Trend Micro™

DEEP DISCOVERY™ ANALYZER

Verbesserter Schutz gegen zielgerichtete Angriffe

Zielgerichtete Angriffe und komplexe Bedrohungen werden so angepasst, um Ihre konventionellen Sicherheitsmaßnahmen zu umgehen (und dabei unentdeckt zu bleiben), während sensible Daten gestohlen oder wichtige Daten verschlüsselt werden, bis Lösegeldforderungen erfüllt sind. Um zielgerichtete Angriffe und komplexe Bedrohungen zu erkennen, sind sich Analysten und Sicherheitsexperten einig, dass Unternehmen fortschrittliche Erkennungstechnologie als Teil einer erweiterten Strategie einsetzen sollten, um den heutigen Umgehungstechniken von Angreifern zu begegnen.

Deep Discovery Analyzer erhöht den Wert bestehender Sicherheitsinvestitionen von Trend Micro und Drittanbietern (über eine Webdienst-API) durch Bereitstellung von benutzerdefiniertem Sandboxing und erweiterten Analysen. Er kann auch erweiterte Sandbox-Funktionen für andere Trend Micro-Produkte bereitstellen. Verdächtige Objekte können zur erweiterten Analyse mithilfe mehrerer Erkennungsmethoden an die Analyzer-Sandbox gesendet werden. Wenn eine Bedrohung entdeckt wird, werden Sicherheitslösungen automatisch aktualisiert.

SCHLÜSSELFUNKTIONEN

Benutzerdefinierte Sandbox-Analyse verwendet virtuelle Images, die genau auf Ihre Systemkonfigurationen, Treiber, installierten Anwendungen und Sprachversionen abgestimmt sind. Dieser Ansatz verbessert die Erkennungsrate von komplexen Bedrohungen, die dazu ausgelegt sind, virtuelle Standard-Images zu umgehen. Die benutzerdefinierte Sandbox-Umgebung enthält einen sicheren externen Zugriff zur Identifizierung und Analyse von Downloads, URLs, Command-and-Control-Kommunikation auf mehreren Ebenen sowie zur Unterstützung der manuellen oder automatisierten Datei- und URL-Übermittlung.

Flexible Bereitstellung Analyzer kann als eigenständige Sandbox oder zusammen mit einer größeren Deep Discovery-Bereitstellung bereitgestellt werden, um zusätzliche Sandbox-Kapazität hinzuzufügen. Er ist skalierbar, um bis zu 60 Sandboxes in einer einzigen Appliance zu unterstützen. Mehrere Appliances können für hohe Verfügbarkeit geclustert oder für eine Hot- oder Cold-Sicherung konfiguriert werden.

Erweiterte Erkennungsmethoden wie statische, heuristische und Verhaltensanalyse sowie Web- und Dateireputation stellen sicher, dass Bedrohungen schnell entdeckt werden. Analyzer erkennt auch schädliche Dateien, ausgehende Verbindungen und wiederholt Command-and-Control-Kommunikation auf mehreren Ebenen von verdächtigen Dateien.

- **Analyse zahlreicher verschiedener Dateitypen** Untersucht mithilfe mehrerer Erkennungsengines und Sandboxing eine große Anzahl an Dateitypen wie ausführbare Microsoft® Office- und PDF-Dateien sowie Internetinhalte und komprimierte Dateien. Benutzerdefinierte Richtlinien können nach Dateityp definiert werden.
- **Erkennung von Dokument-Exploits** Entdeckt Malware und Exploits, die durch gewöhnliche Dokumente eingeschleust werden, durch spezielle Erkennungstechniken und Sandboxing.
- **URL-Analyse** Führt eine Sandbox-Analyse von URLs durch, die in E-Mails oder manuell übermittelten Beispielen enthalten sind.
- **Web-Services-API und manuelle Einreichung** Ermöglicht es jedem Produkt- oder Malware-Analysten, verdächtige Samples einzureichen. Teilt neue Erkennungsdaten von Kompromittierungsindikatoren automatisch mit Produkten von Trend Micro und Drittanbietern.
- Unterstützung für Windows-, Mac- und Android-Betriebssystemen.

Ransomware erkennen Erkennt Skript-Emulation, Zero-Day-Exploits, zielgerichtete und passwortgeschützte Malware, die häufig mit Ransomware in Verbindung gebracht werden. Die IT nutzt außerdem Informationen zu bekannten Bedrohungen, um Ransomware anhand von Muster- und Reputationsanalyse zu erkennen. Die benutzerdefinierte Sandbox kann Massenmanipulationen an Dateien, Verschlüsselungsvorgänge und Änderungen an Sicherung und Wiederherstellung erkennen.

Hauptvorteile

Verbesserte Erkennung

- Überlegene Erkennung im Vergleich zu typischen virtuellen Umgebungen
- Hervorragende Abwehr von Umgehungstechniken

Sichtbarer ROI

- Verbesserung vorhandener Investitionen durch gemeinsame Nutzung von Bedrohungsinformationen und zusätzlicher Verarbeitungskapazität in High-Traffic-Umgebungen
- Zeitraubende manuelle Analyse verdächtiger Dateien abschaffen
- Hohe Kosten für Schäden durch Ransomware vermeiden
- Flexible Bereitstellungsoptionen für zentrale oder dezentrale Analyse

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery

100%

Data Breach Rate
- 2017 -

EMPFOHLEN seit 4 Jahren in Folge

ICSA labs CERTIFIED

EIN WICHTIGER TEIL VON TREND MICRO CONNECTED THREAT DEFENSE

Um angemessen vor der aktuellen Bedrohungslandschaft zu schützen, benötigen Sie eine Schutzplattform auf mehreren Ebenen, die den gesamten Lebenszyklus der Bedrohungsabwehr abdeckt. Trend Micro Connected Threat Defense ist ein neues Cybersicherheitsmodell, das Unternehmen eine bessere Möglichkeit bietet, neue zielgerichtete Bedrohungen schnell zu erkennen, darauf zu reagieren und davor zu schützen, während gleichzeitig die Transparenz und Kontrolle über ihr Netzwerk hinweg verbessert wird.

- **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 für Trend Micro-Sicherheitsebenen und Sicherheit von Drittanbietern mithilfe von YARA und STIX.
- **Transparenz und Kontrolle**: Erhalten Sie zentralisierte Transparenz über das Netzwerk und die Systeme hinweg. Analysieren und bewerten Sie die Auswirkungen von Bedrohungen.

DEEP DISCOVERY ANALYZER APPLIANCE-SPEZIFIKATIONEN

	Hardware-Modell 1100
Kapazität	45.000 Bedrohungsexemplare/Tag
Unterstützte Dateitypen	cell, chm, class, dll, doc, docx, exe, gul, hwp, hwpx, jar, js, jse, jtd, lnk, mov, pdf, ppt, pptx, ps1, rtf, swf, vbs, vbe, xls, xlsx, xml
Unterstützte Betriebssysteme	Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, Mac OS
Formfaktor	2U Rack-Mount, 48,26 cm (19")
Gewicht	32,5 kg
Abmessungen	Breite 48,2 cm (18.98") x Tiefe 75,58 cm (29.75") x Höhe 8,73 cm (3.44")
Management Ports	10/100/1000 Base-T RJ45 Port x 1
Data Ports	10/100/1000 Base-T RJ45 x 3
AC-Eingangsspannung	100-240 VAC
AC-Eingangsstrom	10-5 A
Festplatten	2 x 4 TB 3.5 Inch SATA
RAID-Konfiguration	RAID 1
Stromversorgung	750 W Redundant
Maximale Leistungsaufnahme	847 W (max.)
Wärme	2891 BTU/St. (max.)
Frequenz	50/60 Hz
Betriebstemperatur	10-35 °C
Hardwaregarantie	3 Jahre

ANDERE DEEP DISCOVERY-PRODUKTE

Deep Discovery Analyzer ist Teil der Deep Discovery-Plattform und bietet fortschrittlichen Bedrohungsschutz, der an geschäftskritischen Stellen im Unternehmen zum Einsatz kommt – Netzwerk, E-Mail, Endpunkt oder bestehende Sicherheitslösungen.

- **Deep Discovery Inspector** ist eine virtuelle oder Hardware-Appliance, die eine ganzheitliche Erkennung von zielgerichteten Angriffen und komplexen Bedrohungen ermöglicht. Durch die Verwendung spezieller Erkennungsengines und einer angepassten Sandbox-Analyse sind Sie mit Deep Discovery Inspector in der Lage, komplexe und unbekannte Malware, Ransomware, Zero-Day-Exploits, Command-and-Control-Kommunikation, Seitwärtsbewegungen und Umgehungstechniken von Angreifern zu erkennen, die von üblichen Sicherheitsmethoden unentdeckt bleiben.
- **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.

Deep Discovery Analyzer ist Teil der Trend Micro Network Defense Lösung, unterstützt durch XGen™ Security.

Securing Your Journey to the Cloud