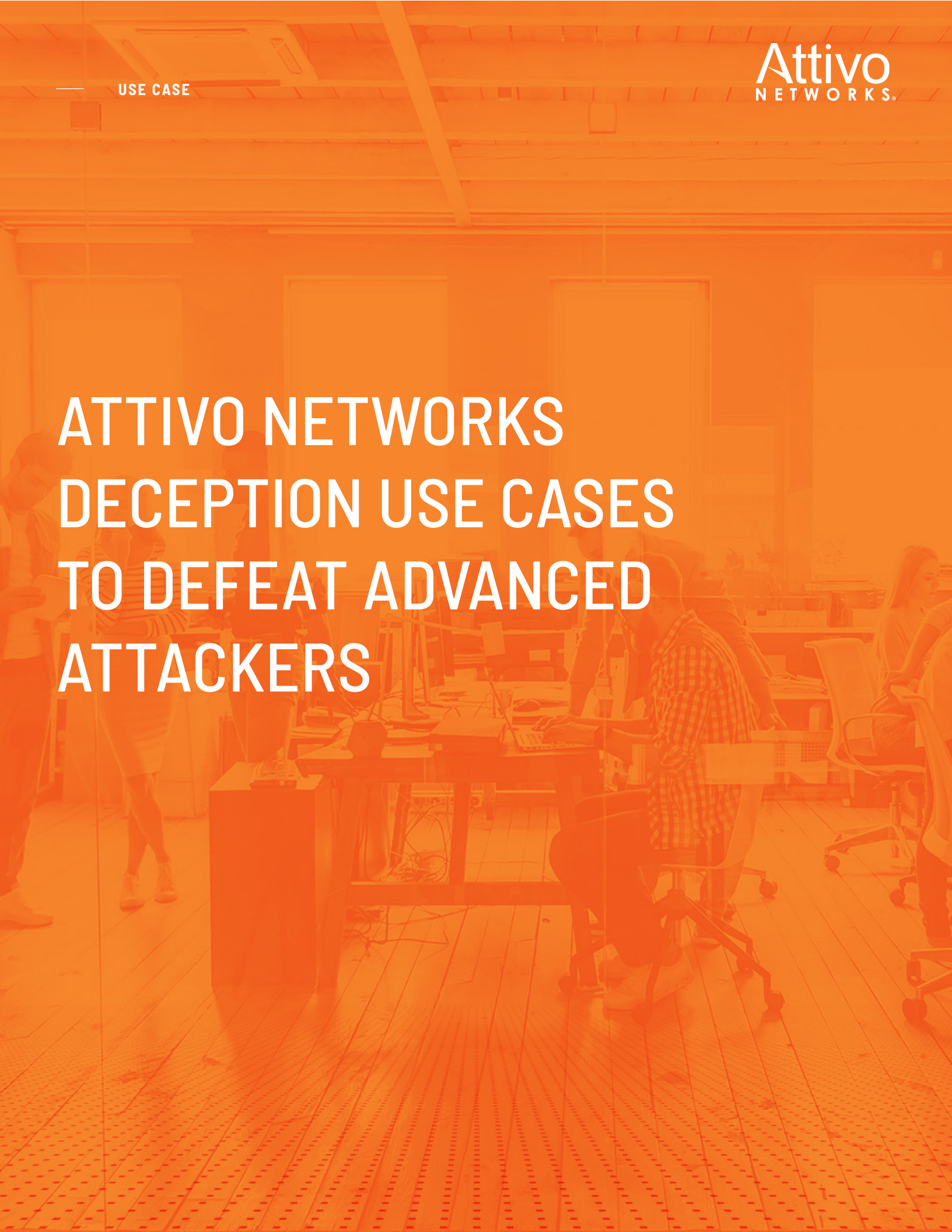
USE CASE

Attivo NETWORKS®

ATTIVO NETWORKS DECEPTION USE CASES TO DEFEAT ADVANCED ATTACKERS



INTRODUCTION

Organizations no longer see traditional prevention-based security solutions as a reliable line of defense against today's cyber attackers. Attackers are increasingly more sophisticated, and breaches continue to happen at unprecedented rates. Forward-thinking organizations are now looking to deception technology to fortify their security stack. Organizations need to be able to detect threats that have bypassed perimeter and antivirus defenses and can efficiently detect the in-network lateral movement and credential theft.

The Attivo ThreatDefend Deception and Response Platform has created a new class of deception-based threat detection that ups the game against attackers. The ThreatDefend platform offers a comprehensive network and endpoint-based deception solution, which turns user networks, data centers, cloud, remote offices, and even specialty environments such as IoT, ICS-SCADA, point-of-sale, telecom, and network infrastructure systems into a "hall of mirrors" environment that will confuse, misdirect, and reveal the presence of attackers.

Visibility tools empower organizations to proactively strengthen overall security defenses by showing exposed attack paths and attacker movement in a time-lapsed replay. The Attivo Deception and Response Platform creates a comprehensive early detection and continuous threat management defense against today's advanced threat actors.

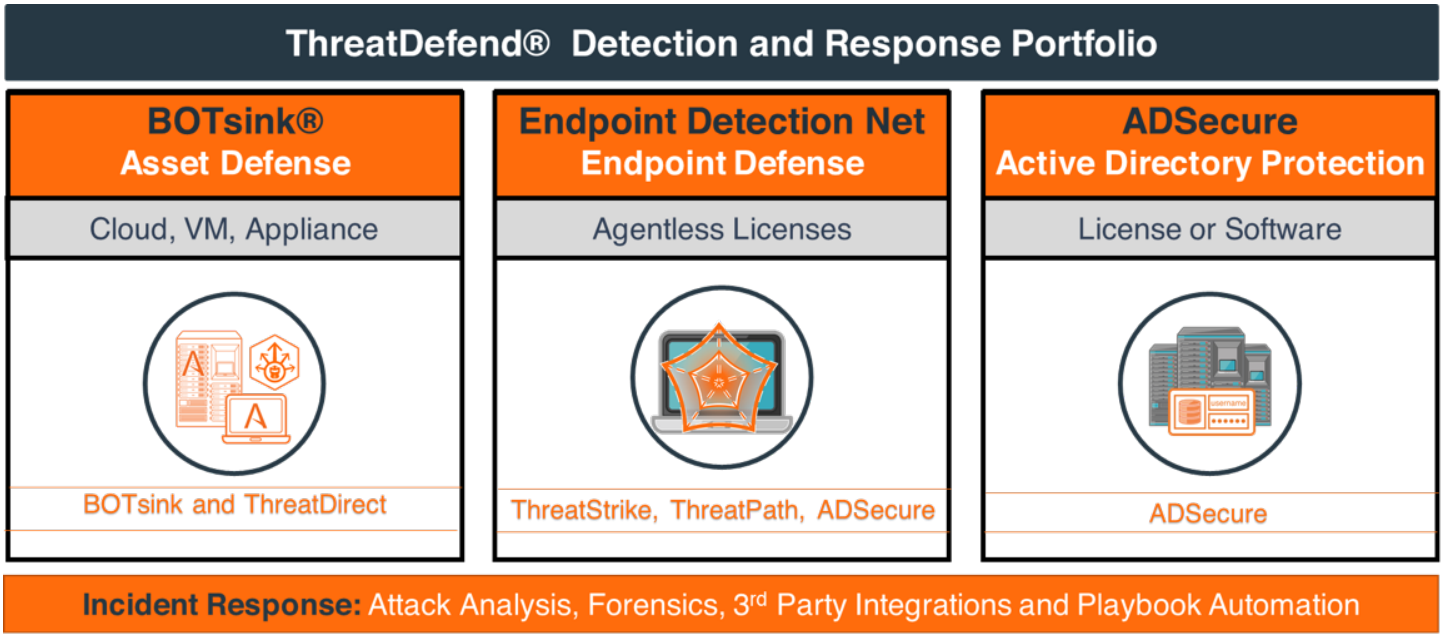


TABLE OF CONTENTS

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, as opposed to egress/ingress, including Insider Threats.
- Detects attacks targeting the Active Directory infrastructure through Active Directory deceptions.
- Enables high fidelity threat detection inside the network without relying on large-scale log analysis or traffic capture.

ACTIVE DIRECTORY RECONNAISSANCE ACTIVITIES

- Detects unauthorized querying of active directory services preventing an attacker from enumerating Active Directory
- Intercepts production AD query responses and hides real asset details (Privileged Domain Admin Accounts, Service Accounts, Users/Computers, Domain Controllers, etc.)
- Substantially reduces the ability for an adversary to escalate privileges as a part of their campaign
- Returns false information to the attacker and redirects them to a deceptive environment to initiate response and remediation efforts.
- Requires no modifications to the production Active Directory.
- 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 are used to divert attackers from production-critical assets and redirect them to a deceptive 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; it doesn't require extensive training or additional staff to achieve proficiency and is transparent to end-users.

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 are used to divert attackers from production-critical assets and redirect them to a deceptive 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, it doesn't require extensive training or additional staff to achieve proficiency and is transparent to end users.

REMOTE WORKFORCES

- Detects threats due to increased exposure from damaging emails, websites, malware, etc.
- Deployment of deceptive VPN credentials and VPN concentrator decoys within the network helps detect exploits targeting VPN infrastructures.
- Because engagement with deceptive assets is a high indicator of compromise, it enables rapid, high fidelity detection and triaging of anomalies from remote workers' devices.
- Identifies network scanning and MITM attacks (including ransomware, cryptocurrency mining)
- Monitors for the use of disabled SAAS accounts & services, as well as unauthorized querying of Active Directory
- Helps SOC teams monitor new vectors and gather forensics from remote EPs that may behave differently than what the SOC is used to seeing
- Creates detection campaigns that reference cloud administration activities and alerts in the event a remote worker's EP attempts to gain administrative access to cloud resources.

MAN-IN-THE-MIDDLE 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 decoys that 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.
- 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.

> Intelligence gathered from the Attivo solution can be leveraged by internal hunt teams for broader validation and assessment of potential vulnerabilities that exist in the enterprise.

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 ThreatStrike® solution to engage, trap, and slow down the attack.
- Misdirects ransomware attacks to deceptive network shares that store deceptive files, slowing and stalling the attack through high-interaction continuous engagement, preventing the encryption process from completing.

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

IDENTIFYING CREDENTIAL VULNERABILITIES AND AVAILABLE ATTACK PATHS

- The 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 on the use of 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. Security teams are provided a detailed report after 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 fast 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.

> 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 critical 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 that are representative of the data and information that an attacker seeks.
- Tracks these deceptive documents which beacon home when they get opened, 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 details around the threat: lateral movement patterns, C&C 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.

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.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership. Learn more: www.attivonetworks.com