

McAfee Network Threat Response

Zero in on advanced persistent malware inside your network

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
- Software can run on your existing hardware
- 10+ Gbps carrier-class platform using SAIC/CloudShield appliances

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.

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.

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.

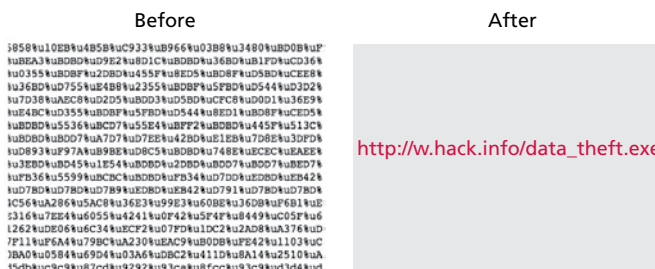


Figure 1. Shellcode: before and after.

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.

To find out more, visit www.mcafee.com/networksecurity.

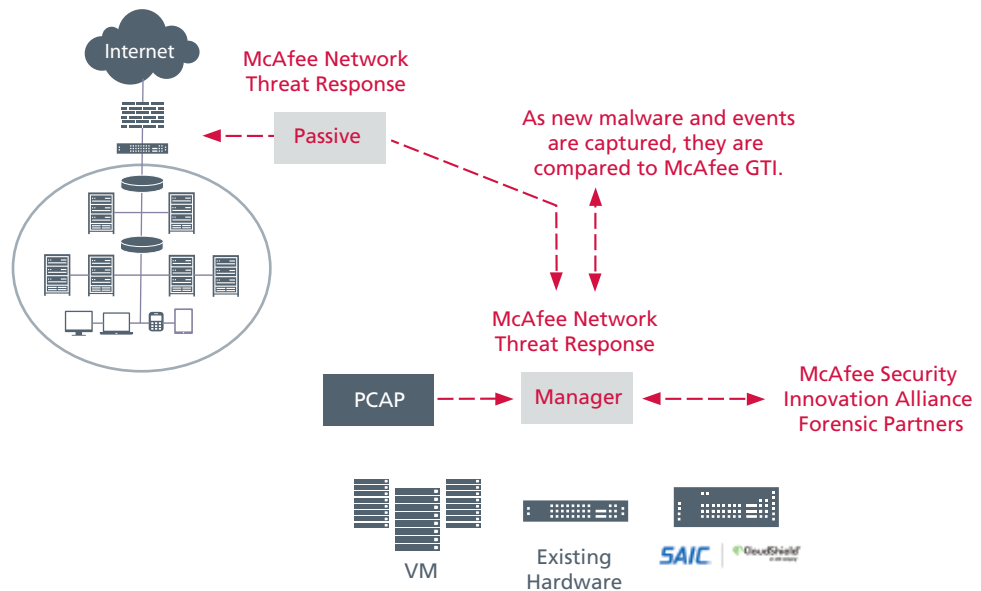


Figure 2. McAfee Network Threat Response typical deployment.

