Trend Micro™

DEEP DISCOVERY™ INSPECTOR

Netzwerkweite Erkennung von gezielten Angriffen, komplexen Bedrohungen und Ransomware

Komplexe, zielgerichtete Angriffe sind speziell auf Ihr Unternehmen zugeschnitten, um Ihre herkömmlichen Sicherheitsmaßnahmen zu umgehen und im Verborgenen Unternehmensdaten, geistiges Eigentum und Kommunikation zu entwenden oder wichtige Daten zu verschlüsseln, bis Lösegeldforderungen erfüllt werden. Analysten und Sicherheitsexperten sind sich einig, dass hochentwickelte Erkennungstechnologien als Teil einer erweiterten Sicherheitsstrategie für Unternehmen unerlässlich sind, um diese gezielten und komplexen Angriffe abzuwehren.

Deep Discovery Inspector bietet als physische oder virtuelle Netzwerk-Appliance ein netzwerkweites Monitoring des gesamten Datenverkehrs und ermöglicht damit umfassende Transparenz für sämtliche Aspekte von gezielten Angriffen, komplexen Bedrohungen und Ransomware. Mithilfe spezieller Engines zur Bedrohungserkennung und benutzerdefinierter Sandbox-Analysen identifiziert Deep Discovery Inspector komplexe und unbekannte Malware, Ransomware, Zero-Day-Exploits, C&C-Kommunikation und versteckte Angreiferaktivitäten, die von Standard-Sicherheitsmechanismen unentdeckt bleiben. Die Erkennungsfunktionen werden durch das Monitoring des gesamten physischen, virtuellen, ein- und ausgehenden sowie internen Datenverkehrs erweitert. Dank dieser Funktion und einer 100%-igen Erkennungsrate erhielt Trend Micro durch NSS Labs bereits das vierte Jahr in Folge eine Auszeichnung mit der Bewertung „Empfehlenswert".

Entscheidende Vorteile

Bessere Erkennung

- Mehrere Erkennungstechniken
- Monitoring des gesamten Netzwerkverkehrs
- Benutzerdefinierte Sandbox-Analysen
- Umfassende Bedrohungsinformationen

Sichtbare Rendite

- Laut Forschungsergebnissen 145 % Rendite in 10 Monaten[1]
- Erweiterung bestehender Investitionen
- Flexible Installationsoptionen
- Automatisierung zuvor manuell ausgeführter Aufgaben

[1] ESG, Validierung des ökonomischen Werts: Oktober 2015

WESENTLICHE FUNKTIONEN

Überprüfung aller Netzwerkinhalte. Deep Discovery Inspector überwacht den gesamten Datenverkehr physischer und virtueller Netzwerksegmente, alle Netzwerk-Ports und über 100 Netzwerkprotokolle, um gezielte Angriffe, komplexe Bedrohungen und Ransomware zu erkennen. Dank unseres ortsunabhängigen Ansatzes zum Schutz des Netzwerkverkehrs kann Deep Discovery gezielte Angriffe, komplexe Bedrohungen und Ransomware im eingehenden und ausgehenden Netzwerkverkehr sowie laterale Ausbreitung, C&C-Kommunikation und anderes Angreiferverhalten in der gesamten Angriffsabwehrkette erkennen.

Umfassende Erkennungsmethoden nutzen File- und Web-Reputation, Reputationsprüfungen von IPs und mobilen Anwendungen, heuristische Analysen, Suche komplexer Bedrohungen, benutzerdefinierte Sandbox-Analysen und korrelierte Bedrohungsdaten, um Ransomware, Zero-Day-Exploits, komplexe Malware und Angreiferverhalten zu erkennen.

Benutzerdefinierte Sandbox-Analysen nutzen virtuelle Images, die genau den Systemkonfigurationen, Treibern, installierten Anwendungen und Sprachversionen eines Unternehmens entsprechen. Dieser Ansatz verbessert die Erkennungsrate von Ransomware und komplexen Bedrohungen, die darauf abzielen, standardmäßige virtuelle Images zu umgehen.

Umfassende Bedrohungsinformationen stellen sicher, dass lokale Erkenntnisse zu Netzwerkbedrohungen mit globalen Bedrohungsinformationen aus dem Trend Micro™ Smart Protection Network™ korreliert werden. So profitieren Unternehmen von einem sofortigen Schutz aller Daten unabhängig vom Speicherort.

Beschleunigte und höhere Rendite durch eine flexible Architektur, die je nach Netzwerkdurchsatz eine Installation als Hardware oder als virtuelle Appliance ermöglicht. Bestehende Investitionen in NGFW/IPS, SIEM und Gateways werden durch den Austausch von Bedrohungsinformationen erweitert.

Erkennung von Ransomware im gesamten Netzwerk. Deep Discovery Inspector erkennt Skript-Emulation, Zero-Day-Exploits sowie zielgerichtete und kennwortgeschützte Malware, die gewöhnlich im Zusammenhang mit Ransomware steht. Darüber hinaus werden Informationen über bekannte Bedrohungen genutzt, um Ransomware mithilfe von Pattern- und Reputation-basierten Analysen zu erkennen. Benutzerdefiniertes Sandboxing erkennt Verschlüsselungsverhalten, Änderungen an großen Mengen von Dateien sowie an Backup-Dateien für die Wiederherstellung.

EINE WESENTLICHE KOMPONENTE VON TREND MICRO CONNECTED THREAT DEFENSE

Um in der heutigen Bedrohungslandschaft optimal geschützt zu sein, benötigen Sie eine mehrschichtige Sicherheitsplattform, die den vollständigen Sicherheitslebenszyklus abdeckt. Trend Micro Connected Threat Defense ist ein mehrschichtiger Sicherheitsansatz, mit dem Ihr Unternehmen neue und gezielte Bedrohungen besser und schneller erkennen, verhindern und darauf reagieren kann. Gleichzeitig bietet der Ansatz mehr Transparenz und Kontrolle im gesamten Netzwerk.

- **Verhindern:** Bewertung potenzieller Sicherheitslücken und proaktiver Schutz von Endpunkten, Servern und Anwendungen
- **Erkennen:** Erkennung von komplexer Malware, Verhaltensweisen und Kommunikation, die von Standard-Sicherheitsmechanismen unentdeckt bleiben
- **Reagieren:** Schnelle Reaktion durch Austausch von Bedrohungsdaten und Bereitstellung von Sicherheitsupdates in Echtzeit
- **Transparenz und Kontrolle:** Zentrale Transparenz im gesamten Netzwerk und in allen Systemen sowie Analyse und Bewertung der Auswirkungen von Bedrohungen

SPEZIFIKATIONEN FÜR DEEP DISCOVERY INSPECTOR HARDWARE-APPLIANCES

	Serie 500/1000	Serie 4000
Hardwaremodell	510/1100	4100
Durchsatz	500 Mbit/s / 1 Gbit/s	4 Gbit/s
Unterstützte Sandboxes	2 (500), 4 (1000)	20
Formfaktor	1U Rack montierbar, 48,26 cm (19 Zoll)	2U Rack montierbar, 48,26 cm (19 Zoll)
Gewicht	19,9 kg	31,5 kg
Abmessungen (BxTxH)	43,4 cm (17,09 Zoll) x 64,2 cm (25,28 Zoll) x 4,28 cm (1,69 Zoll)	48,2 cm (18,98 Zoll) x 75,58 cm (29,75 Zoll) x 8,73 cm (3,44 Zoll)
Verwaltungsports	10/100/1000 BASE-T RJ45 Port x 1 iDrac Enterprise RD45 x 1	10/100/1000 BASE-T RJ45 Port x 1 iDrac Enterprise RD45 x 1
Datenports	10/100/1000 BASE-T RJ45 Port x 5	10 Gbit SFP+ SR Transceiver x 4 0/100/1000 Base-T RJ45 x 5
Wechselstromversorgung	100 bis 240 VAC	100 bis 240 VAC
AC-Eingangsstrom	7,4 A bis 3,7 A	10 A bis 5 A
Festplatten	2 x 1 TB 3,5 Zoll SATA	4 x 1 TB 3,5 Zoll NLSAS
RAID-Konfiguration	RAID 1	RAID 1+0
Stromversorgung	550 W (redundant)	750 W (redundant)
Stromverbrauch (max.)	604 W	847 W (max.)
Wärmeabgabe	2133 BTU/h (max.)	2891 BTU/h (max.)
Frequenz	50/60 Hz	50/60 Hz
Betriebstemperatur	10 bis 35 °C	10 bis 35 °C
Hardwaregarantie	3 Jahre	3 Jahre

Als virtuelle Appliance ist Deep Discovery Inspector für die Kapazitäten von 100/250/500/1000 Mbit/s verfügbar und kann unter VMware vSphere 5 und höher installiert werden. KVM wird ebenfalls unterstützt.

SONSTIGE DEEP DISCOVERY PRODUKTE

Deep Discovery Inspector bietet Schutz vor komplexen Bedrohungen für Netzwerke, E-Mail-Systeme und Endpunkte – also dort, wo es für Ihr Unternehmen besonders darauf ankommt – und ergänzt vorhandene Sicherheitslösungen.

- **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. Deep Discovery Analyzer erkennt Ransomware, komplexe Malware, Zero-Day-Exploits, Command-and-Control-Kommunikation sowie mehrstufige Downloads, die von bösartigen Nutzlasten oder URLs auf Windows- und Mac-Betriebssystemen stammen.
- **Deep Discovery Email Inspector** schützt E-Mail-Systeme durch erweiterte Erkennungstechniken, einschließlich Sandboxing. Email Inspector kann so konfiguriert werden, dass Malware-infizierte E-Mails gesperrt werden. Derartige Malware stellt häufig die erste Phase eines Ransomware-Angriffs dar.

Deep Discovery Inspector ist eine Komponente von Trend Micro Network Defense – unterstützt durch XGen™ Security.

Erkennung und Abwehr von:

- Gezielten Angriffen und komplexen Bedrohungen
- Gezielten und bekannten Ransomware-Angriffen
- Zero-Day-Malware und Exploits in Dokumenten
- Angreiferverhalten und anderen Netzwerkaktivitäten
- Internetbedrohungen, einschließlich Exploits und Drive-by-Downloads
- Phishing, Spear-Phishing und anderen E-Mail-Bedrohungen
- Herausschleusen von Daten
- Bots, Trojanern, Würmern, Keyloggern
- Zerstörerischen Anwendungen

TREND MICRO™

Securing Your Journey to the Cloud