Company Fact Sheet

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for countering threat activity. The Attivo ThreatDefend® Platform provides a customer-proven scalable solution for denying, detecting, and derailing attackers while reducing the attack surface across user networks, data centers, cloud, remote sites, and specialized attack surfaces. The portfolio provides patented innovative defenses at the most critical points of attack, including endpoints, Active Directory, and across the network by preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline and significantly speed incident response.

Founded on the premise that even the best security systems cannot prevent all attacks, Attivo provides the required visibility and substantiated alerts to detect, isolate, and defend against cyber attacks. Unlike prevention systems, Attivo assumes the attacker is inside the network and uses deception and concealment technologies to hide and deny access to sensitive or critical files, folders, and data locally and on Active Directory while deceiving cybercriminals into revealing themselves through interactions with the decoy environment.

The ThreatDefend Platform creates an active defense against attackers using its many modular components. The Attivo BOTsink® deception servers provide decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks. The Endpoint Detection Net suite includes the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The ThreatDirect deception forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

Designed for: Comprehensive Detection | Authenticity | Ease of Use | Accuracy | Intelligence | Automation

Broad Appeal For Threat Detection

Midmarket, Mature Enterprise, Lean Forward Organizations

3 YRS TOP 100	200+	200+	24 of 27	$60M	130+
DELOITTE FAST 500	CUSTOMERS	EMPLOYEES	VERTICALS	SERIES C	AWARDS

Company Mission

Provide defenders with no nonsense detection:
Be predictive. Be prepared. Be proactive.

1. Accurate detection regardless of how or where an attacker attacks
2. Early, scalable detection across all attack surfaces
3. Delivers intelligence on origin, tools, techniques, and attacker motives
4. Arms defender to respond decisively, automates response, builds preemptive defenses

Portfolio Use Cases

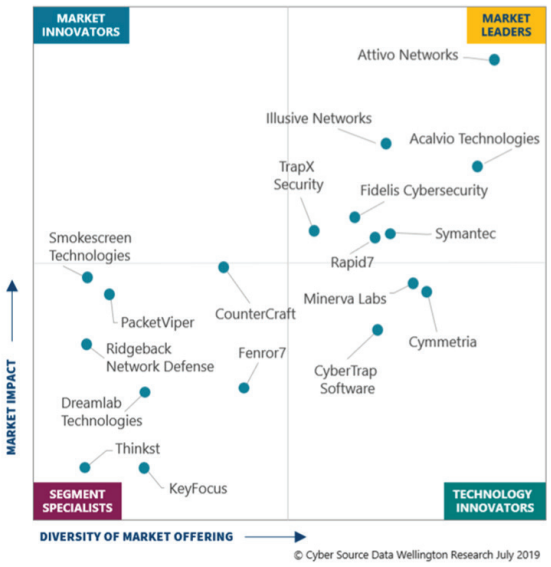
- Reduces Risk: Early Lateral Movement Threat Detection
- Ongoing Assessment of Security Control Reliability
- Active Directory Protection
- Insider and Supplier Policy Violation Detection
- Attack Forensics for Root Cause Analysis
- Analysis, Reporting, and Tracking of Cyber Incidents
- Incident Response, Containment, Eradication
- Return Adversary Mitigation
- Asset and Credential Vulnerability Visibility

Company Fact Sheet

Attivo NETWORKS

Analyst Perspectives

CYBER DECEPTION SYSTEMS MARKET SPOTLIGHT



For the full report, visit https://go.attivonetworks.com/CDS-Market-Segment-Report2019.html

Integration Partners

Automated Incident Response & Operations

ANALYSIS & HUNTING

FIREEYE · FORESCOUT · IBM Radar · LogRhythm · McAfee · MICRO FOCUS · REVERSING LABS · splunk> · TANIUM · ThreatConnect · VirusTotal · WEBROOT an opentext company

ENDPOINT QUARANTINE

aruba a Hewlett Packard Enterprise company · CISCO · CROWDSTRIKE · FIREEYE · FORESCOUT · GoSECURE POWERED BY COUNTERTACK · McAfee · SentinelOne · TANIUM · vmware Carbon Black.

NETWORK BLOCKING

Check Point SOFTWARE TECHNOLOGIES LTD. · CISCO · FORTINET · JUNIPER NETWORKS · paloalto NETWORKS · BROADCOM.

ORCHESTRATION

CORTEX XSOAR · Resilient an IBM Company · splunk> phantom · SWIMLANE

"When defenders couple effective deception with believable artifacts, attackers are forced to spend significant resources on trying to decipher real from fake. With efficient deception, these artifacts can be created with minimal cost to the defense and can be a powerful tool for a number of detection use cases."

- FERNANDO MONTENEGRO, PRINCIPAL ANALYST AT 451 RESEARCH

"In the latest Gartner Threat Deception Platform Comparison, the Attivo Networks ThreatDefend Platform received a score of 'HIGH' In 13 out of 14 categories, the most of any solution evaluated."

– GARTNER, Inc., "SOLUTION COMPARISON FOR SIX THREAT DETECTION PLATFORMS"

"Taken in its totality, ease of setup, ease of management and very low false positives, deception technology creates a layer of detection in the environment that, with very little effort, can analyze topology, explain complex relationships to administrators, suggest recommendations for improving the network and alert only when under attack."

- SIMON GIBSON, ANALYST AT GIGAOM

"Respondents in this research whose organizations were using deception technology and were very familiar with the technology reported dwell times of 5.5 days compared with other studies that report average dwell times of 78 to over 100 days."

– EMA ANALYST DECEPTION SURVEY

Follow us on Twitter @attivonetworks
Facebook | LinkedIn: AttivoNetworks