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—part of the McAfee product offering—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 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. 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

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
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
- 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
- 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 vs NTBA T-1200

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

### Virtual NTBA Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>T-VM</th>
<th>T-100VM</th>
<th>T-200VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended RAM</td>
<td>16 GB</td>
<td>8 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Recommended CPU</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Flows per Second</td>
<td>Up to 25,000 fps</td>
<td>Up to 10,000 fps</td>
<td>Up to 25,000 fps</td>
</tr>
</tbody>
</table>