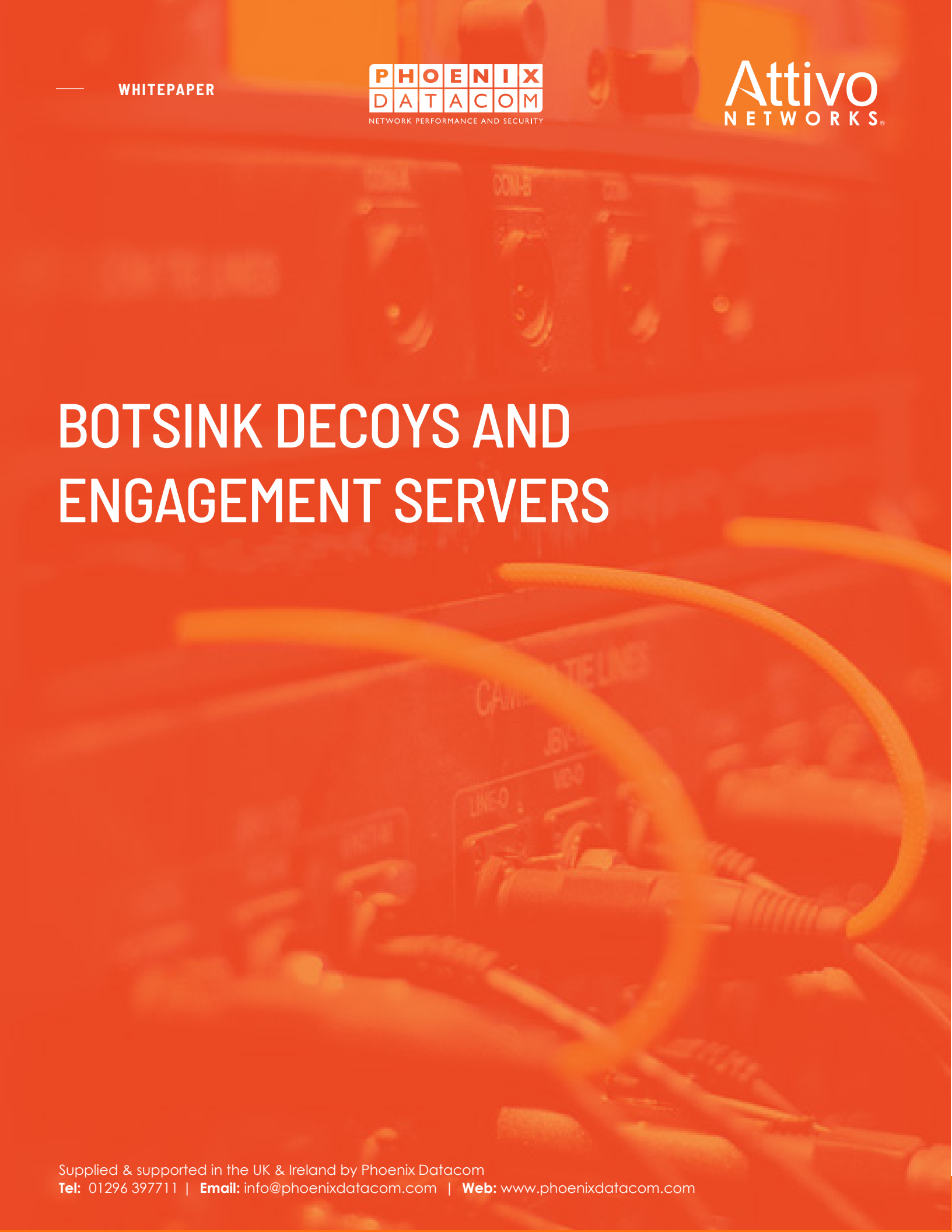
WHITEPAPER

PHOENIX DATACOM
NETWORK PERFORMANCE AND SECURITY

Attivo NETWORKS®

BOTSINK DECOYS AND ENGAGEMENT SERVERS

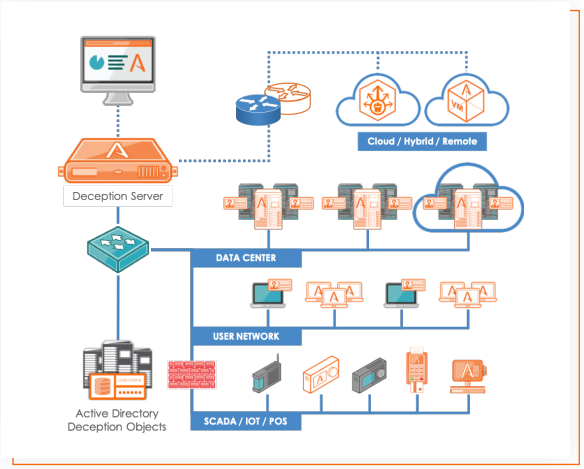


Supplied & supported in the UK & Ireland by Phoenix Datacom
Tel: 01296 397711 | **Email:** info@phoenixdatacom.com | **Web:** www.phoenixdatacom.com

BOTSINK DECOYS AND ENGAGEMENT SERVERS

The Attivo BOTsink® deception solution provides the foundation of the ThreatDefend™ Deception and Response Platform. Using dynamic deception techniques and a matrix of distributed decoy systems, the entire network becomes a trap designed to deceive in-network attackers and their automated tools. As an early warning system for in-network threats, the solution efficiently detects attacker reconnaissance and their lateral movement. Not reliant on known attack patterns or signatures, the BOTsink solution accurately detects threats that have by passed prevention security controls.

The BOTsink deception works by projecting decoys that appear indistinguishable from production assets with the intent to engage and misdirect an attacker. For authenticity, decoys run real operating systems and services and can be customized with production "golden images" to better blend in with other network assets. These decoys are then deployed across all network segments to detect lateral movement. The platform also utilizes dynamic deception at the endpoints, luring and guiding the attacker into the deception "hall of mirrors" environment. Once the attacker engages, the Attack Threat Analysis (ATA) engine analyzes their movement, methods, and actions, generating high-fidelity alerts and visual maps containing attack time-lapsed replay.



These engagement-based alerts include the substantiated attack detail required for incident handling and response and can be used for attack information sharing and forensic reporting. Attack details can be viewed within a threat intelligence dashboard with actionable drill-downs or through a variety of forensic reports, while 3rd party integrations provide automated blocking, quarantine, and threat hunting to accelerate incident response.

IDENTIFYING AND UNDERSTANDING ACTIVE COMPROMISES

Any active compromises, Man-in-the-Middle (MitM) activity, malware, ransomware, APTs, reconnaissance activity, and insider threats that may be in the environment are detected through their interactions with the network decoys or endpoint lures. The BOTsink includes an Attack Threat Analysis engine (ATA) that provides attack correlation and full forensic-based threat reporting for all activity that occurs in the deception environment. The ATA identifies full threat TTPs, including payload drops, registry changes, identified malware propagation methods, and other malicious activity. Detailed forensic products provide significant value in addressing and identifying broader vulnerabilities in the environment that may need addressing.

The Malware Analysis Sandbox is a decoy converted into a dedicated binary analysis VM that analyzes any user-submitted suspicious executables from phishing emails, potential Malware, and other threats to capture lateral movement methods, observe malware behavior, and identify attacker IP addresses, such as Command and Control addresses on the Internet. Because the Attivo architecture is built on full OS environments, the malware can execute completely, providing comprehensive attack analysis. This environment allows exploits to develop without time constraints and can aid in understanding and shutting down sophisticated attacks, such as unrecognized polymorphic malware. The MAS records all threat activity, including payload drops, registry changes, and malware propagation methods. Detailed forensic products provide significant value in addressing and identifying broader vulnerabilities in the environment that may need addressing. Through 3rd party integrations (Firewall, SIEM, NAC, Endpoint), the platform can quickly operationalize with existing security controls to share attack information and remediate vulnerabilities.

CENTRAL MANAGEMENT & DISTRIBUTED LOCATION COVERAGE

If the BOTsink solution (HW or Virtual Appliances) deployed across multiple datacenters, satellite offices, or operational locations, the addition of an Attivo Central Manager (ACM) will provide an efficient way to aggregate deployment management and threat information across distributed production environments. The ACM can currently be deployed physically or virtually on-premises or in Google Cloud, AWS, Azure, or OpenStack.

The BOTsink server can also engage with Darknet traffic through dynamic engagement, to redirect or terminate traffic from a machine that is scanning unused IP addresses.

Models:

• BOTsink 3000 series • BOTsink 5000 series • Attivo Central Manager (ACM)

Customer Benefits:

- Accurate and early in-network threat detection for any threat vector
- Comprehensive solution scalable to the evolving attack surface
- Detailed attack analysis with substantiated alerts and forensic reporting
- Extensive 3rd party integrations for automated quarantine, blocking, and threat hunting and accelerated incident response

Use Cases

- Lateral movement detection
- Attacker in-network reconnaissance
- Stolen credentials (query SIEM)
- Man-in-the-middle attacks
- Detect and slow ransomware attacks
- Phishing threat analysis automation
- Insider, 3rd party, acquisition integration threat visibility
- Sialty environments: IoT, POS, SCADA, telecom, router, SWIFT
- Cloud and datacenter security
- Visibility and streamlined incident response
- Pen Testing validation and CTF performance tracking

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 80 awards for its technology innovation and leadership.

PHOENIX DATACOM
NETWORK PERFORMANCE AND SECURITY

Supplied & supported in the UK & Ireland by **Phoenix Datacom**
Tel: 01296 397711 | **Email:** info@phoenixdatacom.com | **Web:** www.phoenixdatacom.com

ANDS042519