Company Fact Sheet

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, 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 cyberattacks. Unlike traditional systems that rely on known attack data to stop them, Attivo builds its defense based on the techniques an attacker leverages and then uses their force of attack against them. Attivo maps to the MITRE attack phases of Discovery, Lateral Movement, Privilege Escalation, and Collection. Its portfolio includes identifying the attack paths and exposed credentials an attacker will use to conduct their attack. It also provides comprehensive protection for Active Directory, including AD assessments, so security teams have continuous visibility to vulnerabilities that attackers could exploit to gain privileged access and detect live attacks. Combined, these provide powerful visibility to attacker discovery actions. Next, the ThreatDefend® platform uses concealment technologies to hide and deny access to sensitive or critical files, folders, and data locally and on Active Directory while employing cyber deception to derail attacks and deceive cybercriminals into revealing themselves through interactions with the decoy environment.

At-A-Glance

Dedicated to Innovation and Customer Success

Midmarket, Mature Enterprise, Lean Forward Organizations

3 YRS TOP 100	350+	200+	$60M	150+
DELOITTE FAST 500	CUSTOMERS	EMPLOYEES	SERIES C	AWARDS

Portfolio Use Cases

- Active Directory Assessment & Protection
- Credential Theft, Privilege Escalation & Lateral Movement Detection
- Visibility to Enterprise-wide Identity, Privilege, & Entitlement Exposures
- Malware & Ransomware Derailment
- Data Center, Cloud, & Serverless Security
- Insider & Supplier Policy Violation Detection
- Specialized: IoT, POS, SCADA, Network, & Telecom Detection
- Actionable Alerts & Automated Analysis
- Visibility & Streamlined Incident Response
- Attack Path Risk Assessment & Surface Reduction
- Compliance, Breach Investigation, M&A Diligence
- Ongoing Resiliency & Penetration Testing

Company Mission

1. Protection of identities and entitlement access across the entire enterprise
2. Comprehensive, scalable prevention and detection - from endpoints to the cloud
3. Enhanced security coverage for MITRE ATT&CK™ and Shield
4. Delivers intelligence on origin, tools, techniques, and attacker motives
5. Arms defender to respond decisively, automates response, builds preemptive defenses

Company Fact Sheet

THREATDEFEND PLATFORM

The ThreatDefend Platform creates an active defense against attackers and is modular in design for easy expansion.

The ADAssessor solution identifies Active Directory exposures and alerts on attacks targeting the AD controllers, offloading analysis, alerting, and management to a cloud-based console.

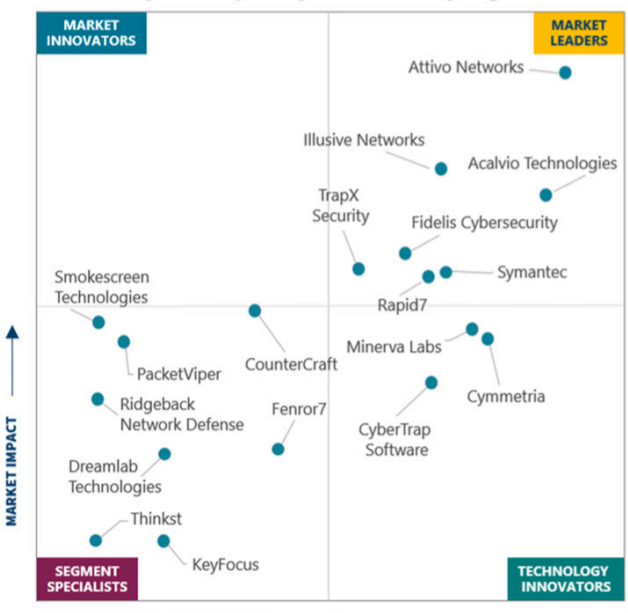
The Endpoint Detection Net suite includes ThreatStrike® for credential theft detection, ThreatPath® for attack path visibility, ADSecure for Active Directory defense (also available as a standalone solution), the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement.

Joining the EDN, ADSecure, and ADAssessor solutions as part of Attivo's identity security offerings, the IDEntitleX solution reduces the attack surface by providing visibility to cloud identity and entitlement exposure. It also includes a central management console that provides end-to-end analysis of identity and entitlement exposures and risks on endpoints, Active Directory (AD) and the cloud.

The Attivo BOTsink® deception servers provide decoys, a high-interaction engagement environment, the Informer dashboard for displaying gathered threat intelligence, and ThreatOps® incident response orchestration playbooks that facilitate automated incident response. It also offers ThreatDirect deception forwarders to support remote and segmented 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

NETWORK BLOCKING

Check Point · CISCO · FORTINET · JUNIPER NETWORKS · paloalto NETWORKS · BROADCOM

ENDPOINT QUARANTINE

aruba · CISCO · CROWDSTRIKE · FIREEYE · FORESCOUT · GoSECURE · McAfee · SentinelOne · TANIUM · vmware Carbon Black.

DISTRIBUTION

CROWDSTRIKE · McAfee · TANIUM

Endpoint management solutions such as SCCM, WMI, Casper, and others

TICKETING

servicenow

CLOUD MONITORING

box · Google Drive · salesforce · Office 365

REDIRECTION

McAfee

ORCHESTRATION

CORTEX XSOAR · IBM Security · splunk> phantom · SWIMLANE

API INTEGRATORS

Digital Defense by HelpSystems · Quantea

Follow us on Twitter @attivonetworks
Facebook | LinkedIn: AttivoNetworks

Company Fact Sheet

WHAT CUSTOMERS AND ANALYSTS ARE SAYING ABOUT US

"fascinating technology", "real competitive advantage" and "far more sophisticated than other tools I've encountered".

- JOHN TOLBERT, KUPPINGERCOLE

"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"

"Attivo helped us Improve our visbility and reduce our time to respond by more than 50%. Attivo's EDN solution helped us detect malicious activity previously undetected. Their ADSecure solution has dramatical improved our AD detection. We are now able to deceive the attackers, keeping them busy while we are able to respond to alerts they generate in a much more agile and efficient way. The visbility and information on the techniques used by adversaries when they access any of the traps is also very helpful in understanding their capabilities."

– GARTNER PEER INSIGHTS

The ADSecure solution is critical for any company that wants to defend and monitor Active Directory solutions. Dont hesitate to include it as part of your implementation."

– GARTNER PEER INSIGHTS