McAfee Network Threat Response

Zero in on advanced, persistent malware inside your network

McAfee® Network Threat Response specializes in finding that single, all-important needle in a haystack of needles: that persistent and targeted attack that sneaks through and infiltrates your network. McAfee Network Threat Response is a framework of next-generation detection engines specializing in user-side attacks, commonly known as advanced persistent threats (APTs). McAfee Network Threat Response prioritizes and presents only those events that require investigation, cutting analysis time down to minutes. Working with McAfee Global Threat Intelligence™ (McAfee GTI™), McAfee Network Security Platform, and McAfee Firewall Enterprise, analysts can protect against today's deadliest security issue: persistent, targeted attacks.

Key Advantages

Detects advanced zero-day malware
- APTs
- Infected PDFs
- Bots
- Drive-by downloads
- Social engineering
- Unique threats solely targeting your company

Reduce time to respond
- Finds malware automatically
- Expedites analysis of complex threats, prioritizing events for review within minutes, not weeks

Advanced analytics for security teams of all sizes
- Finds threats hidden from other tools
- Captures, files, and records network traffic for further analysis
- Accelerates analysis of network packet recording devices

Flexible deployment options
- Virtual sensors
- Appliances delivering up to 2 Gbps detection
- 10+ Gbps carrier-class platform using SAIC/CloudShield appliances

Ease of deployment
- Installing the McAfee Network Threat Response appliance takes only a few minutes

Reveals What They Don't Want Us to See

A distinguishing characteristic of advanced malware is its ability to evade detection. McAfee Network Threat Response foils these attempts by incorporating a framework of tools to address malicious PDFs, botnets, drive-by-downloads, and social engineering. These tools include heuristic PDF scanners, real-time threat databases, file-type verification, and detection of hidden executables.

McAfee Network Threat Response doesn't just alert to the presence of obfuscation; it decodes the traffic, providing analysts with visibility into the attack that is not possible with any other existing tools.

Finds the Smoking Gun

Want to find the bad guy? Look for the one holding the smoking gun. For targeted attacks, that's shellcode.

Shellcode is the set of instructions used by malware to infect and control a device. McAfee Network Threat Response uses patent-pending heuristics to detect the presence of shellcode, without requiring prior knowledge of an ever-changing attack payload.

Assembles Puzzle Pieces Together

Shellcode sneaks into the network a piece at a time, lying in wait to execute its code and expand its attack. McAfee Network Threat Response has the unique ability to uncover these slow moving, persistent attacks, identifying and accumulating portions of attacks that trickle in over time. Nothing else gives you the ability to piece together threat puzzles that steal into your network at a snail's pace.

Shellcode: Before and After

Before

After

http://w.hack.info/data_theft.exe

Cuts Analysis Time Down to Minutes

Network forensic capture solutions give analysts the ability to replay historical traffic to determine both the root cause of and the exposure resulting from a malware event. McAfee Network Threat Response accelerates this analysis via its PCAP import capabilities. As the data is replayed through the McAfee Network Threat Response analysis engines, hidden traffic is decoded and key indicators are highlighted. As a result, an analyst has confirmed anchor points from which to start an investigation—shaving days off of analysis time.

Maximizes Security Staff Effectiveness

Conventional security devices generate multitudes of events a day, only a small percentage of which are indicators of targeted attack activity. McAfee Network Threat Response precisely identifies targeted attacks and allows analysts to fully characterize actionable events within minutes. The power of McAfee Network Threat Response makes every analyst as effective as a team of 20 malware researchers.

Uses Global Intelligence to Provide Local Security

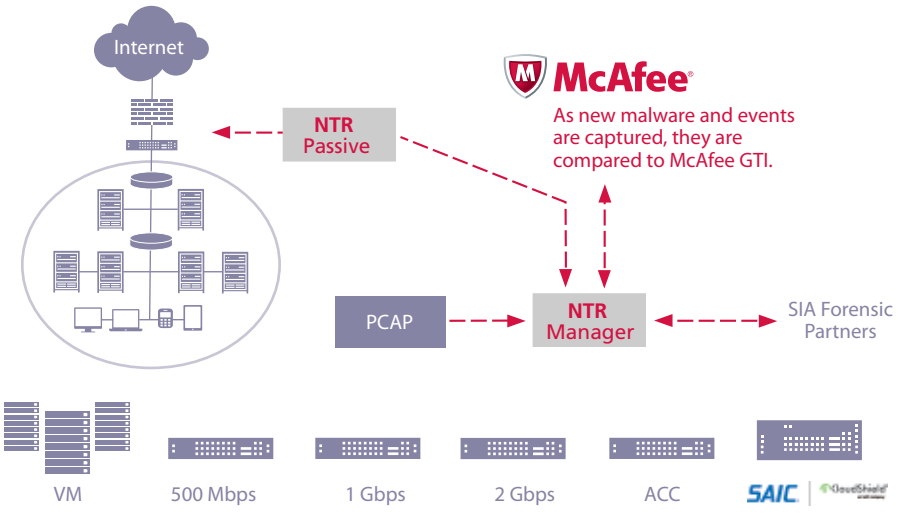
McAfee GTI gathers knowledge from hundreds of millions of devices around the world. Extending beyond just botnet command and control (C&C) detection, McAfee GTI identifies malicious malware source servers used during the initial infection stage. Tapping into our vast, worldwide reputation data banks permits McAfee Network Threat Response to detect communication with known bad actors anywhere on the globe, helping to quickly zero in on potential threats.

Shuts Down All Aspects of APTs

McAfee Network Threat Response is the industry's premier technology to defeat APTs in your network. This threat exposure and forensic framework performs advanced malware detection, out-of-band traffic inspection, and identifies new, unknown attacks that evade all other security technologies. It discovers APTs, bots, Trojans, scripts, and shellcode, capturing their payloads and performing deep analysis to provide a full understanding of their points of origin, infection vectors, and targeted vulnerabilities. McAfee Network Threat Response decodes encoded payloads and reassembled segmented attacks that have been deliberately concealed.

With this precise understanding of the full scope of the threat (from initial infiltration to data-stealing exfiltration), you can shut down all aspects of attacks. In addition, this knowledge gives you the insights to create a comprehensive protection strategy, preventing future threats that might endanger your enterprise.

McAfee Network Threat Response leverages an extensible research framework that advances as attack technology evolves. Its design is centered around getting the most advanced solutions working for you, saving time and scaling to your network.



McAfee Network Threat Response Hardware Specifications

Model Number	A50VM	A50	A100	A200	ACC
Role	Sensor Virtual Machine Appliance	Sensor Appliance	Sensor Appliance	Sensor Appliance	Management Console Appliance
Performance Throughput	200 Mbps	500 Mbps	1 Gbps	2 Gbps	Up to 10 Sensors
Ports					
10/100/1000 Ethernet Sensor Ports	—	4	3	5	—
10/100/1000 Management Ports	—	1	1	1	1
Mode of Operation					
McAfee Network Security Platform M-Series Connectivity	Yes	Yes	Yes	Yes	—
SPAN Port Monitoring	Yes	Yes	Yes	Yes	—
Virtual Machine	Yes	—	—	—	—
Hardware					
Intel Server	—	SR1630HGPRX	SR1625URSAS	SR1625URSAS	SR1625URSAS
CPU Cores	—	4	4	8	8
CPU	—	1	1	2	2
Memory	—	2G	6G	12G	12G
Hard Drives	—	500GB	2x300GB	4x300GB	4x300GB
Operating System	—	RHEL5	RHEL5	RHEL5	RHEL5
High Availability					
Redundant Power	—	NO	YES	YES	YES
RAID Level	—	SATA	RAID1	RAID10	RAID10
Physical					
Form Factor	Virtual Machine	1U	1U	1U	1U
Chassis Dimensions	—	1.70"(H) x 16.93"(W) x 25.51"(D)	1.70"(H) x 16.93"(W) x 26.2" (excluding cable management arm)(D)	1.70"(H) x 16.93"(W) x 26.2" (excluding cable management arm)(D)	1.70"(H) x 16.93"(W) x 26.2" (excluding cable management arm)(D)
Shipping Dimensions	—	23.3"(W) x 41.8"(L) x 8.6"(H)	23.3"(W) x 41.8"(L) x 8.6"(H)	23.3"(W) x 41.8"(L) x 8.6"(H)	23.3"(W) x 41.8"(L) x 8.6"(H)
Weight	—	Approximately 43.5 lbs	Approximately 54.5 lbs	Approximately 56 lbs	Approximately 56 lbs
Power Consumption	Up to two 650-W power supply modules				
Power Input	Auto-switching 110-220 VAC				
Operating Temperature	+10°C to +35°C with the maximum rate of change not to exceed 10°C per hour				
Non-Operating Temperature	-40°C to +70°C				

Continued on next page.

McAfee Network Threat Response Hardware Specifications

Non-Operating Humidity	90%, non-condensing at 35°C
Product Safety Compliance	UL60950—CSA 60950 (USA/Canada), EN60950 (Europe), IEC60950 (International), CB Certificate and Report, IEC60950 (report to include all country national deviations), GS Certification (Germany), GOST R 50377-92—Certification (Russia), Belarus Certification (Belarus), Ukraine Certification (Ukraine), CE—Low Voltage Directive 73/23/EEE (Europe), IRAM Certification (Argentina)
Product EMC Compliance—Class A Compliance	FCC/ICES-003—Emissions (USA/Canada) Verification, CISPR 22—Emissions (International), EN55022—Emissions (Europe), EN55024—Immunity (Europe), EN61000-3-2—Harmonics (Europe), EN61000-3-3—Voltage Flicker (Europe), CE—EMC Directive 89/336/EEC (Europe), VCCI Emissions (Japan), AS/NZS 3548 Emissions (Australia/New Zealand), BSMI CNS 13438 Emissions (Taiwan), GOST R 29216-91 Emissions (Russia), GOST R 50628-95 Immunity (Russia), Belarus Certification (Belarus), Ukraine Certification (Ukraine), KCC Certification (EMI) (Korea)

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

31101ds_ntr_1011