# THREATDEFEND® PLATFORM

## 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 will prevent and detect identity privilege escalation and attacker lateral movement across endpoints, Active Directory, and cloud infrastructure.

### Platform Overview


## Solutions for Business Challenges

**ACTIVE DIRECTORY PROTECTION**
Find exposures and detect malicious activities.

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

**ENDPOINT PROTECTION**
Detect and deny attacker lateral movement across all attack vectors.

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

**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.

**RANSOMWARE PROTECTION**
Delay malware with deception and concealment technologies.

# MITRE ATT&CK/Kill Chain Attack Disruption


**Detect. Deny. Derail.**

| | | |
|---|---|---|
| Vulnerability Assessment | Misdirection | Cyber Deception |
| Attack Path Visibility | Concealment | Threat Intelligence |

## Customer Benefits

- Enterprise Identity Protection
- Visibility to Vulnerabilities and Attack Paths
- Early and High-Fidelity Attack Detection
- Decoy Engagement for Threat Intelligence Collection
- Concealment & Conditional Access Management
- Improve Incident Response with Actionable Alerts

## Active Defense Partner Ecosystem Native Integrations and Playbooks

**INVESTIGATION / ANALYSIS & HUNTING**

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

**CONTAIN / NETWORK BLOCKING**

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

**API INTEGRATORS** DIGITAL DEFENSE INCORPORATED · Quantea

**CONTAIN / ENDPOINT QUARANTINE**

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

**ORCHESTRATION** CORTEX XSOAR BY PALO ALTO NETWORKS · Resilient an IBM Company · splunk> phantom · SWIMLANE

**DISTRIBUTION** CROWDSTRIKE · McAfee · TANIUM · Endpoint management solutions (ECM, WMI, Casper, etc.)

**CLOUD MONITORING** box · Google Drive · Office 365 · salesforce

**TICKETING** servicenow **REDIRECTION** McAfee

Create an active defense with partner integrations and playbooks for automated deployment, blocking and quarantine. Augment existing controls to accelerate incident response with automation



ANAAG031921
www.attivonetworks.com

Follow us on Twitter @attivonetworks
Facebook | LinkedIn: AttivoNetworks