Seceon aiSIEM-CGuard 2.0

Next-Generation Cloud Security & Incident Response

CGuard 2.0 introduces a comprehensive Cloud Security Module that provides robust protection across all major public cloud providers, including Microsoft 365 (O365), Azure, AWS, and Google Cloud Platform (GCP). With advanced detection rules, true multi-rule correlation, and dynamic incident response actions, CGuard 2.0 delivers an unparalleled security posture for modern cloud environments.

Advacned Security for All Organizations

Protect your client's data, applications, systems and users. Reduce downtime and risks from today's cyberthreats.

AI/ML Based Detection and Response

Benefit from security automation through Machine Learning for anomaly detection and Artificial Intelligence. Stop threats and limit blast zones before they turn into major incidents.

Instant 24/7 Response

Enable instant responses to governance policy violations through user-defined controls and initiate automated remediation to threats with high severity and confidence level, targeted at business-critical assets.

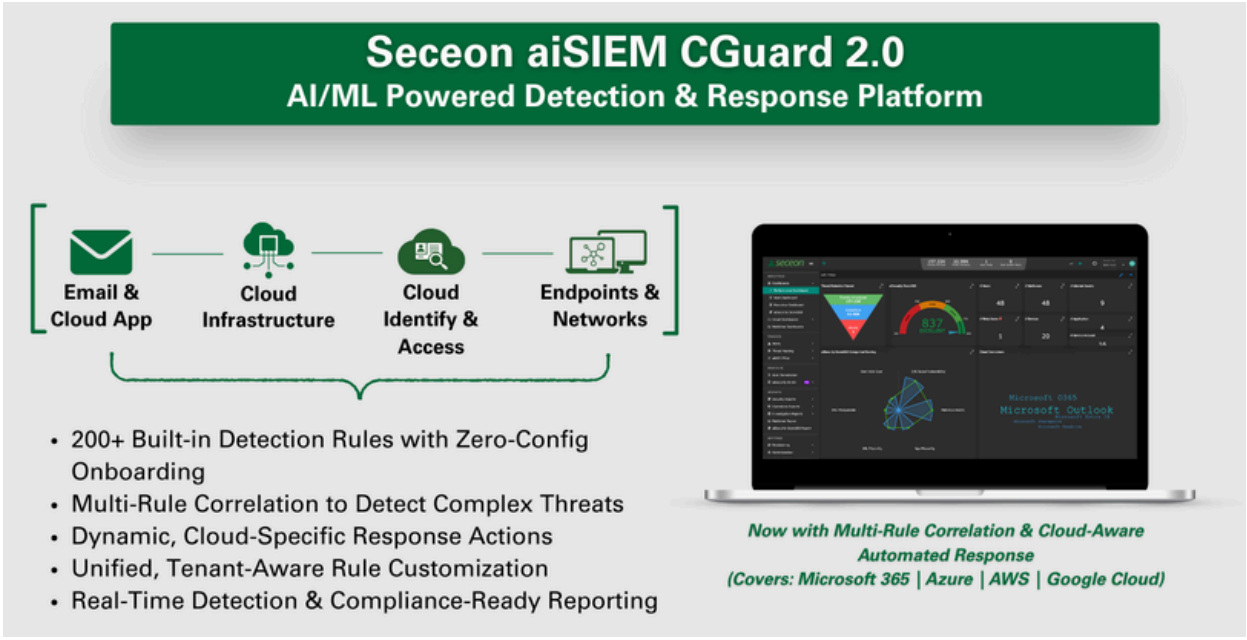
No Agents & Single Pane of Glass

Easily implement with your existing cloud administrator credentials and access the Seceon platform's award winning UX. See and customize all of your threat alerts and automated response playbooks.

Cloud Security Module

Detection Rules: Customizable, Scalable, and Built for Action

- **Custom Rule Definition:** Create your own detection rules using raw telemetry data from O365, Azure, AWS, GCP, and more.
- **200+ Built-in Rules:** Immediate protection from day one with a comprehensive library of pre-defined detection rules.
- **Full Rule Management**: Seamlessly edit, disable, or create new rules tailored to evolving or unique security needs.



- **Advanced Query PPL:** Leverage a Splunk or Linux-like piped PPL query syntax for advanced users to formulate granular rules.
- **Optional Customization:** Defining custom rules is entirely optional—out-of-the-box rules ensure you're protected without additional configuration.
- **Tenant-Aware Personalization:** Use a single-tenant profile interface to personalize built-in rules based on factors like operating locations and executive risk exposure

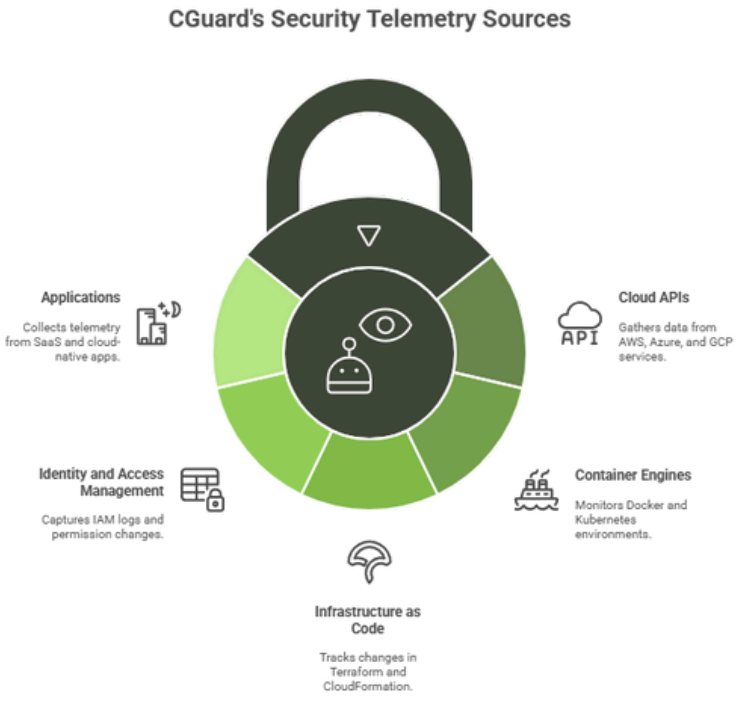
Key Capabilities

- **Cloud Security Posture Management (CSPM)**: Detect and remediate misconfigurations and policy violations across AWS, Azure, and GCP environments with guided remediation and policy enforcement.
- **Cloud-Native Application Protection Platform (CNAPP):** Secure workloads from development to deployment, including Infrastructure as Code (IaC), containers, and serverless applications.
- **Cloud Infrastructure Entitlement Management (CIEM):** Identify and mitigate excessive permissions, enforce least-privilege access, and manage entitlements across multi-cloud environments.
- **Container & Kubernetes Security:** Monitor container and pod behavior, restrict unauthorized communications, and enforce security at the orchestration layer (Docker, Kubernetes).
- **AI-Driven Threat Detection:** Detect cloud-native attacks such as cryptojacking, privilege escalation, and data exfiltration using behavioral analytics, machine learning, and curated threat intelligence.
- **Compliance & Risk Reporting:** Map findings to regulatory and industry frameworks including ISO 27001, HIPAA, NIST, and PCI-DSS, with automated audit-ready reports and dashboards.

Telemetry Sources

CGuard 2.0 gathers security telemetry from:

- **Cloud APIs** – AWS Config, CloudTrail, Azure Monitor, GCP Security Command Center
- **Container Engines** – Docker, Kubernetes
- **Infrastructure as Code** – Terraform, CloudFormation, and other DevOps pipelines
- **Identity and Access Management** – Cloud IAM logs, login events, permission changes
- **Applications** – SaaS and cloud-native app telemetry



Incident Response: Detection, Correlation, and Automated Action

Incident Detection & Multi-Rule Correlation: A Key Differentiator

Unlike many providers that restrict detection to individual rule triggers, CGuard 2.0 delivers multi-rule correlation—a true game-changer in threat detection.

- **Custom Correlation Logic:** Define incidents using custom logic that correlates signals across multiple rules, ensuring comprehensive detection of complex threats.
- **Flexible Detection Windows:** Configure sliding or jumping time windows to accurately capture threat behavior over diverse periods.
- **Advanced Piped PPL Query Syntax**: Craft precise correlation conditions with a powerful query interface that supports Splunk/Linux-like piped syntax.
- **Ease of Expression:** Intuitively define multi-rule expressions to correlate and prioritize alerts from disparate telemetry sources.
- **Flexible Scheduling:** Configure automated correlation logic to run in real-time or on scheduled intervals as per operational requirements

Incident Response Actions: Dynamic, Cloud-Aware, and Automated

CGuard 2.0 not only detects threats but also provides a suite of automated response actions that are tailored to your cloud provider's capabilities.

- **Session Control**
  - Log out all active sessions
  - Invalidate access and refresh tokens
  - Terminate risky browser or mobile sessions
- **Account Restrictions**
  - Block or suspend compromised user accounts
  - Quarantine affected identities
  - Immediately disable high-risk or privileged user access
- **Credential Enforcement**
  - Force password resets
  - Enforce Multi-Factor Authentication (MFA)
  - Revoke OAuth or delegated app permissions
- **Provider-Specific Enforcement**

Response actions are dynamically adapted to leverage the API and policy models unique to each cloud provider, ensuring effective and compliant actions.

- **Orchestrated Playbooks**

Combine multiple response actions into automated playbooks triggered by an incident severity or specific rule matches, ensuring a rapid, coordinated response

Built on Seceon aiXDR Platform

CGuard 2.0 leverages the full capabilities of the Seceon aiXDR platform, including:

- **aiSIEM** – Real-time threat correlation and analytics
- **aiXDR-PMax** – Telemetry fusion from endpoints to cloud
- **aiSecurityScore360** – Posture scoring and continuous risk assessment
- **aiSecurityBI360** – Security KPIs and executive dashboards
- **aiBAS360** – Breach & Attack Simulation

Supported Integrations

CGuard 2.0 integrates seamlessly with:

- **Cloud Platforms:** AWS, Azure, GCP, Oracle Cloud
- **Kubernetes Platforms:** AKS, EKS, GKE, OpenShift
- **Identity Providers:** Okta, Azure AD, AWS IAM
- **DevOps Tools:** GitHub, GitLab, Jenkins, Terraform
- **ITSM & SOAR:** ServiceNow, Jira, Slack, Microsoft Teams
- **Seceon Platforms:** Native integration with aiSIEM and aiXDR-PMax

Ideal For

- Enterprises adopting multi-cloud or hybrid cloud strategies
- MSSPs seeking to offer Cloud MDR/XDR
- Organizations running containerized apps in production
- **Compliance-heavy sectors:** Healthcare, Finance, Government, Pharma

Deployment Options

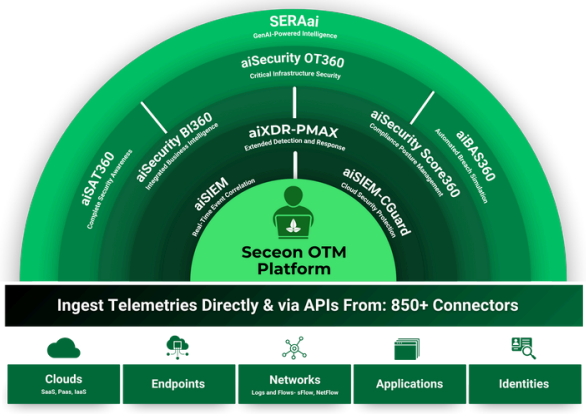
- SaaS (Seceon Cloud)
- Self-Hosted (Kubernetes-ready)
- Multi-Tenant for MSSPs

Summary

CGuard 2.0 sets a new standard in cloud security by offering:

- **True Multi-Rule Correlation** that detects complex and stealthy threats missed by single-rule approaches.
- **Comprehensive Cloud Coverage** across O365, Azure, AWS, and GCP.
- **Zero-Configuration Onboarding** with 200+ built-in detection rules.
- **Dynamic, Automated Response Actions** that are tailored to your cloud environment, enabling rapid mitigation of threats.
- **A Unified, Tenant-Aware Interface** that empowers both novice and advanced security teams.

CGuard 2.0 not only anticipates threats, it actively fights them with intelligent, integrated detection, correlation, and response mechanisms. Protect your cloud environment with a solution designed to tackle today's advanced security challenges.



About Seceon

Seceon enables MSPs, MSSPs, and IT teams 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 augments and automates MSP and MSSP security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 680 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

Learn more about Seceon aiSIEM-CGuard 2.0

Schedule a Demo www.seceon.com/contact-us/