SOLUTION BRIEF

Reduce the Time-to-Breach Detection. Find Advanced Attackers in Your Networks.

Rapidly detect, analyze, and respond to sophisticated attacks

Deception technology is now combined with the speed, accuracy, and low total cost of ownership of your McAfee® Advanced Threat Defense solution—part of the McAfee product offering. Complementary to your McAfee architecture, DeceptionGrid enables you to reduce the time-to-breach detection while leveraging all of the benefits of your existing solutions. Deception technology finds advanced attackers unseen by other defenses.

McAfee Compatible Solution

- TrapX DeceptionGrid Appliance Version 3.1.4
- TSOC Manager 4.0.3 with McAfee Advanced Threat Defense 3.4.4 or Newer.

The Business Problem

Enterprises are under attack today from an expanding roster of global "bad actors" to include large organized crime syndicates, and, in some cases, even nation states. Using advanced malware and representing advanced persistent threats (APTs), these attackers are often able to find unprotected devices within the penetrated networks and then establish back doors, which allow for the full compromise of the enterprise. Internet-of-things (IoT) devices, medical devices, and many network components protected solely by a firewall now represent easy attack vectors for these sophisticated attackers. Once inside the network (the VLANS), attackers move laterally to find high-value data and property. They move silently through your networks, finding valuable data, diverting funds, stealing intellectual property, and perhaps directly attacking your ability to do business.

A better approach is needed—one that helps organizations find these attackers quickly once they have bypassed other cyberdefense capabilities. It is now essential to reduce the time-to-breach detection from what is often months and, in some cases, years, to a much shorter period of time.

McAfee and TrapX Security Joint Solution and Benefits

DeceptionGrid automates the deployment of a network of camouflaged malware traps that are intermingled with your real information technology (IT) resources. From an attacker's perspective, the traps appear identical to your real IT assets. Once malware has penetrated your enterprise, the attacker moves laterally to find high-value targets. Just one touch of the DeceptionGrid by malware sets off a high-confidence alert and triggers the powerful protection of your McAfee solutions. DeceptionGrid's real-time automation captures and passes injected malware directly to McAfee Advanced Threat Defense.

McAfee Advanced Threat Defense then rapidly and accurately performs a complete analysis of the threat and immediately incorporates threat intelligence into existing policy enforcement processes to block additional instances of the same or similar threat throughout the infrastructure in real time. Together, McAfee Advanced Threat Defense and TrapX enable you to reduce the time-to-breach detection for the most sophisticated and advanced threats. Benefits include:

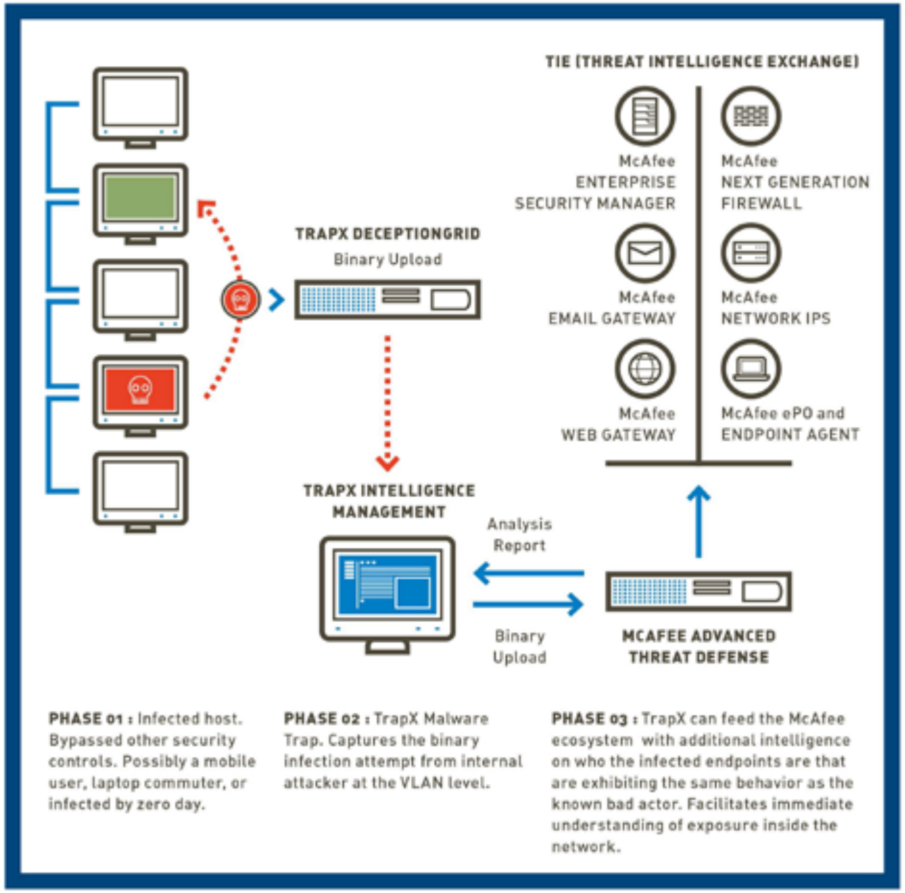
- **Low to no false positives:** DeceptionGrid generates a very small number of highly accurate alerts.
- **Powerful situational awareness:** DeceptionGrid detects the lateral movement of attackers in your VLANs often unseen by other cyber defenses.
- **Automated forensics in real time:** McAfee Advanced Threat Defense provides a complete static and dynamic analysis of malware captured by DeceptionGrid.

About TrapX Security

TrapX Security is a leader in the delivery of deception-based cybersecurity defense. Our solutions rapidly detect, analyze, and defend against new zero-day and APT attacks in real time. DeceptionGrid provides automated, highly actionable insight into malware and malicious activity unseen by other types of cyberdefense. We enable a proactive security posture, fundamentally changing the economics of cyberdefense by shifting the cost to the attacker.

About McAfee Advanced Threat Defense

McAfee Advanced Threat Defense—part of the McAfee product offering—enables organizations to detect advanced targeted attacks and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between McAfee solutions—from network to endpoint—enables instant sharing of threat information across the environment, enhancing protection and investigation.


TIE (THREAT INTELLIGENCE EXCHANGE)
McAfee ENTERPRISE SECURITY MANAGER
McAfee NEXT GENERATION FIREWALL
McAfee EMAIL GATEWAY
McAfee NETWORK IPS
McAfee WEB GATEWAY
McAfee ePO and ENDPOINT AGENT
TRAPX DECEPTIONGRID
Binary Upload
TRAPX INTELLIGENCE MANAGEMENT
Analysis Report
Binary Upload
MCAFEE ADVANCED THREAT DEFENSE

PHASE 01 : Infected host. Bypassed other security controls. Possibly a mobile user, laptop commuter, or infected by zero day.

PHASE 02 : TrapX Malware Trap. Captures the binary infection attempt from internal attacker at the VLAN level.

PHASE 03 : TrapX can feed the McAfee ecosystem with additional intelligence on who the infected endpoints are that are exhibiting the same behavior as the known bad actor. Facilitates immediate understanding of exposure inside the network.

Figure 1. McAfee and TrapX Security Solution.

McAfee
Together is power.

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