PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ INTEGRATION WITH MCAFEE® SOLUTIONS

INTRODUCTION

Attivo Networks® has partnered with McAfee® to detect real-time in-network threats and to automate incident response by enabling the automated quarantine of infected endpoints, redirection of potentially malicious traffic, and threat intelligence sharing with other McAfee partners. The Attivo Networks ThreatDefend™ platform's native integrations with McAfee ePolicy Orchestrator (ePO), Enterprise Security Manager (ESM) SIEM, and Network Security Platform (NSP) allow for an accelerated incident response. The integration in the Data Exchange Layer communication fabric provides a robust and efficient way to share rich forensic information across multiple solutions.

Leveraging these integrations, customers can review alerts and the accompanying attack forensics, assign endpoint policies to automatically block and isolate systems deemed compromised, identify and alert on credential theft and reuse, redirect malicious traffic, and share threat intelligence. Security operations teams can gain time and reduce the resources required for detecting threats, reporting and analysis of attacks, and managing incidents. These integrations improve visibility into in-network threats, enhance policy compliance, and provide additional controls for an active defense.

THE CHALLENGE

The increasing number of advanced threats and damages because of threat actors inside the network has led many organizations to change their overall security posture. The sophistication and high-impact nature of these attacks have compelled security professionals to take a new approach to security, one that provides a balance of prevention and detection security tools and platforms – each designed to play an essential role in safeguarding their business.

As a result, companies are overwhelmed with information and logs that are not readily shared or leveraged between tools, creating silos of information and operational challenges. Manual efforts to collect data from each tool creates complexity and adds to the overall effort and cost of operations. Moving from one tool to another to correlate information for a comprehensive view and collective response to cyber threats can be time-consuming and too often leaves threats unaddressed. Organizations need a new approach, one without false positives but with high-fidelity alerts that allow efficient and timely responses to cyber threats while also leveraging native integrations to share information and initiate response actions automatically.

DECEPTION FOR IN-NETWORK THREAT DETECTION

Organizations are actively turning to deception technology as the preferred security control for early and accurate detection of in-network threats. Some are first-time deception technology adopters, drawn to the accuracy and efficiency of the solution, while others are migrating off homegrown honeypot technology for additional accuracy and operational efficiency. Deception technology works by turning the network into a web of sensors with a maze of misdirection that tricks an attacker into engaging and revealing their presence. In a deception network, the attacker need make only one small engagement mistake to reveal their presence. By being present at the network and endpoint layers, deception technology blankets the network with lures and traps designed to attract and engage an attacker during reconnaissance, lateral movement, while harvesting credentials or when seeking to compromise Active Directory. Deception also addresses alert and log fatigue by only generating an engagement-based alert substantiated with threat and adversary intelligence.

Advanced Distributed deception platforms will also save time and energy by providing automated analysis of each attack, capturing the attacker's valuable Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs); and by providing actionable intelligence of the attack for improved incident response and to better fortify the network.

THE JOINT SOLUTIONS

The ThreatDefend platform is comprised of the Attivo Networks BOTsink® deception servers, ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ for repeatable response playbooks, DecoyDocs for data loss tracking, ThreatDirect for deployment flexibility in micro-segmented, remote, or branch environments, and the Attivo Central Manager (ACM) for enterprise deception and threat intelligence management. Together, these solutions create a comprehensive early detection and continuous threat management defense against information security threats. The BOTsink solution and the ThreatStrike suite are the main integrations with McAfee solutions.

The Attivo Networks BOTsink deception solution improves security in enterprise networks as well as private and public data centers by identifying inside-the-network threats and infected devices in real-time. The Attivo BOTsink solution is based on a deception engagement server that lures attackers to engaging before they can find company production servers. The BOTsink solution uses dynamic application and server level deception techniques to attract and engage attackers so it can collect forensic information to understand the infected endpoint, attacker IP address, and the methods and tools that an attacker is using. Frictionless in its deployment and highly scalable, the BOTsink platform

easily scales to detect threats in the enterprise network and in private and public cloud environments. The BOTsink deception is also designed to detect both reconnaissance and targeted attacks.

The ThreatStrike Suite includes deceptive credentials, lures, and mapped drives for ransomware attacks that bait and lead the attacker to the BOTsink solution engagement server. The engagement server captures the Indicators of Compromise (IOC) and full Techniques, Tactics, and Procedures (TTP) of the attack. Security teams can install the ThreatStrike Suite at endpoints within the BOTsink solution user interface or through integration with McAfee ePO for easy, frictionless deployment. When an attacker attempts usage of these credentials, the BOTsink solution raises a high-fidelity alert, empowering the security operations team to take quick incident response actions.

The integration of the ThreatDefend platform with the various McAfee solutions gives organizations real-time detection of cyberattacks and detailed forensics to proactively address and prioritize critical issues for prompt response, information sharing, and remediation.

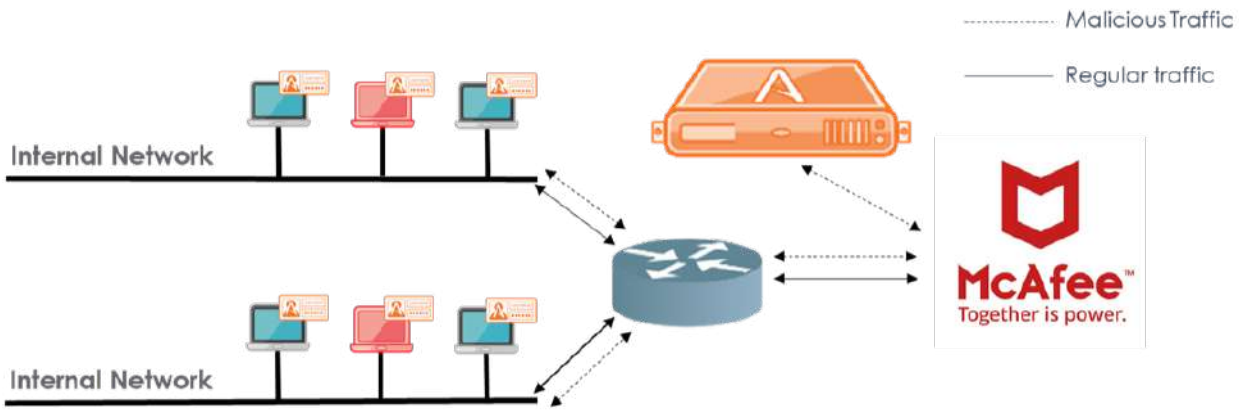
McAfee Enterprise Security Manager (ESM) is a security information and event management (SIEM) solution that delivers actionable intelligence and integrations to prioritize, investigate, and respond to threats. McAfee ESM provides continuous visibility into threats and risk, actionable analysis to guide triage and speed investigations, and orchestration of security remediation. Prioritized alerts surface potential threats before they occur while analyzing data for patterns that may indicate a more significant threat.

McAfee's Network Security Platform (NSP) is a next-generation IPS, built for the accurate detection and prevention of intrusions, DoS, DDoS, malware download, and network misuse. Signature-less intrusion detection technology allows the IPS to identify malicious network traffic and stops never-before-seen attacks for which no signatures exist.

The McAfee Data Exchange Layer (DXL) communication fabric connects and optimizes security actions across multiple vendor products, as well as internally developed and open source solutions. Enterprises gain secure, real-time access to new data and lightweight, instant interactions with other products. Rapid sharing of information and orchestration of tasks shrink the time to detect, contain, and remediate newly identified threats. Applications can now share the timely threat data they generate and work together to take immediate action. Messages can trigger automated responses from McAfee ePolicy Orchestrator to update, clean, quarantine, and more.

THREATDEFEND PLATFORM INTEGRATION WITH MCAFEE EPO

The ThreatDefend platform and McAfee ePolicy Orchestrator are integrated to offer customers a collective defense solution that empowers detection of real-time threats, gathering of attack analysis, manual or automated blocking of attacks and quarantining of endpoints based on suspicious activity. The combined solution also offers a centralized portal that allows easy deployment of the ThreatStrike Suite at endpoints. Together, the solution enables continuous threat management through early detection, analysis, and remediation capabilities.



A vital part of the ThreatDefend platform, the BOTsink solution includes distributed decoy systems based on real operating systems and services for the highest levels of authenticity and attractiveness to an attacker. The solution is dispersed across the network to lure the attacker into engaging with it. Once engaged, the attack continues to play out safely in the BOTsink solution, which in turn identifies the infected endpoints, the attacker IP address, and generates attack signatures it communicates to the ePO platform. The BOTsink solution or the ThreatOps solution will then initiate endpoint policies enforcing the automated blocking and quarantining of the devices, thus preventing the attacker from completing their mission.

The integration of the ThreatDefend platform with the ePO platform allows customers to shorten response time with detailed insight provided by actionable dashboards with advanced queries and reports. Organizations receive an efficient solution for early detection of active attacks and prompt incident response handling of cyberattacks.

THREATDEFEND PLATFORM INTEGRATION WITH MCAFEE ESM

Attivo Networks and McAfee have collaborated to provide continuous threat management using dynamic deceptions for the real-time detection, analysis, event correlation and accelerated response to cyber incidents and ESM. The

BOTsink solution generates deception-based detection alerts it displays in its dashboard, but it can also send these alerts and events to McAfee ESM. Substantiated alerts and detailed attack forensics shared with McAfee ESM enhances visibility and helps prioritize critical events for prompt incident response.

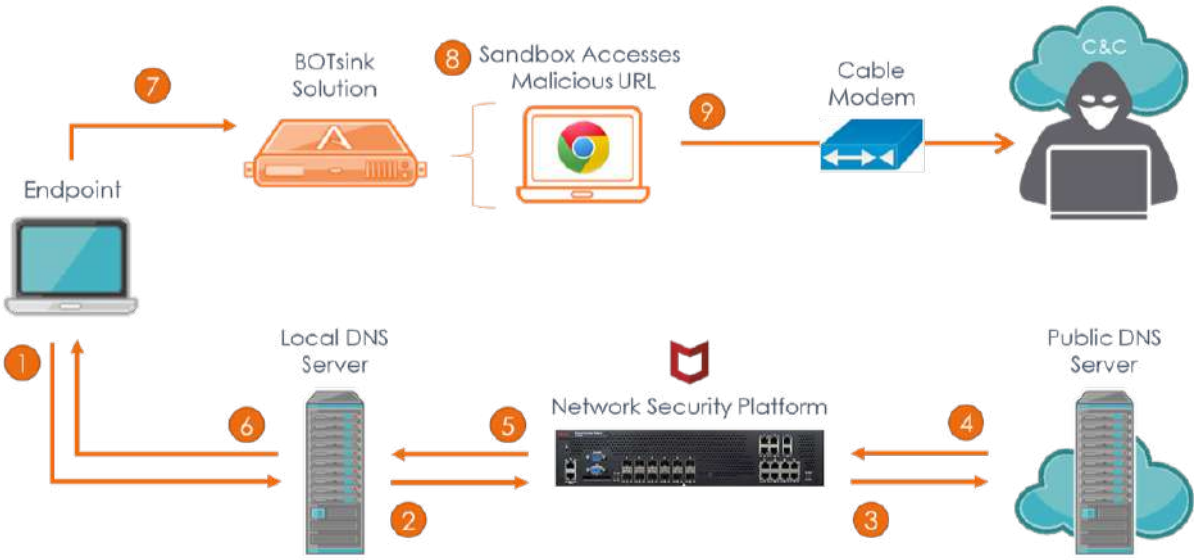
The configuration is merely a matter of specifying the syslog profile and pointing the specified output to McAfee ESM. Once configured, McAfee ESM becomes the single pane of glass for SOC analysts to manage events and alerts. They will have access to any alerts the BOTsink generates when an attacker engages with a decoy. They can then pull the engagement-based forensic evidence from the BOTsink servers for a thorough analysis of attacker activity.

THREATDEFEND PLATFORM INTEGRATION WITH MCAFEE NSP

Botnets are a complex and pervasive form of cyberattack that has been used by attackers, for over a decade, to compromise millions of endpoints to carry out cyberattacks. Botnets have been the weapon-of-choice for almost all the major finance-related cyberattacks in the recent years and their evolution in terms of packaging, delivery, strategy, and distribution continually creates challenges for security administrators worldwide.

The Network Security Platform (NSP) employs multiple mechanisms to detect advanced botnets. One of the mechanisms is to inspect DNS traffic to blacklisted domains. McAfee's security lab regularly releases updated callback detector files, which contain IP addresses, domains, and URLs of malicious (blacklisted) C&C servers. Analysts can automatically or manually download callback detectors into the Network Security Platform. When McAfee NSP detects a blacklisted domain in the DNS traffic, it modifies the DNS packets such that the C&C traffic is sinkholed to the loopback address or a different server of your choice.

The Attivo BOTsink deception server integrates with McAfee NSP, taking the DNS sinkhole concept to the next level, by capturing the full intent of the attack and by providing the forensics required to remediate infected devices. Together, McAfee NSP and Attivo BOTsink deception servers offer a unique method to analyze the TTPs of a targeted attack. This knowledge empowers organizations to quickly identify and remediate infected devices and prevent future cyberattacks.



Together, the McAfee Network Security Platform and Attivo BOTsink deception servers offer a unique method to analyze the tactics, techniques, and procedures of a targeted attack. This knowledge empowers organizations to quickly identify and remediate infected devices and defend against future cyberattacks.

THREATDEFEND INTEGRATION WITH MCAFEE DXL

The McAfee Data Exchange Layer application framework increases integration flexibility and simplicity. Unlike typical integrations, each application connects to the universal DXL communication fabric with just one integration process. Applications can attach and communicate over a universal orchestration layer. One app publishes a message or calls a service; one or more apps consume the message or respond to the service request. The Attivo ThreatDefend platform is a DXL partner and provides deception-based capabilities to other DXL-compliant solutions in the organization Because McAfee ePO handles all DXL messages, the configuration is a matter of specifying the access certificate and private key information, the broker certificate and list information, and then confirming connectivity. Any DXL partner solution can then take advantage of the detections, forensic information, network visibility, and threat intelligence IOCs the ThreatDefend platform provides once configured, accelerating incident response and strengthening the overall security posture.

SUMMARY

The partnership between Attivo Networks and McAfee provides organizations with an effective method of detecting and responding quickly to threats inside the network. The integration of the ThreatDefend solution with the various McAfee solutions allows customers to shorten response time with accurate detection and detailed insight provided by actionable threat intelligence. Organizations receive an efficient solution for early detection of active attacks and accelerate incident responses.

ABOUT ATTIVO NETWORKS

Attivo Networks® is the leader in deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyberattacks. The Attivo ThreatDefend™ Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. Attivo Camouflage dynamic deception techniques and decoys set high-interaction traps to efficiently lure attackers into revealing themselves. Advanced attack analysis and lateral movement tracking are auto-correlated for evidence-based alerts, forensic reporting, and automatic blocking and quarantine of attacks. For more information visit www.attivonetworks.com.

ABOUT MCAFEE

McAfee ePO software is the industry-leading security and compliance management platform. McAfee solutions deliver the highest levels of threat visibility and antimalware protection, including comprehensive system and endpoint protection, network security, cloud security, database security, endpoint detection and response, and data protection. The complete security solutions extend beyond virus software and antimalware protection to server security, SIEM, and intrusion prevention systems (IPS). Backed by McAfee Global Threat Intelligence, the solutions help companies enhance visibility into their security postures, allowing businesses to embrace virtualization, cloud services, and mobile devices while protecting critical assets and sensitive data, and improving incident response. For more information visit www.mcafee.com.