PARTNER BRIEF

# ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH PALO ALTO NETWORKS TO AUTOMATICALLY BLOCK AND QUARANTINE INFECTED ENDPOINTS

A modern day adaptive security approach requires a blend of prevention and detection solutions. Together, these solutions will protect an organization by blocking and quarantining known and unknown threats. With the increase in zero-day, stolen credential, insider, and phishing attacks, threat actors will find a way to bypass even the most sophisticated security prevention systems. Attivo Networks has integrated with Palo Alto Networks to provide advanced real-time inside-the-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints.

## HIGHLIGHTS

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

## THE CHALLENGE

The manual sharing of information between detection and prevention systems can cause delays in isolating an attacker or blocking data from being exfiltrated. This situation can be compounded when an attack happens during non-business hours or in organizations with limited IT resources. Such constraints and challenges hamper an organization's ability to respond quickly and effectively to attacks as they occur and propagate inside the network. An organization that can't effectively respond to fast-moving threats will experience difficulty preventing a compromise from becoming a full-scale breach.

## THE ATTIVO THREATDEFEND AND PALO ALTO NETWORKS JOINT SOLUTION

With the joint solution customers can detect and defend against advanced threats by automating a Palo Alto Networks initiated quarantine from the Attivo ThreatDefend Deception and Response Platform based on suspicious activity and the severity of the attack. Palo Alto Networks along with the Attivo ThreatDefend Platform provides enhanced visibility and control, resulting in higher productivity and efficiencies in security management, ultimately reducing the organization's risk of breaches and data loss.

Deception technology, which is not reliant on signatures or known attack patterns, provides the visibility needed to promptly detect these threats inside the network. This lets an organization easily identify an attacker and pass the information onto an active defense to stop them in their tracks. Additionally, analysis and forensic data allows security teams to identify weaknesses and improve their policies and defenses.

The Attivo ThreatDefend platform seamlessly integrates with the Palo Alto Networks next-generation firewall to provide the needed intelligence to block the infected nodes from gaining Internet access and exfiltrating valuable company data. Once the Attivo ThreatDefend platform identifies an infected node, its IP address is sent to the Palo Alto Networks next-generation firewall through its API for policy enforcement; quarantining the device, stopping any communication with the Command and Control (CNC) and preventing any data exfiltration.

The Attivo ThreatDefend platform will provide a full coverage attack surface to engage the attack during its discovery and lateral infection phase (as the BOT/APT probes and scans the network looking for high-value targets) or during a targeted attack. The Attivo BOTsink decoys are real operating systems based on Windows XP, 7, 8, 10, 2008, 2012 Servers, CentOS, and Ubuntu. In addition, the BOTsink decoys host various applications and protocols including Apache, SNMP, SMTP, File Shares, MySQL, etc. The BOTsink solution supports "golden image" customization to match an organization's network or datacenter environment and allow customers to import their virtual machines to deploy as a decoy.

## 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 alongside Palo Alto Networks empower organizations with an active defense platform that provides real-time detection of attackers and a critical time advantage, which can be used to block an attacker from exfiltrating data or causing other harm. With the automated delivery of attack information, organizations can promptly and efficiently quarantine and remediate infected systems as part of their incident response program.

## 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 PALO ALTO NETWORKS

The Palo Alto Networks® Security Operating Platform prevents successful cyberattacks through intelligent automation. Our platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.
**www.paloaltonetworks.com**