

Seceon Cloud Forensics

Public cloud, private cloud, and hybrid investigation

One evidence model and one investigation workflow across AWS, Azure, GCP, VMware, Nutanix, OpenStack, and Hyper-V with CCE, APE, and LTS.



Product Overview

When an incident happens in a cloud tenant, there is no disk to seize. Evidence is scattered across audit logs, identity events, flow records, workload telemetry, storage access logs, and SaaS activity, and much of it is short-lived by default. Private cloud changes the constraints without removing the problem: the organisation owns the hypervisor, but workloads are still ephemeral, and evidence is still fragmented.

Seceon Cloud Forensics turns that into a single correlated investigation. Telemetry is ingested through the Collection and Correlation Engine (CCE), analyzed by the Analytics and Policy Engine (APE), retained in Long-Term Storage (LTS), and investigated through search, timeline, cases, and reports.



How Cloud Forensics Differs

Aspect	Traditional	Public cloud	Private cloud
Evidence location	Disks, memory, endpoints	Provider APIs, audit logs, snapshots, object stores	Hypervisor/management plane, VM snapshots, virtual switch flows



Highlights



Investigate public cloud, private cloud, and hybrid incidents as one case and one timeline



Evidence from control-plane audit, identity, network flow, workloads, storage, and SaaS



Continuous ingest and LTS retention so look-back is possible when detection comes late



Same investigation workflow across AWS, Azure, GCP, VMware, Nutanix, OpenStack, and Hyper-V



Timeline reconstruction, IOC/IOA hunting, MITRE ATT&CK mapping, chain of custody, and reporting

Aspect	Traditional	Public cloud	Private cloud
Physical access	Direct	None	Possible, but workloads are virtual
Volatility	Memory and disk	Short-lived instances, containers, serverless	Short-lived VMs and containers
Scope	Host or network	Multi-account, multi-region, identity-centric	Multi-cluster, often spanning into public cloud
Primary attack surface	Endpoints and network	Identities, keys, APIs, misconfigurations	Management-plane credentials, orchestration APIs, east-west traffic



Architecture (CCE · APE · LTS)

Component	Role	Forensic value
CCE	Collect, parse, normalize, enrich, correlate	One evidence model across public and private cloud
APE	AI/ML, UEBA, threat intelligence, ATT&CK-mapped policies	Prioritised, explainable leads
LTS	Retain raw and normalised events	Look-back, preservation, audit support



Public Cloud Telemetry

Class	AWS	Microsoft Azure	Google Cloud
Control-plane	CloudTrail	Azure Activity Log	Cloud Audit Logs
Identity	IAM / STS / console sign-in	Entra ID sign-in and audit	Cloud IAM, service accounts
Network	VPC Flow Logs, Route 53, ELB	VNet/NSG, Firewall, DNS	VPC Flow Logs, Cloud DNS
Workloads	EC2, EKS, Lambda / CloudWatch	VM diagnostics, AKS, Functions	GCE, GKE, Cloud Run
Storage	S3 access / CloudTrail data events	Blob resource logs	Cloud Storage Data Access logs

Oracle Cloud Infrastructure and IBM Cloud follow the same pattern: control plane, identity, flow, and object storage access in a single schema.



Private Cloud and Virtualisation

Layer	Example evidence	Forensic value
Management plane	vCenter, Prism, OpenStack Keystone/Nova, SCVMM	Who created, moved, cloned, snapshotted, or deleted a workload
Hypervisor hosts	ESXi, AHV, KVM, Hyper-V host and shell access	Direct virtualization-layer access that bypasses guest controls
Virtual network	NSX, distributed firewall, overlay flows	East-west movement that never hits a physical firewall
Guest workloads	Process, file, registry, authentication via agents/EDR	What executed after the workload was created

Investigation Workflow

- Detect and triage (APE risk-scored threats with ATT&CK context)
- Scope and preserve (affected accounts, projects, workloads; retain in LTS)
- Correlate identity, control-plane, network, and workload events
- Reconstruct timeline (initial access through persistence and data access)
- Contain and hunt remaining keys, roles, and persistence
- Report with evidence inventory, hashes, and custody records



Primary Use Cases

Use case	How Seceon Cloud Forensics helps
Compromised cloud identity / access key	Tie sign-in and STS/IAM events to API calls, regions, and resources
Misconfiguration leading to exposure	Correlate config and audit events with subsequent data access
Container / Kubernetes incident	Ingest cluster audit and runtime events; attribute to the creating identity
Hybrid intrusion	One timeline from private-cloud VM to public-cloud tenant
Insider or privileged SaaS abuse	Storage and SaaS access logs with identity context
Late detection / look-back	LTS retention when default provider logs have already rolled off



Why Seceon Cloud Forensics

Differentiator	Benefit
No disk to seize still one case	Control-plane, identity, flow, and workload evidence in one investigation
Public + private in one model	Same workflow for AWS/Azure/GCP and VMware/Nutanix/OpenStack/Hyper-V
Hybrid as one timeline	Incidents that cross on-prem virtualization and public cloud stay connected
Preserve before the incident	Continuous collect + LTS, not an after-the-fact log request
Defensible output	Integrity hashing, custody, audit-ready reports

Assumptions

Evidence exists only for sources onboarded before or during the incident, and only for the LTS retention configured. Connector coverage depends on the deployed OTM release and on log types enabled in the customer tenant.

One-Line Pitch

Seceon Cloud Forensics investigates public cloud, private cloud, and hybrid incidents as one correlated case control-plane, identity, network, workload, and storage evidence retained and reported on the Seceon OTM platform.

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon



Schedule a Demo

www.seceon.com/contact-us/

