

# McAfee Network Threat Behavior Analysis

Get complete visibility into network behavior and threats

McAfee® Network Threat Behavior Analysis provides real-time visibility of the network infrastructure. It leverages Cisco network flow data to identify and characterize threats beyond the perimeter of the intrusion prevention system (IPS). By analyzing traffic from Cisco switches and routers, McAfee Network Threat Behavior Analysis can pinpoint risky behavior to specific points in the network and effectively prevent internal and external threats. McAfee Network Threat Behavior Analysis rapidly drills down into complex, multivector attacks and blended threats. 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 distributed denial of service (DDoS), botnets, or worms.

The McAfee Network Threat Behavior Analysis appliance is fully equipped 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.

McAfee Network Threat Behavior Analysis seamlessly integrates with the McAfee Network Security Platform IPS. It facilitates the common management of McAfee Network Threat Behavior Analysis, McAfee Network Access Control (McAfee NAC), and IPS sensors through McAfee Network Security Manager.

McAfee Network Threat Behavior Analysis enforces stricter compliance by providing visibility to events such as unauthorized application usage and user behavior. It verifies key PCI DSS requirements and significantly enhances “audit confidence.”

It also correlates threat information across the network under the common umbrella of McAfee Network Security Manager and McAfee ePolicy Orchestrator® (McAfee ePO™) software. McAfee Network Threat Behavior Analysis facilitates the maintenance of a comprehensive and efficient network security infrastructure while maintaining sensitivity to cost and human effort.

## Key Benefits

### Minimize IT and business risk

- Proactive, behavior-based threat detection
- Effective detection of unknown threats
- Monitors and reports unusual network behavior by network traffic analysis
- Detects attacks to help avoid network penetration
- Identifies and responds to unauthorized application usage quickly
- Helps ensure regulatory compliance through integration with McAfee Network Security Platform, McAfee ePO, and McAfee Vulnerability Manager

### Maximize coverage and value

- Provides cost-effective, network-wide visibility
- Effortless sorting and analysis of network traffic
- Prevents manual diagnosing of network-related traffic problems
- Pinpoints problem segments
- Anomaly detection includes zero-day, spam, botnet, and reconnaissance attacks

### Enhance competitive advantage

- Provides an additional layer of security
- Prevents network threats and exploits from interrupting business operations

- Performs analysis tasks quickly and efficiently
- Delivers enterprise-level performance and ensures reliability
- Simplifies operations concerned with threat and signature management
- Accelerates network performance, scalability, and flexibility
- Empowers real-time security decisions

**Key Features**

**Fully equipped for high performance**

- Each McAfee Network Threat Behavior Analysis appliance incorporates:
  - » Quad-core processors
  - » RAID disk array
  - » Gigabit Ethernet connectivity
  - » Offline SAN storage
  - » Distinct flow capacity
- Addresses today's evolving security and network needs
- Provides affordable and reliable network-class performance

**Unmatched network visibility and insight**

- Enables cost-effective, network-wide visibility by collecting traffic from the entire network

through a single McAfee Network Threat Behavior Analysis sensor

- Monitors and reports unusual network behavior through traffic analysis
- Identifies threats through behavior-based algorithms
- De-duplicates NetFlows
- Analyzes both host and application behavior
- Inspects networks for worm, botnet, or spam-associated behavior
- Probes against zero-day threats and reconnaissance attacks

**Easy integration and policy enforcement**

- Integrates with McAfee Network Security Platform IPS to correlate any unusual network behavior caused by network intrusions
- Integrates seamlessly with McAfee ePO software and McAfee Vulnerability Manager software
- Compatible with Cisco's switches/routers (NetFlow v5 or v9)
- Facilitates common management of McAfee Network Threat Behavior Analysis, McAfee Network Access Control, and IPS sensors through the McAfee Network Security Manager
- Promotes internal and regulatory policy enforcement

Specifications	T-200	T-500
Processor	1xE5540	2xE5540
Memory	6x2 GB DDR3 1333 MHz	6x2 GB and 6x1 GB DDR3 1333 MHz
Hard Drive	2x73 GB and 4x300 GB 2.5" serial attached SCSI hot swappable	2x146 GB and 4x600 GB 2.5" serial attached SCSI hot swappable
NIC	4-port copper	2-port copper and 2-port fiber
Miscellaneous	Redundant power supplies Tool-less sliding rail	Redundant power supplies Tool-less sliding rail
Flows per Second	25,000	50,000
Cisco NetFlow	v5 and v9	v5 and v9

