

INTERCEPTING LIVE ATTACKS WITH THE ATTIVO NETWORKS ADSECURE SOLUTION

OVERVIEW

Active Directory (AD) is a Microsoft product that consists of several services to administer permissions and access to networked resources on a Windows Network. By design, AD will readily exchange information with any member system it manages. Attackers can also leverage this access to extract information on the entire domain quickly. Security teams may not realize that attacks on AD are occurring because the activities will appear as if AD is providing the data to a member system as part of normal operations. Attackers can extract user accounts, system accounts, and trusted domain information from any compromised member system on the AD domain to find privileged accounts, overlapping security rights that provide elevated privileges, or significant systems to target as part of their attacks. These can include trusted domain controllers, essential servers, or databases with critical data. Detection of AD attacks can be difficult because organizations must typically manually defend against such activities. The ADSecure solution that is part of the Attivo Networks ThreatDefend® Detection Platform provides a new approach to preventing cyber criminals from successfully reaching and compromising AD.

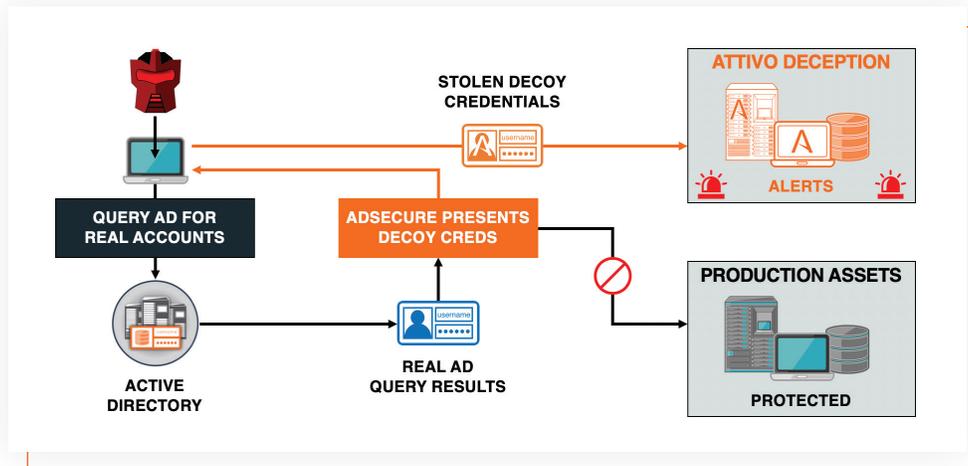
THE ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend Detection and Response platform uses deception technology to accurately and efficiently detect and derail the lateral movement of attacks across all primary attack vectors. With the Attivo detection fabric interwoven throughout the entire network infrastructure, from user segments, data centers, cloud, specialized networks, or remote locations, organizations create a virtual layer of landmines and lures designed to confuse, slow down and misdirect an attacker. The system alerts when an attacker engages with a decoy through network scans, stolen deceptive credentials, or other methods.

ADSECURE

The ADSecure solution is a modular component of the ThreatDefend platform, designed to defend against AD attacker data gathering. It augments the existing AD defense capabilities the platform already offers such as deceptive credentials based on production accounts and decoy AD infrastructure servers. ADSecure sits at every endpoint and responds to queries attempting to harvest AD data from an unauthorized system. The solution inserts deceptions to

counter the AD attack by replying with deceptive data, hiding the privileged credentials, and altering real credentials values. This interception includes engagement of the activities into the deception environment where the system safely studies the attack and collects threat intelligence.



With ADSecure, organizations can efficiently intercept advanced attacks (APTs) and contain them automatically at the endpoint. With the engagement of activities into the deception environment, the ThreatDefend platform can safely study the attack and gather Tactics, Techniques, and Procedures (TTPs), along with company-specific threat intelligence.

The solution can be purchased standalone or as part of the ThreatDefend Endpoint Suite.

Sign up for free trial. Link: <https://attivonetworks.com/adsecure-trial-sign-up/>

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications, MITRE Shield, and its capabilities are tightly aligned to the MITRE ATT&CK Framework. Attivo has won over 130 awards for its technology innovation and leadership.

www.attivonetworks.com.