DECEPTION SOLUTION OVERVIEW

Attivo NETWORKS

INTRODUCTION

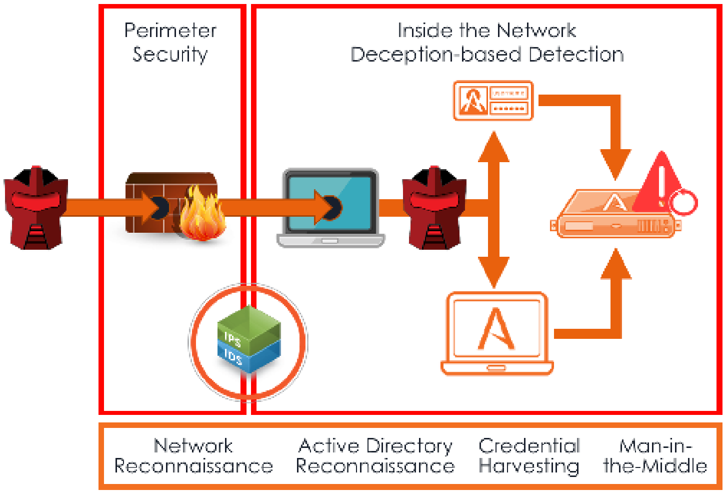
Cyberattacks are occurring at an unrelenting pace as sophisticated attackers continue to find ways to penetrate perimeter defenses. With each breach, security professionals are faced with mounting concerns about their ability to quickly detect and stop threats, before damages can be done. In addition to pressures from compliance expectations, new breach notification laws are being proposed with the promise of significant fines and potential jail time if notification expectations are not met. Organizations across all industries are seeking new innovation to close detection gaps, better understand their attacker and to be able to accurately disclose the details of an attack. This new approach is rooted in the assumption that attackers can and will evade a perimeter defense and organizations must adjust their security posture to one of an active defense, which is not solely based on stopping attacks but instead provides an equal emphasis on detecting and neutralizing attacks in real-time.

DECEPTION TECHNOLOGY

Deception technology provides the innovation required to easily execute an active defense. By deploying deception-based detection throughout the network stack, companies achieve efficient detection for every threat vector and every phase of attack. Utilizing high-interaction decoys and lures, deception solutions deceive attackers into revealing themselves, thereby closing detection gaps on threats that have evaded other security controls.

With early visibility into threats and actionable alerts for incident handling, deception solutions are rapidly becoming the solution of choice for proactively uncovering and responding to internal and external threat actors. Organizations across all major industries are aggressively adopting deception technologies for their easy deployment and maintenance in mitigating risks in data and employee credential exfiltration, ransomware, and/or harm to public safety.

In 2018, analysts continue to recognize deception for its efficiency in detecting advanced threats and Gartner, Inc. has recommended deception for the third year in a row, as a top strategic security priority. By 2019, the deception technology market is forecasted to exceed $3 billion according to FBR Capital Markets.



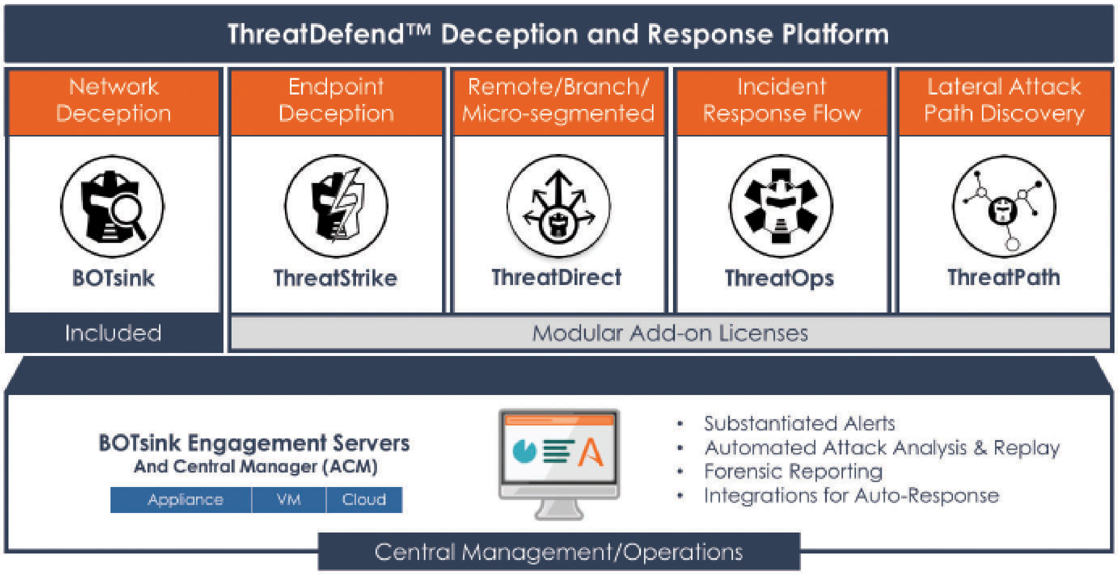
Detection for all Attack Vectors

THE ATTIVO NETWORKS SOLUTION

The ThreatDefend™ Deception and Response Platform is designed to make the entire network a trap and to force the attacker to be right 100% of the time or risk being discovered. The solution combines network and endpoint highinteraction deception lures and decoys designed to provide early visibility into in-network threats, efficient continuous threat management, and accelerated incident response.

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

The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink® engagement servers, decoys, and deceptions, the ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM), which together create a comprehensive early detection and active defense against cyber threats.


ThreatDefend™ Deception and Response Platform
Network Deception
Endpoint Deception
Remote/Branch/ Micro-segmented
Incident Response Flow
Lateral Attack Path Discovery
BOTsink
ThreatStrike
ThreatDirect
ThreatOps
ThreatPath
Included
Modular Add-on Licenses
BOTsink Engagement Servers
And Central Manager (ACM)
Appliance
VM
Cloud
Substantiated Alerts
Automated Attack Analysis & Replay
Forensic Reporting
Integrations for Auto-Response
Central Management/Operations

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 scan network clients, servers, and services for targets and seek to harvest credentials.

The decoys attract and detect attackers in real-time raising evidence-based alerts while, actively engaging with them so that their lateral movement and actions can be safely analyzed. 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. The Attivo Adaptive Deception Campaigns apply machine learning to keep the network and endpoint deceptions fresh and for easy deployment and ongoing maintenance.

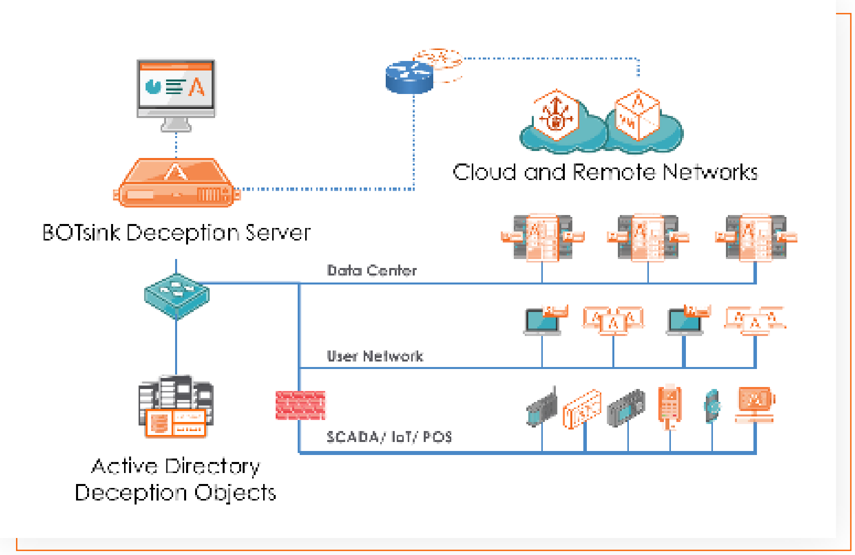
Additionally, to increase deception authenticity, the solution incorporates with Active Directory. By inserting deception into all key areas that attackers target for reconnaissance, the deception deployment appears as part of the production environment in multiple layers, while providing visibility in the event an attacker breaches the AD server.

Endpoint deceptions and mapped shares provide easy and highly effective redirection of attacks seeking to harvest credentials or execute a ransomware attack. Additionally, high interaction deception can be instrumental in slowing a ransomware attack and providing the time advantage to stop the attack before it can cause extensive damage.

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

DECEPTION FOR ACTIVE DEFENSE AND ACCELERATED INCIDENT RESPONSE

In addition to detecting attackers inside the network, the ThreatDefend Platform's actionable alerts, automated analysis, and incident handling automations can dramatically improve incident response. When an attacker engages with a deception asset, through engagement with a decoy or reuse of deception credentials, the engagement server will record and alert on the activity while simultaneously responding to the attacker. The activity is assessed by the Analysis, Monitoring, and Recording engine, which correlates events and raises evidence-based 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. Furthermore, the alerts are substantiated with attack analysis that can be used to automate the blocking of an attacker, to isolate an infected system, and to hunt for other compromises 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 systems and C&C addresses, so that security teams can promptly address the incident. The information also provides the detail to understand what phase in the "Kill Chain" the attacker was in and specifies additional information so that SHA1 and forensic artifacts can be researched in other devices.

Organizations can also use the ThreatOps solution to automate incident handling and create repeatable incident response playbooks. This threat orchestration can be fully customized to match their environment and policies so that organizations can make faster and better-informed incident response choices.

In addition to threat and adversary intelligence, a key function of the ThreatDefend Deception Platform is to provide counterintelligence capabilities. Deception is an offensive counterintelligence function designed to disrupt the attacker's ability to collect accurate information. It also provides defensive counterintelligence functions as it diverts attacks from production assets, and collective counterintelligence information on attacker TTPs, IOCs, and insight into attacker objectives. The solution's DecoyDocs feature delivers data loss tracking, allowing organizations to track stolendocuments inside or outside the network.

ACTIVE DEFENSE PARTNERS

Native integrations for information sharing and automated response

INVESTIGATION / ANALYSIS & HUNTING		CONTAIN / NETWORK BLOCKING		CONTAIN / ENDPOINT QUARANTINE	
Carbon Black.	ForeScout	Check Point	CISCO	aruba	Carbon Black.
IBM Radar	LogRhythm	FORTINET	JUNIPER	CISCO	CounterTack
McAfee	MICRO FOCUS	paloalto	Symantec. + BLUE COAT	ForeScout	McAfee
splunk>	TANIUM				
THREATCONNECT	virustotal				

DISTRIBUTION	McAfee TANIUM Endpoint mgmt solutions such as SCCM, WMI, Casper...	TICKETING	servicenow
CLOUD MONITORING	box Google Drive salesforce	TRAFFIC REDIRECTION	McAfee

POPULAR USE CASES

1. Lateral Movement & Credential Theft
2. Malware: Ransomware, Crypto Mining, and more
3. Insider & Supplier Threats
4. Specialized: IoT, POS, SCADA, Network, & Telecom
5. Data Center, Cloud, & Serverless Security
6. Application, Service & Data Deception
7. Actionable Alerts & Automated Analysis
8. Visibility & Streamlined Incident Response
9. Attack Path Risk Assessment
10. Compliance, Breach Investigation, M&A Diligence
11. Penetration Testing

WHY TO BUY

The ThreatDefend Deception and Response Platform offers customers:

- Early in-network threat detection for any threat vector
- Easy deployment and low maintenance
- Comprehensive solution scalable in all environments
- Substantiated alerts, detailed analysis, and forensic reporting
- Engagement-based threat, adversary, and counterintelligence
- Native Partner Integrations Accelerate Incident Response
- Attack path risk assessment for threat visibility
- Attack time-lapsed replay to strengthen overall defenses

ABOUT ATTIVO NETWORKS

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com