Company Fact Sheet

Attivo Networks®, the leader in identity security and lateral attack movement prevention, specializes in the comprehensive protection of identities, credentials, and high-value assets across endpoints, Active Directory, and cloud infrastructure. The company's ThreatDefend® platform provides customers worldwide with unprecedented visibility to risks, attack surface reduction, and high-fidelity attack detection. By applying its patented innovative defenses at critical points of attack, Attivo solutions close security gaps related to identity-based and lateral movement attack techniques that endpoint protection and identity access management solutions do not address.

The company's mission is to provide a superior defense for countering in-network threat activity with visibility to identity risk and entitlement exposures and stage two attack activities. The ThreatDefend Platform has three core elements that protect against identity compromise, privilege escalation, and lateral movement attack activities, covering Identity Exposure (IEV) Visibility, Identity Detection and Response (IDR), and Attacker Engagement (Deception Technology).

The IEV solutions reduces the enterprise attack surface by finding and categorizing identity risks, entitlement exposures, attack paths to critical assets, and cloud security postures, spanning endpoints, Active Directory, and cloud environments. The IDR solutions provide detection and response for attacks targeting identities, entitlements, and the systems that manage them, including unique credential protection functions that cloak real credentials and plants lures for threat intelligence gathering. Rounding out the portfolio, the platform provides decoy assets at endpoints, in Active Directory, and the cloud to engage attackers, collect forensic information, and develop threat intelligence.

At-A-Glance

Dedicated to Innovation and Customer Success

Midmarket, Mature Enterprise, Lean Forward Organizations

3 YRS TOP 100	450+	200+	$60M	180
DELOITTE FAST 500	CUSTOMERS	EMPLOYEES	SERIES C	AWARDS

Portfolio Capabilities

- Active Directory Assessment & Remediation
- Active Directory Attack Detection
- Credential Theft, Privilege Escalation & Lateral Movement Detection and Prevention
- Protection from Malware and Ransomware
- Data Center, Cloud, & Serverless Security
- Data and Active Directory Cloaking
- Production Credential Cloaking and Protection
- Cloud Security Posture Assessment
- Entitlement Exposure Visibility for endpoint, AD, and the cloud

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 Engage
4. Delivers intelligence on origin, tools, techniques, and attacker motives
5. Arms defender to respond decisively, automates response, builds preemptive defenses

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.

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.

INTEGRATION PARTNERS

Automated Incident Response & Operations

WHAT CUSTOMERS AND ANALYSTS ARE SAYING ABOUT US

"Fascinating technology."

"Real competitive advantage."

"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, "SOLUTION COMPARISON FOR SIX THREAT DETECTION PLATFORMS"

"Attivo helped us Improve our visibility 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 visibility 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