THREATDEFEND PLATFORM SOLUTION OVERVIEW

Attivo NETWORKS

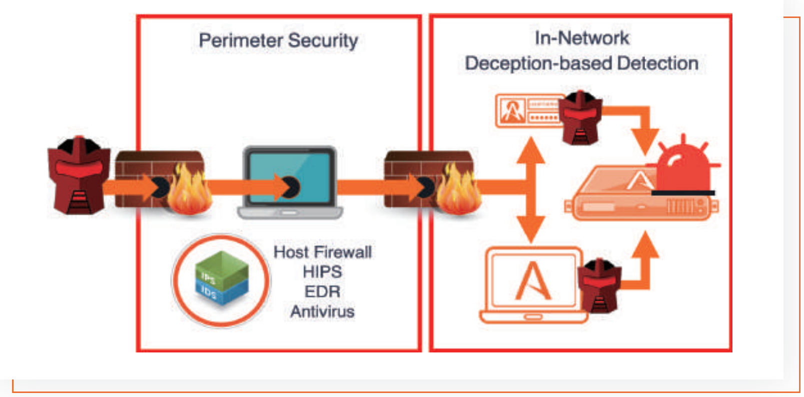
INTRODUCTION

Cyberattacks are occurring at an unrelenting pace as sophisticated attackers continue to find ways to penetrate perimeter defenses. With each breach, security professionals face mounting pressure to detect and stop threats quickly before attackers can do damage. In addition to compliance expectations, proposed breach notification laws promise significant fines and potential jail time if an organization does not meet notification expectations. Organizations of all sizes and across all industries are seeking innovation to mature their security models, close detection gaps, better understand their adversaries, and adhere to breach tracking and disclosure requirements. They are now shifting their security strategies from a reactive defense to one of an Active Defense, which is not based solely on reacting to attacks but instead seeks a balanced investment in pre-emptive derailment, early detection, and rapid response to threats.

INNOVATION IN THREAT DETECTION

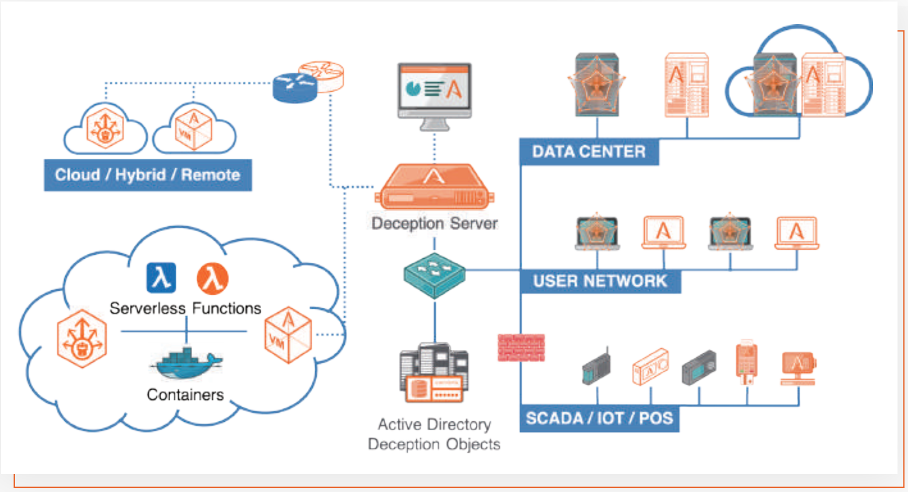
Detection using deception-based methods provides the innovation required to non-disruptively evolve to an Active Defense security posture. By placing a detection net over endpoints or by deploying a fabric of decoy-based detection throughout the network stack, companies can achieve efficient detection for every threat vector, early in the life-cycle of an attack. Deception uses a mix of high-interaction decoys, lures, and misdirections to deceive attackers into revealing themselves, quickly alerting on and identifying the lateral movement of threats that have evaded other security controls.

With early visibility into threats and actionable alerts for incident handling, these solutions are rapidly becoming the solution of choice for proactively uncovering and responding to external, internal, and third-party threat actors. Organizations of all security maturity levels are aggressively adopting these technologies to mitigate risks related to employee credential theft, data exfiltration, ransomware, crypto-mining, and attacks that try to disrupt services or impact public safety. The accuracy and ease of use of this detection method have been a significant driver in its adoption and wide-spread deployment.



In 2018, analysts began actively recognizing these technologies for their efficiency in detecting advanced threats. Gartner, Inc. has recommended it for the third year in a row as a top strategic security priority and in their COVID guidance as a technology for reducing security risks related to the rapid shift in remote working. A variety of recent surveys and research reports have also recorded the technology's positive impact on security controls, given its efficacy and efficiency in deterring attackers.

THE ATTIVO NETWORKS SOLUTION PORTFOLIO



The ThreatDefend® Detection and Response Platform turns the entire network into a trap, forcing the attacker to be right 100% of the time or risk discovery. The solution combines endpoint lures, misdirections, and high-interaction deception decoys that provide early visibility into in-network threats, efficient continuous threat management, and accelerated incident response.

The ThreatDefend platform, recognized as the industry's most comprehensive in-network detection solution provides a detection fabric for cloud, network, endpoint, application, data/database, and Active Directory decoys and is highly effective in detecting threats from virtually all vectors such as APTs, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, port knocking 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 creates an active defense against cyber threats. It includes the Attivo BOTsink® deception servers for decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks; and the Endpoint Detection Net (EDN) suite, composed of the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, and ADSecure for Active Directory defense. The ThreatDirect deception forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) for BOTsink and the Endpoint Detection Manager for EDN deployments add enterprise-wide deception fabric management.

The pricing models of all the main componets and features of the Attivo Networks ThreatDefend Platform are subscription base as described below:

Main Components	Platform Support	Pricing Model
BOTsink Deception System (Standard Edition)	KVM, VMware, AWS, GCP, Azure	Subscription per System
BOTsink Deception System (Enterprise Edition)	KVM, VMware, AWS, GCP, Azure	Subscription per System
Endpoint Detection Net	Windows, Linux, MacOS	Subscription per Endpoint
ThreatDirect	Windows, Linux, VMware	Subscription per remote VLAN
Attivo Central Manager	KVM, VMware, AWS, GCP, Azure	Subscription per Manager

BOTsink Deception System also includes the informer dashboard and the ThreatOps incident reponse orchestrationplaybooks, and the main difference of the two versions are:

Edition	VLANs	Engagement VMs	Decoys
BOTsink Deception System (Standard Edition)	32 VLANs monitored	6 Engagement VMs with 1 Windows Server VM	2192 Network Decoys
BOTsink Deception System (Enterprise Edition)	100 VLANs monitored	12 Engagement VMs with 2 Windows Server VM	2384 Network Decoys

ADSecure for Active Directory Defense of the Endpoint Detection Net (EDN) suite can also be purchased standalone. In this case, it needs an Endpoint Detection Manager to manage all endpoints:

Components	Platform Support	Pricing Model
ADSecure for Active Directory Defense	Windows	Subscription per Endpoint
Endpoint Detection Manager	KVM, VMware, AWS, GCP, Azure	Subscription per Manager

DETECTION AND ATTACK PATH VISIBILITY

The ThreatDefend 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 to target 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 the platform can safely analyze their lateral movement and actions. 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 baited with lures and traps designed to redirect attackers away from company assets. Machine learning prepares and deploys the decoys, keeping the network and endpoint deceptions fresh and making ongoing maintenance easy.

To increase decoy authenticity and for visibility into attempts to compromise systems or recon Active Directory, the solution creates AD decoys both as fake AD controllers and at the endpoints to modify unauthorized AD queries. By inserting deception into areas that attackers target for reconnaissance, the deployment appears as part of the production environment in multiple layers. The ADSecure solution looks out for unauthorized AD queries, alerts on the activity, and alters the response to return fake AD objects that lead to decoys for engagement.

The solution disrupts network discovery attempts by detecting and alerting on ping sweeps and port scans. Additionally, it redirects any port scans that touch a closed port on a host to an open port on a decoy, making host fingerprinting difficult and misinforming the attacker as to the actual ports and services accessible on a host. This capability does not interfere with any production services while providing early detection of attacker lateral movement. The solution can natively isolate any inbound or outbound traffic on a host to connect only with the decoy environment.

Endpoint deceptions and hidden mapped shares provide easy and highly effective redirection of attacks seeking to harvest credentials or execute a ransomware attack. Additionally, the endpoint defenses can hide local files, folders, removable drives, and mapped network and cloud shares, while high interaction deceptions slow and occupy a ransomware attack, providing the time to stop it before it can cause extensive damage.

For remote workers, the ThreatDefend platform protects both the VPN infrastructure and credentials for VPN, cloud PaaS, IaaS, and SaaS. The solution can deploy decoys within the VPN network segment to identify network discovery and AD reconnaissance activities that indicate lateral movement. It seeds fake VPN credentials at remote endpoints that alert on remote theft and reuse and integrates with cloud services to monitor for unauthorized use.

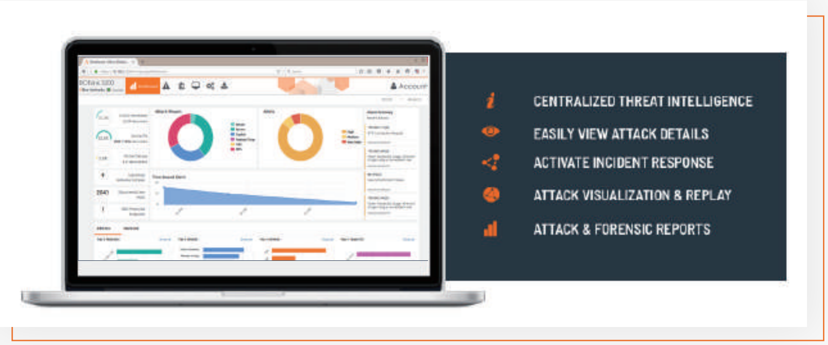
With the rapid migration to the cloud, the detection fabric needs to scale seamlessly anywhere the enterprise network sits. The ThreatDefend platform offers extensive support for AWS, Azure, Google, and Oracle cloud environments inclusive of decoys and lures for containers, storage buckets, and other native cloud technologies. The ThreatDefend platform capabilities include support for serverless functions, access keys, reconnaissance, credential harvesting, and verifying the efficacy of security controls, along with CloudWatch/SIEM monitoring for finding attempted use of deception credentials.

The ThreatPath solution reduces the attack surface and proactively increases security by identifying misconfigurations and credential exposures that create attack paths for attackers to use for lateral movement. A topographical visualization and attack path associations provide a straight-forward view of how attacks can reach their target. When paired with the BOTsink server's threat intelligence and attack time-lapsed replay, defenders achieve unprecedented levels of threat visibility and the information required to build a pre-emptive defense against its adversaries.

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 decoy system, credential, application, data, or Active Directory object, the ThreatDefend platform records, and alerts on the activity while simultaneously responding to the attacker. The Informer dashboard consolidates the data and assembles forensics, correlates events, and raises evidence-based alerts on malicious activity.

Alerts only occur on confirmed attacker interactions with the decoys or engage within the Endpoint Detection Net, and, unlike other detection methods, does not depend on signatures or behavioral analysis to detect an attack. The attack analysis substantiates alerts can the security teams can use 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. Minimizing false positives and creating high-fidelity alerts save valuable hours for security teams in both investigation and response time.


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

The Informer dashboard presents a comprehensive view of the incident and forensic information gathered during an attack. Forensic reports include identifying infected systems and C&C addresses and available as exported IOC, PCAP, and STIX file 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.

The solution enables offensive counterintelligence functions 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 and IOCs, giving insight into attacker objectives. Additionally, DecoyDocs delivers data loss tracking, allowing organizations to track stolen documents inside or outside the network, and the ADSecure solution gives insight into attacker goals based on the high-priority AD objects they are targeting.

Organizations can also use the ThreatOps functions of the BOTsink server to automate incident handling and create repeatable incident response playbooks. Organizations can fully customize this threat orchestration function to match their environment and policies so that security teams can make faster and better-informed incident response choices.

ACTIVE DEFENSE PARTNERS

Native integrations for information sharing and automated response

INVESTIGATION / ANALYSIS & HUNTING

FIREEYE
FORESCOUT
IBM QRadar
LogRhythm
McAfee
MICRO FOCUS
REVERSING LABS
splunk>
TANIUM
ThreatConnect
VirusTotal
WEBROOT an opentext company

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
CISCO
FIREEYE
FORESCOUT
GoSecure POWERED BY COUNTERTACK
McAfee
TANIUM
vmware Carbon Black.

API INTEGRATORS

DIGITAL DEFENSE INCORPORATED

ORCHESTRATION

DEMISTO
Resilient an IBM Company
splunk> phantom
SWIMLANE

TICKETING

servicenow

REDIRECTION

McAfee

CLOUD MONITORING

box
Google Drive
Office 365
salesforce

DISTRIBUTION

McAfee
TANIUM
Endpoint management solutions such as SCCM, WMI, Casper, and others

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 130+ awards for its technology innovation and leadership.