ShadowPlex Cloud Security

Cloud Detection and Response (CDR)

AI-Powered Enterprise Scale Honeytokens for Multi-cloud Threat Detection

Attackers are targeting Cloud workloads

Cloud environments are increasingly under attack by threat actors, including Advanced Persistent Threats (APTs), ransomware operators, and malicious insiders. Recent research shows a 75% year-over-year increase in cloud attacks. As attackers evolve, they are adapting their techniques to exploit cloud-specific vulnerabilities, leading to a sharp rise in offensive cloud-based techniques. Cloud-specific attacks, also known as Living off the Cloud attacks (LOTC), are highly stealthy and evasive in nature as they involve very limited to no use of malware and exploit existing cloud APIs and permissions in the exploits.

Cloud exploits are gravitating toward identity compromise

Access to intellectual property and sensitive data stored in cloud workloads is the primary goal of threat actors. This data resides in cloud resources such as databases, storage buckets, and compute instances.

Adversaries often gain initial access to cloud environments through techniques like exploiting vulnerabilities in publicly accessible cloud workloads. To reach sensitive cloud resources, adversaries must pivot within the cloud environment, often targeting the cloud control plane to escalate privileges or compromise key administrative functions. Increasingly, attackers are using identity-driven exploits to achieve this. By targeting an IAM user or role with the necessary permissions, adversaries can gain trusted access to sensitive resources and complete their mission.

Through reconnaissance, adversaries identify cloud credentials (access keys, secrets) and permissions that allow them to exploit IAM roles for lateral movement. Exploiting IAM users and roles has become a primary attack vector in cloud environments.

Multi-cloud workloads lead to additional complexity

Organizations are increasingly adopting multiple cloud providers to enhance resilience, reduce business risk, and leverage each provider's unique capabilities. Over 90% of organizations now use more than one cloud provider. However, multi-cloud deployments increase security risk due to different cloud provider security controls. Different IAM models result in an expanded identity attack surface.

Cloud Security at a Glance

Prevention vs Detection

Prevention is the act of taking proactive measures to stop attacks from happening. However, as we have all learned from a variety of breaches and attacks over the years, prevention is good hygiene but not sufficient. Effective mechanisms are required to detect and respond to attacks that have breached the preventive measures.

CNAPP (Cloud Native Application Protection Platform)

CNAPP is the broad category that consolidates various areas of cloud security. It includes preventive security areas such as posture management, entitlement management, and workload (VMs, containers, serverless functions) protection all under a variety of acronyms. CNAPP also includes Runtime Protection to detect and respond to attacks and this area is consolidating under Cloud Detection & Response (CDR).

What is Cloud Detection and Response (CDR)

Cloud Detection and Response (CDR) focuses on detecting threats within cloud workloads during runtime that have bypassed prevention-based defenses. It identifies malicious activities that aim to propagate and gain unauthorized access to cloud resources and data.

State of CDR Solutions

Current CDR offerings are either agent-based or built on log analytics.

The increasing adoption of cloud-native workloads—such as containers, serverless functions, and Platform as a Service (PaaS)—presents new challenges for threat detection. These workloads are incompatible with agent-based solutions, making traditional Endpoint Detection and Response (EDR) tools ineffective in protecting them.

Log analytics solutions are based on workload log monitoring. These solutions analyze the event logs (e.g., CloudTrail in AWS) generated by the cloud providers, build baselines and apply rules and/or look for anomalies. Log monitoring suffers from some inherent disadvantages, especially at scale. Cloud workloads generate tremendous volumes and different types of logs, increasing the complexity. Besides, the workloads are highly dynamic, and traffic patterns are not static. For example, containerized environments rapidly provision and deprovision resources based on traffic and usage patterns, while serverless workloads are often short-lived. This dynamic, ephemeral nature makes log analytic approaches less effective in cloud environments. As a result, log analytics solutions miss real threats in addition to generating a lot of false positives.

Cyber Deception and Honeytokens

Cyber deception

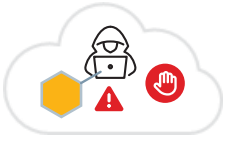
Cyber deception is a proactive detection strategy that sets traps based on adversary's objectives and monitors interactions with those traps. Since deception artifacts are not part of legitimate business or IT workflows, any interaction with them serves as a direct indicator of malicious activity. This provides defense teams with high-fidelity early warnings of intrusions, offering actionable intelligence for SOC teams.

Honeytokens

Honeytokens are a type of cyber deception. These traps are particularly effective in detecting identity threats and are also used in threat-hunting efforts. In cloud environments, honeytokens are categorized into two main types: *IAM Honeytokens* and *Workload Honeytokens*.

IAM honeytokens are deceptive representations of identity and access management (IAM) users, roles/service principals, and policies. ***Workload honeytokens*** are deceptive credentials (such as access keys and secrets) deployed in various cloud resources like compute instances, secrets managers, and instance metadata.

Honeytokens are designed as traps for adversaries and placed across the cloud resources. When attackers infiltrate cloud workloads and search for credentials or policies to escalate privileges or move laterally, they encounter these honeytokens. Any attempt to use the honeytokens triggers an immediate alert to the SOC team, providing instant visibility into the attacker's actions.



Preemptive Threat Detection

Detection based on agents or log analytics is "reactive", alerting only after the compromise is done. Honeytokens provide ***preemptive detection*** and detect cloud threats early. Attackers often seek to elevate privileges, access sensitive data, or infiltrate critical systems. By placing honeytokens at strategic points, defenders can entice attackers and detect malicious activity early in the attack lifecycle. This early detection enables rapid response actions to isolate and neutralize the threat before it propagates.

For example, if an attacker gains access to a cloud environment and searches for IAM policies to escalate privileges, a well-placed honeytoken disguised as an IAM account with relevant privileges will expose the attacker's actions at the reconnaissance stage.

Acalvio ShadowPlex Cloud Security

ShadowPlex Cloud Security (SCS) is an ***agentless*** solution that can deploy both IAM and workload honeytokens at scale across major cloud workloads. ***No Acalvio software is deployed in the customer's workload***. The honeytokens cover various places across different cloud resources where typically credentials are stolen from. IAM honeytokens also include honeytokens for policies and roles.

SCS does not require any read or write privileges for discovering the cloud workload resources or for deploying the honeytokens. The honeytokens are configured by an AI engine to blend into the user environment. The solution provides complete control to the users to select the type of honeytokens and the resources where they want honeytokens to be deployed.

SCS detects honeytoken usage by monitoring the cloud logs (e.g., CloudTrail in AWS) and raises alerts when a honeytoken access is detected.

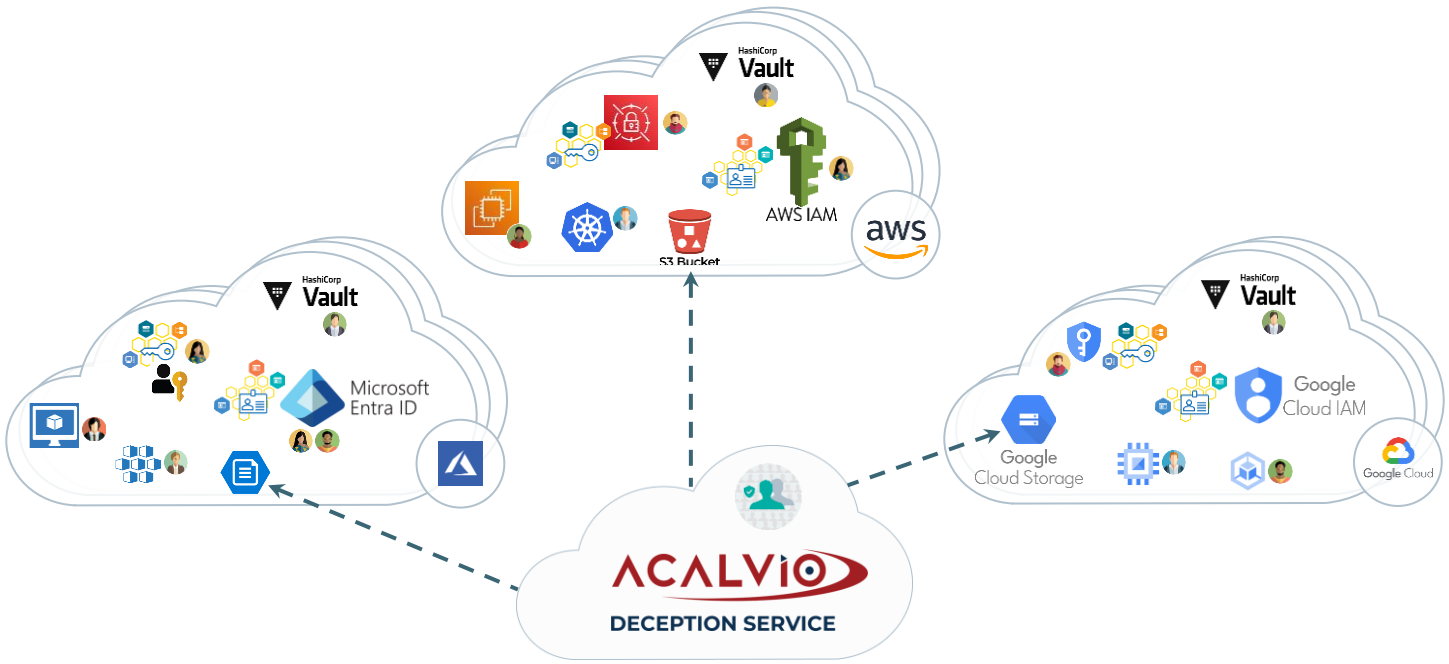
SCS is available in two modes – a SaaS service managed by Acalvio or a low-footprint deception service that can be hosted and managed by the customer in their cloud.

IAM Honeytokens

- Honey accounts
- Honey policies
- Honey roles

Workload Honeytokens

- Compute instances
  - Instance metadata
  - Bash history
  - Environment variables
- Secrets Manager / Vault
- Storage buckets
- Kubernetes clusters
- Third-party software
  - HashiCorp Vault
- CI/CD Pipelines
- Code repositories



Core Capabilities

Comprehensive palette	ShadowPlex deploys a wide array of IAM and workload honeytokens to deliver coverage across cloud assets and workloads. This includes virtual machines, containers, serverless functions, Platform as a Service (PaaS) such as cloud databases.
Agentless solution	ShadowPlex is an agentless solution, eliminating the deployment complexity associated with the rollout of agents in cloud workloads. This greatly simplifies the adoption of the solution.
Scalable platform for honeytoken deployment	The platform is built to scale across complex cloud environments, supporting thousands of users and multiple cloud providers. For example, ShadowPlex supports deployment of honeytokens into AWS environments with hundreds of AWS accounts, allowing for wide-reaching coverage and protection.
AI for automated configuration and placement	ShadowPlex leverages AI to generate relevant honeytokens that are realistic and enticing for adversaries to exploit. For example, an IAM role might be generated with a realistic name, based on the characteristics of the cloud workload, making it attractive for adversaries to target.
Actionable alerts mapped to MITRE	ShadowPlex alerts are actionable and mapped to the MITRE ATT&CK framework to provide a standardized taxonomy for SOC teams, , improving threat intelligence and incident response workflows.
Unified console for multi-cloud workloads	ShadowPlex supports the deployment of honeytokens across multiple cloud service providers. The detections are surfaced through a single console, providing defense teams with unified visibility for threats that may cross cloud boundaries.
Response automation	ShadowPlex includes pre-built integrations with cloud orchestration platforms and SOAR systems to enable response automation. SOC teams can use these integrations to trigger response actions based on ShadowPlex alerts, improving the speed and effectiveness of incident response.

Summary: Acalvio Cloud Detection and Response (CDR) is a necessary solution to protect multi-cloud environments

Cloud environments face an increasing number of cyber threats. Organizations require both prevention solutions and cloud-specific preemptive threat detection to provide comprehensive security.

Acalvio offers a scalable platform for deploying honeytokens—designed to detect identity threats across cloud environments, including cloud-native workloads. Leveraging AI, ShadowPlex configures realistic and enticing honeytokens for attackers to target, providing defense teams with early and accurate threat detection. This platform is essential for identifying and mitigating threats across multi-cloud environments, ensuring robust Cloud Detection and Response (CDR). ShadowPlex is a proven, effective, and necessary solution for securing modern cloud infrastructures.

ACALVIO

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Detection, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy
on-premises, in the cloud or via marquee managed service providers. For more information, please visit **www.acalvio.com**