McAfee Network Threat Behavior Analysis

Visibilità completa su comportamenti e minacce in rete

McAfee® Network Threat Behavior Analysis è un componente integrato di McAfee Network Security Platform che fornisce visibilità in tempo reale e protezione dalle minacce all'infrastruttura di rete. Analizzando il traffico che passa attraverso switch e router, McAfee Network Threat Behavior Analysis evidenzia i comportamenti a rischio sulla rete e previene in modo efficace gli attacchi furtivi. La valutazione olistica delle minacce a livello della rete consente di identificare il comportamento complessivo di ogni elemento della rete stessa e permette di isolare istantaneamente potenziali anomalie o tipi di attacco, fra i quali malware, attacchi zero-day, botnet e worm. McAfee Network Threat Behavior Analysis, inoltre, integra alcuni motori di analisi avanzata di McAfee Network Security Platform, tra cui il motore di emulazione in tempo reale che identifica i malware privi di firme.

Vantaggi principali

Visibilità a protezione della rete

- Monitoraggio e segnalazione di comportamenti insoliti tramite l'analisi del traffico di rete.
- Rilevamento proattivo delle minacce, in base ai comportamenti.
- Rilevamento efficiente delle minacce sconosciute.
- L'individuazione delle anomalie comprende spam, botnet e attacchi zero-day e di ricognizione.

Protezione completa dal malware

- Blocca i malware grazie all'emulazione in tempo reale dei file dannosi.
- Correlazione avanzata su tutta la rete per il rilevamento di attività botnet.
- Intelligence e correlazione a livello di endpoint per eventi e flussi di rete.

Visibilità intelligente contro i moderni attacchi furtivi

La vostra rete deve affrontare attacchi furtivi avanzati in grado di oltrepassare i tradizionali metodi di rilevamento e di causare violazioni e interruzioni alla rete aziendale. McAfee Network Threat Behavior Analysis monitora e segnala i comportamenti insoliti tramite l'analisi del traffico che passa attraverso switch e router, consentendo di identificare e neutralizzare rapidamente le aggressioni alla rete.

L'appliance McAfee Network Threat Behavior Analysis, dotata di processori quad-core, array di dischi RAID e connettività gigabit Ethernet, sfrutta i flussi di dati NetFlow e J-Flow per identificare le minacce anche al di fuori del tradizionale perimetro del sistema di prevenzione delle intrusioni (IPS). Inoltre, fornisce la connettività offline alla rete SAN (Storage Area Network) e, grazie alla sua distinta capacità di flusso, è in grado di gestire grandi quantità di traffico di rete, velocizzandone così l'analisi.

Visibilità e analisi della rete senza confronti

McAfee Network Threat Behavior Analysis consente di prendere decisioni informate in relazione alle applicazioni e ai protocolli in uso sulla vostra rete, monitorando e segnalando i comportamenti di rete insoliti e identificando le minacce tramite algoritmi basati sui comportamenti. Tramite l'analisi del funzionamento di host e applicazioni, consente inoltre di rilevare le anomalie causate da spam, botnet e attacchi zero-day e di ricognizione. Sulla base dei flussi di traffico, è in grado di identificare l'utilizzo non autorizzato delle applicazioni ed evidenziare i segmenti di rete problematici.

Controllo e prevenzione delle infezioni da malware

McAfee Network Threat Behavior Analysis, in sinergia con McAfee Network Security Platform, offre l'emulazione in tempo reale per la funzionalità avanzata di analisi e blocco dei file sospetti. Il motore di emulazione in tempo reale sottopone a scansione i file sospetti per individuare e neutralizzare comportamenti dannosi. Tramite la correlazione avanzata su diversi dispositivi di rete e IPS, inoltre, individua le botnet occulte in grado di eludere le tradizionali difese basate sulle firme digitali e sfrutta McAfee Endpoint Intelligence Agent per rilevare e tenere sotto controllo gli endpoint compromessi che trasmettono traffico dannoso camuffato da traffico legittimo. L'analisi basata sulla reputazione dell'attività degli endpoint, infine, limita l'esfiltrazione dei dati e previene le infezioni da malware.

Operazioni di sicurezza ottimizzate e risparmio garantito

McAfee Network Threat Behavior Analysis offre la visione approfondita e fruibile di cui avete bisogno per gestire in modo efficiente la sicurezza a costi contenuti. L'appliance riduce i tempi di risposta agli eventi e ottimizza le prestazioni di rete, impedendo alle minacce provenienti dalla rete e agli exploit di interrompere le attività aziendali.

Funzionalità aggiuntive

- Sicurezza rafforzata grazie all'integrazione con McAfee Global Threat Intelligence (McAfee GTI).
- Disponibile come appliance virtuale per contenere i costi di implementazione.
- Visibilità e correlazione estese grazie all'integrazione con i software McAfee ePolicy Orchestrator® (McAfee ePO™), McAfee Enterprise Security Manager e McAfee Vulnerability Manager.
- Ordinamento e analisi del traffico di rete semplificati.
- Dashboard con metadati divisi per flusso (ID applicazione, file, URL).
- Opzioni di quarantena complete per un livello di sicurezza superiore.
- Visibilità esterna di host con classificazione dettagliata dei fattori di minaccia.
- Compatibilità con switch e router Cisco (NetFlow v5 e v9) e Juniper (J-Flow v5 e v9).

	NTBA T-600	NTBA T-1200
Specifiche		
Flussi per secondo	Fino a 60.000	Fino a 100.000
Cisco NetFlow	v5 e v9	v5 e v9
Juniper J-Flow	v5 e v9	v5 e v9
Processore	1 x Xeon E5-2658	2 x Xeon E5-2658
Memoria	46 GB	96 GB
Archiviazione utilizzabile	4,4 TB in Raid 10	8,8 TB in Raid 10
Interfacce di rete	4 rame, 10/100/1000	4 rame, 10/100/1000
Ambiente		
Fattore di forma	1U	2U
Larghezza	43,8 cm	43,8 cm
Profondità	70,94 cm	70,78 cm
Altezza	4,32 cm	8,76 cm
Peso massimo	14,96 kg	21,6 kg
Consumo di corrente stimato (worst-case scenario)	402 W	667 W
Alimentatore ridondante	750 W	750 W
Requisiti di raffreddamento (BTU/hr)	1.370	2.280
Temperatura di funzionamento	Da 10 °C a 35 °C con velocità di cambiamento massima non superiore a 10 °C per ora	

Specifiche NTBA virtuale	T-VM	T-100VM	T-200VM
RAM consigliata	16 GB	8 GB	16 GB
CPU consigliate	4	4	4
Flussi per secondo	Fino a 25.000	Fino a 10.000	Fino a 25.000

McAfee
An Intel Company

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

60839ds_ntba_0214_ETMG