PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH MCAFEE® EPOLICY ORCHESTRATOR®

Attivo Networks® has partnered with McAfee® to provide advanced real-time in-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints. With the joint solution, customers can review alerts and the accompanying attack forensics and assign endpoint policies to automatically block and isolate systems deemed compromised. Security operations teams can gain time and reduce the resources required for detecting threats, reporting and analysis of attacks, and managing incidents. McAfee ePO Orchestrator along with the Attivo ThreatDefend Platform provides enhanced visibility and control into in-network threats, enhances policy compliance, and provides additional controls for continuous threat management.

HIGHLIGHTS

- Actionable High-fidelity Alerts
- Accelerated Incident Response
- Stronger Security Ecosystem
- Cross-platform Information Sharing

THE CHALLENGE

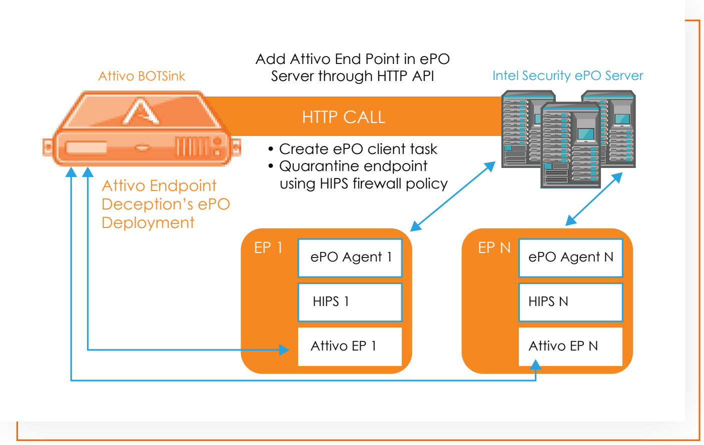
The increasing number of advanced threats and damages as a result of internal threat actors has led many organizations to change their overall security posture. The sophistication and high-impact nature of these attacks have compelled security professionals to take a new approach to security, one that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

As a result, companies are overwhelmed with information and logs that are not easily 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.

THE ATTIVO THREATDEFEND AND MCAFEE EPOLICY ORCHESTRATOR JOINT SOLUTION

The integration of the Attivo ThreatDefend Platform with the McAfee ePO Orchestrator empowers organizations with the realtime detection of cyber-attacks and detailed forensics to proactively prioritize and address critical issues for prompt response and remediation. Offering a single unified console across multi-vendor network systems, McAfee ePO ensures a timely and accurate response to high-fidelity alerts raised for attacks detected by the ThreatDefend solution.

The ThreatStrike Suite includes deceptive credentials, lures, and mapped drives for ransomware attacks that bait and route the attacker to the Attivo BOTsink® solution engagement server. Once in the engagement server, the full Techniques, Tactics and Processes (TTP) of the attack are captured. Installation of the ThreatStrike Suite at endpoints can be completed within the BOTsink solution user interface or through the McAfee ePO Orchestrator 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.


Attivo BOTSink
Add Attivo End Point in ePO Server through HTTP API
Intel Security ePO Server
HTTP CALL
• Create ePO client task
• Quarantine endpoint using HIPS firewall policy
Attivo Endpoint Deception's ePO Deployment
EP 1
ePO Agent 1
HIPS 1
Attivo EP 1
EP N
ePO Agent N
HIPS N
Attivo EP N

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, and insider threats. The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers, decoys, lures, and breadcrumbs, the ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) which together create a comprehensive early detection and active defense against cyber threats.

SUMMARY

The Attivo ThreatDefend Platform plays a critical role in empowering an active defense with in-network threat detection and native integrations to dramatically accelerate incident response. Together, Attivo Networks and McAfee ePO Orchestrator allow customers to shorten response time with detailed insight provided by actionable dashboards with advanced queries and reports. Combined, organizations receive an efficient solution for early detection of active attacks and for prompt incident responses handling of cyberattacks.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT MCAFEE

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

www.mcafee.com