ACALVIO
AI-POWERED DECEPTION

DATASHEET

ShadowPlex Cloud Security
Built on Enterprise-scale Honeytokens

CHALLENGES

Cloud breaches are widespread, and insecure identities are the primary cause. Identity threats are involved in over 80% of all cyberattacks (including APT threats, Ransomware attacks, and Advanced malware). Attackers harvest identities from multiple cloud resources where secrets/keys are stored. Attackers target identities (user and service accounts, roles, policies) for both privilege escalation and access to key cloud data resources. When the threat actors obtain access to valid cloud credentials, their activities and movement within the cloud workload are masked as legitimate traffic. In any cloud workload, the identity attack surface can be large, and eliminating all the attack surface is challenging for security teams.

SOLUTION

ShadowPlex Cloud Security (SCS) provides a new Deception Technology-based cloud threat detection. More than 90% of the enterprise networks utilize multiple cloud providers and ShadowPlex Cloud Security seamlessly extends to multi-cloud networks.

Honeytokens is a Deception Technology technique that is proven to be **extremely powerful and effective in detecting a variety of threats.** 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 deception-based Cloud Threat Detection solution.**

KEY BENEFITS

- Comprehensive cloud threat detection based on unique Honeytokens technology
- Protects 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.**
- Complete customer control over types and counts of honeytokens created
- No privileged access to customer cloud workloads required. Read-only access to CloudTrail logs.
- Two deployment modes
  - Acalvio SaaS service
  - Packaged service that customer can host on their own

ACALVIO
AI-POWERED DECEPTION

ShadowPlex Cloud Security
Built on Enterprise-scale Honeytokens

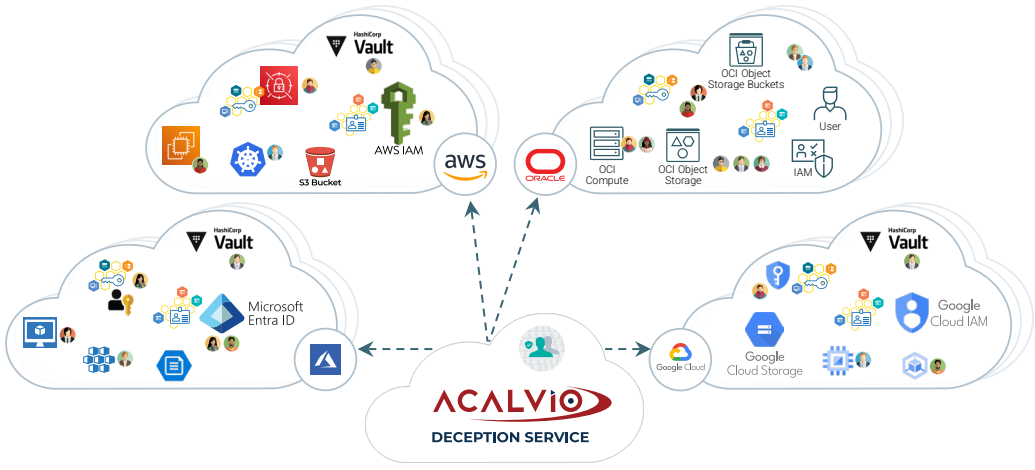
BUSINESS VALUE

Challenge	Solution	Benefits
Detect attacks targeting exposed cloud credentials.	Deception technology based Honeytokens are an effective solution to detect apex attackers. ShadowPlex Cloud Security operationalizes Honeytokens for cloud workloads at scale.	High-fidelity cloud threat detection based on Deception Technology
Detection of threats in cloud resources where no security solution can be deployed (e.g. secrets manager, serverless functions, storage buckets etc.)	Honeytokens enable threat detection in all 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 detection across multi-cloud networks	ShadowPlex Cloud Security is a scalable offering that enables deployment across a large hybrid enterprise network 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 network is essential to avoid detection gaps and blind spots for the 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 Acalvio software is deployed in customer's cloud. SCS only needs Read access to one storage bucket that stores the cloud logs (e.g., CloudTrail) for detecting honeytoken access. Deployment and management of honeytokens are done using a configurable, dynamically generated script.



Acalvio is the leader in autonomous cyber deception, defending against APTs, insider threats, and ransomware. Its AI-powered Preemptive Cybersecurity Platform, protected by 25 patents, delivers threat detection across IT, OT, and cloud environments and advances Identity Threat Detection and Response (ITDR) with Honeytoken-driven Zero Trust security.

Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from the Cloud, on-premises, or through managed service providers. **www.acalvio.com**