Attivo
NETWORKS®

ATTIVO NETWORKS DECEPTION USE CASES TO DEFEAT ADVANCED ATTACKERS

Attivo
NETWORKS®

INTRODUCTION

Security professionals acknowledge that determined criminals can evade traditional prevention-based security solutions. Attackers are increasingly more sophisticated, and breaches continue to happen at unprecedented rates. Forward-thinking organizations are now looking to deception and concealment technologies to fortify their security stack. Organizations need to identify threats that have bypassed perimeter and antivirus defenses and efficiently detect in-network lateral movement and credential theft.

The Attivo Networks ThreatDefend® platform provides early and accurate detection of in-network threats, regardless of attack method or surface. It creates a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirections that derail adversaries early in the attack lifecycle. It also conceals and denies access to sensitive files, folders, data, and accounts that attackers use to further their attacks. Visibility tools empower organizations to proactively strengthen overall security defenses by showing exposed attack paths and attacker movements in a time-lapsed replay. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The components of the platform include the BOTsink server, the Endpoint Detection Net (EDN) suite, and ADSecure for Active Directory protection.

The Attivo ThreatDefend platform creates a comprehensive early detection and continuous threat management defense against today's advanced threat actors for an informed Active Defense.
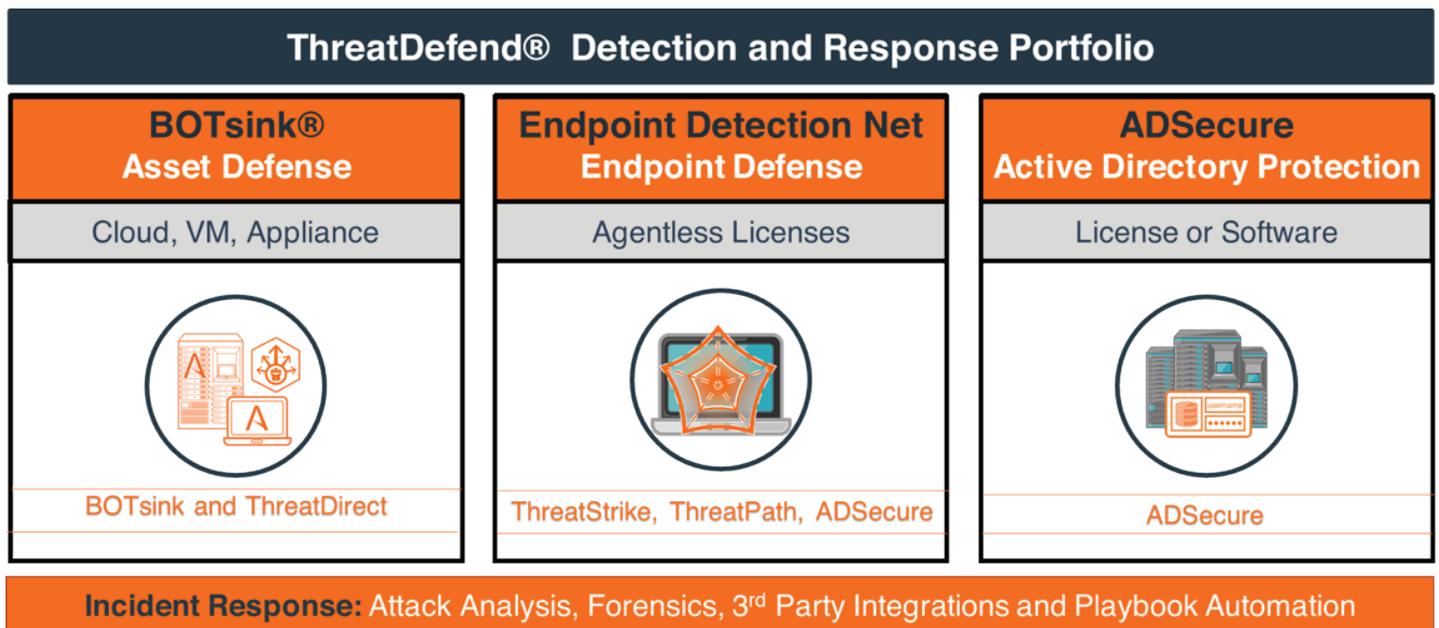

ThreatDefend® Detection and Response Portfolio

BOTsink® Asset Defense	Endpoint Detection Net Endpoint Defense	ADSecure Active Directory Protection
Cloud, VM, Appliance	Agentless Licenses	License or Software
BOTsink and ThreatDirect	ThreatStrike, ThreatPath, ADSecure	ADSecure

Incident Response: Attack Analysis, Forensics, 3rd Party Integrations and Playbook Automation

TABLE OF CONTENTS

POST-COMPROMISE IN-NETWORK DETECTION: RECONNAISSANCE, ACTIVE DIRECTORY ATTACKS, AND LATERAL MOVEMENT

- Provides the ability to rapidly establish a critical control to identify reconnaissance activity inside the network, which is typically a blind spot for most security organizations.
- Provides visibility and detection of threats moving inside the network instead of egress/ingress traffic, including Insider Threats.
- Detects attacks targeting the Active Directory (AD) infrastructure through AD deceptions.
- Detects unauthorized queries to AD that indicate attacker discovery, credential theft, and privilege escalation attempts. Hides real results and returns decoy accounts or data that lead to decoys for engagement.
- Enables high fidelity threat detection inside the network without relying on large-scale log analysis or traffic capture.
- Redirects port and service discovery traffic that touches closed ports to decoys with a corresponding open port and service. Misinforms endpoint fingerprinting and makes every endpoint part of the decoy fabric.

MAN-IN-THE-MIDDLE (MITM) NETWORK-BASED ATTACK DETECTION: CREDENTIAL AND DATA THEFT

- Provides automatic or manual detection of all MitM attack methods looking to steal credentials and data.
- Learns domain requests, DHCP, and ARP resolutions from production systems and uses heuristics to detect attackers trying to mount a MitM attack responding to 3 or more domain queries. A very proactive, simple, and transparent approach to detect those would-be victims, not just attackers.
- Detects queries for user-configured false domains. Any response to these is considered malicious.
- Provides deceptive responses to a confirmed MitM attack, sending deceptive credentials to the attacker and querying the SIEM for their use.

ENGAGING INSIDERS AND 3RD PARTY CONTRACTORS

- Creates authentic, organization-specific decoysthat look like production assets, allowing the Attivo Networks ThreatDefend® platform to observe attacks in real time.

- Slows the attack, buying SOC and IR teams precious time to understand the threat, its key characteristics, and the threat vectors being employed. This additional time gives organizations the opportunity to accelerate containment and remediation.

- Detects attacks based on engagement, not on its signature.

> Internal hunt teams can leverage Intelligence gathered from the Attivo solution for broader validation and assessment of potential vulnerabilities that exist in the enterprise.

- Provides evidence-based engagement with the attacker for full analysis, forensics capture, and TTP development (including C&C traffic capture), delivering deep insight and understanding of the nature and intent of an attack.
- Provides intelligence for internal hunt teams to validate and assess the enterprise environment for other potential vulnerabilities.

ENDPOINT CREDENTIAL THEFT AND RANSOMWARE ATTACKS

- Detects endpoint attacks focused on credential harvesting and data theft by deploying deceptive credentials, bait, lures, and artifacts on the endpoint.
- Redirects attacker back to Attivo Engagement Servers via the Endpoint Detection Net ThreatStrike® solution to engage, trap, and slow down the attack.
- Misdirects ransomware attacks to decoy network shares that house fake files to slow and stall the attack through high-interaction continuous engagement, preventing the malware from completing the encryption process.
- Hides local files, folders, mapped network and cloud shares, and removable drives to prevent local exploitation and encryption of sensitive data.

> Endpoint Deception Net solution redirects attackers back to Attivo Engagement Servers to engage, trap, and slow down the attack.

IDENTIFYING CREDENTIAL VULNERABILITIES AND AVAILABLE ATTACK PATHS

- The EDN ThreatPath® solution provides valuable insight into potential vulnerabilities and available attack paths that an attacker could exploit to move laterally to production-critical assets.
- Identifies stored, exposed, or orphaned credentials along with misconfigurations an attacker can exploit to move laterally.
- Alerts when anyone uses invalid or deactivated cloud credentials from applications like Salesforce, Box, and Google Drive, etc.

PHISHING MALWARE ANALYSIS

- Provides supplementary automated analysis of suspicious emails containing executables or URLs that users self-submit. Provides security teams with a detailed report after the automated examination.
- Eliminates the need for IT Security Teams to do manual evaluations, freeing them up for higher priority initiatives.
- Reduces the risk associated with having a backlog of suspicious emails that require investigation.

> Eliminates the need for IT Security Teams to do manual evaluation, freeing them up for higher priority initiatives.

THREAT DETECTION FOR OPERATIONAL ENVIRONMENTS: SCADA, ICS, IOT, POINT OF SALE, MEDICAL DEVICES

- Rapidly establishes deception-based threat detection in operational environments, providing a critical control that is increasingly falling under the jurisdiction of traditional IT Security Teams.
- Projects deceptive decoys into SCADA, ICS, IoT, Point of Sale, and Medical Device networks, identifying attacker lateral movement and reconnaissance activity targeting production-critical systems.
- Provides flexibility to deploy out-of-the-box SCADA images and protocols, and facilitates custom images specific to an organization's infrastructure.
- Enterprise-wide deception-based threat detection from a single platform provides complete coverage for an evolving attack surface inclusive of traditional enterprise IT and OT networks.

REMOTE LOCATION THREAT DETECTION

- Provides scalable and flexible threat detection for remote offices; branch offices; power generation, distribution, and service centers; or retail locations.
- Redirects traffic back to an appliance for engagement and evaluation.
- Eliminates the need for an appliance in each location to establish deception at remote sites

PROTECTING LEGACY ENVIRONMENTS

- Provides customized deception decoys that mirror legacy systems for authentic and attractive targets.
- Deploys decoys in production-critical legacy system networks that are traditionally difficult to patch, creating a minefield to detect lateral movement and reconnaissance activity.

MERGER & ACQUISITION ASSESSMENT AND VALIDATION

- Quickly establishes visibility into the networks and infrastructure of newly-acquired entities by deploying and remotely monitoring engagement servers.
- Provides a quick way to ascertain risks and vulnerabilities that may exist in these unknown environments, the state of current security controls, and potential gaps.
- Identifies potentially active compromises and areas of risk.
- Delivers intelligence of the existing infrastructure across cloud, data center, end-user networks, and even into operational networks like SCADA/ICS/IoT/POS networks.
- Establishes a critical threat detection control to elevate the security posture of immature environments.
- Provides insights as part of assessment activities. After addressing deficiencies, red teams can validate the remediation efforts and verify risk mitigation.
- Provides counterintelligence and insight into data targeted by attackers.

SECURING THE CLOUD

- Provides dynamic threat detection for AWS, Azure, and OpenStack environments that are present in today's public, private, or hybrid cloud environments.
- Offers full deception capabilities enabled and deployable to the cloud.

THREAT HUNTING AND RED TEAM TESTING

- Provides forensics and intelligence gathered from an attack to internal hunt teams for broader validation and assessment of potential vulnerabilities that exist in the enterprise.
- Provides counterintelligence and insight into data targeted by attackers.
- Allows decoy-creation modeled after planned production assets to learn about the types of attacks that may affect new technologies.
- Provides business-aware, targeted threat detection of APT-grade actors.
- Provides specific threat detection using threat assessment results (such as likely attacker interests and assets attackers intend to steal).
- Validates network resiliency during Red Team and penetration tests.

PROTECTING CRITICAL INTELLECTUAL PROPERTY AND SENSITIVE CLIENT INFORMATION

- Allows fully customizable decoys built to replicate production systems and databases that contain intellectual property, like application code for a software company, proprietary formulas for a pharmaceutical company, or confidential client data.
- Creates tripwires or landmines by deploying these decoys into the networks where critical IP or sensitive client information lives, surrounding the essential assets and providing lateral movement reconnaissance activity detection.

> Decoys are highly authentic and can be tailored to specific environments.

- Produces highly authentic and tailor-made decoys to specific environments, including the use of golden images. Decoys embedded with deceptive content represent an attractive and realistic target to lure an attacker.
- Provides counterintelligence and insight into patent theft or IP targeted by attackers.

PROTECTING CRITICAL AND CONFIDENTIAL DATA OF KEY EXECUTIVES AND EMPLOYEES

- Deploys deceptive decoys into critical network segments where key executive and strategic employee systems reside, providing the ability to detect lateral movement and reconnaissance activity targeted at discovering these high-value systems and data.
- Detects credential theft of executives who possess highly privileged access to systems and resources that contain sensitive and confidential information. Deceptive credentials placed on the user's systems redirect attackers back to the Attivo Networks engagement environment to engage, trap, and slow the attack.

DECOYDOCS

- Deploys enticing deceptive decoy documents throughout the environment, seeding fake artifacts representing the data and information that an attacker seeks.
- Tracks these deceptive documents designed to beacon home when attackers open them, whether internally or externally, providing additional detection capabilities, geographical location, counterintelligence, and insight into attacker activity and potential egress of stolen data.

FORENSICS

- Allows the full forensic collection of detected malicious activity to gain insight into an attacker's tactics, techniques, procedures (TTPs).
- Gives rich forensics output to gain an advantage against an adversary and an accurate and deeply intuitive understanding of the threat.
- Provides easily sharable details in IOC, STIX, CSV, and PCAP formats for specific information around the threat: lateral movement patterns, C2 communication, registry changes, files drops, etc.

> At the heart of effective deception, isn't just the ability to detect malicious activity, but the ability to gain insight into what an attacker's tactics, techniques, procedures strategy are.

ENGAGE, IDENTIFY, AND UNDERSTAND ATTACKER BEHAVIOR

- Safely engages an attacker, yielding an advantage of how best to respond, remediate, and proactively fortify an organization. Authentic, real-OS-based decoys engage an attacker in a manner where the attacker believes that the decoy is a legitimate production system.
- Deceives the threat actor into spending hours executing their strategy and employing their tactics while trapped within the decoy, all under the watchful eye of the SOC and IR teams. Security teams can observe and gather tactical details necessary to understand their adversary while increasing the attacker's costs.
- Delays attacks, giving security teams precious time and comprehension to quickly contain, remediate, and minimize the impact of a compromise.
- Provides the most comprehensive evidence and analysis of an attacker's behavior based on actual engagement.

MOBILE- OFFLINE USERS REMOTE OFFICES

- Provides deception-based threat detection capabilities to mitigate risks associated with credential theft of offline endpoints that can compromise enterprise networks when they reconnect.
- Shifts the posture of security teams securing their organizations from a reactive, prevention-based position to a proactive, evidenced-based stance derived from high fidelity alerts and validated attacker behavior in remote locations.
- Deceptive credentials, files and, artifacts divert attackers from production-critical assets and redirect them to a decoy environment, triggering the incident handling process.

- Ability to rapidly deploy decoys into the networks of remote offices, gaining visibility and enabling detection of lateral reconnaissance campaigns.
- Flexible and scalable across geographically dispersed and multinational organizations, their affiliates, subsidiaries, and joint ventures.
- Ability to inventory and identify production credentials that could provide an available attack path that attackers could leverage to gain access to production-critical systems and data.
- Easy and intuitive to use, doesn't require extensive training or additional staff to achieve proficiency and is transparent to end-users.

HIGH PROFILE AND ONE-TIME EVENTS (SPORTS CHAMPIONSHIPS, STRATEGIC SENIOR LEVEL OFFSITE MEETINGS, ETC.)

- Provides advanced monitoring and detection of threat actors targeting highly visible/high-value targets and events.
- Shifts the posture of security teams securing those events from a reactive, prevention-based position, to a proactive, evidenced-based stance derived from high fidelity alerts, and validated attacker behavior in unsecured locations.
- Rapidly and unobtrusively delivers innovative deception-based threat detection to identify attackers that rely on reconnaissance, lateral movement, and credential theft to compromise systems and obtain confidential and proprietary data of high-value targets attending off-premise events.
- Accelerates detection and response to incidents that occur, expediting remediation and mitigating the impact of the compromise.
- Provides quick provisioning and de-provisioning through simplicity and speed of deployment, allowing for rapid fielding and repurposing for current and future events.

COLLECT COMPANY-SPECIFIC PRIVATE THREAT INTELLIGENCE

- Allows for decoy deployment to the DMZ to collect and develop threat intelligence.
- Automatically collects source IP addresses of attacking systems and C2 servers.
- Provides automated or manual network blocking based on native integrations with supported firewalls.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.