Attivo NETWORKS

Deceive. Detect. Defend.

The Attivo ThreatDefend™ Deception Platform

Effective and Efficient Continuous Threat Management

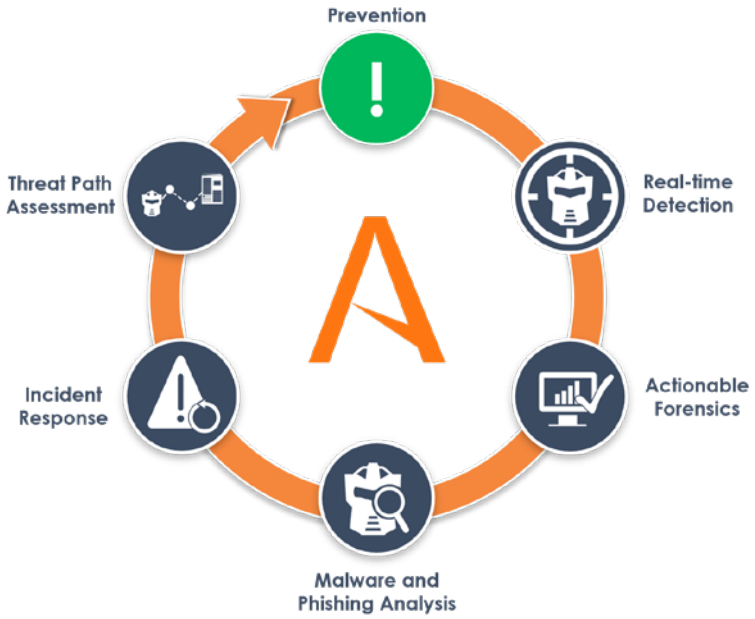
Why Customers Buy the ThreatDefend Platform

- Accurate and early in-network threat detection
- Efficient detection of malicious actors and insiders
- Comprehensive and scalable to all environments
- Substantiated alerts and forensic reporting
- Attack analysis accelerates response times
- Auto-quarantining and blocking of attacks
- Threat path risk assessment for attack prevention

"Attivo is my eyes and ears in my network."

"Attivo makes it so hackers have to be right all of the time."

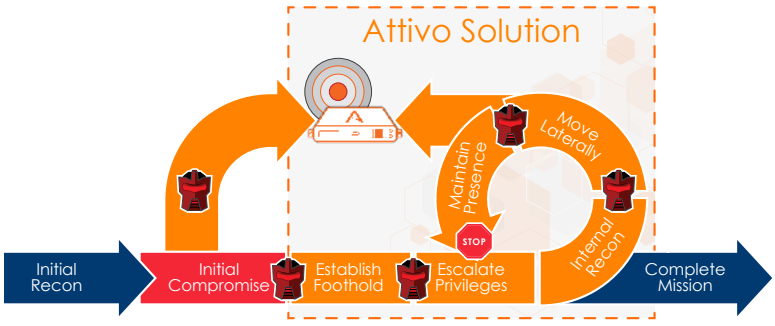
"Attivo lets you know that someone is in your house with their hand in the cookie jar."



Deceive. Even the Most Sophisticated Attacker.

Deception and decoys put the attacker on the defensive

What's Lurking Inside Your Network?



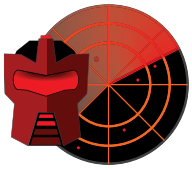
A modern-day adaptive defense requires early and accurate in-network threat detection.

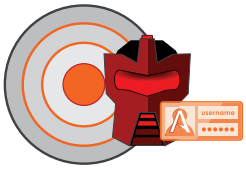
Authentic Deception

- Dynamic end-point, server, network, application, data, and active directory deceptions
- Decoys and lures misdirect and reveal attackers
- Real OS/image, services, and application customization mirror the production environment
- Self-learning dynamic behavioral deception for authenticity and automated deployment
- Agent-less end-point deception for credential theft

Detect. Any Type of Attack. Anywhere in the Network.

Real-time detection of known and unknown attackers


Reconnaissance



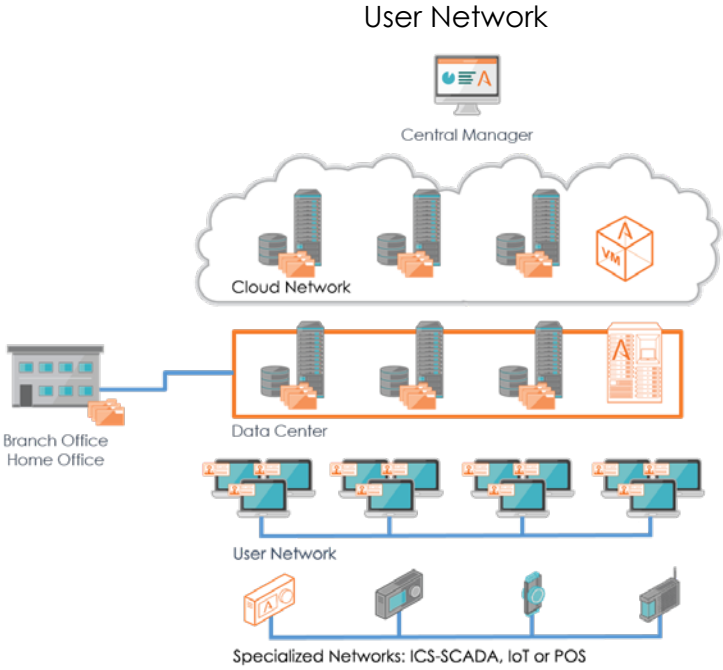
Stolen Credentials


Man-in-the-Middle


Ransomware

Active Directory

Attivo Networks ThreatDefend™ Deception and Response Platform



Early and efficient attack detection

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

Visibility across an evolving attack surface

- User network, data center, cloud, IoT, SCADA, POS, SWIFT, telecom, router
- Attack path predictions
- Time lapse attack replay

Advanced attack analysis capabilities

- Malware and phishing attack analysis
- Substantiated alerts and forensics
- Threat intelligence viewing and attack detail drill down

Defend. Accelerate Incident Response with Automation.

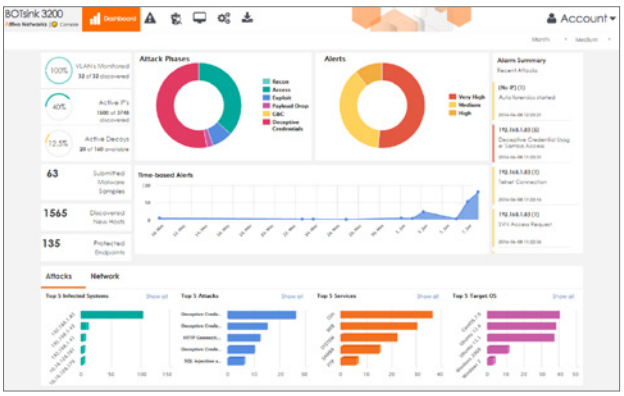
Create an adaptive defense with third party integrations and playbooks for automated deployment, blocking, and quarantine

Preparation (Credential Distribution)
- ForeScout • McAfee • Tanium
- Endpoint management solution such as SCCM, Casper...

Investigation/Analysis and Hunt
- Carbon Black • ForeScout • Micro Focus
- IBM QRadar • Splunk • ThreatConnect • VirusTotal

Contain/End-Point Quarantine
- HP Aruba • Carbon Black • Cisco • CounterTack
- ForeScout • McAfee

Contain/Network Blocking
- Blue Coat • Check Point • Fortinet • Juniper
- Palo Alto Networks



www.attivonetworks.com
Follow us on Twitter @attivonetworks