PARTNER BRIEF

Attivo NETWORKS

PROTECTING MICROSOFT MANAGED ACTIVE DIRECTORY ON THE GOOGLE CLOUD PLATFORM 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. Google offers organizations a highly available, hardened Managed Service for AD on its Google Cloud Platform. Organizations can deploy AD on the Google Cloud Platform as a managed service. 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 for successfully reaching and compromising AD.

MANAGED SERVICE FOR AD ON GOOGLE CLOUD

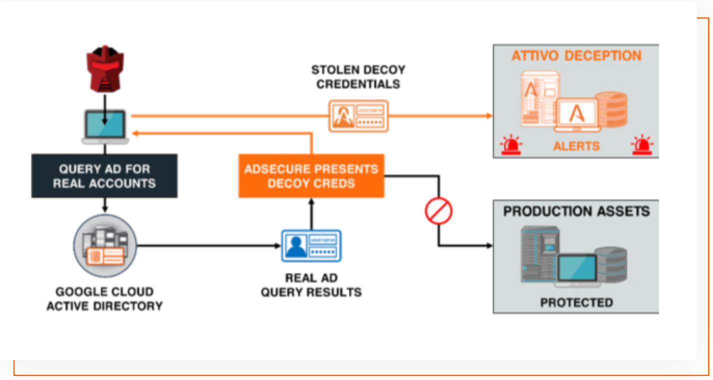
Managed Service for Microsoft Active Directory (AD) is Google Cloud service running actual Microsoft AD that enables an organization to manage its cloud-based AD-dependent workloads, automate AD server maintenance and security configuration, and connect its on-premises AD domain to the cloud. The AD Service is compatible with AD-dependent applications, and IT and security teams can use built-in Active Directory features and standard AD administration tools. The service is virtually maintenance-free, highly available, automatically patched, configured with secure defaults, and protected by appropriate network firewall rule. An organization can connect an on-premises Active Directory domain to Google Cloud or deploy a standalone domain in multiple regions for its cloud-based workloads, including VMs and applications. The managed Microsoft AD service offers flexibility, scalability, and availability for any organization to reduce workloads and increase efficiency, allowing the IT and security teams to focus on higher-value projects.

While the Managed AD service gets patches and secure policies as part of a secure deployment, attackers that compromise an internal endpoint can use various tools such to extract data from the AD controllers to advance their attacks. This is where the ADSecure solution can fill the gap.

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, and is compatible with the Google Managed AD service. It augments the existing AD defense capabilities the ThreatDefend 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 Detection Net Suite.

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.

www.attivonetworks.com

ABOUT GOOGLE CLOUD PLATFORM

Google Cloud Platform (GCP), offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail and YouTube. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning.

cloud.google.com