Enterprise Identity Protection and Lateral Movement Detection
for Attack Prevention, Derailment, and Threat Intelligence

The Attivo Networks ThreatDefend platform use modern day innovations to provide a superior protection against sophisticated attackers. Products are modular and can be purchased individually or as a platform for a scalable defense. Comprehensively, the solution protects credentials from theft and prevents and detects identity privilege escalation and attacker lateral movement across endpoints, Active Directory, and cloud infrastructure.

Platform Overview

Solutions for Business Challenges

- **IDENTITY DETECTION & RESPONSE**
  Find exposures and detect malicious activities.

- **CRITICAL INFRASTRUCTURE PROTECTION**
  Detect targeted attacks against ICS/SCADA/IoT infrastructure.

- **CREDENTIAL PROTECTION**
  Conceal and deny access to stop attacker theft and misuse.

- **REMOTE WORKER RISK REDUCTION**
  Protect VPN access points and remote workforce.

- **SECURE CLOUD OPERATIONS**
  Deploy native cloud technology deceptions for threat detection.

- **DERAIL LATERAL MOVEMENT**
  Detect reconnaissance and prevent privilege escalation on-premises and in the cloud.

- **CREATING AN ACTIVE DEFENSE**
  Adaptive, informed protection against any attack vector.

- **RANSOMWARE PROTECTION**
  Delay malware with deception and concealment technologies.
Create an active defense with partner integrations and playbooks for automated deployment, blocking and quarantine. Augment existing controls to accelerate incident response with automation.

Customer Benefits

- Identity Detection & Response
- Visibility to Vulnerabilities & Attack Paths
- Early and High-Fidelity Attack Detection
- Decoy Engagement for Threat Intelligence Collection
- Credential Protection & Attack Misdirection
- Improve Incident Response with Actionable Alerts

Active Defense Partner Ecosystem Native Integrations and Playbooks

INVESTIGATION / ANALYSIS & HUNTING

CONTAIN / NETWORK BLOCKING

CONTAIN / ENDPOINT QUARANTINE

API INTEGRATORS

ORCHESTRATION

DISTRIBUTION

CLOUD MONITORING

TICKETING

REDIRECTION

Endpoint management solutions (ECM, WMI, Casper, etc.)