Trend Micro™

ENDPOINT SENSOR

Angriffe auf Endpunkten und Servern erkennen, untersuchen und darauf reagieren

Zielgerichtete Angriffe und komplexe Bedrohungen haben eindeutig gezeigt, dass sie in der Lage sind, konventionelle Sicherheitsmaßnahmen zu umgehen und unentdeckt zu bleiben, während sie Unternehmensdaten und geistiges Eigentum stehlen. Fortschrittliche Appliances für den Bedrohungsschutz können zwar Angriffsaktivitäten auf Netzwerkebene erkennen, aber eine Infiltrierung von Endpunkten nicht immer sicher nachweisen. Im Alleingang ist es zudem unmöglich, die Details und den Umfang von unternehmensweiten Angriffen zu untersuchen.

Trend Micro Endpoint Sensor ist eine kontextsensitive Endpunktsicherheitslösung, die zielgerichtete Angriffe erkennen kann, indem sie kontinuierliche Verhaltensanalysen auf Basis von Regeln für die Angriffsentdeckung durchführt. Darüber hinaus werden verdächtige Objekte für Sandbox-Analysen gesammelt. Endpoint Sensor ist auch ein fortschrittliches Forensik-Tool, das Aktivitäten auf Systemebene detailliert aufzeichnet, sodass Bedrohungsforscher die Art und den Umfang eines Angriffs schnell beurteilen können. Endpoint Sensor verwendet Kompromittierungsindikatoren von Trend Micro™ Deep Discovery™ und anderen Quellen, um eine Suche auf mehreren Ebenen über Benutzerendpunkte und Server hinweg durchzuführen.

Mit dieser Funktion können Sie:

- Endpunkt-Infiltrierungswarnungen von Trend Micro™ Deep Discovery™ Inspector oder anderen Sicherheitslösungen verifizieren
- Endpunkte mit spezifischen Kompromittierungsindikatoren, Malware oder Command-and-Control-Aktivitäten finden
- Tatsächliches Verhalten und Ergebnisse der Malware-Ausführung analysieren
- Vollständigen Kontext, zeitlichen Verlauf und Umfang eines Angriffs erfahren

HAUPTFUNKTIONEN

Endpunktresidente Ereignisaufzeichnung

Endpoint Sensor verwendet einen schlanken Client, um wichtige Aktivitäten und Kommunikationsereignisse auf der Kernel-Ebene aufzuzeichnen. Diese Ereignisse werden im zeitlichen Ablauf und im Kontext verfolgt, sodass eine detaillierte Historie entsteht, auf die in Echtzeit zugegriffen werden kann.

Umfangreiche Suchparameter

Endpunkte können auf spezifische Kommunikation und Malware, Registry- und Kontoaktivitäten sowie aktive Prozesse untersucht werden. Suchparameter können einzelne Parameter, OpenIOC- oder YARA-Dateien sein.

Fortschrittliche Verhaltensüberwachung

Die fortlaufenden Überwachungsfunktionen können bekannte und unbekannte Bedrohungen erkennen. Basis hierfür sind vordefinierte Regelsätze oder OpenIOC-Regeln. Das Monitoring entdeckt Angriffe, indem der Kontext und die Beziehungen von Verhaltensweisen untersucht werden. Angriffe können anhand der Taktik, den Methoden oder der Technologie der Bedrohung ermittelt werden.

Zentrale Suche und Analyse

Suchvorgänge können direkt vom Endpoint Sensor Manager oder innerhalb von Trend Micro™ Control Manager™ ausgeführt werden. So können Sie auf Angriffe sofort reagieren, die auf Kompromittierungsindikatoren in Echtzeit und Aktivitätsdaten anderer Produkte basieren.

Kontextanalyse und Ergebnisse auf mehreren Ebenen

Interaktive Dashboards ermöglichen es Ihnen, Systemaktivitäten über eine Zeitspanne hinweg anzuzeigen und zu analysieren, unternehmensweite Aktivitätszeitleisten zu beurteilen und Untersuchungsergebnisse zu exportieren.

Deep Discovery Einbindung

Verdächtige Objekte, die von Endpoint Sensor erkannt werden, können gesammelt und zur detaillierten Analyse an die Trend Micro™ Deep Discovery™ Analyzer Sandbox gesendet werden.

Lokal, remote und Cloud

Endpoint Sensor meldet und protokolliert detaillierte Aktivitäten auf Systemebene für Windows-basierte Server, Desktops und Laptops, unabhängig vom Standort.

Kompatibilität mit anderen Virenschutzlösungen

Kann zusammen mit beliebiger Antiviren-Software ausgeführt werden.

Entscheidende Vorteile

Bedrohungserkennung

Identifiziert Eindringungsversuche mithilfe der neuesten verfügbaren Sicherheitsdaten und Signaturen

Forensische Untersuchung

Deckt vollständigen Kontext, Zeitspanne und Umfang eines Angriffs auf

Verhaltensüberwachung

Erkennt verdächtige Verhaltensweisen anhand vordefinierter und benutzerdefinierter Regeln

Schnelle Reaktion

Reduziert die Zeit für die Beurteilung und Reaktion auf zielgerichtete Angriffe

NSS LABS RECOMMENDED

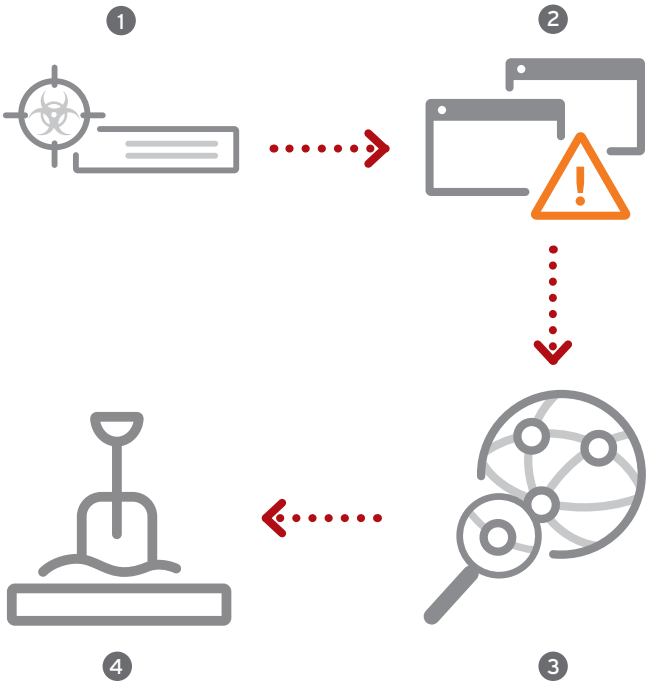
Trend Micro™ Deep Discovery

100%

Data Breach Rate

- 2017 -

EMPFOHLEN seit 4 Jahren in Folge



Entdecken, untersuchen und reagieren mit Bedrohungserkennung für Netzwerk und Endpunkte

1. Deep Discovery erkennt einen zielgerichteten Angriff auf das Netzwerk.
2. Kompromittierungsindikatoren werden von Deep Discovery an Endpoint Sensor gesendet.
3. Endpoint Sensor sucht nach Infiltrierung und ähnlichen Kompromittierungsindikatoren und bildet Zeitspanne/Fortschritt ab.
4. Mithilfe von Trend Micro und benutzerdefinierten Regeln überwacht Endpoint Sensor das Verhalten von Endpunkten. Wenn ein verdächtiges Objekt entdeckt wird, wird es gesammelt und zur Analyse-Sandbox an den Deep Discovery Analyzer gesendet.

SO FUNKTIONIERT ENDPOINT SENSOR

Endpoint Sensor Agent

Der Agent wird als ressourcenschonender Hintergrundprozess ausgeführt und sammelt ein detailliertes Profil von Systemereignissen und Kommunikation. Diese Informationen werden indiziert und lokal gespeichert, um auf Manager Such- und Analysetätigkeiten zu reagieren. Der Agent reagiert auch auf eine Vielzahl von Echtzeitanforderungen, einschließlich Momentaufnahmen von Speicher und Registry.

Zentrale Verwaltung und Kontrolle

Das Management der Agenten erfolgt über einen zentralisierten Server, der wiederum zur Bedrohungsuntersuchung über den Trend Micro Control Manager verwaltet wird.

Untersuchungskriterien

Suche und Untersuchung können auf mehreren Ebenen durchgeführt werden, basierend auf individuellen Kompromittierungsindikatoren oder Objekten sowie Open IOC- und YARA-Dateien. Zu den möglichen Suchparametern gehören:

- Kommunikation: IP, Port, Domain, DNS
- Malware oder jede Datei durch: Sha1-Hash, Dateiname, Dateipfad, Dateityp
- Registry-Aktivitäten
- Aktive Prozesse
- Anomalieerkennung von Benutzerkonten

Verhaltensüberwachung

Mithilfe vordefinierter Regeln und benutzerdefinierter Kompromittierungsindikatoren überwacht Endpoint Sensor das Systemverhalten, die Beziehungen und den Kontext, um das Angriffsverhalten zu ermitteln.

Sammlung verdächtiger Objekte

Verdächtige Objekte und Anhänge können automatisch zur weiteren Analyse an eine zentralisierte Deep Discovery Sandbox übermittelt werden.

Forschung und Ergebnisse

Endpoint Sensor bietet eine umfassende Kontextanalyse auf mehreren Ebenen über interaktive Dashboards, mit denen Sie detaillierte Systemaktivitäten im zeitlichen Verlauf anzeigen und analysieren, unternehmensweite Aktivitätszeitleisten untersuchen und Untersuchungsergebnisse exportieren können. Die Ergebnisse umfassen:

- Interaktive Zeitleiste der Systemaktivität
- Schrittweise Ermittlung und Konstruktion einer Angriffs-Kill-Chain
- Erkennung bösartiger Tools, Prozesse und Kommunikation
- Unternehmensweite Endpunktsuche basierend auf spezifischen Untersuchungsergebnissen

EIN WICHTIGER TEIL VON TREND MICRO CONNECTED THREAT DEFENSE

Um angemessen vor der aktuellen Bedrohungslandschaft zu schützen, benötigen Sie eine mehrschichtige Sicherheitsplattform, die den gesamten Lebenszyklus der Bedrohungsabwehr abdeckt. Trend Micro Connected Threat Defense ist ein Cybersicherheitsmodell, das Unternehmen eine bessere Möglichkeit bietet, neue zielgerichtete Bedrohungen schneller zu erkennen, auf sie zu reagieren und sich vor ihnen zu schützen. Gleichzeitig werden Transparenz und Kontrolle über das gesamte Netzwerk hinweg verbessert.

- **Schutz:** Bewerten Sie potenzielle Schwachstellen und schützen Sie proaktiv Endpunkte, Server und Anwendungen.
- **Erkennung:** Erkennen Sie komplexe Malware, Verhaltensweisen und Kommunikation, die herkömmliche Abwehrmethoden nicht entdecken.
- **Reaktion:** Ermöglichen Sie eine schnelle Reaktion durch gemeinsame Informationen über Bedrohungen und die Bereitstellung von Echtzeit-Sicherheitsupdates.
- **Transparenz und Kontrolle:** Erhalten Sie zentralisierte Transparenz über das Netzwerk und die Systeme hinweg. Analysieren und bewerten Sie die Auswirkungen von Bedrohungen.

SCHUTZSTRATEGIE AUSBAUEN

Endpoint Sensor ist Teil einer fortschrittlichen Bedrohungsstrategie, die an geschäftskritischen Stellen in Unternehmen zum Einsatz kommt – Netzwerk, Endpunkt, E-Mail oder integrierte Sicherheit. Mit Endpoint Sensor erhalten Sie Unterstützung bei der Untersuchung und Reaktion auf zielgerichtete Angriffe, die von Deep Discovery Inspector identifiziert werden. Deep Discovery (IOC) Kompromittierungsindikatoren werden von Endpoint Sensor dazu eingesetzt, um Endpunktinfiltrierungen zu verifizieren und den vollständigen Kontext, den Zeitraum und den Umfang des Angriffs zu ermitteln.

Deep Discovery Inspector bietet erweiterten Netzwerkschutz gegen zielgerichtete Angriffe und überwacht alle Ports sowie mehr als 100 Protokolle, um praktisch den gesamten Netzwerkverkehr zu analysieren. Spezielle Erkennungs-Engines und ein angepasstes Sandboxing identifizieren und analysieren Malware, Command-and-Control-Kommunikation und Umgehungstechniken von Angreifern. Inspector stellt dann die Untersuchungsdaten bereit, um eine schnelle Reaktion auf Angriffe und eine wirksame Abwehr zu unterstützen.

Mit **Control Manager** können Sie mehrere Trend Micro Schutzschichten über eine einzige Konsole zentral verwalten und überwachen. Die Funktionalität von Endpoint Sensor Manager ist in den Control Manager eingebettet, um zentrale Untersuchungen zu ermöglichen, die die Kompromittierungsindikatoren der meisten Trend Micro Produkte nutzen. So kann der Untersuchungsbeauftragte durch sofortige Maßnahmen auf den Angriff reagieren.

Deep Discovery Analyzer bietet erweiterte Sandbox-Analysen, mit denen der Wert von Sicherheitsprodukten wie Endpunktschutz, Web- und E-Mail-Gateways, Netzwerksicherheit und anderen Deep Discovery Produkten gesteigert wird. Endpoint Sensor kann verdächtige Objekte sammeln und zur Analyse senden. Sandbox-Umgebungen sind an die individuellen Vorgaben des jeweiligen Unternehmens angepasst, zum Beispiel hinsichtlich Betriebssystemen, Spracheinstellungen und Konfigurationen. Dadurch kann Deep Discovery Analyzer Ransomware, komplexe Malware, Zero-Day-Exploits, Command-and-Control-Kommunikation identifizieren. Zudem werden auch mehrstufige Downloads erkannt, die ihren Ursprung in einem bösartigen Schadteil oder einer URL unter Windows oder Mac OS haben.

Deep Discovery Email Inspector bietet komplexe Malware-Erkennung, einschließlich Sandboxing für E-Mail. Der Email Inspector kann so konfiguriert werden, dass die Bereitstellung von komplexer Malware per E-Mail blockiert wird. Diese Malware ist oft die erste Stufe eines Ransomware-Angriffs.

SPEZIFIKATIONEN

SYSTEMVORAUSSETZUNGEN	
SERVER	Mindestens 4 GB, empfohlen 16 GB. Festplattenspeicher: Mindestens 500 GB, empfohlen 1 TB. **Betriebssysteme** Windows Server 2008 SP2 (32 Bit/64 Bit) Windows Server 2008 R2 (64 Bit) Microsoft Internet Information Services (IIS) 7 mit allen folgenden Diensten: • Statischer Inhalt • Standarddokument • Verzeichnis durchsuchen • HTTP-Fehler • HTTP-Umleitung • ASP.NET • ASP • CGI • ISAPI-Erweiterungen • ISAPI-Filter • Anfragefilter • IIS-Verwaltungskonsole • PHP-Version 5.4.38 **Datenbank** Microsoft SQL Server 2008 Express Microsoft SQL Server 2008 R2 Standard empfohlen **Webbrowser** Microsoft Internet Explorer 9 oder höher Neueste Version von Google Chrome Neueste Version von Mozilla Firefox
AGENT	**Hardware** RAM: • Mindestens 512 MB für Windows XP • Mindestens 1 GB für andere Betriebssysteme Festplattenspeicher: • Mindestens 3 GB für Windows XP, Vista, 7, 8 oder 8.1 • Mindestens 3 GB für Windows Server Betriebssysteme **Software** Betriebssystem: • Windows Vista Service Pack 1 (32 Bit und 64 Bit) • Windows XP Service Pack 3 (32 Bit) • Windows 7 (32 Bit und 64 Bit) • Windows 8 (32 Bit und 64 Bit) • Windows 8.1 (32 Bit und 64 Bit) • Windows 10 (32 Bit und 64 Bit) • Windows Server 2003 (32 Bit und 64 Bit) • Windows Server 2003 R2 (32 Bit und 64 Bit) • Windows Server 2008 (32 Bit und 64 Bit) • Windows Server 2008 R2 (64 Bit) • Windows Server 2012 (32 Bit und 64 Bit) • Windows Server 2012 R2 (64 Bit)

Ausführliche Informationen erhalten Sie von Ihrem Trend Micro Vertriebsmitarbeiter.

Trend Micro Network Defense Lösung wird unterstützt durch XGen™, einem intelligenten, optimierten und vernetzten Sicherheitsansatz.

POWERED BY XGen™ SECURITY

TREND MICRO™

Ihr sicherer Weg in die Cloud