THREATDEFEND™ DECEPTION AND RESPONSE PLATFORM

WHY CUSTOMERS BUY

- Early in-network threat detection
- Detect malicious actors and insiders
- Attack surface scalability
- Substantiated alerts and forensic reporting
- Easy to deploy and operate
- Attack analysis accelerates response times
- Threat path risk assessment for attack prevention

DECEIVE. EVEN THE MOST SOPHISTICATED ATTACKER.

Lures and decoys misdirect and reveal in-network threats

DECEIVE AND MISDIRECT ATTACKS

- External, insider, and 3rd party threats
- Early reconnaissance/credential theft
- Threat lateral movement
- Not reliant on signatures or pattern matching

BUILT FOR EVOLVING ATTACK SURFACE

- Endpoints, User Network, Data Center, Cloud, IoT, SCADA, POS, SWIFT, Telecom, Router

VISIBILITY, ANALYSIS, FORENSICS

- Substantiated alerts and forensics
- Advanced attack analysis
- Attack path predictions
- Time lapse attack replay

AUTHENTIC DECEPTION: ATTACKERS ARE UNABLE TO TELL REAL FROM DECEPTION

- Dynamic endpoint, server, network, application, Active Directory, and data deceptions
- Real OS, customizable services and applications
- Machine learning authenticity and QuickDeploy
- Agentless endpoint deception incorporates with Active Directory for authenticity
DETECT. ANY TYPE OF ATTACK. ANYWHERE IN THE NETWORK.

Real-time detection of known and unknown attackers

ACCURATE DETECTION
- Ever-changing attack vectors
- Credential, lateral, polymorphic
- Evolving attack surface
- Engagement-based and actionable
- Easy deployment and operations

ACTIVE DEFENSE PARTNERS: NATIVE INTEGRATIONS FOR INFORMATION SHARING AND AUTOMATED RESPONSE

ANALYSIS & HUNTING
- FireEye
- ForeScout
- IBM
- LogRhythm
- McAfee
- Micro Focus
- Reversing Labs
- Splunk
- Tanium
- ThreatConnect
- VirusTotal
- Webroot

NETWORK BLOCKING
- Check Point
- Cisco
- CrowdStrike
- FireEye
- Fortinet
- GoSecure
- Juniper
- Symantec
- paloalto Networks
- VMware Carbon Black

ENDPOINT QUARANTINE
- aruba
- McAfee
- Tanium

DISTRIBUTION
- McAfee
- Tanium
- Endpoint management solutions such as SCOM, WMI, Casper, and others

TICKETING
- servicenow

CLOUD MONITORING
- box
- Google Drive
- Office 365
- McAfee

REDIRECTION
- McAfee

ORCHESTRATION
- Demisto
- Splunk
- Qumulo

API INTEGRATORS
- www.attivonetworks.com
- Facebook | Twitter @attivonetworks

© 2019 Attivo Networks. All rights reserved.