McAfee Network Threat Behavior Analysis

Real-time visibility and comprehensive threat protection

The McAfee® Network Threat Behavior Analysis (NTBA) virtual appliance is an integrated component of the McAfee® Network Security Platform that provides real-time visibility and threat protection for network infrastructure. By analyzing traffic from switches and routers, McAfee NTBA pinpoints risky behavior in the network and effectively prevents stealthy attacks. It holistically evaluates network-level threats and identifies the overall behavior of each network element, including malware, zero-day attacks, botnets, and worms. NTBA also provides components of the McAfee Network Security Platform advanced engines, including the real-time emulation engine that identifies malware without signatures.

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. NTBA intelligently monitors and reports unusual behavior by analyzing network traffic from your switches and routers, so you can quickly identify and respond to attacks on your network.

The NTBA virtual appliance leverages NetFlow and JFlow data to identify threats beyond the typical perimeter of the intrusion prevention system (IPS). With its distinct flow capacity, it can handle large amounts of network traffic, facilitating faster traffic analysis.

Comprehensive Insight Simplifies Management

NTBA 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.

Key Advantages

- Monitors and reports unusual network behavior
- Protects against known and unknown threats
- Anomaly detection includes zero-day, botnet, spam, and reconnaissance attacks
- Endpoint intelligence and correlation for network flows and events
- Flexible virtual appliance deployment options
- Integrates with the McAfee solution portfolio

Connect With Us

Control and Prevent Malicious 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, NTBA 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.

Streamlined Security and Optimized Operations

NTBA provides the actionable insight you need for cost-effective security management. It 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)
- Expanded 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
- Improve 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)

Learn More

- **Securing Your Amazon Web Services Virtual Networks**
- **Securing Your Microsoft Azure Virtual Networks**

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

High Performance NTBA Virtual Appliance Configurations	T-200VM			
Recommended RAM	16 GB (Default)	32 GB	48 GB	96 GB
Recommended CPU	4 (Default)	8	16	32
Flows per Second	Up to 60,000 fps	Up to 70,000 fps	Up to 80,000 fps	Up to 95,000 fps

McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at mcafee.com. No network can be absolutely secure.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com