DATA SHEET

Attivo NETWORKS®

ATTIVO NETWORKS® BOTSINK® DECEPTION SERVERS

BOTSINK PRODUCT FAMILY OVERVIEW

The Attivo Networks® BOTsink® server provides the foundation for 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 attackers and their automated tools. As an early warning system for in-network threats, the Attivo Networks BOTsink solution quickly and accurately detects threats that have by bypassed other security controls. The solution efficiently detects attacker reconnaissance and lateral movement without relying on known attack patterns or signatures.

The Attivo deception solution works by projecting decoys that appear indistinguishable from real production assets and are designed 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. Out-of-the-box decoy deception campaigns cover a wide variety of attack surfaces and include configurations for identical appearance to production servers, endpoints, industrial control systems, IoT devices, point-of-sale units, network infrastructure and VOIP systems.

The BOTsink family can also project deception into remote locations, requiring minimal additional resources.

The solution creates a deception "hall of mirrors" for the adversary and when combined with application, data, database, and endpoint deceptions is able to detect attacks from all attack vectors early in the attack cycle. Once an attacker engages, the Attack Threat Analysis (ATA) engine analyzes their movement, methods, and actions, generating high-fidelity alerts and visual maps containing a time-lapsed attack replay. Security operations team will gain the adversary intelligence they need to fully understand the attack and for root cause analysis.

The Attivo Networks solution delivers substantiated engagement-based alerts with the details required for incident handling and response, in a format that's designed for optimal attack information sharing and forensic reporting. Operators can view attack details within the threat intelligence dashboard that presents actionable, detailed, drill-downs, or through a variety of forensic reports. Over 30 native integrations with 3rd party tools provide automated blocking, quarantine to accelerate incident response, and support threat hunting.

[1]BOTsink forms the core of Attivo's ThreatDefend® platform

CUSTOMER BENEFITS AND USE CASES

Deception technology provides a full range of benefits that are unmatched by other security solutions for efficiently and effectively addressing security challenges.

BENEFITS

- Accurate and early in-network threat detection for any threat vector
- Comprehensive solution with scalability for evolving attack surfaces
- Automated deployment and operation through Machine learning
- Detailed attack and root cause analysis with substantiated alerts and forensic reporting
- Accelerated incident response through 3rd party integrations that automate isolation, blocking, and threat hunting

USE CASES

- Detect lateral movement and internal reconnaissance
- Credential theft detection (with – ThreatStrike® Suite)
- Accurate external adversary, insider and supplier threat visibility
- Improve threat response and verify reliability of existing security controls
- Detect malware infection and slow its spread
- Specialty Detections: datacenter, user networks, Cloud, IoT, POS, SCADA, telecom, router, application decoys, SWIFT, database, DecoyDocs

THE BOTSINK FAMILY

The Attivo Networks BOTsink family offers a range of systems to meet the diverse needs of organizations, and are available as physical appliances, virtual appliances, or as a Cloud instance. The BOTsink family can also project deception into remote locations, requiring minimal additional resources. Hardened, FIPS compliant, versions are available.

BOTsink 3000 series

The 3000 series is scaled to support small to medium-sized deployments while offering a full range of deception functionality. The physical unit is a 1RU chassis designed for easy deployment as an appliance.

BOTsink 7000 Series

The 7000 series has twice the resources of the 5000 series for the ultimate level of flexibility. It can easily accommodate more demanding decoy environments for complex organizations, and supports full replacement of any number or all Linux VMs to Windows, and vice versa.

BOTsink 5000 Series

The 5000 series is designed for larger organizations or deployments and supports the full range of configuration options, delivering roughly twice the capacity of the 3000 series. The physical unit is a 1RU chassis built with the standard features expected for a datacenter deployment.

Attivo Central Manager

The Attivo Central Manager (ACM) provides a centralized platform to manage and control a distributed BOTsink deployment. Like all members of the BOTsink family, ACM supports a full range of deployment options. The physical version of ACM starts with the same proven platform as the 5000 series.

BOTSINK PHYSICAL APPLIANCES

MODEL 3000 Series			
Power	1 x 350W AC, Gold certified	Form Factor	1RU
Storage	1 TB	Dimensions	1.7" H x 17.2" W x 14.5" D
CPU	1 x Intel Xeon	Weight	16.5 lbs
Network	4 Network ports + 1 Management port + 1 Proxy port		

MODEL 5000 Series			
Power	2 x 400W AC, Gold certified	Form Factor	1RU
Storage	2 TB RAID	Dimensions	1.7" H x 17.2" W x 19.85" D
CPU	2 x Intel Xeon	Weight	38 lbs
Network	4 Network ports + 1 Management port + 1 Proxy port		

MODEL 7000 Series			
Power	2 x 800W AC, Platinum certified	Form Factor	1RU
Storage	4 TB SSD RAID	Dimensions	1.7" H x 17.2" W x 19.8" D
CPU	2 x Intel Xeon	Weight	30 lbs
Network	4 Network ports + 1 Management port + 1 Proxy port		

ATTIVO CENTRAL MANAGER			
Power	2 x 400W AC or DC, Gold certified	Form Factor	1RU
Storage	4 TB RAID	Dimensions	1.7" H x 17.2" W x 19.8" D
CPU	2 x Intel Xeon	Weight	38 lbs

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.