PARTNER BRIEF

ATTIVO NETWORKS® THREAT DECEPTION FOR AWS EARLY CLOUD ATTACK DETECTION

Attivo Networks® has created solutions for AWS 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™ Deception and Response Platform, customers can detect and defend against advanced threats in AWS.

HIGHLIGHTS

- Early visibility and in-network threat detection
- Accurate lateral movement and AWS credential theft detection
- 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 inherently has its own 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.

Leveraging the Attivo Networks ThreatDefend™ Deception and Response Platform, customers can detect and defend against advanced threats in AWS. The ThreatDefend Platform provides enhanced visibility and control, resulting in higher productivity and efficiencies in security management, ultimately reducing the organization's risk of breaches and data loss.

THE ATTIVO NETWORKS SOLUTION FOR AWS 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 is available as a native image for AWS and can deploy BOTsink® engagement servers and ThreatStrike™ deception credentials within the cloud for full VPC threat visibility. It provides alerting for threats in east-west traffic inside any cloud infrastructure, whether public, private, or hybrid. 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 only alerts on attacker engagement and supports full automated deployment using AWS templates, making the solution simple to deploy and operationally efficient.

The Attivo BOTsink solution deploys as a native AMI within AWS, or as a ThreatDirect forwarder that redirects attacker traffic to a central hardware or virtual BOTsink solution. The cloud BOTsink solution can deploy any number of decoys and can even take existing VM images and deploy them as decoys, allowing for greater deception authenticity.

When the BOTsink solution detects attacker lateral movement activity in the VPC, it generates an alert on the Threat Intelligence Dashboard while engaging with the attacker, diverting attacks from production cloud systems while providing full forensics on the activity.

The ThreatStrike endpoint suite is designed to detect attempts to steal and reuse AWS credentials, and can create extensive AWS bait to install on endpoints, such as deceptive logins, access keys, containers, database tables, and database connectors. 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.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, and insider threats.

The ThreatDefend Deception and Response Platform is a modular solution comprised of Attivo BOTsink® engagement servers, decoys, and deceptions, the ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM). Collectively, these create a comprehensive early detection and active defense against modern cyber threats.

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 AWS 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 an early detection for active attacks and accelerated incident responses.

ABOUT ATTIVO NETWORKS

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT AWS

AWS provides building blocks that you can assemble quickly to support virtually any workload. With AWS, you'll find a complete set of highly available services that are designed to work together to build sophisticated scalable applications. AWS is trusted by the largest enterprises and the hottest start-ups to power a wide variety of workloads, including web and mobile applications, game development, data processing and warehousing, storage, archive, and many others.

aws.amazon.com