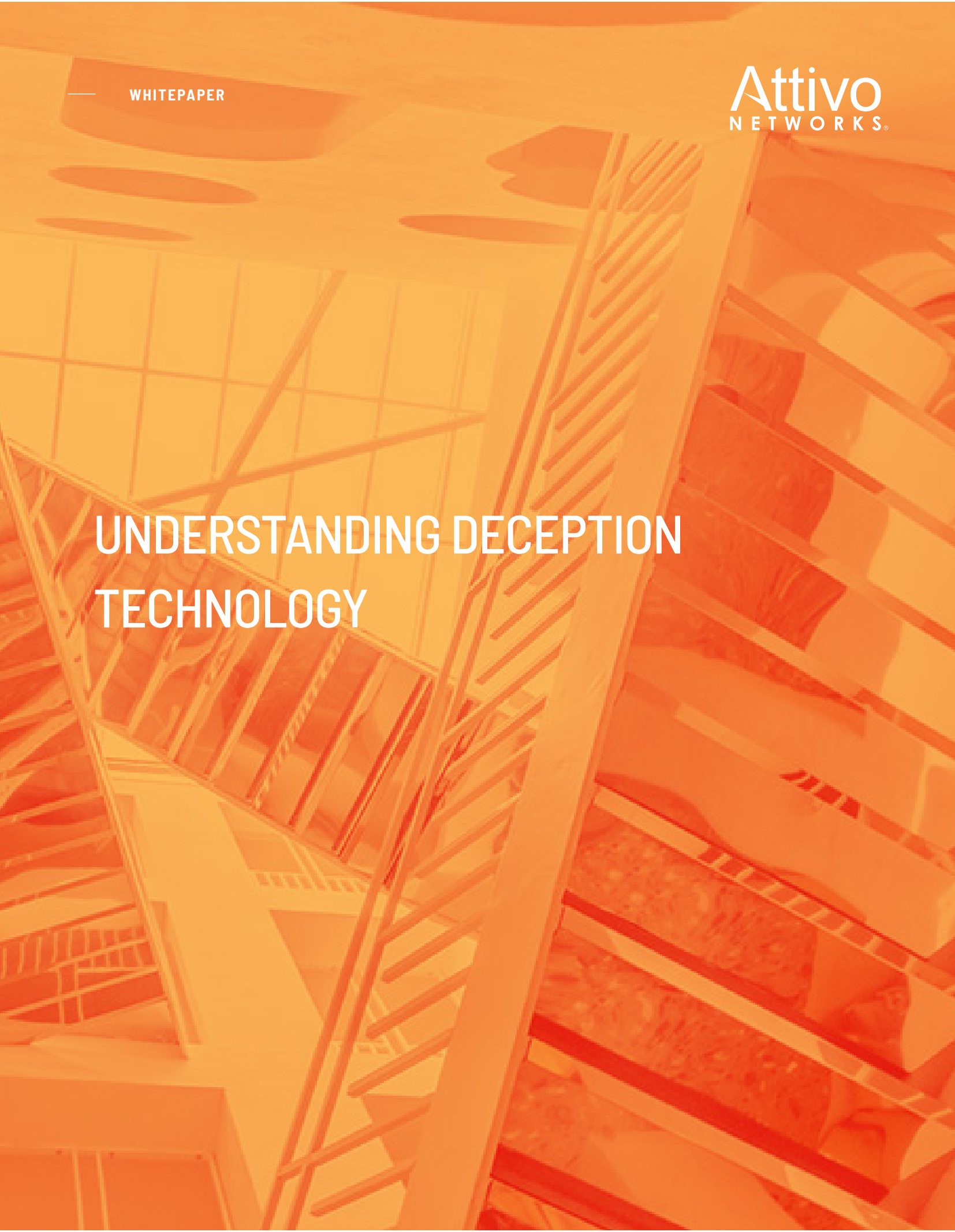
WHITEPAPER

Attivo NETWORKS®

# UNDERSTANDING DECEPTION TECHNOLOGY



With over 700 reported breaches occurring annually, a modern-day comprehensive security defense must be adaptive and requires a combination of prevention, detection, response, and predictive technologies to actively work together. Attackers have proven time and again their ability to penetrate defenses. Detecting threats early inside the environment is critical to prevent the exfiltration of data, sensitive personal information, or potential harm to an organization's critical infrastructure or brand and reputation.

This document explains the role deception has historically played in attack and defense as well as highlights why it has become a necessary part of a modern cybersecurity stack. Deception technology is becoming a core necessity in any security architecture.

## WHAT IS DECEPTION?

Deception has been part of the fabric of attack and defense for as long as human beings have been recording their actions. From Sun Tzu to Niccolò Machiavelli, deception has long been a critical element any commander would use to win. Deception was integral in ensuring the success of the Normandy invasion by the Allies in WWII. Operation Quicksilver diverted German forces away from the actual invasion site to Pas-de-Calais. The Axis forces diverted whole battallions north away from Normandy to defend against decoy military forces, reducing their defenses where the Allies intended to land.

Similarly, the "Empty Fort Strategy," one of the "Thirty-Six Stratagems," has been successfully employed to distract and defeat attackers numerous times in ancient China. In The Romance of the Three Kingdoms, Zhuge Liang was trapped in a city with a small force while a more numerous army led by Sima Yi approached. He ordered all the gates to be opened and told his men to sweep and dust the ground. Sima Yi knew Zhuge Liang's reputation as a very cautious and prudent commander. Seeing this apparent lack of concern displayed by Zhuge Liang, Sima Yi feared an ambush and withdrew his troops. This story, while likely embellished for dramatic purposes, shows how valuable deception can be in creating confusion and doubt in an adversary.


The ability to misdirect an attacker, to make them believe one is strong where one may be weak and to display false weakness to

lure them in, is invaluable. If an attacker falls for a deceptive strategy and engages, they become hesitant about doing so going forward for fear of being deceived again. Moreover, it causes them to reveal their strengths and tactics in a manner that causes little risk and harm to the defender.

## WHAT DOES DECEPTION MEAN FOR CYBERSECURITY?

Deception is a valuable but, unfortunately, sometimes overlooked tool for anyone building a cybersecurity infrastructure. The reality of the modern world, with its billions of networked devices and millions of applications, is that static defenses are not sufficient. Consider the following quote from world-renowned hacker and security expert Chris Roberts;

> "What we've been doing has failed! ... **We need to accept the fact that it's impossible to stop adversaries from getting into a network**—it just isn't going to happen. Once you've accepted that, you just have to decide what to do about it. Look at it this way: a home alarm won't stop a burglar from breaking into your house, but if it goes off and scares them away before they can take anything valuable, it's done its job."
>
> – Chris Roberts, Attivo Networks

Adding deception technology changes the game on attackers. With deceptive assets mixed into the environment, the attacker must now be correct 100% of the time through every stage of the attack cycle. A single scan or access attempt against a deceptive asset or object, and attackers trip an alarm through the whole network. The core concept of modern deception technology is that no one should ever interact with any of the deceptive assets. Therefore, any detection indicates suspicious or malicious activity. Making the decoy assets indistinguishable from production assets makes it extremely difficult for an attacker to avoid exposure.

## HOW DOES ATTIVO BRING DECEPTION TO CYBERSECURITY?

Deception platforms are designed to detect and analyze internal attack activity, including discovery scans, credential theft, man-in-the-middle activity, mapped share access, and Active Directory (AD) reconnaissance. The Attivo Networks ThreatDefend platform uses fully customizable virtual machines as decoys to mimic production assets ranging from Windows and Linux servers to network infrastructure to IoT and SCADA devices, projecting them throughout the network.

To an attacker looking for critical systems, credentials, drive share, and data, these decoys appear as tantalizing targets that are indistinguishable from production assets and worthy of exploration.

The ThreatStrike Endpoint solution also allows organizations to create a variety of deceptive credentials, fake objects such as SSH tokens, cloud platform keys, and SMB shares to place on real production systems that lead attackers back to the decoys. The hidden SMB mapped shares act as lures for ransomware seeking to spread via network drives, stalling the malware by continuously feeding it data while throttling the connection to give security teams time to respond to it. Additionally, the ADSecure module looks for unauthorized AD queries and intercepts the results, hiding legitimate credentials and inserting deceptive lures. The solution also makes any production endpoint a decoy that redirects attacks targeting ports and services into the deception environment for engagement, essentially locking down endpoints from attacker lateral movement.

> Attackers on average infiltrate a network within less than five hours, and within fifteen hours they can exfiltrate data.

When an attacker engages with the deception environment, the ThreatDefend Platform immediately alerts on the activity for security teams to quickly identify the source of the attack for automated incident response. As the attacker accesses a decoy directly or engages with a webpage or SMB share hosted on it, the platform logs all relevant information about the activity and displays it to the security team in the dashboard. The platform captures the forensic data providing information for incident response and remediation actions, including recording all command and control (C2) traffic and conducting memory forensics analysis. For the security team, this is a wealth of organization-specific threat intelligence they can use to improve their defenses further.

The ThreatDirect solution provides for scaling across remote offices, branch offices, micro-segmented networks, and cloud environments. The forwarder is available as a VM, endpoint module, or containerized application, and can run on endpoints, servers, VM environments, or routers and switches that contain a hypervisor or can run container applications. This deployment flexibility benefits organizations with extensive and varied network infrastructures.

The TheatPath solution identifies credential exposures and misconfigurations on endpoints that allow attackers to move laterally across the network from system to system. The solution maps out the connections, identifies first, second, and third-order hops, and indexes the data for searching and analysis. By identifying such vulnerabilities, the security team can clean the stored credentials, fix the misconfigured policies, or add ThreatStrike credentials to further defend endpoints.

The DecoyDocs solution creates deceptive files with an embedded beaconing function that notifies security teams of improper access. When alerting within the network, the solution provides the full details of the host accessing it. If the attacker exfiltrates the document, it will beacon home with the geolocation of every IP address that opens it. This capability gives security teams knowledge of what attackers are targeting.

With the ThreadOps solution, the ThreatDefend platform leverages the many native partner integrations built into the platform to create repeatable playbooks for a consistent and automated incident response process. This function removes complexity and accelerates incident response and eases workloads for security teams that face resource challenges.

Overall, the ThreatDefend platform provides comprehensive threat deception solution available that scales across any size network, regardless of location, and accelerates incident response while providing critical adversary intelligence to improve defenses.

## WHY IS DECEPTION NECESSARY FOR SECURITY TEAMS?

Traditional prevention postures have proven inadequate as attackers have repeatedly demonstrated their ability to bypass perimeter defenses. Research reports an average dwell time of 78 days, according to the FireEye 2018 M-Trends report. According to Nuix, attackers on average infiltrate a network within less than five hours, and within fifteen hours they can exfiltrate data. From a 2019 Crowdstrike study, attackers take an average of 4.5 hours to break out of a system, but sophisticated and advanced attackers accomplish the feat in less than nineteen minutes. Carbon Black, in its 2019 global threat report, indicated that 60% of attacks involve a lateral movement component. In other words, not only can attackers break into a network quickly, but they can also move around rapidly once they do, making them extremely difficult to stop.

> Attackers take an average of 4.5 hours to break out of a system.

The ThreatDefend platform comes as a much-needed detection tool for today's modern security teams of any size. Current tools such as SIEMs provide large volumes of data that require dedicated time and resources to separate false positives from actual security incidents. Signature-based systems such as anti-virus and endpoint monitoring tools can easily miss zero-day or sophisticated attacks. Behavioral analytics methods generate alert fatigue and will routinely overlook advanced attackers and insider threats since human attackers are not fully computable objects. The ThreatDefend platform allows security teams to focus on finding and responding to attacks, as well as giving them visibility into new and complex attacks, by turning the entire IT environment into a trap. Additionally, the high fidelity and low volume of alerts allow the system to be run with low maintenance and overhead while providing incredibly accurate and relevant threat data.

Deception technology is straightforward and quick to deploy. Within hours of installing an Attivo BOTSink appliance, security teams can project thousands of decoys through their network providing deception and early alerting. With a proper "crawl, walk, run" strategy, this can mature into a fully integrated and authentic deception layer that will fool and catch even the most careful and mature threats.

## SUMMARY

The Attivo ThreatDefend Platform plays a critical role in empowering an adaptive defense with real-time detection of threats, attack vulnerability assessments, attack forensic analysis, and the integrations to dramatically accelerate incident response. High fidelity threat information provided by Attivo reduces alert fatigue among security teams. Technology integrations with partners serve as a force multiplier effect, which improves existing technologies, process, and resource productivity, making them better and ultimately reducing the time to detect and remediate an exploit or malicious threat actor. Working hand-in-hand with many partners, Attivo Networks continues to expand its platform and 3rd-party integrations to deliver the fastest detection and incident response to stop attackers in their tracks.

## 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 90 awards for its technology innovation and leadership.

www.attivonetworks.com