PARTNER BRIEF

McAfee™ Together is power.

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND® INTEGRATION WITH MCAFEE® SOLUTIONS

Attivo Networks® has partnered with McAfee® to detect real-time in-network threats and automate incident response by enabling automated infected endpoints quarantine, potentially malicious traffic redirection, and threat intelligence sharing with other McAfee partners. The Attivo Networks ThreatDefend® platform's native integrations with McAfee ePolicy Orchestrator (ePO) and Enterprise Security Manager (ESM) SIEM accelerate 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, and share threat intelligence. They can assign endpoint policies to automatically block and isolate systems deemed compromised, identify and alert on credential theft and reuse, and redirect malicious connection attempts. Security operations teams gain time to respond and reduce the resources required to detect threats, report and analyze attacks, and manage incidents. These integrations improve visibility into in-network threats, enhance policy compliance, and provide additional controls for active defense.

THE CHALLENGE

The increasing number of advanced attackers and the damage they cause inside the network have 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 security approach that provides a balance of prevention and detection security tools and platforms – each designed to play an essential role in safeguarding their business.

Companies are overwhelmed with information and logs that security controls do not readily share or leverage between each other, creating information silos and operational challenges. Manual efforts to collect data from each control add complexity and add to overall effort and operations cost. 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 automatically leveraging native integrations to share information and initiate response actions.

IN-NETWORK THREAT DETECTION

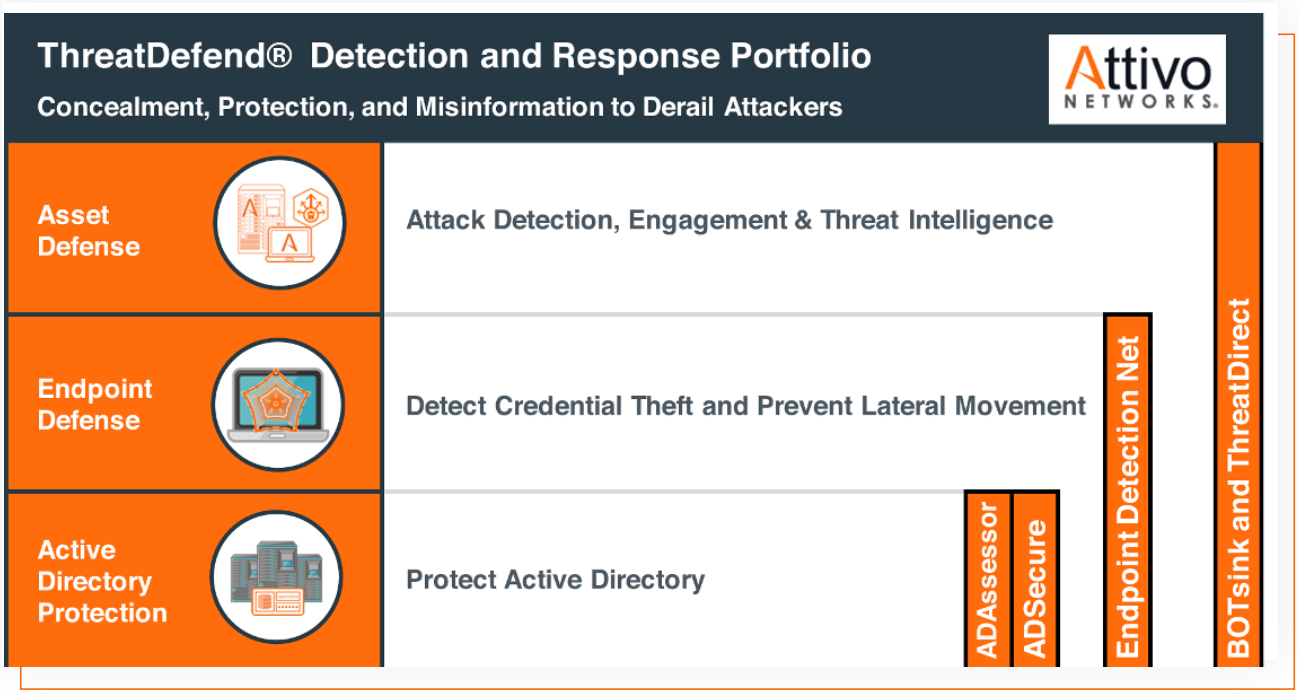
Attackers have proven that they can evade existing security controls to infiltrate a network. To counter these attackers, organizations actively turn to new solutions to detect in-network threats accurately and early in the attack cycle. One such solution involves deception and concealment technologies, which work by denying, detecting, and deflecting attackers as they attempt to break out of the initially infected system that is their beachhead into the network. By being present at the network, endpoint, and active directory layers, deception and concealment technologies add friction into attack activities and

reveal tactics and techniques that would typically evade detection. They also address alert and log fatigue by only generating an engagement-based alert substantiated with threat and adversary intelligence. These technologies 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 attack intelligence to improve incident response and better fortify the network.

THE JOINT SOLUTIONS

The Attivo Networks ThreatDefend® platform provides early and accurate in-network threat detection and defense, regardless of attack method or surface, using deception and concealment technologies. It covers the network, endpoints, and Active Directory to deny, detect, and derail adversaries early in the attack life cycle. The platform creates a threat-informed defense against attackers using its many modular components. The Attivo BOTsink® deception servers provide decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks. The Endpoint Detection Net suite includes the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The ADAssessor solution identifies AD exposures and alerts on attacks targeting it, while the ThreatDirect deception forwarders support remote and segmented networks. The Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

The ThreatDefend platform enhances existing security controls to give the organization internal network visibility, prevention, and detection for attack tactics that evade traditional defenses. With native integration to many security controls, including several McAfee solutions, the platform accelerates incident response and enables efficient information sharing.



The ThreatDefend platform provides innovative detection and prevention solutions for reconnaissance, credential theft, privilege escalation, lateral movement, and data collection solutions to combat today's advanced threats and ransomware attacks. The platform offers scalable protection, detection, data concealment, and access denial solutions for endpoints with comprehensive coverage and attack path visibility for user networks, data centers, clouds, remote worksites, and specialized attack surfaces.

The Endpoint Detection Net (EDN) suite anticipates attacker methods to break out from infected endpoints and ambushes their every move with lures, bait, and misdirections. The suite complements existing endpoint security solutions, such as those offered by McAfee, by hiding and denying access to critical files and data. The solution prevents discovery, credential theft, privilege escalation, data collection, and lateral movement. The EDN suite finds attack paths that adversaries can use to move between systems and closes detection gaps to identify attackers early so that they cannot further infiltrate the network.

The EDN suite includes deceptive credentials, lures, Active Directory protection, and data concealment combined with decoy mapped shares for ransomware attacks that bait and lead the attacker to network decoys while restricting access to sensitive local data. The decoys capture attack Indicators of Compromise (IOC) and Techniques, Tactics, and Procedures (TTP). Security teams can install the EDN suite onto endpoints within the ThreatDefend platform's user interface or through integration with McAfee ePO for easy, frictionless deployment. When attackers attempt to use these credentials, the platform raises a high-fidelity alert, empowering the security operations team to take quick incident response actions.

The Attivo Networks ADSecure solution, available as part of the EDN suite or as a standalone offering, gives organizations Active Directory (AD) security without interfering with production domain controllers. The solution identifies unauthorized AD queries, hiding sensitive objects, and returning fake results to misdirect attackers to decoys for engagement. The mere act of attacker observation triggers an alert on unauthorized activity.

The standalone Attivo Networks ADAssessor solution provides organizations with the visibility they need to secure AD by revealing and remediating exposures and misconfigurations to the domain, users, and devices that leave them vulnerable to attack. It also detects mass changes to AD objects in real-time that indicate an attack is underway, providing an early warning for organizations to derail activities that would usually go undetected. The solution deploys to a standard workstation that belongs to the AD forest and comes with a cloud console for analysis and management.

The BOTsink® server provides a comprehensive network-based defense for on-premises, cloud, remote, and OT environments. Decoy systems and documents that appear identical to production assets provide early and accurate in-network threat detection. Its high-interaction engagement environment safely collects adversary intelligence and automates analysis and incident response. Machine-learning makes customizations, deployment, and operations scalable and straightforward. Over 30 native integrations, including several McAfee solutions, automate isolation, blocking, and threat hunting.

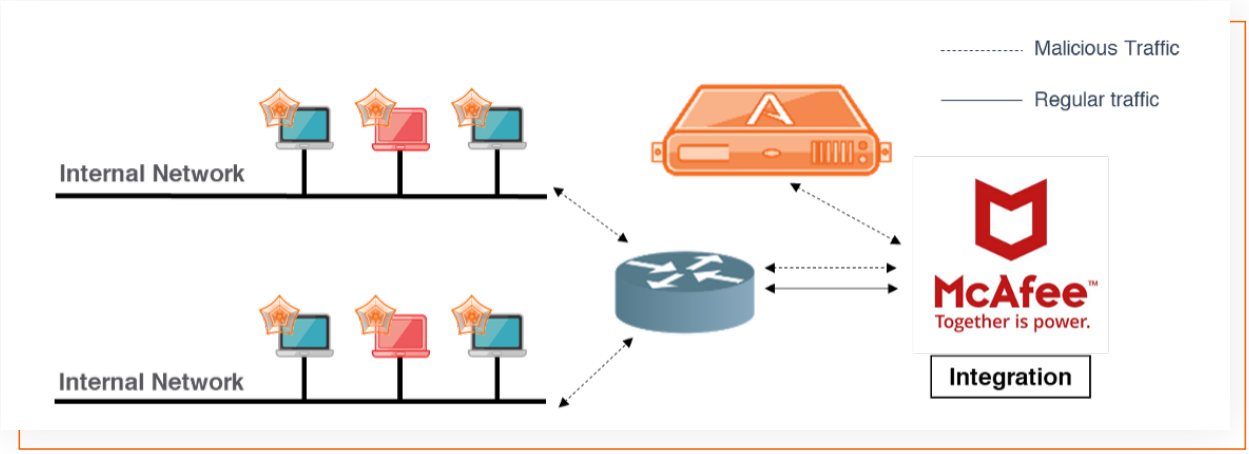
The ThreatDefend platform's integration with the various McAfee solutions gives organizations real-time detection of cyberattacks and detailed forensics to proactively address and prioritize critical issues for prompt incident response, information sharing, and remediation.

McAfee's 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.

The McAfee Data Exchange Layer (DXL) communication fabric connects and optimizes security actions across multiple vendor products and internally developed and open source solutions. Enterprises gain secure, real-time access to new data and lightweight, instant interactions with other products. Rapid information sharing and task orchestration 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 integrate to offer customers a collective defense solution that empowers real-time threat detection, attack analysis, manual or automated attack blocking, and endpoints quarantining based on suspicious activity. The combined solution also offers a centralized portal that allows easy deployment of the EDN 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 server creates the decoy engagement environment based on real operating systems and services for the highest levels of authenticity and attractiveness to an attacker. The solution projects these decoys across the network to engage attackers. Once engaged, the decoys allow the attack to play out safely in the engagement environment, which in turn identifies the infected endpoints and the attacking IP address, generating attack signatures it communicates to the ePO platform. The ThreatDefend platform then initiates endpoint policies enforcing the automated blocking and quarantining of the devices, thus preventing the attackers 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 real-time detection, analysis, event correlation, and accelerated response to cyber incidents. The ThreatDefend platform generates engagement-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 enhance visibility and prioritize critical events for prompt incident response.

McAfee™ COMPATIBLE

The configuration merely specifies the syslog profile and points the specified output to McAfee ESM. Once configured, McAfee ESM becomes the single pane of glass for SOC analysts to manage events and alerts. Once they have access to any alerts the ThreatDefend platform generates when an attacker engages with a decoy, they can then pull the engagement-based forensic evidence from the ThreatDefend platform for a thorough analysis of attacker activity.

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. Once 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 detections and capabilities to other DXL-compliant solutions. Because McAfee ePO handles all DXL messages, the simple configuration involves 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 data, 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 ThreatDefend solution's integration with the various McAfee solutions allows customers to shorten response time with accurate detection and detailed insight from actionable threat intelligence. Organizations receive an efficient solution to detect active attacks early and accelerate incident response.

Free trials for the EDN, ThreatPath, and ADSecure solutions are on the McAfee MVISION Marketplace at https://marketplace.mcafee.com/.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership.

www.attivonetworks.com

ABOUT MCAFEE

McAfee Corp. is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates consumer and business solutions that make our world a safer place.

www.mcafee.com