WHITEPAPER

Attivo NETWORKS®

# ENHANCING CLOUD SECURITY WITH DECEPTION TECHNOLOGY

# CLOUD THREATS AND THE NEED FOR DECEPTION

According to the June 2019 Symantec Cloud Security Report  and the AWS Cloud Security Report , the greatest cloud threats revolve  around visibility, access controls, and securing data. Deception addresses these concerns directly.

The reports indicate that 82% of companies store data in some form of cloud infrastructure, whether public, private, hybrid, IaaS, or SaaS. However, visibility into these cloud workloads is a problem, with 93% of respondents reporting issues maintaining awareness of the activity in their cloud infrastructure. What's more, about half of the respondents confirmed that their cloud-security resources are inadequate to deal with all incoming alerts. The most prominent security operations challenge that organizations face is visibility into infrastructure security at 44%. This finding is followed by setting consistent security policies across cloud and on-premises environments tying with compliance at 42% each.

The top three cloud security challenges highlighted by cybersecurity professionals in the surveys  are protecting against data loss and leakage at 68%, threats to data privacy at 61%, and breaches of confidentiality at 52%. The greatest single vulnerability to cloud security was cloud platform misconfiguration at 62%, followed by unauthorized access through misuse of employee credentials and improper access controls at 55%, and insecure interfaces/APIs at 52%.

Organizations have actively turned to data encryption at 62%, followed by network encryption and SIEMs at 51%, respectively, to mitigate risk within the cloud. However, they have also adopted deception technology to provide visibility into unauthorized lateral movement, reconnaissance, and access activity into the cloud environment. Deception technology gives organizations threat detection early in the attack cycle, accelerated incident response, and company-specific intelligence. By nature of an engagement-based design, deception also scales to meet the needs of high-volume data environments and doesn't face limitations associated with logs and behavioral monitoring or their corresponding bulk of false positives. Since the technology is engagement-based, the solution only generates alerts when there is direct engagement with the deception environment, and substantiates them with attacker activity data required for prompt incident response.

# CLOUD SECURITY CONTROLS AND BEST PRACTICES

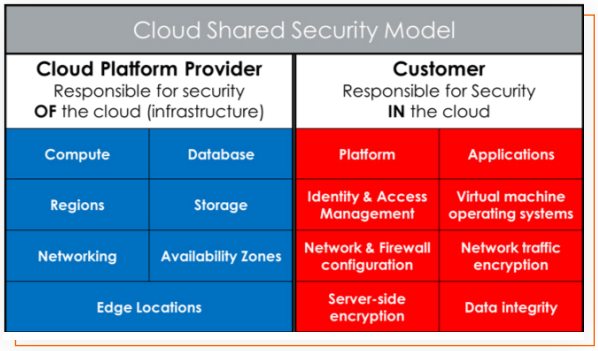
Cloud security controls range from broad measures, such as virtual private clouds and network segments, to fine-grained access controls on storage and compute resources. Cloud administrators and information security professionals select and combine the solutions appropriate for their applications and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

- Virtual clouds, which isolate cloud 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

In addition to these security controls, most cloud providers publish a set of security best practices that include:

- Categorizing and protecting assets in the cloud
- Managing users, groups, and roles
- Maintaining OS-level security
- Securing data
- Monitoring and auditing

For organizations that need additional measures, cloud providers recommend a threat protection layer that could include third-party firewalls, unified threat management systems, data loss prevention systems, and other threat protection measures.



# CASB, CWPP, AND CSPM

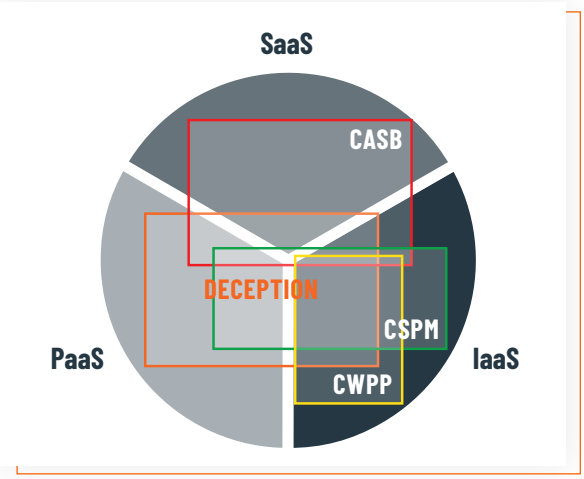
Cloud Access Security Brokers (CASB), Cloud Work Protection Platforms (CWPP), and Cloud Security Posture Management (CSPM) are new cloud security solutions that address public cloud environments.

A CASB is a security policy enforcement solution placed 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 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
        - Independent of location
- Multi-cloud
- Hybrid/Data Center
- 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 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

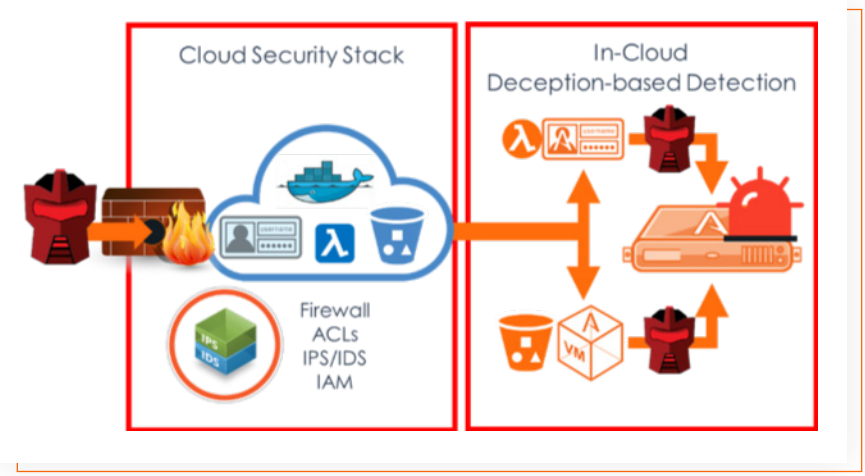
Another solution that organizations are deploying is Deception technology, which is an increasingly important detection solution that augments these security controls with in-network threat visibility and detection of policy violations of insiders and suppliers.

- East-west traffic detection
- Obfuscating real assets with decoy 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 enumeration
- Information sharing with platforms like Cloud Watch and Cloud Trail

## DECEPTION DEFENSES FOR CLOUD ENVIRONMENTS

The introduction of deception technology for cyber defense has added valuable assets that are shifting the advantage to the defenders. Organizations place deceptive decoys, breadcrumbs, and lures throughout the network to make the entire environment a trap, turning it into a virtual minefield to proactively lure and misdirect an in-network attacker into engaging and revealing their presence. Information security teams can go on the offense against attackers, allowing them to detect an attack early in the cycle, hide and deny access to target assets and data, gather company-specific threat intelligence, and derail the attacker before they can do any severe damage. Active Directory and data deceptions are amongst the latest deception innovations and can play a valuable role in feeding false information to attackers, further slowing down and derailing attacks.

Deception platforms are also instrumental in attack analysis, forensics, and remediation. Deception systems automate the correlation of attack data and raise only substantiated alerts backed by details on the attacker's tactics, techniques, and procedures (TTPs). They can also collect accurate Indicators of Compromise (IOC) information to gain enhanced adversary intelligence and build better overall defenses.




Deception platforms can extend onto the endpoints, where attackers frequently leverage stolen credentials or misconfigurations or access to file shares to expand their foothold across the environment. By inserting deceptive credentials and lures onto endpoints, hiding local admin accounts, redirecting attacks on services, or intercepting an attacker's efforts to leverage network authentication systems such as Active Directory, the information security team gains valuable insights and visibility into an attacker's activities while making the task much more complicated for them.

For the cloud, deception platforms offer decoys for technologies and capabilities specific to a virtual cloud infrastructure. With cloud-based decoy assets, deception technology closes gaps that attackers can slip through to compromise cloud-based data and workloads.

## SAMPLE USE CASES FOR DECEPTION IN THE CLOUD

Deception Technology scalably adds in-cloud visibility and awareness to other security controls. Below are some examples of typical use cases where organizations leverage deception to address the gaps in coverage their cloud security controls provide.

## Identity and Access Management

The organization is responsible for controlling access to its cloud environment, often with an Identity and Access Management (IAM) solution that acts as a primary line of defense. However, misconfigured policies, improper Access Control Lists (ACLs), and overlapping permissions can result in privilege escalation attacks that provide attackers access and elevated rights to the cloud. Because the attacker is leveraging production credentials, detecting this type of activity proves challenging.

Deception can defend against such attacks by misdirecting and misinforming attackers and with early detection. By creating and distributing decoy cloud objects (such as access certificates, virtual machines, credentials, containers, storage buckets, or serverless functions) and identifying and monitoring privileged accounts, the organization can recognize successful unauthorized access. Additionally, some deception platforms offer mechanisms that can identify and remediate policy misconfigurations allowing attackers to move laterally across the cloud environment. Whether the attacker leverages a weakness in an ACL, steals fake credentials, or uses monitored production credentials, Deception technology adds a layer of awareness to any IAM solution that closes the gaps attackers exploit for unauthorized access.

## External Attacker, Supplier, or Insider Threat Detection

Organizations have many internal and third-party relationships requiring access to their cloud environments. These relationships provide access that malicious actors can take advantage of to compromise the organization. Whether it is a supplier, temporary worker, contractor, or internal employee who violates a policy, they can use the access the organization has given them to steal data or compromise the cloud environment. Additionally, misconfigurations can allow external attackers access to storage buckets, giving access to internal data that they would normally be denied.

Deception can identify these attempts by deploying decoy systems, data, databases, or documents that detect when internal or third-party bad actors attempt to compromise objects in the cloud. As they misuse their credential authorization to access these objects, the deception platform generates an alert of the malicious or suspicious activity that indicates a policy violation. The organization can respond with evidence-backed administrative actions to address the breach and prevent a recurrence. Insider threats or external attadkers will no longer have unlimited access to the cloud environment without the organization first detecting them

## Security Evaluations – Penetration or Red Team Testing

Organizations evaluate their security programs with penetration tests and Red Team engagements, to meet a regulatory requirement or as part of their security strategy. The cloud environment can make this challenging, as it adds an entirely new set of targets for the evaluators to test. Whether it is an API, virtual machine, ACL, storage bucket, containerized application, or other cloud workload, the evaluators have a wide array of targets to attack.

As with the previous examples, deception can detect these testing activities with the decoy cloud objects it provides. With an extensive blanket of decoy assets such as credentials, access certificates, documents, data, or databases, serverless functions, storage buckets, or virtual machines, the organization has numerous ways to detect the evaluators in their cloud environment while recording all testing activity, adding a safety net that gives them the upper hand in such engagements.

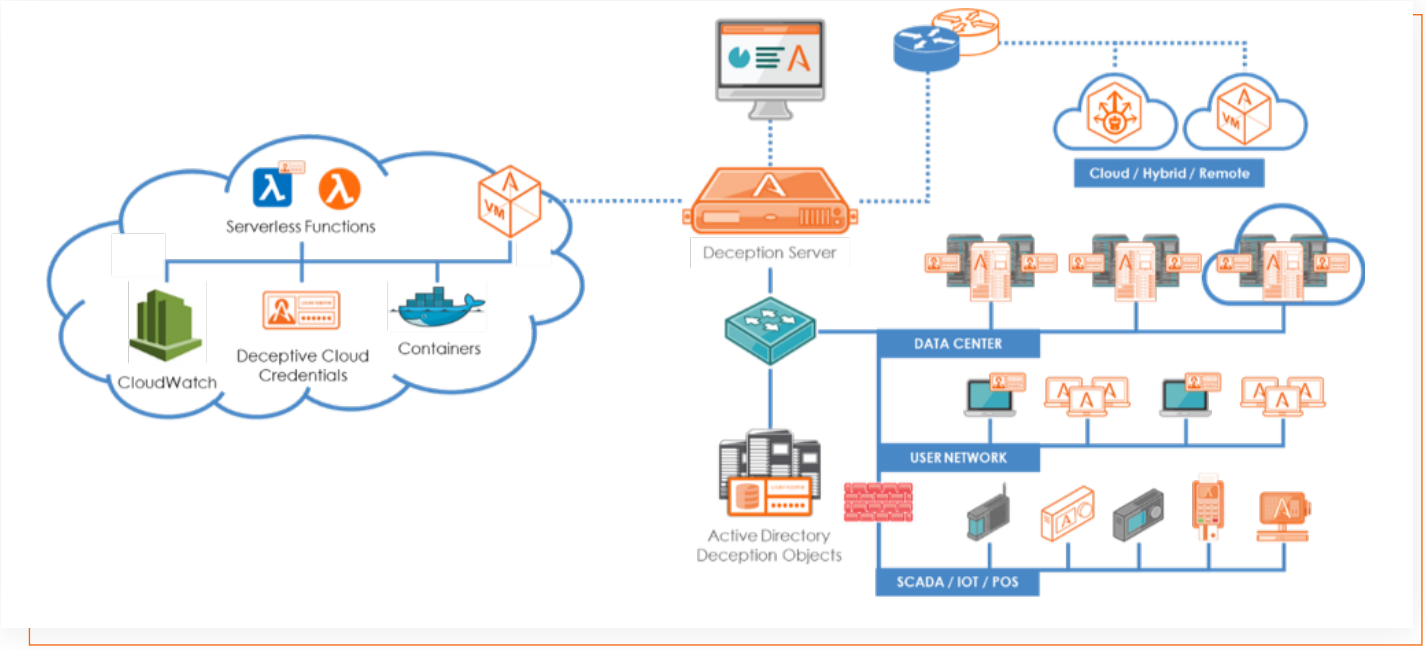
# THE ATTIVO NETWORKS THREATDEFEND® PLATFORM

Deception platforms are designed to identify and analyze internal attack activity, including discovery scans, credential theft, man-in-the-middle activity, mapped share access, and Active Directory (AD) reconnaissance. The Attivo Networks ThreatDefend® platform uses fully customizable virtual machines as decoys to mimic production assets ranging from Windows and Linux servers to network infrastructure to IoT and SCADA devices, projecting them throughout the network. To an attacker looking for critical systems, credentials, drive share, services, and data, these decoys appear as tantalizing targets that are indistinguishable from production assets and worthy of exploration.

The Endpoint Detection Net (EDN) suite includes the ThreatStrike® Endpoint solution, which allows organizations to create a variety of deceptive credentials, fake objects such as SSH tokens, and SMB shares to place on real production systems that lead attackers back to the decoys. The hidden SMB mapped shares act as lures for ransomware seeking to spread via network drives,

stalling the malware by continuously feeding it data while throttling the connection to give security teams time to respond to it. Additionally, the ADSecure module looks for unauthorized AD queries and intercepts the results, hiding legitimate credentials and inserting deceptive lures. The Deflect function makes any production endpoint a decoy that redirects attacks targeting ports and services into the deception environment for engagement, in essence locking down systems from discovery or lateral movement activities. Another essential element of the EDN platform is the DataCloak function which hides and denies access to local, network, and cloud storage as well as local administrator group accounts. Together, these capabilities harden an endpoint from discovery or lateral movement activities.

For the cloud, the ThreatDefend solution supports deceptions for cloud-specific technologies such as cloud credentials, access keys, serverless functions, data/databases, storage buckets, and other native cloud technology decoys. The ThreatDefend platform can deploy the deception BOTsink® server to all the major cloud service providers, as well as private and hybrid cloud infrastructures. It can also project the full OS decoys natively in the cloud and supports on-premises deception from a cloud virtual BOTsink server, or cloud deception from an on-premises BOTsink server.




When an attacker engages with the deception environment, the ThreatDefend Platform immediately alerts on the activity for security teams to quickly identify the source of the attack for automated incident response. While the attacker accesses a decoy directly or engages with a webpage or SMB share hosted on it, the platform logs all relevant information about the activity and displays it to the security team in the dashboard. The platform captures the forensic data providing information for incident response and remediation actions, including recording all command and control (C2) traffic and conducting memory forensics analysis. For the security team, this is a wealth of organization-specific threat intelligence they can use to further improve their defenses.

The ThreatDirect solution provides for scaling across remote offices, branch offices, micro-segmented networks, and cloud environments. The forwarder is available as a VM, endpoint module, or containerized application, and runs on endpoints, servers, VM environments, or routers and switches that contain a hypervisor or can run container applications. The solution can also run in the cloud as a full VM or as a container application. This deployment flexibility benefits organizations with extensive and varied network infrastructures, as well as public, private, and hybrid clouds.

The TheatPath® solution identifies credential exposures and misconfigurations on endpoints that allow attackers to move laterally across the network from system to system. The solution maps out the connections, identifies first, second, and third-order hops, and indexes the data for searching and analysis. It can identify accounts with extra permissions (so-called "shadow-admin" accounts), identifies newly created administrator accounts, cloud accounts, and many more. By identifying such vulnerabilities and accounts, the security team can clean the stored credentials, fix the misconfigured policies, or add ThreatStrike credentials to defend endpoints further.

The DecoyDocs™ solution creates deceptive files with an embedded beaconing function that notifies security teams of improper access. When alerting within the network, the solution provides the full details of the host accessing it. If the attacker exfiltrates the document, it will beacon home with the geolocation of every IP address that opens it. This capability gives security teams knowledge of what attackers are targeting. The organization can store these DecoyDocuments in the cloud as well as on-premises.

The Informer dashboard collates all attacker information into one easily managed screen for analysis, response, and company-centric threat intelligence development.  It brings all essential functions into a simple-to-use interface to make accelerate investigations and incident response.

With the ThreadOps® solution, the ThreatDefend platform leverages the many native partner integrations built into the platform to create repeatable playbooks for a consistent and automated incident response process. This function removes complexity and accelerates incident response and eases workloads for security teams that face resource challenges.

These overlapping deception assets create a net that blankets the entire network infrastructure from on-premises endpoints to virtual datacenters in the cloud. Overall, the ThreatDefend platform provides a comprehensive threat deception solution that scales across any size network, regardless of location, and accelerates incident response while providing critical adversary intelligence to improve defenses.

## CONCLUSION

Many organizations that are expanding their presence into the cloud face challenges in defending against attackers. Whether it is a misconfiguration of an Access Control List, a stolen credential, or a vulnerable API, threat actors have opportunities they can exploit to access ever-expanding cloud environments. For organizations seeking to close detection and threat visibility gaps in their cloud security stack, the Attivo Networks ThreatDefend® Platform will be a valuable force-multiplier to the security controls provided by their cloud provider.

## 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.