Attivo NETWORKS

Deceive. Detect. Defend.

The Attivo ThreatMatrix Deception Platform

Effective and Efficient Continuous Threat Management

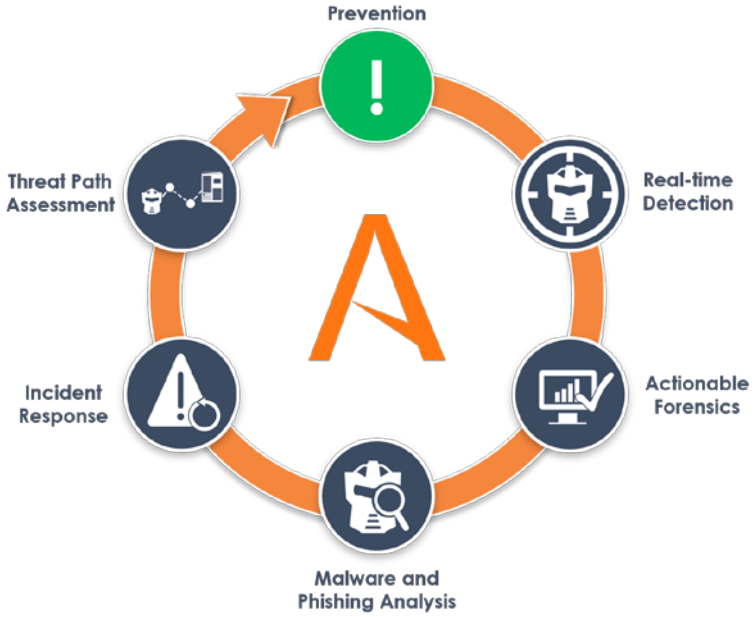
Why Customers Buy the ThreatMatrix Platform

- Accurate and early in-network threat detection
- Efficient detection of insider and 3rd party threats
- 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."

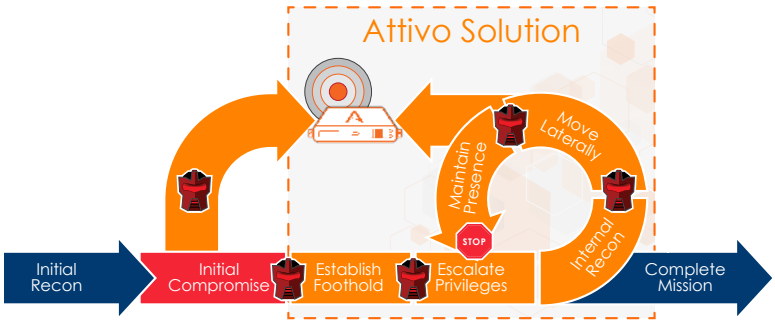
"Attivo lets you know that someone is in your house with their hand in the cookie jar."



Deceive. Even the Most Sophisticated Attacker.

Deception and decoys put the attacker on the defensive

What's Lurking Inside Your Network?



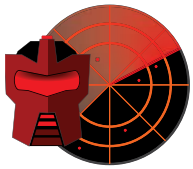
A modern-day adaptive defense requires early and accurate in-network threat detection.

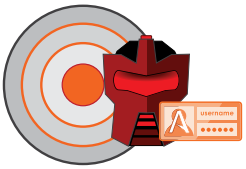
Authentic Deception

- Decoys and lures reveal attackers without relying on signatures
- Real OS/image, services, and application customization mirror the production environment
- Dynamic end-point, server, network, application, database, and active directory directions misdirect attackers
- Self learning dynamic behavioral deception streamlines deployment

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

Real-time detection of known and unknown attackers


Reconnaissance

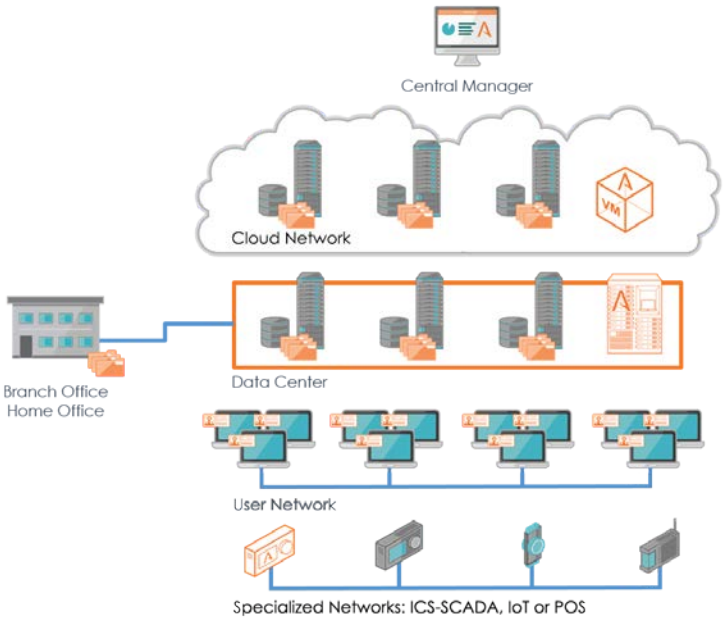

Stolen Credentials


Man-in-the-Middle


Ransomware


Phishing

Attivo Networks ThreatMatrix™ Deception and Response Platform



Early and efficient attack detection

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

Visibility across all networks

- User network, data center, cloud, IoT, SCADA, and POS environments
- Attack path predictions
- Time lapse attack replay

Advanced attack analysis capabilities

- Malware and phishing attack analysis
- Substantiated alerts
- 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

Prevention/Blocking

- BlueCoat
- CarbonBlack
- Checkpoint
- Cisco
- ForeScout
- HP Aruba
- Intel/McAfee
- Juniper
- Palo Alto Networks

SIEM

- HP ArcSight
- IBM Qradar
- McAfee Nitro
- Qradar
- Splunk
- ThreatConnect

Deployment

- Casper
- ForeScout
- Microsoft Active Directory
- McAfee EPO

Reporting

- IOC, PCAP, STIX, CSV
- VirusTotal

www.attivonetworks.com
Follow us on Twitter @attivonetworks