# Seceon aiSIEM Cloud Security

**AI driven threat intelligence, detections & alert correlation based on cloud flows and other logs**

A platform that enables MSPs/MSSPs to build and offer efficient, high-margin advanced security services in both cloud and hybrid environments.

## aiSIEM™ based Cloud Security for MSPs/MSSPs

MSPs/MSSPs and their clients are adopting cloud platforms such as Microsoft Azure, AWS, Google Cloud, and Oracle Cloud and need to modernize their security programs. While these platforms have many security capabilities, service providers are responsible for securing their client's data, applications and infrastructure. Cloud access and perimeter security may not be enough to provide protection against evolving security issues. Seceon OTM cloud security capabilities enable your teams to build trust with your clients as they embrace the efficiency of cloud services. Seceon cloud security capabilities include parsing of bidirectional raw flows and logs for threat signatures and anomalous behaviors and correlating seemingly disparate anomalies/events into contextual events of focus and remediation.

## Highlights

### GAIN TRUST WITH UNIFIED VISIBILITY (BOTH CLOUD AND NON-CLOUD) AND THREAT INTELLIGENCE CAPABILITIES

In your cloud infrastructure, uncover a myriad of threat vectors lurking inside existing logs, auto discovered hosts, network, cloud, OT and IoT infrastructure, Seceon aiSIEM combines this telemetrywith 360° inferences drawn from cloud logs events, network traffic, packets, identities and behavioral patterns.

### REDUCE MEAN TIME TO DETECT AND RESPOND

Considerably shorten Mean-Time To-Detect (MTTD) and Mean-Time To-Response (MTTR) with automated threat detection and remediation in real-time and score them by confidence level and criticality.

### EFFORTLESS DEPLOYMENT AND INTEGRATIONS IN THE CLOUD

With just one collector, you can start sending flows and logs and deploy Seceon aiSIEM. Then you can connect your existing technology stack with hundreds of integrations.

### COMPLETE USER PROTECTION

Cloud Security is part of the Seceon OTM™ Suite, powered by aiSIEM. It combines a broad range of cloud platform threat protection capabilities. it enables you to manage threats and alarms across multiple threat vectors from a single unified management console. This gives you complete user- based single pane of glass visibility, into the security of your environment.

### SUPERIOR THREAT PROTECTION WITH VERY HIGH THREAT COVERAGE

Gain superior protection with higher threat coverage. Threat coverage with legacy MSP/MSSP vendor tools typically ranges from 20-40 %. With Seceon, it can be as high as 99.9%.

## Cloud Security Today

Over the years cloud vulnerabilities have exploded and continue to cost organizations billions of dollars and lost productivity. For example, remote workers, partners, and customers may unknowingly upload malicious files using cloud file sharing services. The potential costs are too high to accept a baseline cloud security posture that only protects against a small portion of threats. Security responses are designed to detect known cloud vulnerabilities however a majority of cloud vulnerabilities are unknown and require continuous, real-time detection and fast responses to threats.

## Cloud Security Overview

- Uses multiple Artificial Intelligence (A.I.) and Machine Learning (ML) techniques with alert correlation to examine raw cloud logs from sources like AWS VPC and Azure NSG flows and cloud logs to predict attacks.
- Ingests device-independent raw flows (in/out) & device dependent logs (Syslog, CEF)
- Secure log flows and protocol data ingestion with support for log transportation & protocols like Push-UDP, TCP & TCL over TLS, Pull –APIs with HTTPs.
- Combines pre-execution machine learning, anti-malware, heuristics, and dynamic learning to detect ransomware and other zero-day malware.
- Cloud security posture management, drift detection and, governance capabilities.
- Parses bidirectional raw flows and logs for threat signatures, and correlates seemingly disparate anomalies/events into contextual events of focus and remediation.
- Supports comprehensive cloud security audit policy reports

## Platform Overview

**Ingestion of cloud flows from all .major cloud platform providers, non-cloud flows events, logs, user activity data** from almost all sources; identities, networks, endpoints, clouds, and applications.

**Contextual enrichment** with threat intelligence (40+ sources) combines with vulnerability assessments and historical data.

**Behavior baselining and profiling** for anomaly detection leveraging Machine Learning and Artificial Intelligence techniques.

**Advanced event correlation** (on-prem and cloud) and behavioral patterns with AI and Dynamic Threat Models.

**Identification of threats based on rules-based policy** creation, enforcement and notification for appropriate action and governance

**Protection and response** based on automated remediation (based on incident triaging and or prebuilt playbooks) and real-time remediation.

## Key User Scenarios:

- Seceon's remediation capabilities support pushing polices with Microsoft Azure NSG to block malicious attacks and monitor communication in real time
- Seceon can take action on a specific user to disable the user from Azure AD using Artificial Intelligence based techniques.
- Seceon can push the policy on Amazon AWS VPC–Network ACL to block a malicious communication in real time.
- Seceon aiSIEM can consume logs from any application which can provide security logs (Docker container, Web servers etc.)

***Seceon Dashboard for Microsoft Azure***

**“A few of our clients have apps deployed on Azure, Seceon provides us with the visibility and threat detection and response we need to protect them”.**
**- Seceon MSSP partner**

**Supercharge your ability to protect cloud environments with real-time AI and ML powered detection of threats and breaches.**

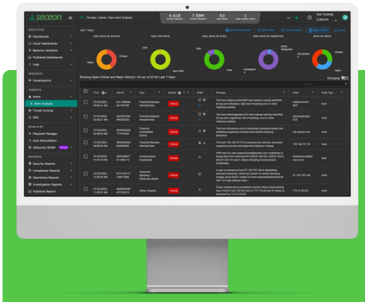
Continuous real-time, automatic, anomaly detection, and behavior analysis of all ingested logs, events, flows combined with user and application-level data like Microsoft AD, enables Seceon to detect indicators of compromise and threats and apply a confidence and risk score to surface and alert on only the events that matter.
You’ll lower your mean time to detect (MTTD) and cut the number of false positives your teams may be struggling with.

**Finally, an easy-to-use incident response platform designed to make it easy to set and forget automated response playbooks, in the cloud environment.**

With automated and analyst assisted remediation (blocking, quarantine etc.) based on alert type and severity that provides all of the correlation and situational awareness your teams need enables you to decrease the mean-time-to response (MTTR). With our innovative playbook builder GUI that allows incident responders to seamlessly convert searches and alerts into multi-step playbooks to drive deeper automation.

**Launch advanced cybersecurity services for both cloud and non-cloud environments with high margins and reduce the risks of cyber threats for your clients - at scale.**

With Seceon’s multi-tenant, flexible ‘best-fit’ deployment options, and flexible retention periods, including geographically dispersed deployments many service providers tell us they have more efficient security operations and higher margins than alternative solutions. Seceon supports hundreds of integrations for EDRs, network log sources, context sources, ITSM systems, and more. Seceon will rapidly add value to your existing investments. Many of our service provider partners report that they can onboard new customers without the massive amount of hardware that NDR platforms or custom scripting that SOAR platforms require and achieve faster MTTD/MTTR vs legacy store and query SIEMs of the past.



### REDUCE TOOL SPRAWL AND TCO

Most vendors require MSPs/MSSPs to buy many solutions like IDS/IPS, TI and VA data, EDR, NDR etc. Seceon's aiSIEM includes these and integrates with your existing investments.

### CONTINUOUS COMPLIANCE

Ensure compliance 24x7 with Seceon’s audit and reporting capabilities for PCI DSS, HIPAA, NIST, GDPR and more. Additionally monitor security postures, operations and investigations reporting.

### ACCURACY, SPEED, PRIORITIZATION

Gain the edge over adversaries and hackers with Seceon’s real-time processing of large amounts of data at speed, combined with behavioral anomalies and threat intelligence to arrive at validated and prioritized threat indicators.

### FLEXIBILE LICENSING FOR MSPS AND MSSPS

Harness the power of flexible ‘best-fit’ cost and licensing through on-premises, cloud or MSP hosted solution spanning multiple sites – data center and branch offices – with multi-tenancy and data segregation at the core of platform architecture.

## ADVANTAGES MSPS AND MSSPS HAVE WITH SECEON

- Comprehensive, unified visibility, threat detection and response with aiSIEM, reducing your team's time to investigate & respond.
- Quick and simplified responses powered by orchestration and automation that leverage AI and ML to reduce MTTD/MTTR without adding overhead.
    - Choose automated responses with included playbooks( out-of-the-box) that allow automation of response actions for common use cases.
    - Create your own automated playbooks for analysts, or take action based on correlated data and transparent detection insights.
- Seceon partners benefit from mature onboarding processes, automated deployments and trainings that jumpstarts their service delivery.

### About Seceon

Seceon enables MSPs and MSSPs to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platform. The platform delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 300 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,500 clients.

**Learn more about Seceon aiXDR and**

**Schedule a Demo** www.seceon.com/contact/