Attivo NETWORKS

# ENHANCING AWS CLOUD SECURITY WITH THE ATTIVO NETWORKS THREATDEFEND PLATFORM

## INTRODUCTION

As businesses adopt cloud computing at an increasing pace, they realize the benefits of on-demand, scalable infrastructure. They also find themselves relieved of some security concerns, such as managing data center physical security. Unfortunately, the same threats that plague on-premises devices and systems are just as problematic in the cloud. AWS provides a range of security controls to protect the confidentiality, integrity, and availability of applications, data, and devices. While these controls are necessary, sophisticated advanced threat actors can find ways to evade them. AWS customers can, however, enhance the overall level of security protections by deploying an informed defense in their AWS infrastructure.

New security controls, such as Cloud Access Security Brokers (CASB), Cloud Workload Protection Platforms (CWPP), and Cloud Security Posture Management (CSPM), add to native AWS security controls and best practices. However, advanced attackers still find ways to access the cloud environment and compromise data. The Attivo Networks ThreatDefend® platform complements other security controls and measures, especially regarding protecting against sophisticated attackers targeting the cloud.

## CLOUD AND AWS SECURITY CONTROLS AND BEST PRACTICES

AWS security controls range from broad measures, such as virtual private clouds and network segments, to fine-grained access controls on storage and compute resources. Cloud administrators and information security professionals select and combine them appropriately for their applications and business requirements. Commonly examples include:

- Virtual Private Clouds (VPC), which isolate AWS resources in a virtual data center
- Network segments, for separating network traffic
- Security groups, to control the ingress and egress flow of traffic to servers
- Network access control lists (NACLs), to limit access to resources within network segments
- Identity management, for granting privileges to users and groups
- Configuration controls, to help ensure deployed devices meet configuration requirements

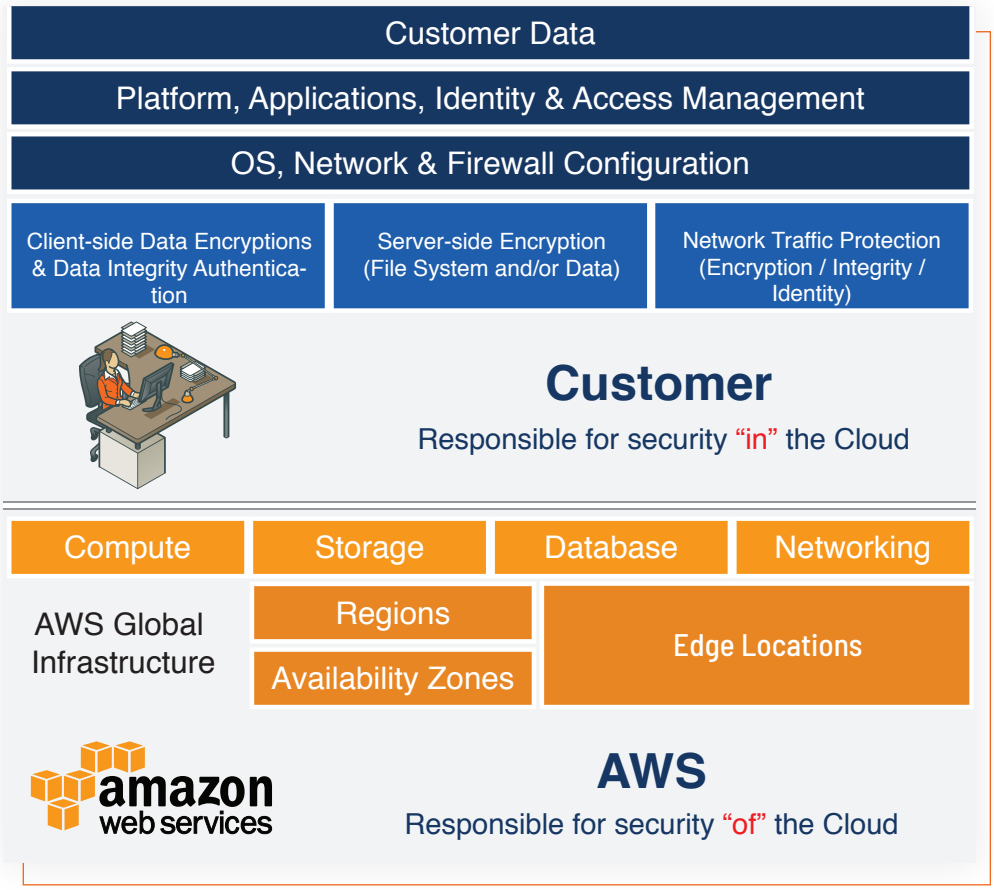



*Figure 1. Amazon Shared Security Model*

## CASB, CSPM, AND CWPP

CASB, CWPP, and CSPM are new cloud security solutions that address public cloud environments.

A CASB is a security policy enforcement solution between cloud service consumers and providers to enforce access and control policies. A CASB offers the following functions:

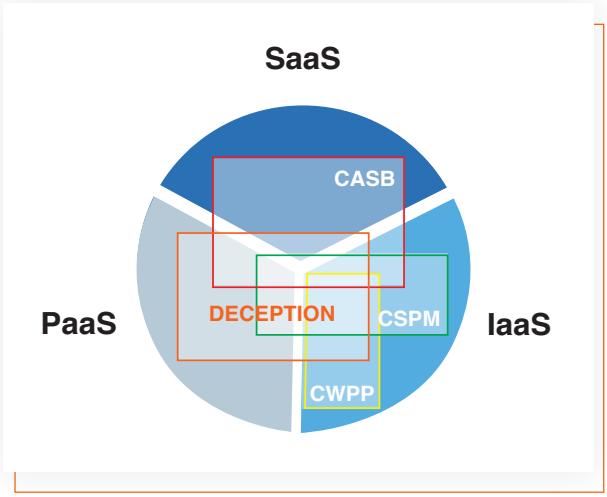
- Control access to cloud services
- Consolidated view of all utilized cloud services
- Create and apply centralized control policies across cloud
  - Deployed either on-premises or via cloud-based security policy enforcement points
  - Interject enterprise security policies as the cloud-based resources are accessed
- Consolidate multiple types of security policy enforcement
  - authentication
  - single-sign-on/authorization
  - credential mapping
  - device profiling
  - encryption/tokenization
  - logging
  - alerting/malware detection/prevention

CWPPs are software platforms designed for monitoring and protecting cloud workloads. The following functions are characteristic of CWPPs:

- Workloads-centric security
  - ➢ Abstraction of workload
    - Physical Machines
    - Virtual Machines
    - Containers
    - Serverless & Native
    - Location independent
- Multi-cloud
- Hybrid/ Datacenter
- Dynamic environment protection
- Consistent visibility and control from a single console
- Protection for multi-cloud/hybrid cloud architectures
  - ➢ Hardening
  - ➢ Vulnerability management
  - ➢ Host-based segmentation
  - ➢ System integrity monitoring
  - ➢ Application whitelisting

CSPM continuously checks for, and alerts on, compliance of cloud platform accounts and cleans the cloud environment of any misconfigurations that increase risk. CSPM has the following properties:

- Centrally manages the security posture of all cloud assets
- Focuses on security assessment and compliance
- Provides a unified view across multi-cloud environments
- Encompasses tools and best practices for:
  - ➢ DevOps and DevSecOps integrations
  - ➢ Incident response
  - ➢ Compliance assessment
  - ➢ Operational monitoring
  - ➢ Risk identification and visualization



Organizations are also deploying deception and concealment technologies for an increasingly important detection solution that augments these security controls with in-network threat visibility and detection of policy violations of insiders and suppliers. Deception and concealment technologies offer the following capabilities:

- East-west traffic detection
- Obfuscating real assets with deceptive serverless functions, containers, storage buckets, and services
- Hiding and denying access to files, folders, cloud, and network mapped shares
- Detection of credential theft: Cloud, SaaS, Local Admin
- Prevention of cloud-based Active Directory (AD) enumeration and decoy
- Information sharing with platforms like AWS CloudWatch and CloudTrail

## THREAT DETECTION AND PREVENTION FOR AWS WITH THE THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend platform uses deception and concealment technologies to create a detection fabric that deploys authentic-looking decoy assets on the network, endpoints, and AD, coupled with hiding and denying access to essential data and accounts.

As attackers attempt to move from the initially compromised system, the deception and concealment technologies detect and derail their discovery, lateral movement, and privilege escalation activities. Attackers will attempt to steal credentials, access local files, and query AD for critical accounts and objects. The concealment technology hides the sensitive local files and privileged AD account and objects while the deceptive credentials lead the attackers to the full VM decoys for engagement. In other words, the attacker cannot steal or encrypt files they cannot find.

The platform detects illicit activity early in the attack cycle. It actively engages attackers by hosting network services on various virtual devices, placing lures and breadcrumbs on endpoints, and replacing AD query results with fake information that leads to its engagement servers. For example, an attacker can steal decoy credentials to a decoy cloud share, generating an alert on access. It is important to remember that advanced attackers are, by their nature, highly adaptive, and will use "living-off-the-land" techniques to stay hidden. As attackers unknowingly engage with the decoy environment, it captures all activity as forensic evidence, accelerating investigations and allowing the organization to capture adversary intelligence in the form of Indicators of Compromise (IoCs) and develop Tactics, Techniques, and Procedures (TTPs). This intelligence serves to not only help remediate the existing compromise but to defend against future incursions.

The ThreatDefend platform complements other security controls designed to block malicious activity. While other security controls such as firewalls, proxies, and endpoint security solutions prevent an initial compromise, the ThreatDefend platform detects if the attackers successfully evade the prevention solutions and attempt to move deeper into the network. As attackers move around the AWS VPC, the platform detects when they touch the native cloud technology decoys, giving security teams sufficient early warning to stop the attack.

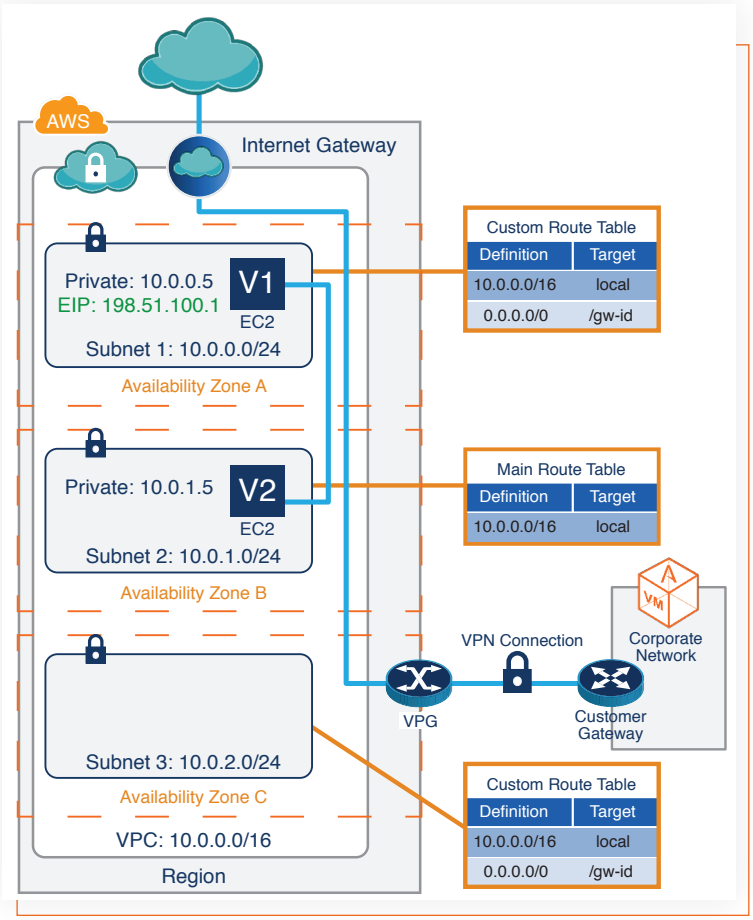
# COMPREHENSIVE COVERAGE AND VISIBILITY

The ThreatDefend platform can deploy as a physical, virtual, or cloud appliance and protects on-premises, cloud, and remote locations. In particular, it offers native cloud deceptive assets, such as AWS S3 buckets, cloud credentials, Lambda functions, decoy EC2 instances, decoy VMs in the cloud, and others.

The Attivo ThreatDefend platform can deploy instances across multiple network segments, availability zones, and regions to provide comprehensive coverage of the AWS infrastructure.

The Attivo ThreatDefend deception platform provides visibility into inside-the-network threats across the enterprise, public, private, and cloud environments. It detects attacks whether the attacker is external, an insider threat, a supplier, contractor, or other trusted third party. The platform offers east-west attack visibility and awareness of lateral attack paths between systems due to stored credentials or misconfigurations, with automatic remediation to reduce the attack surface.

The Attivo Networks ThreatDefend platform includes easy-to-use reporting and analysis tools and a centralized threat intelligence dashboard. These give cloud administrators and information security professionals visibility into activity on their networks. They can assess threats in real-time and collect forensic data needed to shut down attacks and improve the cloud infrastructure's overall security.



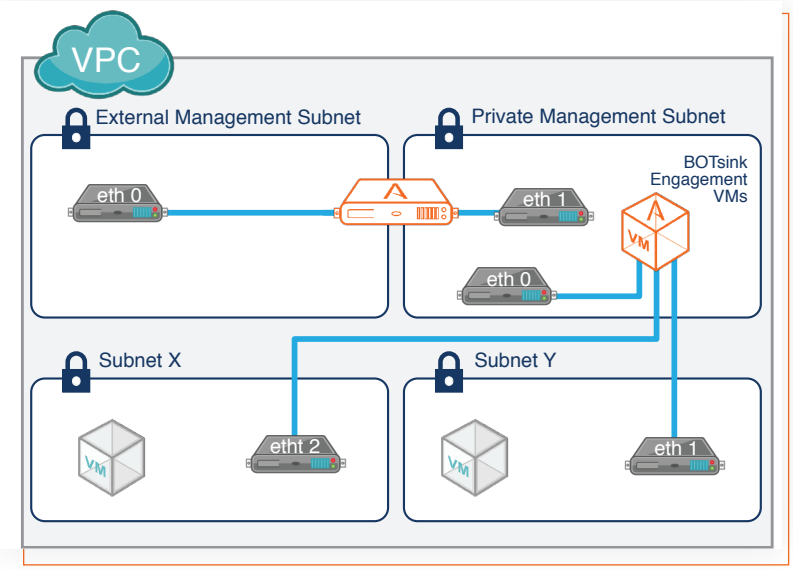




*Figure 4. Attivo BOTsink deception platform detects intrusion, engages the attacker, and generates attack forensics.*

# CONCLUSION

Advanced attackers pose some of the most significant challenges in information security. Traditional prevention security measures for AWS are insufficient to protect against patient, organized, skilled, and determined attackers who find ways to evade such defenses. Fortunately, the ThreatDefend platform offers substantial protections to the increasingly costly consequences such attacks.  To learn more, please visit www.attivonetworks.com

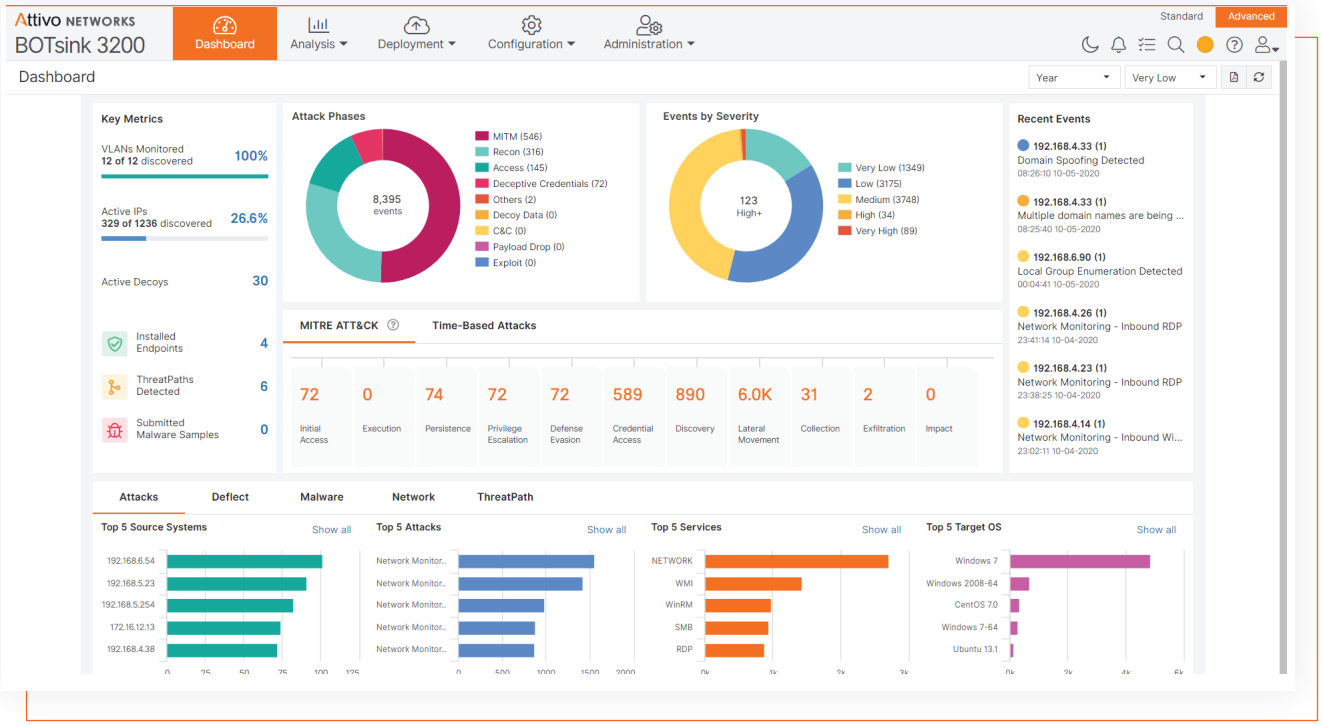



*Figure 5. The Attivo Networks Threat Intelligence Dashboard provides a single point of access to information about the state of deception servers.*

# 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.