

THREATDEFEND PLATFORM OVERVIEW

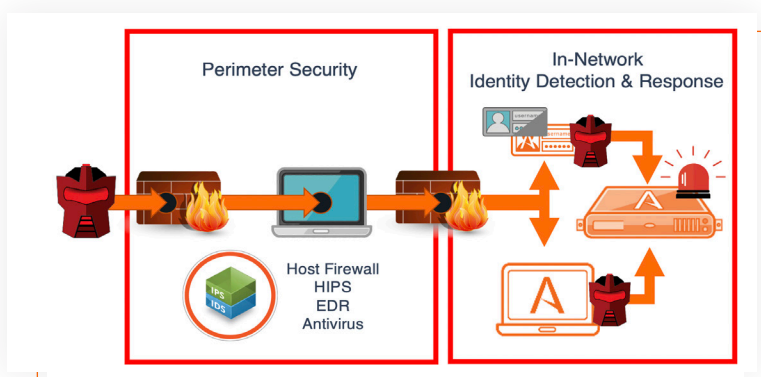
INTRODUCTION

Cyberattacks occur at an unrelenting pace as sophisticated attackers continue to find ways to penetrate perimeter defenses and move laterally to advance their attacks. Security professionals face mounting pressure to detect and stop attacks quickly before attackers can cause damage with each breach. 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 must seek innovation to mature their security models, close detection gaps, better understand their adversaries, and adhere to breach tracking and disclosure requirements. They are shifting their security strategies from a reactive posture to one of an Active Defense, which is not based solely on reacting to attacks but instead seeks a balanced investment in denying lateral movement and privilege escalation activities, detecting malicious activity early, and derailing attacks preemptively.

INNOVATION IN THREAT DEFENSE

Defending a network requires an identity-first security posture that can provide visibility to vulnerabilities that create risk, prevent attacks, and quickly detect activities such as credential theft and misuse, privilege escalation, and lateral movement. By hiding credentials at the endpoint and binding them to applications, detecting and remediating Active Directory exposures, and concealing sensitive or critical objects, organizations can efficiently guard against known and unknown threats early in the attack cycle. Using a mix of visibility tools alongside concealment and deception technologies, security teams can deny, detect, and derail threats while tricking attackers into revealing themselves. Equipped with a high-fidelity alert, security teams can take action quickly respond to threat activities that have evaded other security controls.

With early visibility into identity- and network-based security threats, Attivo solutions are rapidly becoming a preferred 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 unauthorized credentials use, privilege escalation, data exfiltration, and ransomware attacks that disrupt services or impact public safety. The accuracy and ease of using these technologies have significantly driven their adoption and wide-spread deployment.

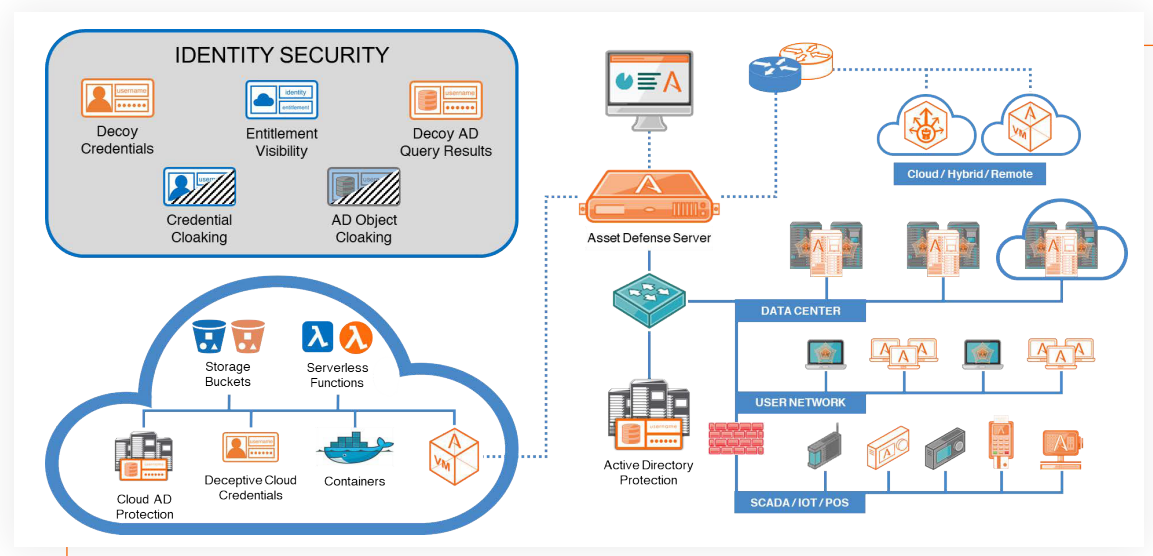


Analysts have recently actively recognized these technologies for their efficiency in detecting advanced threats. Gartner, Inc. has consistently recommended deception technology, endpoint lateral movement detection, and identity entitlement protection as top strategic security priorities. They have also included these technologies in their recent guidance for reducing security risks related to the rapid growth of remote work and cloud adoption. A variety of recent [surveys and research reports](#) have also recorded their positive impacts on security controls, given their efficacy and efficiency in deterring attackers.

THE ATTIVO NETWORKS SOLUTION

The Attivo Networks ThreatDefend® Platform provides a superior solution for assessing exposures, stopping credential theft and misuse, detecting lateral movement, and preventing privilege escalation. It delivers visibility to exposures that create attack paths and risks and detecting in-network threats, regardless of attack method or surface. It identifies vulnerabilities within AD and at the endpoints that enable lateral movement. Additionally, it conceals sensitive or critical data to prevent attackers from exploiting them during an attack.

The security industry recognizes the ThreatDefend platform for its comprehensive in-network detection, which extends coverage from the endpoint to the cloud. The platform disrupts discovery activities and effectively detects threats from virtually any vector such as APTs, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, port and service discovery, and more. It also scalably deploys across all types of networks, including endpoints, user networks, servers, data centers, remote worksites, cloud, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications.



The ThreatDefend Platform creates an active defense against attackers and is modular in design for easy expansion.

The ADAssessor solution identifies Active Directory exposures and alerts on attacks targeting the AD controllers, offloading analysis, alerting, and management to a cloud-based console.

The Endpoint Detection Net suite includes the following modules:

- ThreatStrike® for credential protection and endpoint threat detection
- ThreatPath® for attack path visibility
- ADSecure for Active Directory defense - also available as a standalone solution
- DataCloak function to hide and deny access to data
- Deflect function to redirect malicious connection attempts to decoys for engagement

The IDEntitleX solution provides cloud identity and entitlements visibility as part of the Attivo Identity Security Offerings (with ThreatStrike, ThreatPath, ADSecure, and ADAssessor), reducing the attack surface and limiting exposures across the enterprise.

The Attivo BOTsink® deception servers provide decoys, a high-interaction engagement environment, the Informer dashboard for displaying gathered threat intelligence, and ThreatOps® incident response orchestration playbooks that facilitate automated incident response. It also offers ThreatDirect deception forwarders to support remote and segmented networks.

The Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

PLATFORM BENEFITS

IDENTITY DETECTION AND RESPONSE

Defend identities across the entire enterprise with identity-based, least-privilege access programs and defenses capable of detecting attack escalation and lateral movement on-premises and in the cloud. The ThreatStrike, ThreatPath, ADSecure, ADAssessor, and IDEntitleX solutions implement identity-first security, providing visibility to exposures, reducing the addressable attack surface, protecting credentials from theft and misuse, and preventing and detecting attacks at endpoints, in Active Directory, and the cloud.

ENDPOINT LATERAL MOVEMENT DETECTION

The EDN suite provides effortless and highly effective protection against attacks seeking to harvest credentials or execute a ransomware attack. Additionally, the solution hides and binds credentials to applications, hides local files, folders, removable drives, and mapped network and cloud shares, while high interaction deceptions slow and occupy a ransomware attack. This delay provides the time needed to stop an attack before it can cause extensive damage.

NETWORK-BASED DETECTION AND ATTACKER ENGAGEMENT

Fake credential lures and decoy systems 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 attack activities. The decoy systems mirror-match production assets by running real operating systems, services, and applications. Machine learning prepares and deploys the decoys and lures, making initial deployment and ongoing maintenance easy. The platform can also customize the organization's decoy environment by importing golden images and applications for more authenticity.

CLOUD

With the rapid migration to the cloud, the detection fabric scales seamlessly anywhere the enterprise network sits. The ThreatDefend platform offers extensive support for AWS, Azure, Google, and Oracle cloud environments, including 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.

REMOTE WORK SECURITY

The ThreatDefend platform protects 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 theft and reuse and integrates with cloud services to identify unauthorized use.

VISIBILITY TO DISCOVERY ACTIVITIES

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

ATTACK SURFACE REDUCTION

The ThreatPath solution reduces the endpoint 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. The IDEntitleX solution provides visibility to entitlements exposures that form attack paths in the cloud. When paired with the BOTsink server's threat intelligence and attack time-lapsed replay and used in conjunction with the ADAssessor solution, defenders achieve unprecedented threat visibility levels and the information required to build a pre-emptive defense against their adversaries across endpoints, Active Directory, and the cloud.

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.

The platform will also correlate and substantiate its alerts so the security teams can automate responses like blocking an attacker, isolating an infected system, and hunting for other compromises to eradicate the threat from the network entirely. Minimizing false positives and creating high-fidelity alerts save valuable hours for security teams in investigation and response times. [Independent research](#) shows efficiency savings of 32% when responding to a deception-based alert.











































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		CONTAIN / NETWORK BLOCKING		CONTAIN / ENDPOINT QUARANTINE	
					
					
					
		API INTEGRATORS   			
		ORCHESTRATION  			
		DISTRIBUTION  			Endpoint management solutions (ECM, WMI, Casper, etc.)
CLOUD MONITORING					TICKETING 
					REDIRECTION 

POPULAR USE CASES

1. Active Directory Assessment & Protection
2. Credential Theft, Privilege Escalation & Lateral Movement Detection
3. Malware & Ransomware Derailment
4. Data Center, Cloud, & Serverless Security
5. Insider & Supplier Threat Detection
6. Specialized: IoT, POS, SCADA, Network, & Telecom Detection
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

- Comprehensive solution scalable in all environments
- Enhanced security across MITRE ATT&CK phases
- Early threat detection for any threat vector
- Credential cloaking & policy-based application access
- Early insight into unauthorized privileged access & credential misuse
- Identity and entitlement access protection
- Ability to create an Active Defense & alignment to MITRE Shield
- Easy deployment & low maintenance
- Substantiated alerts, detailed analysis, & forensic reporting
- Engagement-based threat, adversary, & counterintelligence
- Native partner integrations accelerate incident response

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com