ATTIVO NETWORKS® THREAT DECEPTION FOR EARLY CLOUD ATTACK DETECTION

Attivo Networks® has created solutions for multi-cloud environments, including AWS, Azure, Google Cloud, OpenStack, and Oracle Cloud, to provide advanced real-time in-the-cloud threat detection with flexible and automated deployments across any number of Virtual Private Clouds (VPCs). Leveraging the Attivo ThreatDefend® Platform, customers can detect and defend against advanced threats in all of these cloud environments.

HIGHLIGHTS

- Early visibility and in-network threat detection
- Accurate lateral movement and cloud
- Active Directory Protection
- Data Concealment, Decoy Documents, and Access Denial
- Easy, automated deployment for operational efficiency and scalability

THE CHALLENGE

The cloud has expanded an organization's capabilities, but also its attack surface. Moving to the cloud has its own inherent set of security issues, partly due to the ubiquity of cloud presence and access, and partly from the sharing of security responsibilities. Because cloud environments share computing and resources, traffic between individual virtual systems in the cloud bypasses traditional network monitoring. This lack of visibility leads to a detection gap that attackers can exploit to hijack cloud resources or access confidential information. Organizations can deploy Cloud Access Security Brokers (CASB), Cloud Work Protection Platforms (CWPP), and Cloud Security Posture Management (CWPP), but there are still gaps in their coverage.

The Attivo ThreatDefend Platform gives customers the ability to detect and defend against advanced threats in AWS, Azure, Google Cloud, OpenStack, and Oracle Cloud, and adds to the coverage afforded by CASB, CWPP, and CSPM. It provides enhanced visibility and control to cloud attack activity, resulting in higher productivity and efficiencies in security management, ultimately reducing the organization's risk of breaches and data loss

ATTIVO NETWORKS THREATDEFEND PLATFORM

The ThreatDefend platform is recognized as the industry's most comprehensive in-network detection solution, and provides a detection fabric for cloud, network, endpoint, application, data/database, and Active Directory and is highly effective in detecting threats from virtually all vectors such as APTs, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, port knocking and more. These deceptions can deploy within all types of networks, including endpoints, user networks, server, data center, ROBO, cloud, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications.

The ThreatDefend Deception Platform creates an active defense against cyber threats. It includes the Attivo BOTsink® deception servers for decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration

playbooks, and DecoyDocs to track exfiltrated data; and the Endpoint Detection Net suite, composed of the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, and ADSecure for Active Directory defense . The EDN suite also adds the Deflect function to detect and deny discovery and lateral movement activities and the DataCloak function, which hides and denies access to local files and folders, removable storage, and network or cloud mapped shares. The ThreatDirect deception forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) for BOTsink and the Endpoint Detection Manager for EDN deployments add enterprise-wide deception fabric management.

THE ATTIVO NETWORKS SOLUTION FOR CLOUD DEPLOYMENTS

The ThreatDefend Platform can operate in the cloud as it does on-premises with no loss of functionality to detect threats and misdirect attacks. The solution can deploy decoys or ThreatDirect® forwarders across any number of VPCs, providing network deception capabilities to detect lateral movement and reconnaissance. The ThreatDefend cloud capabilities can detect east-west traffic and provide engagement-based alerts on threats inside any cloud infrastructure, whether public, private, or hybrid.

The Attivo BOTsink server easily scales to deploy any number of decoys in the cloud and can even implement VM images as decoys, allowing for greater deception authenticity. When the BOTsink solution detects attacker lateral movement activity in the VPC, it generates a high-fidelity alert on the Threat Intelligence Dashboard while simultaneously engaging the attacker, diverting threats from production cloud systems, and providing full forensics on the activity. Additionally, the solution alerts on credential theft and reuse and cloud application activity, while diverting attackers from cloud production assets and data to authentic deception decoys.

The ThreatDefend Platform BOTsink server and Central Manager are available as native machine images for AWS, Azure, Google Cloud, OpenStack, and Oracle Cloud. They are also available as a ThreatDirect forwarder that redirects attacker traffic to a central BOTsink solution.

The Attivo Endpoint Detection Net (EDN) ThreatStrike endpoint suite detects attempts to steal and reuse cloud credentials. The solution can create wide-ranging cloud bait to install on endpoints, such as deceptive logins, access keys, containers, database tables, storage buckets, and database connectors, depending on the platform.

SUMMARY

The Attivo ThreatDefend Platform plays a critical role in an active defense strategy by providing in-network threat detection and native integrations to dramatically accelerate incident response, especially for businesses moving to the cloud. Attivo Networks offers cloud customers a significant improvement in reducing attacker dwell time, changing the asymmetry of an attack, and improving incident response. By automating the deception deployment and providing full-VPC visibility of attacker reconnaissance, lateral movement, and cloud credential theft, organizations benefit from early detection for active attacks and accelerated incident responses.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory, and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.