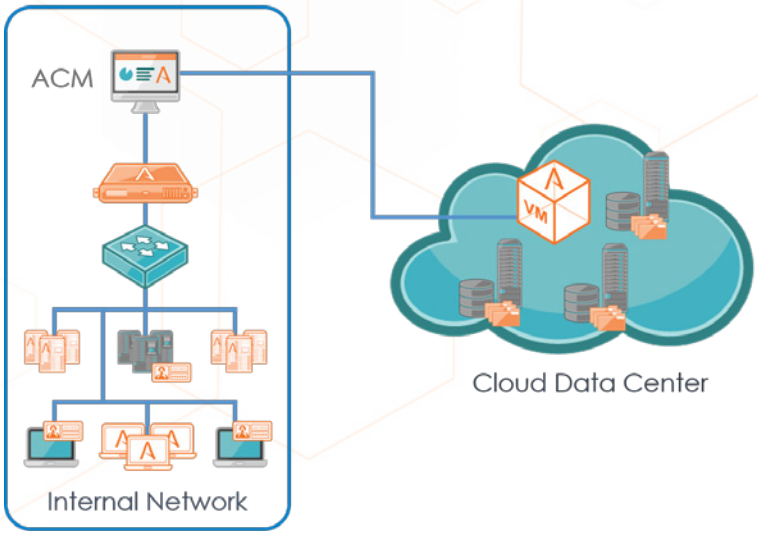
ThreatDefend™ Deception Platform for Enhanced Cloud Security

The public cloud services market is estimated by Gartner, Inc. to reach $246.8B in 2017, which represents an 18% growth over 2016. The benefits of on-demand, scalable infrastructure and the rapid shift to cloud-based applications are driving this growth and are presenting a new set of security challenges. Cloud providers offer a range of security controls to help protect the confidentiality, integrity, and availability of applications, data, and devices. However, within their shared security modules, they stop short of protecting operating systems and data, and do not automatically provide detection solutions for attacker lateral movements. The same threats that plague on-premises devices and systems are just as problematic in the cloud and are often compounded by gaps that arise from mistakes and miscommunications that leave backdoors for sophisticated advanced persistent threats. AWS, Azure, and OpenStack customers can, however, proactively prepare for and address these security gaps by deploying active deception technologies in their cloud infrastructure. Deception-based detection is designed for datacenter scalability and will set attractive and enticing traps and bait for attackers, deceiving them into revealing themselves.

Challenges

On top of "traditional" security threats that cloud infrastructures face, they also have the drawback of being particularly juicy targets for attackers since organizations store an exhaustive amount of data in the cloud. A recent survey of over 2,000 cloud security professionals stated that 72% of organizations store sensitive data in the cloud. Security teams face difficulties mitigating the risk of a breach of sensitive data in the cloud as they lose control over the data as the physical IT bonds are broken. Moreover, security teams are forced to adopt new strategies as they are potentially required to work with a variety of new tools across multiple different platforms.



In addition to increased responsibility and workload, security teams must grapple with the industry-wide cybersecurity skills shortage. Almost half of all organizations report that the cybersecurity skills shortage has slowed their usage and adoption of cloud services.

To address these challenges, organizations need security tools that not only provide extensive visibility into their cloud environment but also do not require extensive security teams or additional headcount to operate.

Cloud Security

By nature, a cloud environment is difficult to secure. Security challenges stem from shared security models, unknown security controls, and complexity associated with high volumes of traffic. The unsegmented nature of the cloud, the lack of widespread encryption for data stored therein, and the flat nature of cloud instances means that an attacker who gets access to an organization's cloud environment is often free to range across the entire instance, usually undetected. Access is usually from a trusted network location, often from inside the organization's own network infrastructure through a compromised system. Without a means to detect such access accurately, the attacker can steal data, use resources in the instance, or even conduct ransom attacks by encrypting data stored in the cloud. The ThreatDefend™ Deception and Response Platform is ideally situated to detect such attackers before they can execute their plans, regardless of whether the malicious activity is in the physical datacenter or in the cloud.

ThreatDefend Deception Technology

The Attivo ThreatDefend Detection Platform is an advanced class of deception-based threat detection that ups the game against attackers. The ThreatDefend platform is recognized for its comprehensive network and endpoint-based deception, which turns user networks, data centers, cloud, remote offices, and specialty environments such as IOT, ICS-SCADA, and POS systems into a "hall of mirrors" environment based on traps, lures, and breadcrumbs that will confuse, misdirect, and reveal the presence of attackers. The solution is designed for a scalable, adaptive defense, which starts with deception-based detection of in-network threats and adds in automated attack analysis, forensic reporting, and 3rd party integrations (Firewall, NAC, end-point, SIEM) to accelerate incident response (block, quarantine, threat hunt). Visibility tools empower organizations to proactively strengthen overall security defenses by showing exposed attack paths and attacker movement in time-lapsed replay.

The ThreatDefend Platform is comprised of Attivo BOTsink engagement servers, decoys, and deceptions and the Multi- Correlation Detection Engine (MCDE), the ThreatStrike end-point deception suite, the Attivo Central Manager (ACM), ThreatPath, ThreatDefend, and ThreatOps, which together create a comprehensive early detection and continuous threat management defense against today's advanced threat actors.

The ThreatDefend Detection and Response Platform is designed to integrate seamlessly with AWS, OpenStack, and Azure deployments and to scale with an organization's cloud needs. An organization can deploy deception to the cloud, either by deploying a virtual cloud BOTsink in their AWS, OpenStack, or Azure instance, or by utilizing the ThreatDefend solution in conjunction with a BOTsink deployed in their physical datacenter. This flexibility in deployment gives organizations options with their deception deployment that best meets their needs. A properly deployed set of dynamic deception servers can provide a new level of protection not available from cloud provider's security measures alone.

Why Attivo Deception

- Deployment is not inline and doesn't impact traffic or increase compute needs
- Scalable for both private and public clouds
- Attack Threat Analysis Engine automates attack analysis and provides forensic reports
- Attack time-lapsed replay provides insight into network changes and attack lateral movement
- Central ACM manager provides management dashboard and aggregation of threat information across deception devices

Conclusion

As organizations continue to grow their cloud infrastructure, it is critical for security teams to have visibility across the entire cloud in order to close security gaps and decrease the detection deficit. The ThreatDefend Detection and Response Platform allows organizations to fully scale deception in the cloud for in-network threat detection of all threat vectors including advanced threats, Man-in-the-Middle, ransomware, stolen credential, and insider threats. Implementation of deception technology provides organizations with a new level of protection that is not available through cloud-provided security measures. By gaining network threat visibility through the ThreatDefend platform, security teams can be confident that the new security challenges that come with the increased use of cloud infrastructure can be significantly mitigated.

About Attivo Networks

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. www.attivonetworks.com