.
2. Metadaten zu den aufgezeichneten Informationen werden an den Apex One™ Server geschickt.
3. Erkennt Apex One™ eine Bedrohung, so können Sicherheitsforscher die Metadaten durchsuchen, um den erkannten Vorfall zu analysieren und zu verstehen wie weit sich die Malware ausgebreitet hat und wer im Unternehmen davon betroffen ist.



4. Eine vollständige Ursachenanalyse lässt die Sicherheitsforscher die Quelle der gefundenen Malware verstehen und sofortige Reaktionen aufsetzen, die die Wiederherstellung betroffener Systeme beinhalten und ein Update von Apex One™, sodass künftige ähnliche Angriffe blockiert werden.



5. Alternativ können Forscher vor der Entdeckung mithilfe von Parametern oder IOCs sowie YARA-Regeln nach Indicators of Attack (IOAs) suchen.



Schutzpunkte

- Windows®
- Macintosh*

*nur Suche

Kernfähigkeiten

- IOC-Suche
- IOA-Jagd
- Ursachenanalyse nach einer Entdeckung
- Analyse der Auswirkungen der Entdeckung
- Sofortige Reaktion
- Offene APIs
- Unterstützung durch den Anbieter

MINDESTANFORDERUNGEN FÜR DEN AGENTEN

Apex One Endpoint Sensor ist als optionales Add-on zu Apex One Endpoint Protection verfügbar. Es gibt ihn On-premises zusammen mit Apex One oder als SaaS mit Apex One™ as a Service. Informieren Sie sich über die Systemanforderungen für Apex One.

Apex One Endpoint Sensor wird auf den folgenden Endpunkten mit Apex One unterstützt:

Windows

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

Hardware:

2GB minimum RAM, 2GB vorhandener Festplattenplatz (3GB empfohlen)

Mac

- macOS™ Mojave 10.14
- macOS™ High Sierra 10.13
- macOS

TREND MICRO™

Securing Your Connected World