DATA SHEET

Attivo NETWORKS®

ATTIVO NETWORKS® BOTSINK® 3550

BOTSINK 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 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.

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
- No false positives with minimal resource requirements
- 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
- Prioritize on the basis of numerical score for every alert
- Credential theft detection (with – ThreatStrike™ Suite)
- Accurate external adversary, insider and supplier threat visibility
- Automatically isolate the attacking source
- Receive alerts into your SIEM, email or Phone
- Improve threat response and verify reliability of existing security controls
- Detect malware infection and slow its spread
- Deploy breadcrumbs in an agent-less mode to the endpoints in your network
- Integrate with production Microsoft Active Directory without any trust relationships
- Use backscatter threat intelligence to know who is attacking your internet facing decoys
- Post detection, use built-in orchestration and take specific actions based on event meta data
- Specialty Detections: datacenter, user networks, Cloud, IoT, POS, SCADA, telecom, router, application decoys, SWIFT, database, DecoyDocs
- Create file decoys that raise alerts when opened, copied, modified or deleted
- Spin up and project one-to-one Linux Decoys with individual IP

THE BOTSINK 3550

The 3550 is scaled to support medium-sized deployments offering a full range of deception functionality and additional features. The physical unit is a 1RU chassis designed for easy deployment as an appliance. Available in India only.

MODEL 3550			
Power	2 x 400W AC, Gold certified	Form Factor	1RU
Storage	1 TB	Dimensions	1.7" H x 17.2" W x 19.85" D
CPU	1 x Intel Xeon	Weight	314 lbs

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.