Seceon aiSIEM-CGuard

Seceon aiSIEM-CGuard takes a holistic approach to cybersecurity and cloud and SaaS posture management (CSPM, SSPM) by gathering deep insights from clouds, endpoints, applications, and identity and applies threat intelligence to detect indicators of compromise and indicators of behavior like malware, ransomware, and other high-risk attacks.

It alerts your teams and automates a response which may include blocking, stopping, or placing the threat into quarantine. It all happens in real time and reduces risks and meets compliance and security audit requirements.

- Instant agentless detection and response - no software and no hardware required.
- Protect email, identities, cloud storage, collaboration, cloud infrastructure, and endpoints.
- Detect high-risk threats like malware, ransomware, phishing, data loss, advanced persistent threats, brute force attacks, and millions of today's cyber threats.
- Automatically block, stop, and quarantine attacks, reducing downtime and dangerous malicious attacks against your data, applications, devices, and users.
- Easily answer audit questions with extensive reports and data capture for insurance, industry compliance regulations and your customers.

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

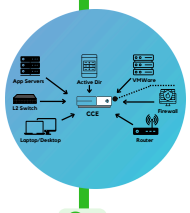
Enable instant responses to governance policy violations through user-defined controls and initiate automated remediation to threats with high severity and confidence level, targeted at business-critical assets.

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.

Sample Threat Types & Use Cases Addressed by Seceon aiSIEM-CGuard

Remote Workplace

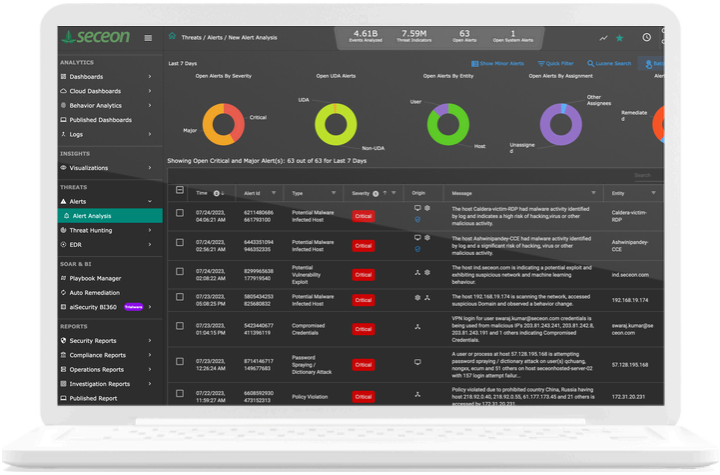


On Prem/Data Centre

- Early Malware & Ransomware Detection
- Insider Threats
- Data Breach (Exfiltration)
- DDoS Attacks
- Web Exploits
- Brute-Force Attacks
- Vulnerability Exploits
- IoT-IIoT Security
- DNS Protection
- Endpoint Isolation
- Threat Containment
- Data Loss Prevention
- Deep Threat Hunting
- File Integrity Monitoring
- MITRE ATT&CK TTPs
- Policy Enforcement (Network, Database, Internet etc)

Connect Cloud-Based Telemetry Sources

- **Amazon/AWS**
  CloudWatch, CloudTrail, S3, RDS
- **Microsoft Azure Environments**
  M365, OneDrive, SharePoint, NSG, Government Cloud, Cloud App Security
- **Google Cloud**
  Google Workspace, StackDriver Flow Logs, Pub/Sub APIs
- **Other Cloud (IaaS / SaaS)**
  Oracle Cloud, ServiceNow, Slack, others
- **Endpoints**
  Sources like SentinelOne, CrowdStrike
- **Networks**
  Cloud networks, and cloud telemetry sources like Zscaler
- **Identities**
  Azure AD, Okta, Google Workspace and other cloud identities
- **Other cloud-based telemetry**



Seceon Dashboard

PRODUCT FEATURES	Seceon aiSIEM-CGuard	Seceon aiXDRPMax
Automated Threat Detection for Cloud Telemetry Enabled Sources	✓	✓
Automated and Semi-Automated Remediation	✓	✓
Advanced Correlation with Contextual Enrichment	✓	✓
Network Behavior Anomaly Detection and Network Traffic Analysis	✓	✓
User Entity Behavior Analytics	✓	✓
Visualization, Alerts, Notification and Incident Management	✓	✓
Threat Hunting and MITRE ATT&CK Framework	✓	✓
Log Collection, Retention and Forensics	✓	✓
Administration and Provisioning	✓	✓
Continuous Compliance, Audit and Reporting	✓	✓
Multi-tenant, designed for isolation between clients or organizations	✓	✓
Seceon aiSecurity Score360 Reports	✓	✓
Windows OS Logs Linux Logs Collection (Configurable)	✓	✓
Endpoint Detection & Response, EPP	✓	✓
Device Control	✓	✓
Data Control & Data Security	✓	✓

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 640 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 8,800 clients.

Learn more about Seceon aiSIEM-CGuard

Schedule a Demo www.seceon.com/contact/