McAfee Network Threat Behavior Analysis

Get complete visibility into network behavior and threats

McAfee® Network Threat Behavior Analysis is an integrated component of McAfee Network Security Platform that provides real-time visibility and threat protection of the network infrastructure. By analyzing traffic from switches and routers, McAfee Network Threat Behavior Analysis pinpoints risky behavior in the network and effectively prevents stealthy attacks. It holistically evaluates network-level threats, identifies the overall behavior of each network element, and enables instant abstraction of potential anomaly or attack type—including malware, zero-day attacks, botnets, and worms. McAfee Network Threat Behavior Analysis also houses some of McAfee Network Security Platform's advanced engines, including the real-time emulation engine that identifies malware without signatures.

Key Advantages

Visibility to secure your network

- Monitors and reports unusual network behavior by network traffic analysis.
- Proactive, behavior-based threat detection.
- Effective detection of unknown threats.
- Anomaly detection includes zero-day, spam, botnet, and reconnaissance attacks.

Comprehensive malware protection

- Stop malware with real-time emulation of malicious files.
- Advanced correlation across your network for botnet activity detection.
- Endpoint intelligence and correlation for network flows and events.

Intelligent Visibility for Today's Stealthy Attacks

Your network faces advanced, stealthy attacks that evade traditional detection methods, leaving your network exposed to crippling breaches and downtime. McAfee Network Threat Behavior Analysis intelligently monitors and reports unusual behavior by analyzing network traffic from your switches and routers, so you identify and quickly respond to attacks on your network.

The McAfee Network Threat Behavior Analysis appliance leverages NetFlow and JFlow data to identify threats beyond the typical perimeter of the intrusion prevention system (IPS). It is a fully equipped appliance with quad-core processors, RAID disk array, and gigabit Ethernet connectivity. It also provides offline storage area network (SAN) connectivity. With its distinct flow capacity, it can handle large amounts of network traffic, facilitating quicker traffic analysis.

Unmatched Network Visibility and Insight

McAfee Network Threat Behavior Analysis lets you make informed decisions about the applications and protocols on your network. It monitors and reports unusual network behavior and identifies threats through behavior-based algorithms. By analyzing both host and application behavior, it provides anomaly detection of zero-day attacks, spam, botnets, and reconnaissance attacks. With comprehensive flow analysis, unauthorized application usage is identified and problem network segments are pinpointed.

Control and Prevent Malware Outbreaks

McAfee Network Threat Behavior Analysis, working in conjunction with McAfee Network Security Platform, provides real-time emulation for advanced inspection and blocking of suspicious files. The real-time emulation engine scans suspicious files to detect and block malicious behavior. With advanced correlation across multiple IPS and network devices, McAfee Network Threat Behavior Analysis finds stealthy botnets that evade traditional, signature-based defenses. Working with McAfee Endpoint Intelligence Agent, compromised endpoints transmitting malicious traffic disguised as legitimate network traffic are detected and controlled. Reputation-based analysis of endpoint activity limits data exfiltration and prevents malware outbreaks.

Streamline Security Operations and Save Money

McAfee Network Threat Behavior Analysis provides the actionable insight you need for cost-effective security management. The appliance accelerates incident response time and streamlines network performance while preventing network threats and exploits from interrupting business operations.

Additional Features

- Enhanced security via integration with McAfee Global Threat Intelligence (McAfee GTI).
- Virtual edition for cost effective implementations.
- Expand visibility and correlation with integration of McAfee ePolicy Orchestrator® (McAfee ePO™) software, McAfee Enterprise Security Manager, and McAfee Vulnerability Manager software.
- Effortless sorting and analysis of network traffic.
- Per-flow metadata (App ID, Files, URLs) dashboard.
- Increase security posture with comprehensive quarantine options.
- External host visibility with detailed Host Threat Factor ratings.
- Compatible with Cisco and Juniper switches and routers (NetFlow v5 and v9 and JFlow v5 and v9).

	NTBA T-600	NTBA T-1200
Specifications		
Flows per Second	up to 60,000	up to 100,000
Cisco NetFlow	v5 and v9	v5 and v9
Juniper JFlow	v5 and v9	v5 and v9
Processor	1x Xeon E5-2658	2 x Xeon E5-2658
Memory	46 GB	96 GB
Usable Storage	4.4 TB / Raid 10	8.8 TB / Raid 10
Network Interfaces	x4 Copper 10/100/1000	x4 Copper 10/100/1000
Environment		
Form Factor	1U	2U
Width	17.244 in (438 mm)	17.244 in (438 mm)
Depth	27.93 in (709.37 mm)	27.87 in (707.8 mm)
Height	1.7 in (43.2 mm)	3.45 in (87.6 mm)
Maximum Weight	14.96 kg (33 lbs)	21.6 kg (47.65 lbs)
Estimated Inlet Power Utilization (Worst-Case Scenario)	402W	667W
Redundant Power Supply	750W	750W
System Cooling Requirements (BTU/Hr)	1370 BTU/Hr	2280 BTU/Hr
Operating Temperature	+10°C to +35°C with the maximum rate of change not to exceed10°C per hour	

Virtual NTBA Specifications	T-VM	T-100VM	T-200VM
Recommended RAM	16 GB	8 GB	16 GB
Recommended CPU	4	4	4
Flows per Second	up to 25,000 fps	up to 10,000 fps	up to 25,000 fps

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60839ds_ntba_0214_fnl_ETMG