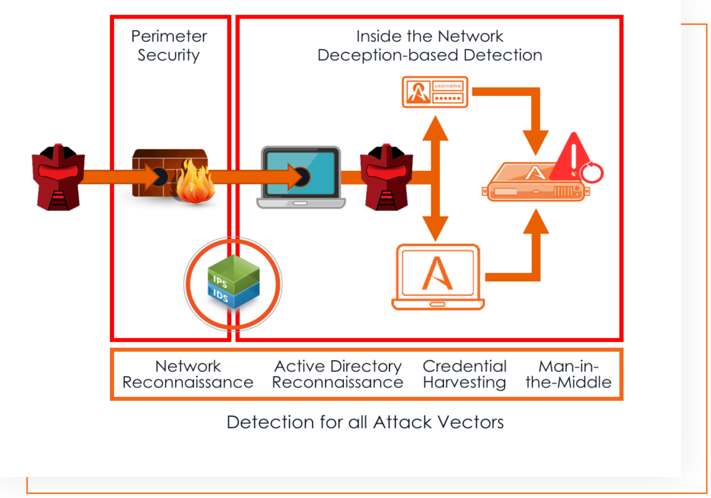
DECEPTION SOLUTION OVERVIEW

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 pressure to quickly detect and stop threats, before damage is done. In addition to 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 of all sizes and across all industries are seeking innovation to mature their security models, close detection gaps, better understand their adversaries, and be prepared to adhere to breach tracking and disclosure requirements. Organizations are now shifting their security strategies from a reactive defense to one of an Active Defense, which is not solely based on reacting to attacks but instead a balanced investment in the early detection and rapid response to threats.

DECEPTION TECHNOLOGY

Deception technology provides the innovation required to non-disruptively evolve to an Active Defense security posture. By deploying a fabric of deception-based detection throughout the network stack, companies are able to achieve efficient detection for every threat vector and the life-cycle of an attack. Utilizing high-interaction decoys and lures, deception deceives attackers into revealing themselves, thereby alerting on and identifying detection gaps on threats that have evaded other security controls.

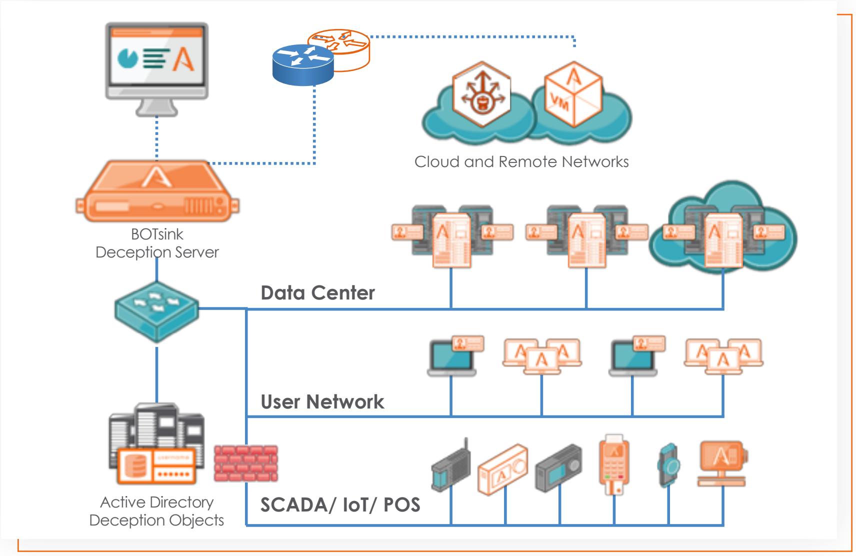

Perimeter Security
Inside the Network Deception-based Detection
IPS
IDS
Network Reconnaissance
Active Directory Reconnaissance
Credential Harvesting
Man-in-the-Middle
Detection for all Attack Vectors

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 external, internal, and supplier threat actors. Organizations of all security maturity levels are aggressively adopting deception technologies in order to mitigate risks related to employee credential theft, data exfiltration, ransomware, crypto-mining, and attacks with the intent to disrupt services or impact public safety. The accuracy and ease of use of threat deception has been a major driver in its adoption and wide-spread deployment.

In 2018, analysts recognized deception for its efficiency in detecting advanced threats and Gartner, Inc. recommended deception for the third year in a row as a top strategic security priority. A variety of recent surveys have also recorded the market's intent to add deception technology to their security controls given its efficacy and efficiency in deterring attackers.

THE ATTIVO NETWORKS SOLUTION

The ThreatDefend™ Deception and Response Platform is designed to turn the entire network into a trap, forcing the attacker to be right 100% of the time or risk being discovered. The solution combines network and endpoint high-interaction 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 solution, the ThreatDefend platform provides an overall deception fabric for cloud, network, endpoint, application, and data/database deceptions and is highly effective in detecting threats from virtually all vectors such as advanced persistent threats, stolen credential, Man-in-the-Middle, Active Directory, ransomware, and more. 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, ThreatStrike® endpoint service, ThreatPath® for attack path visibility, ThreatDirect deception forwarding for remote and segmented networks, the Informer for adversary intelligence, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM), for creating an active defense against cyber threats.

DECEPTION FOR DETECTION AND ATTACK PATH VISIBILITY

The ThreatDefend Deception and Response Platform provides unparalleled visibility into threats inside the network and attacker lateral movements and tactics. The platform detects advanced threats propagating 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.

Lures and decoys work together to 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 attacker believability, the decoy systems mirror match production assets by running real operating systems, full services, and applications, along with the ability to customize the environment by importing the organization's golden images and applications. As a result, the platform creates a "hall of mirrors" environment that is baited with lures and traps designed to redirect attackers away from company assets. Machine learning is used to prepare and deploy deceptions, keeping the network and endpoint deceptions fresh and for making ongoing maintenance easy.

To increase deception authenticity and for visibility into attempts to compromise, the solution incorporates with Active Directory. By inserting deception into areas that attackers target for reconnaissance, the deployment appears as part of the production environment in multiple layers.

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 and occupying the attention of a ransomware attack providing the time advantage to stop the attack before it can cause extensive damage.

With the rapid migration to the cloud, it is critical for the deception fabric to scale seamlessly into the cloud. The ThreatDefend platform offers extensive support for AWS, Azure, Google, and Oracle cloud environments inclusive of decoys and lures for containers, serverless, and cloud shared-security models. The ThreatDefend Platform capabilities include support for Lambda functions, access keys, reconnaissance, credential harvesting, as a means to verify the efficacy of security controls along with CloudWatch/SIEM monitoring for finding attempted use of deception credentials.

For proactive threat prevention and attack surface reduction, the ThreatPath solution provides visibility into attack paths that an attacker could traverse through misconfigured systems, credential exposure, or misuse. A topographical illustration and attack path associations provide a straight-forward view of how attacks can move laterally to reach their target. When paired with the BOTsink solution threat intelligence and attack time-lapsed replay, defenders achieve unprecedented levels of threat visibility and the information required to build pre-emptive defense against its adversaries.

DECEPTION FOR ACTIVE DEFENSE AND ACCELERATED INCIDENT RESPONSE

In addition to the early detection of attackers inside the network, the ThreatDefend Platform's actionable alerts, automated analysis, and native integrations for incident handling work collectively to dramatically improve a responder's time-to-remediation. When an attacker engages with a deception decoy, credentials, application, or data the engagement server will record and alert on the activity while simultaneously responding to the attacker. The activity is consolidated in the Informer dashboard, which assembles forensics, correlates events, and raises evidence-based alerts on malicious activity.

Alerts only occur on confirmed attacker interactions with deceptions and unlike other detection methods, is not dependent on signatures or behavioral analysis to detect an attack. 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. The elimination of false positives and the high-fidelity alerts save valuable hours for InfoSec teams.

CENTRALIZED THREAT INTELLIGENCE
EASILY VIEW ATTACK DETAILS
ACTIVATE INCIDENT RESPONSE
ATTACK VISUALIZATION & REPLAY
ATTACK & FORENSIC REPORTS

Information is presented in the Informer dashboard, which delivers a comprehensive view of incident and forensic information gathered during an attack. Forensic reports include identification of infected systems and C&C addresses and are created with full IOC, PCAP, and STIX formats to allow easy information sharing and attack recording. By correlating all relevant information and forensics from an event into a single interface, the Informer dashboard gives analysts and incident response teams a streamlined view of an attack to effectively contain and remediate the incident. This accelerates intelligence-driven response, enhances network visibility, and creates a predictive defense to improve their security posture.

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. Additionally, DecoyDocs delivers data loss tracking, allowing organizations to track stolen documents inside or outside the network.

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.

ACTIVE DEFENSE PARTNERS

Native integrations for information sharing and automated response

INVESTIGATION / ANALYSIS & HUNTING

Carbon Black. ForeScout
IBM QRadar LogRhythm
McAfee MICRO FOCUS
splunk> TANIUM
THREATCONNECT virustotal

CONTAIN / NETWORK BLOCKING

Check Point SOFTWARE TECHNOLOGIES LTD. CISCO
FORTINET JUNIPER NETWORKS
paloalto NETWORKS Symantec. + BLUE COAT

CONTAIN / ENDPOINT QUARANTINE

aruba a Hewlett Packard Enterprise company Carbon Black.
CISCO CounterTack
ForeScout McAfee
TANIUM

DISTRIBUTION McAfee TANIUM Endpoint mgmt solutions such as SCCM, WMI, Casper...

TICKETING servicenow

CLOUD MONITORING box Google Drive salesforce

TRAFFIC REDIRECTION McAfee

ORCHESTRATION DEMISTO

POPULAR USE CASES

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

WHY TO BUY

The ThreatDefend Deception and Response Platform offers customers:

- Comprehensive solution scalable in all environments
- Early in-network threat detection for any threat vector
- Easy deployment and low maintenance
- Substantiated alerts, detailed analysis, and forensic reporting
- Engagement-based threat, adversary, and counterintelligence
- Native partner integrations accelerate incident response
- Attack path risk assessment visibility for reducing attack surfaces
- Attack time-lapsed replay to strengthen overall defenses

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 70 awards for its technology innovation and leadership.