Attivo NETWORKS®

Portfolio Overview

Introduction

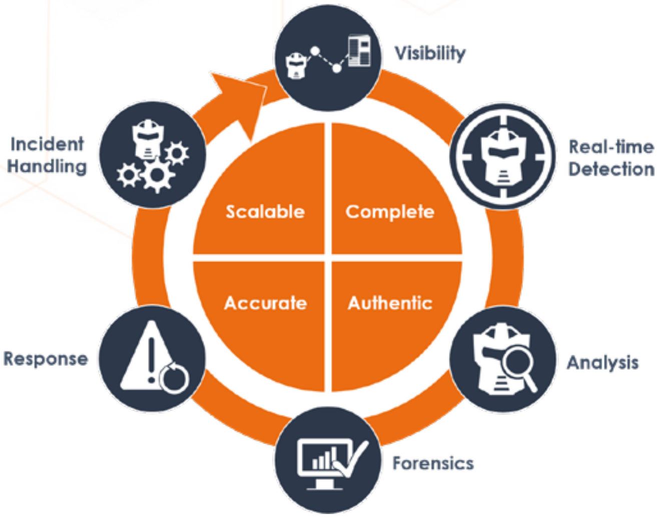
The concept of assumed breached is no longer a novel concept, as demonstrated by the faster than expected shift of investment from prevention to detection technologies in 2016[1]. With over 1,000 breaches occurring in 2016 alone[2] and a relentless amount of new malware, ransomware, and phishing attacks emerging, companies are embracing that a new approach is needed to defend against the today's information security attacker.

Early adopters of detection technology faced challenges with accurate detection since these solutions were either based on known signatures, attempting to pattern match, or looking for anomalous behavior. Unfortunately, the results were unreliable and generated high volumes of logs and false positives. With staffing and time limitations, many of these alerts were simply ignored, due to volume or the inability to correlate the incidents that would reveal an attack in waiting. Attackers leveraged this inefficiency and as such, have been afforded an average of 200+ days before discovery[3] and unfortunately, 4 out of 5 times this discovery came from external parties.[4]

Deception Technology

Deception technology is a unique and modern approach that solves the problems organizations are facing in the current cyber climate. These platforms offer the capability to exercise deception-based detection throughout every layer of the network stack, enabling efficient detection for every threat vector. Utilizing high-interaction decoys and lures, deception solutions effectively deceive attackers into revealing themselves, thereby closing the "detection deficit". With early visibility into threats and the evidence-based alerts required to expedite incident handling, deception solutions are rapidly becoming the solution of choice for proactively uncovering and responding to attackers that have evaded all other security devices. In 2016, analysts actively reported on and began recognizing deception for its efficiency in detecting advanced threats and now recommend deception as a top security infrastructure initiative.

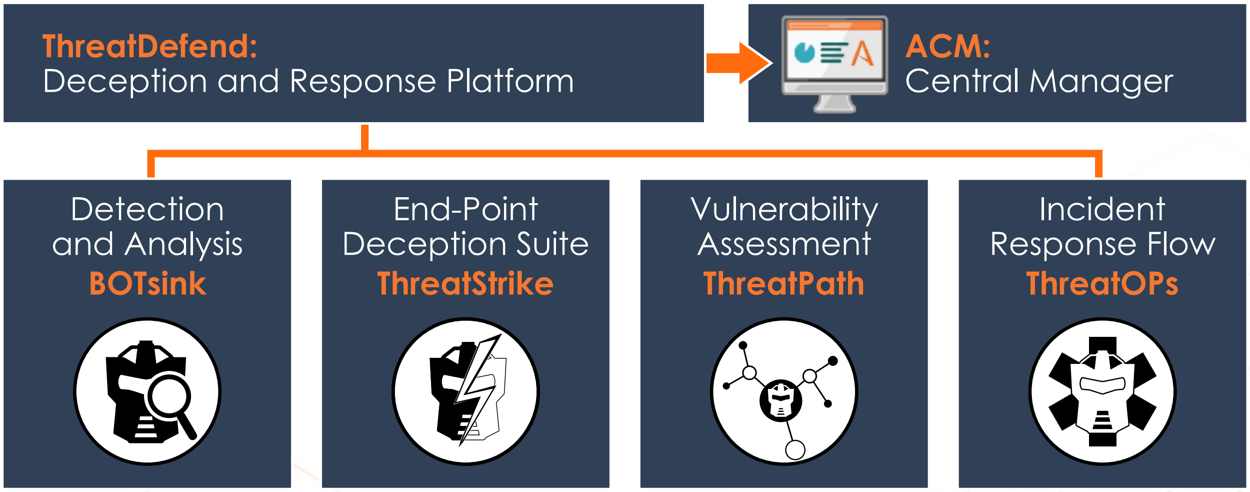
As a result of the effectiveness of deception technology, organizations across all major industries are aggressively adopting deception detection technologies for early visibility into threats, improved incident response, and mitigated risks associated with data and employee credential exfiltration. By 2020, the deception technology market is forecasted to exceed $2 billion.



Attivo ThreatDefend™ Deception and Response Platform
Continuous Threat Management

The Attivo Solution

The ThreatDefend Deception and Response Platform is designed to make the entire network a trap and to force the attacker to have to be right 100% of the time or risk being discovered. The solution combines distributed, high-interaction deception lures and decoys designed to provide early visibility into in-network threats, efficient continuous threat management, and accelerated incident response. The solution is based on six pillars, which include visibility, real-time detection, malware and phishing analysis, forensic reporting, incident handling, and response.


ThreatDefend:
Deception and Response Platform

ACM:
Central Manager

Detection and Analysis
BOTsink

End-Point Deception Suite
ThreatStrike

Vulnerability Assessment
ThreatPath

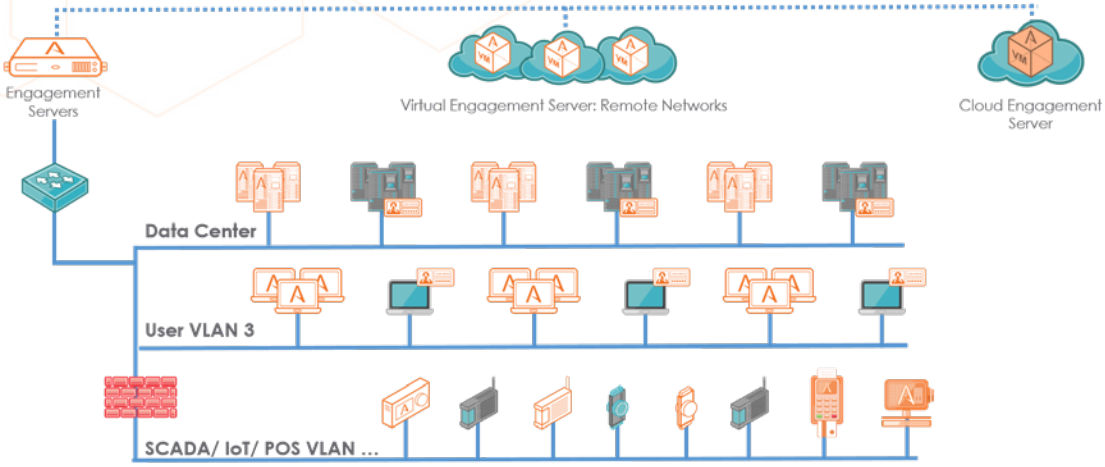
Incident Response Flow
ThreatOPs

Recognized as the industry's most comprehensive deception platform, the solution provides network and endpoint deceptions and is highly effective in detecting threats from all vectors such as advanced, stolen credential, Man-in-the-Middle, ransomware, phishing, and insider threats that are lurking within all types of networks including server, data center, user networks, ROBO, cloud, and specialty environments such as IoT, SCADA, and POS.

The ThreatDefend Deception Platform is comprised of Attivo BOTsink engagement servers, decoys, and deceptions, the ThreatStrike end-point deception suite, ThreatPath for attack path visibility, ThreatOps threat orchestration playbooks, and the Attivo Central Manager (ACM), which together create a comprehensive early detection and continuous threat management defense against cyber threats.

Deception for Detection and Attack Path Visibility

With the ThreatDefend Deception and Response Platform, organizations gain unparalleled visibility into threats inside their network and into attacker lateral movements and tactics. The platform detects advanced threats as they propagate throughout the network by laying strategic decoys and lures to deceive, detect, and defend against attacks as they begin scanning, targeting, and probing network clients, servers, and services for targets.



Distributed Deception & Response Platform
Entire Network is a Trap with Decoys, Deceptions, End-Point Lures

The decoys attract and detect attackers in real-time, actively engaging with them so that their lateral movement and actions can be safely analyzed and evidence-based alerts raised. For authenticity, the decoy systems run real operating systems, full services, and applications, along with the ability to completely customize the environment by importing the organization's golden images and applications. As a result, the platform provides a "hall of mirrors" environment that is baited with lures and traps, while making deception decoys completely indistinguishable from company assets.

As part of the ThreatDefend Deception Platform, the ThreatPath™ solution provides visibility into attack paths that an attacker could traverse, through misconfigured systems, credential exposure or misuse. A topographical illustration of the attacker path provides insight into the avenues that an attacker can use for a straight-forward view of how an attacker can move laterally to advance their attack. This, when paired with the BOTsink attack path replay, can provide unprecedented levels of threat visibility and the information required to close vulnerabilities before they can be leveraged by an attacker.

Deception for Accelerated Incident Response

In addition to detecting attackers inside of the network, the ThreatDefend Deception and Response Platform greatly accelerates the incident response process to address threats quickly and efficiently.

When an attacker engages with a deception asset, they will continue to attempt to conduct reconnaissance to find other systems to attack. With the attack safely contained, the decoys record and alert on the activity while simultaneously responding to the attacker. As the attacker engages with the decoys, the activity is analyzed by the Analysis, Monitoring, and Recording engine, which correlates events, raising alerts on malicious activity.

The platform only alerts on confirmed attacker activities that have interacted with the decoys and is not dependent on signatures or behavioral analysis, eliminating false positives, as well as false negatives. Furthermore, the alerts are substantiated with evidence-based analysis that can be used to automate the blocking of an attacker, the isolation of an infected system, and threat hunting so that a company can completely eradicate the threat from the network. Forensic reports are also created with full IOC, PCAP, and STIX formats to allow easy information sharing and attack recording. Attack forensic analysis includes information on infected IP addresses and C&C addresses, so that the incident can promptly be addressed. The information will also provide the detail to understand what activity in the "Kill Chain" the attacker was executing and additional drill down to information so that SHA1 and forensic artifacts can be researched in other devices.

Additionally, the ThreatOps solution automates incident handling and creates repeatable incident response playbooks. Organizations can customize this threat orchestration to match their environment and policies so that, based on attack scoring and aggregated attack information, organizations can make faster and better informed incident response choices.

Adaptive Defense Partners: Integrations for information sharing and automated response

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

Popular Use Cases

1. Lateral Movement Detection
2. Insider, 3rd Party, Acquisition Integration
3. Stolen Credential
4. Exposed Credential & Attack Path Assessment
5. Man-in-the-Middle
6. Ransomware
7. Phishing
8. Specialized Environments: IOT, POS, SCADA
9. Cloud and Data Center Security
10. Visibility and Streamline Incident Response

Why to Buy

The ThreatDefend Deception and Response Platform offers customers:

- Accurate and early in-network threat detection for any threat vector
- Comprehensive solution scalable to all environments
- Detailed attack analysis through substantiated alerts and forensic reporting
- Accelerated incident response with auto-quarantining and extensive 3rd party integrations
- Threat path risk assessment for attack prevention

> "It's a level of assurance and a feeling of safety that you just don't get with other security product… it's a no brainer"
>
> Chief Information Security Officer, Large HR Consulting Firm

The ThreatDefend Deception and Response Platform
Achieves Common Criteria EAL 2+ Certification

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments.
www.attivonetworks.com

[1] Survey Report: Need for Visibility and Efficiency Drives Rapid Shift to Detection
[2] Verizon's 2016 Data Breach Investigations Report Understand what you're up against.
[3] www.etutorials.org Types of Security Threats
[4] McAfee Labs Threats Report September 2016