PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH COUNTERTACK DEFENDS THE ENDPOINT

Attivo Networks® has partnered with CounterTack to provide advanced real-time inside-the-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints. With the joint solution, customers can detect and defend against advanced threats by automating a quarantine from the Attivo Networks ThreatDefend™ Deception and Response Platform based on suspicious activity and severity of the attacks, CounterTack along with Attivo ThreatDefend Platform provides enhanced visibility and control, resulting in higher productivity and efficiencies in security management, ultimately reducing the organizations risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Automated Quarantine and Blocking
- Expedited Incident Response
- Attack Analysis and Forensics

THE CHALLENGE

Cyberattacks are occurring at an unrelenting pace and organizations across all industries are seeking new innovations to close detection gaps. Security professionals are also facing mounting concerns about their ability to quickly detect and stop threats, before damages can be done.

Whether the attacker finds their way in through the use of stolen credentials, zero-day exploitation, a ransomware attacks or simply start as an insider, they will establish a foothold and will move laterally throughout the network until they can complete their mission. Once attackers bypass the existing security prevention mechanisms they can easily move around the network undetected by existing security solutions. To quickly detect and shut down these attacks, a new approach to security is needed. This approach focuses on the threats that are inside the network and does not use typical measures such as looking for known signatures or attack pattern matching. This new method to detect attacks uses deception to deceive attackers into revealing themselves and once engaged, can capture valuable attack forensics that can be used to promptly block the attacker from continuing or completing their mission.

THE ATTIVO THREATDEFEND AND COUNTERTACK JOINT SOLUTION

The integration of the Attivo ThreatDefend Platform with CounterTack empowers organizations with an integrated and active defense platform. Together they provide effective endpoint control through policy and threat prevention, real-time detection of cyber attackers, and the ability to mitigate risks by instantly quarantining the infected endpoints.

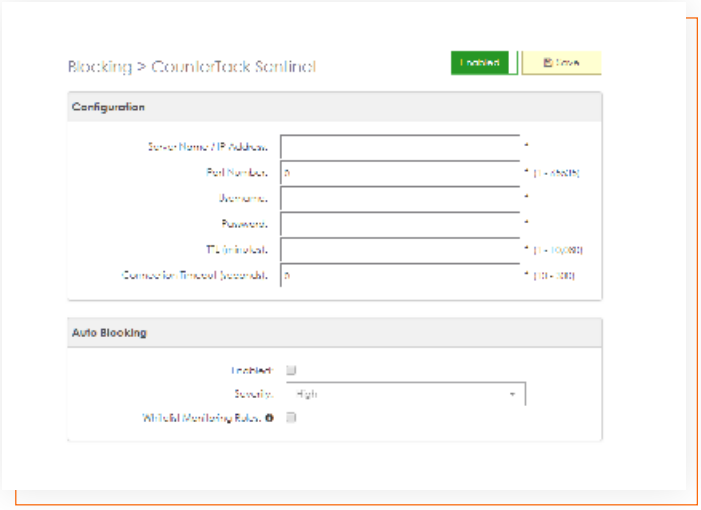
ATTIVO NETWORKS THREATDEFEND PLATFORM

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 Attivo ThreatDefend Deception Platform is 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.

The Attivo BOTsink solution integrates with the CounterTack Sentinel solution to automate blocking and quarantining of infected systems to curtail any lateral movement attempts. As the BOTsink solution detects infected systems, it can be configured to automatically push the infected IP addresses to the CounterTack Sentinel server to be quarantined. Alternatively, infected IP addresses can also be quarantined manually.

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 CounterTack provide joint customers significant improvement in their active defense. By automating the quarantine and blocking of attackers, and automated analysis of suspicious or malicious files, organizations benefit from process and resource efficiencies.



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 COUNTERTACK

CounterTack is the leading provider of Predictive Endpoint Protection, Detection and Response technology for the enterprise. CounterTack's Endpoint Protection Platform (EPP) delivers multi-technique detection, prevention, and response by applying a unique combination of behavioral analysis, memory forensics, machine learning, and reputational techniques to counter the most advanced threats.

www.CounterTack.com