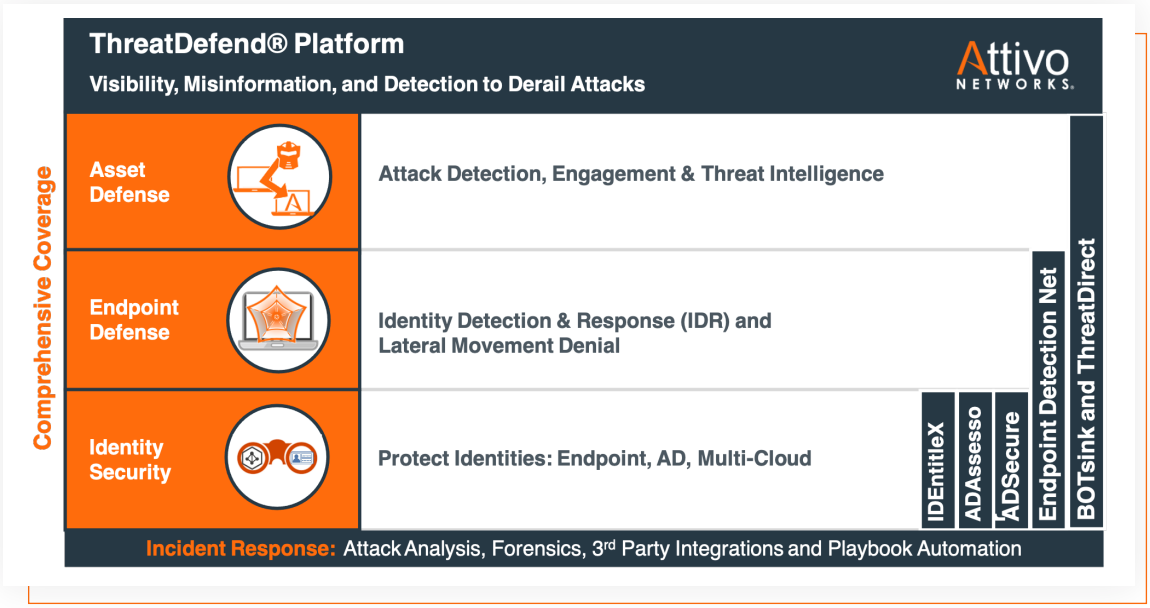
THREATDEFEND® PLATFORM

Enterprise Identity Protection and Lateral Movement Detection For the Insurance Industry

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 Insurance Industry Challenges

IDENTITY DETECTION & RESPONSE
Find exposures and detect malicious activities.

AUDIT & COMPLIANCE
Fulfill compliance with continuous AD pen testing and on-demand assessments

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

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

Insurance Company 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

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 by HelpSystems · Quantea · Siemplify

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 · IBM Security · 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

ANAAG102521
www.attivonetworks.com

Follow us on Twitter @attivonetworks
Facebook | LinkedIn: AttivoNetworks