McAfee Network Threat Behavior Analysis

Vollständige Übersicht über Netzwerkverhalten und Bedrohungen

McAfee® Network Threat Behavior Analysis ist eine integrierte Komponente von McAfee Network Security Platform zur Bereitstellung einer Echtzeitübersicht sowie von Bedrohungsschutz für die Netzwerkinfrastruktur. Durch die Analyse des Datenverkehrs von Switches und Routern kann McAfee Network Threat Behavior Analysis riskantes Verhalten auf ganz bestimmte Punkte im Netzwerk eingrenzen und somit Stealth-Angriffe wirksam verhindern. Die Lösung wertet Bedrohungen auf Netzwerkebene ganzheitlich aus, erfasst das Gesamtverhalten jedes einzelnen Netzwerkelements und ermöglicht die sofortige Abstraktion potenzieller Anomalien oder von Angriffen durch Malware, Zero-Day-Angriffe, Botnets oder Würmer. McAfee Network Threat Behavior Analysis nutzt auch einige hochentwickelte McAfee Network Security Platform-Module, darunter das Echtzeit-Emulationsmodul, das Malware auch ohne Signaturen erkennen kann.

Hauptvorteile

Transparenz zur Absicherung des Netzwerks

- Überwachung von ungewöhnlichem Netzwerkverhalten durch Netzwerk-Datenverkehrsanalyse und Berichterstellung
- Präventive, verhaltensbasierte Bedrohungserkennung
- Wirksame Erkennung unbekannter Bedrohungen
- Erkennung von Anomalien einschließlich Zero-Day-, Spam-, Botnet- und Erkundungsangriffen

Umfassender Malware-Schutz

- Malware-Abwehr durch Echtzeit-Emulation schädlicher Dateien
- Fortschrittliche Korrelation aller Netzwerkaktivitäten zur Erkennung von Botnet-Aktivitäten
- Endgeräteinformationen und Korrelation von Netzwerkdatenflüssen und -ereignissen

Intelligente Transparenz zur Abwehr aktueller Stealth-Angriffe

Ihr Netzwerk ist hochentwickelten, verborgenen Angriffen ausgesetzt, die herkömmlichen Entdeckungsmethoden entgehen. Dadurch ist Ihr Netzwerk von schwerwiegenden Kompromittierungen und Ausfällen bedroht. McAfee Network Threat Behavior Analysis überwacht und analysiert auf intelligente Weise den Netzwerkverkehr Ihrer Switches sowie Router und meldet Verhaltensauffälligkeiten, damit Sie Angriffe auf Ihr Netzwerk erkennen und zeitnah darauf reagieren können.

Die McAfee Network Threat Behavior Analysis-Appliance nutzt Daten von NetFlow und J-Flow zur Erkennung von Bedrohungen, die außerhalb der typischen Grenzen des Eindringungsschutzsystems aktiv sind. Die Appliance ist vollständig ausgestattet mit Vierkern-Prozessoren, einem RAID-Disk-Array sowie Gigabit-Ethernet-Anschlüssen. Sie lässt sich auch offline mit einem Storage Area Network (SAN) verbinden. Dank ihrer Fähigkeit zur Unterscheidung von Datenströmen kann sie große Mengen von Netzwerk-Datenverkehr bewältigen und die Datenströme schneller auswerten.

Unübertroffene Netzwerktransparenz und -informationen

Mithilfe von McAfee Network Threat Behavior Analysis können Sie informierte Entscheidungen über Anwendungen und Protokolle in Ihrem Netzwerk treffen. Die Appliance überwacht sowie meldet ungewöhnliches Netzwerkverhalten und kann mithilfe verhaltensbasierter Algorithmen Bedrohungen identifizieren. Die Analyse des Verhaltens von Hosts und Anwendungen ermöglicht die Anomalie-Erkennung von Zero-Day-Angriffen, Spam, Botnets sowie Erkundungsangriffen. Durch eine umfassende Datenflussanalyse können die Nutzung nicht autorisierter Anwendungen entdeckt und problematische Netzwerkbereiche lokalisiert werden.

Eindämmung und Verhinderung von Malware-Ausbrüchen

Dank der Verzahnung mit McAfee Network Security Platform bietet McAfee Network Threat Behavior Analysis Echtzeit-Emulation für die fortschrittliche Untersuchung und Blockierung verdächtiger Dateien. Das Echtzeit-Emulationsmodul scannt verdächtige Dateien zur Erkennung und Blockierung von schädlichem Verhalten. Mithilfe der hochentwickelten Korrelation über mehrere Eindringungsschutzsysteme und Netzwerkgeräte hinweg findet McAfee Network Threat Behavior Analysis getarnte Botnets, die herkömmliche signaturbasierte Schutzmaßnahmen umgehen können. Dank der Verzahnung mit McAfee Endpoint Intelligence Agent werden kompromittierte Endgeräte entdeckt und unter Kontrolle gebracht, die schädlichen Datenverkehr als legitimen Netzwerkverkehr tarnen. Die reputationsbasierte Analyse der Endgeräteaktivitäten schränkt die Datenexfiltration ein und verhindert Malware-Ausbrüche.

Optimierung von Sicherheitsabläufen und Kosteneinsparung

McAfee Network Threat Behavior Analysis bietet umsetzbare Informationen, die eine kostengünstige Sicherheitsverwaltung ermöglichen. Die Appliance beschleunigt die Reaktionszeiten, optimiert die Netzwerkleistung und verhindert, dass Netzwerkbedrohungen sowie Exploits den Geschäftsbetrieb unterbrechen.

Weitere Funktionen

- Verbesserte Sicherheit durch die Integration von McAfee Global Threat Intelligence (McAfee GTI)
- Virtuelle Variante für kostengünstige Implementierung
- Verbesserung des Überblicks und der Korrelation durch die Integration von McAfee ePolicy Orchestrator® (McAfee ePO™), McAfee Enterprise Security Manager und McAfee Vulnerability Manager
- Mühelose Einordnung und Analyse von Netzwerk-Datenverkehr
- Dashboard zur Erfassung von Metadaten zu einzelnen Datenflüssen (App ID, Dateien, URLs)
- Verbesserung der Sicherheitslage durch umfassende Quarantänemöglichkeiten
- Übersicht über externe Hosts mit detaillierter Darstellung des Host-Bedrohungsfaktors
- Kompatibel mit Switches und Routern von Cisco (NetFlow Versionen 5 und 9) und Juniper (J-Flow Versionen 5 und 9)

	NTBA T-600	NTBA T-1200
Spezifikationen		
Datenflüsse pro Sekunde	maximal 60.000	maximal 100.000
Cisco NetFlow	Versionen 5 und 9	Versionen 5 und 9
Juniper J-Flow	Versionen 5 und 9	Versionen 5 und 9
Prozessor	1 x Xeon E5-2658	2 x Xeon E5-2658
Arbeitsspeicher	46 GB	96 GB
Nutzbarer Speicher	4,4 TB / RAID 10	8,8 TB / RAID 10
Netzwerkschnittstellen	4 x 10/100/1000 (Kupfer)	4 x 10/100/1000 (Kupfer)
Technische Daten		
Formfaktor	1 HE	2 HE
Breite	43,8 cm	43,8 cm
Tiefe	70,94 cm	70,78 cm
Höhe	4,32 cm	8,76 cm
Maximales Gewicht	14,96 kg	21,6 kg
Geschätzte Eingangsleistungsaufnahme (Maximalwert)	402 W	667 W
Redundante Netzteile	750 W	750 W
Systemkühlung (Wärmeabgabe)	1.370 BTU/Stunde	2.280 BTU/Stunde
Betriebstemperatur	+10 bis +35 °C mit Temperaturschwankungen von max. 10 °C pro Stunde	

Spezifikationen der virtuellen NTBA	T-VM	T-100VM	T-200VM
Empfohlener Arbeitsspeicher	16 GB	8 GB	16 GB
Empfohlene Prozessoren	4	4	4
Datenflüsse pro Sekunde	maximal 25.000 fps	maximal 10.000 fps	maximal 25.000 fps

McAfee
An Intel Company

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

60839ds_ntba_0214_ETMG