ACALVIO
AI-POWERED DECEPTION

DATASHEET

ShadowPlex Cloud Security
Preemptive security to deny and disrupt agentic AI attacks

Gartner® recognized Acalvio as the "Company to beat" in Preemptive Cyber Deception.

CHALLENGES

Attackers are using built-in APIs and SDKs to perform cloud exploits, known as living off the cloud attacks. Agentic AI attacks automate cloud attacks from reconnaissance to data exfiltration within minutes. Attackers target identities (cloud IAM users, service accounts) for privilege escalation and access to key cloud data resources. The use of legitimate credentials makes it difficult to distinguish normal usage from malicious use. The dynamic and ephemeral nature of cloud workloads makes it difficult to build a baseline and find deviations from the baseline. Agentic AI attacks occur at machine-speed, overwhelming traditional security controls that are unable to keep pace with these fast-moving threats.

SOLUTION

ShadowPlex Cloud Security (SCS) provides a preemptive security solution to deny and divert agentic AI attacks. ShadowPlex Cloud Security supports multi-cloud workloads, providing a unified security solution across AWS, Azure, GCP, and OCI.

Honeytokens is a Deception Technology technique that is proven to be **extremely powerful and effective in detecting and diverting agentic AI attacks and living off the cloud attacks.** ShadowPlex honeytokens cover both IAM directories and cloud workloads. IAM Honeytokens are deceptive credentials (representing user and service accounts, roles, policies) in Identity and Access Management (IAM) that are specifically designed to lure attackers and deflect them away from real credentials. Workload Honeytokens include deceptive credentials and data embedded in legitimate cloud resources such as compute instances, secrets manager/vault, serverless functions, container clusters etc. where attackers look for exposed credentials. Any usage or manipulation of these honeytokens is a high-fidelity indicator of a threat.

ShadowPlex Cloud Security leverages native APIs supported by Cloud providers to not only deploy and manage but also monitor and alert on honeytoken usage to provide a **scalable and effective preemptive security solution for the cloud.**

KEY BENEFITS

- Deny and divert agentic AI attacks based on unique Honeytokens technology
- Single platform to secure multiple cloud providers, including deployment and refresh lifecycles
- Advanced AI-based recommendation engine for honeytokens
- Powerful capability to detect threats to all cloud resources to strengthen Zero Trust environments

FEATURES

Agentless deployment

- Administrative policies for control over types and counts of honeytokens created
- No privileged access to customer cloud workloads required. Read-only access to cloud service provider logs
- Two deployment modes
  - Acalvio SaaS service
  - Packaged service that customer can host on their own
- Pre-integrated with Cloud Security Posture Management (CSPM) solutions for automated discovery of cloud workloads

ACALVIO
AI-POWERED DECEPTION

ShadowPlex Cloud Security
Built on Enterprise-scale Honeytokens

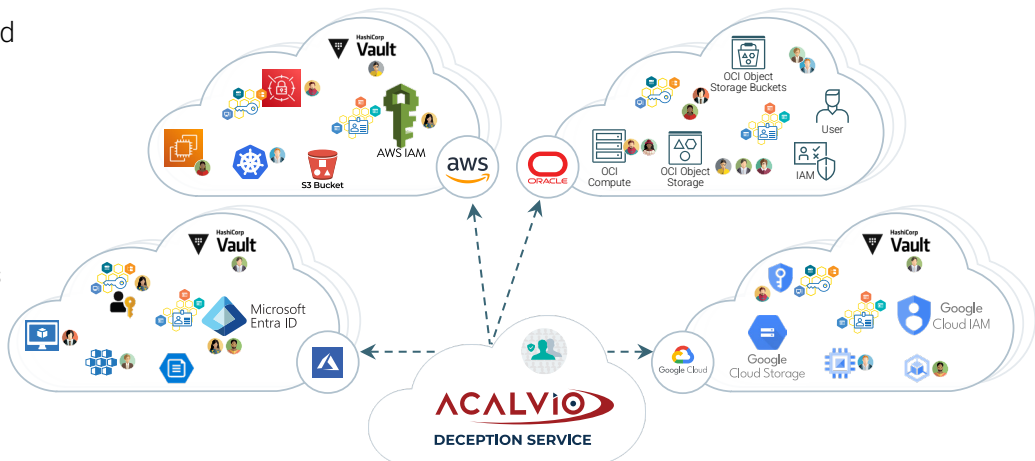
BUSINESS VALUE

Challenge	Solution	Benefits
Detect agentic AI attacks at the reconnaissance phase and divert the threats.	Deception technology based Honeytokens is an effective solution to detect and divert agentic AI attacks at the reconnaissance phase. ShadowPlex Cloud Security operationalizes Honeytokens for cloud workloads at scale.	High-fidelity detection and threat diversion based on Deception Technology
Detect living off the cloud attacks that target cloud-native resources	Honeytokens enable threat detection across cloud resources. Honeytokens are versatile and can be embedded as honey users, honey roles, honey policies, honey parameters etc. in any cloud resource.	Cloud threats can target any resource. It is important to have visibility into these threats for analysis and timely responses to arrest the attack progression. Additionally, honeytoken deceptions are very effective in luring attackers and deflecting them away from real credentials.
Ability to extend security across multi-cloud workloads	ShadowPlex Cloud Security is a scalable offering that enables deployment across a large environment with workloads in multiple clouds.	Attackers can target any cloud workload and use it to pivot to other clouds. Comprehensive coverage across the entire multi-cloud environment is essential to avoid detection gaps and blind spots for defense teams.

ARCHITECTURE

ShadowPlex Cloud Security (SCS) is a SaaS solution that covers multiple clouds.
SCS is also available as a packaged service that can be hosted by the customer.

SCS is agentless – no agents deployed in the customer's cloud. SCS only needs Read access to a storage bucket that stores the cloud logs (e.g., CloudTrail) for detecting honeytoken access. SCS provides Infrastructure as Code (IaC) templates based on Terraform for CI/CD based deployment and refresh of honeytokens across cloud workloads.



Acalvio is an AI-powered preemptive cybersecurity company focused on countering AI-driven identity and infrastructure intrusion. Its 360 Deception platform combines Dynamic Deception, evolving HoneyPaths, and cloaking of production assets within deception fabric to disrupt automated reconnaissance, credential abuse, and lateral movement across identity systems, endpoints, cloud, network, and cyber-physical environments. By altering what attackers can perceive and trust, Acalvio shifts detection from post-compromise analysis to pre-impact exposure, enabling organizations to detect, delay, disrupt, and deny malicious activity at machine speed. The company serves enterprise and government organizations determined to break automated intrusion at its source. https://www.acalvio.com/