MARKETSANDMARKETS™

seceon
SECURITY FOR EONS

MODERNIZING SIEM FOR HIGH-VOLUME AND HIGH-COMPLEXITY ENVIRONMENTS

From Log-centric Monitoring to AI-driven Security Intelligence - **With Seceon aiSIEM**



EXECUTIVE SUMMARY

Security Operations Centers (SOCs) are approaching a structural tipping point. The volume, velocity, and diversity of security telemetry have outpaced the architectural assumptions underlying traditional SIEM platforms, creating growing challenges in detection, correlation, and response.

Global data volumes are projected to exceed 221 zettabytes by 2026, while approximately 90% of enterprise data remains unstructured. At the same time, 89% of organizations now operate in multi-cloud environments, expanding telemetry across endpoints, identities, networks, SaaS applications, and cloud workloads.

These trends are increasing the scale and complexity of security operations beyond what traditional SIEM architectures were originally designed to manage.

LEGACY SIEM UNDER PRESSURE — BY THE NUMBERS

221 Zettabytes Global Data Volume by 2026

90% Of Unstructured Enterprise Data

89% Of Organizations Operating Multi-cloud Environment

Source: Flexera State of the Cloud Report 2025; Rubrik Cloud Data Security Research

The challenge is no longer collecting data—it is extracting actionable intelligence from massive volumes of distributed telemetry. Legacy SIEM platforms rely on centralized log collection, rule-based correlation, and volume-driven licensing models that become increasingly expensive and difficult to scale. As attack surfaces expand and response windows shrink, organizations require greater visibility, context, and automation to identify and contain threats faster.

The Global SIEM Market Is Projected To Grow Significantly, Driven By Cloud Adoption, AI, And Convergence.

USD 8.39 BILLION (2026) → 10.3% CAGR (2026–2031) → USD 13.67 BILLION (2031)

Strong and sustained growth reflects the industry's shift toward intelligence-driven, cloud-native security operations.

12.2% CAGR

NEXT-GENERATION SIEM

Driven by advanced analytics, AI, automation, and improved security outcomes.

13.0% CAGR

CLOUD-BASED DEPLOYMENT

Accelerated by cloud adoption, scalability, flexibility, and cost efficiency.

Source: MnM Research and Analysis

GLOBAL SIEM MARKET OUTLOOK

MarketsandMarkets research indicates a clear industry shift toward AI-driven, scalable, and operationally efficient security platforms. Growth is being driven not by incremental demand for log management, but by a broader transformation in how security data is collected, correlated, analyzed, and acted upon.

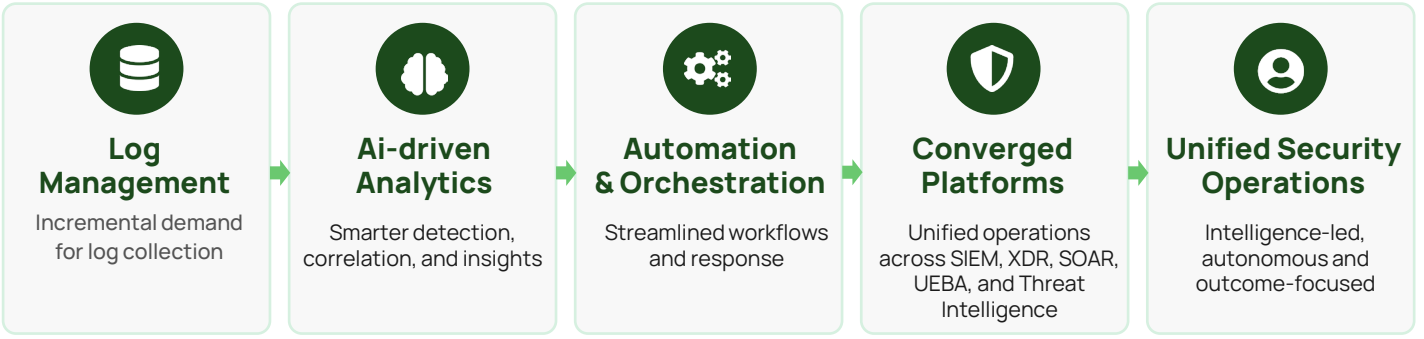
The transition to AI-native SIEM is being driven by four structural shifts:

- Security telemetry is growing faster than traditional architectures can efficiently process
- Organizations are consolidating fragmented security tools into unified operational platforms
- AI, automation, and behavioral analytics are becoming essential for improving detection and response outcomes.
- Security teams are prioritizing operational efficiency, faster investigations, and measurable business value

The Evolution Toward Ai-native Security Operations

Organizations that modernize their security operations around AI-native SIEM architectures will be better positioned to manage growing telemetry volumes, reduce operational complexity, and improve cyber resilience. The shift is no longer from one SIEM platform to another—it is from log-centric monitoring to intelligence-driven security operations.

Investment Is Shifting Toward Ai-native Security Operations



Source: MnM Research and Analysis

What Ai-native Security Operations Enable?

- ✓ Continuous Detection - Correlate telemetry, behavioral signals, and threat context in real time to improve detection accuracy and reduce alert fatigue.
- ✓ Automated Investigation - Reduce manual triage and accelerate root-cause analysis through AI-driven correlation, enrichment, and prioritization.
- ✓ Orchestrated Response - Automate containment, remediation, and response workflows to reduce response times and improve operational consistency.
- ✓ AI-Assisted Decision Making - Prioritize alerts based on risk, confidence, and business context, enabling analysts to focus on the most critical threats.
- ✓ Operational Scalability - Improve security outcomes without proportionally increasing headcount, allowing SOC teams to operate more efficiently at scale.

Executive Implications

- ➢ **Platform consolidation is becoming a strategic priority,** as organizations seek to reduce tool sprawl and unify security operations across SIEM, XDR, SOAR, UEBA, NDR, and threat intelligence.
- ➢ **Visibility and context can no longer be treated as separate disciplines.** Modern security operations require unified telemetry, behavioral analytics, and contextual intelligence to transform data into actionable insights.
- ➢ **Human-centric scaling models have reached their limits.** The challenge is no longer how many analysts an organization can hire, but how much of the detection, investigation, and response lifecycle can be safely automated.
- ➢ **Detection speed is emerging as a critical measure of cyber resilience,** with organizations increasingly prioritizing faster identification, investigation, and containment of threats.

> As MarketsandMarkets perspective, the growth is being driven not by incremental demand for log management but by a wholesale re-architecture of security operations—in which data, analytics, automation, and response are unified to deliver measurable business outcomes.

TABLE OF CONTENTS

Chapter 01 — The Core Challenge: Scaling SIEM in a High-Volume Threat Landscape — 04

Chapter 02 — Bridging the Gap: The Gap with Legacy SIEM and the Shift Toward AI-Native SIEM — 05-06

Chapter 03 — The Seceon Perspective: Enabling AI-Driven, Scalable Security Operations with aiSIEM — 07-11

- ✓ Seceon's aiSIEM Platform
- ✓ Seceon's aiSIEM CGuard 2.0 Platform
- ✓ Seceon - Applied Use Cases: Seceon aiSIEM Platform

Chapter 04 — Conclusion -The Future of SIEM is AI-Native, Unified, and Autonomous — 12

This whitepaper is designed for **CISOs, CIOs, SOC leaders, MSSP/MDR executives, security architects, IT operations leaders, and technology decision-makers** evaluating next-generation SIEM strategies. It examines why legacy SIEM models are failing, how AI-native SIEM platforms are reshaping the market, and how solutions such as Seceon can help organizations reduce complexity, improve detection accuracy, and build a scalable, future-ready security operations foundation.

The Core Challenge: Scaling SIEM in a High-Volume Threat Landscape

Modern enterprises are not short on security data—they are drowning in it. Logs, network flows, endpoint telemetry, cloud workload events, identity signals, and application activity now stream continuously from dozens of sources. Many organizations operate **20–30 security tools,** each generating its own alerts and data formats. A 20,000-employee enterprise can see **3,000+ security alerts per day;** the average enterprise SOC receives 4,400+ daily alerts, and large organizations often exceed 10,000 **per day.** The challenge is no longer data collection; it is converting relentless signal volume into decisions fast enough to matter.

The Economics of Legacy SIEM

The financial model of legacy SIEM is the root cause that the operational metrics merely express. Volume-based licensing turns every additional log source into a recurring cost decision, forcing security teams into a corrosive trade-off: ingest less data to control costs, or ingest everything and absorb runaway costs.

Studies show **59% of SOC teams** report dealing with too many security alerts, while **55% struggle** with excessive false positives—highlighting the growing operational burden of alert overload and investigation fatigue.

Source: Splunk State of Security 2025

OPERATIONAL METRICS: THE PRESSURE ON SOCS

Operational Metric	Typical Value	Operational Consequence
Security Tools Operated By Organizations	20–30	Fragmented telemetry; no unified context
Alerts per Day (Large Enterprise)	3,000+	Triage capacity routinely exceeded
Average Daily Alerts (SOC)	4,400+	Manual review becomes statistically impossible
Alerts per Day (Large Organizations)	10,000+	Throughput collapses under volume
Investigation Time per Alert	~30 minutes	Critical signals queue behind noise
SOC Overwhelmed	90%	Sustained operating-in-deficit state
Analysts Behind Workload	80%	Genuine threats silently expire in the queue
Uninvestigated Alerts	25-62%	Half of analyst effort spent on non-events
False Positive SIEM Alerts	60%+	Fragmented telemetry; no unified context

Source: Splunk State of Security 2025; D3 Security Alert Fatigue Research; Microsoft Security Research; MarketsandMarkets Analysis

The hidden tax compounds operationally: Microsoft research indicates that the organizations running highly fragmented SOCs spend roughly **40% more on operational labor** than those with consolidated tooling.

> **The target to reach remains the canonical illustration: find the right alert, buried beneath noise and disorienting false positives. The core challenge is transformation—not the collection of data or detection itself, but the acceleration of automated, content-rich prioritization.**

IMPLICATIONS FOR CISOS

- ✓ **Alert volume is not the real problem** - Context and prioritization determine what matters.
- ✓ **Human-driven scaling has reached its limits** - More analysts do not proportionally improve security outcomes.
- ✓ **Operational efficiency is a security imperative** - Faster investigations drive resilience
- ✓ **Fragmented visibility creates blind spots** -Silos delay detection and increase risk.

Modernizing SIEM is no longer a technology decision—it is a strategy for workforce resilience, operational efficiency, and cyber-risk reduction.

BRIDGING THE GAP: The Gap with Legacy SIEM and the Shift Toward AI-Native SIEM

SIEM platforms once transformed cybersecurity operations by centralizing logs, correlating events, and giving SOC teams a single view of security activity. However, the enterprise attack surface has fundamentally changed. Modern organizations now operate across hybrid cloud, SaaS, remote users, identities, APIs, endpoints, IoT, and OT environments, creating security data that is faster, broader, and far more complex than legacy SIEM architectures were built to manage. As a result, the gap between traditional SIEM performance and modern security requirements continues to widen.

Where Legacy SIEM Falls Short?

Across hybrid and multi-cloud environments, Mandiant's M-Trends research stated that the global median dwell time sits in the 11-to-14-day range, and IBM's 2025 Cost of a Data Breach Report measured that the full breach lifecycle at 241 days, 158 days to identify, and 83 days to contain, even after reaching a nine-year low. Set that against CrowdStrike's 29-minute average breakout time, and the asymmetry is stark: adversaries penetrate an environment in minutes, while defenders measure detection and containment in days to months. The gap is not incremental; it is the central problem AI-native architecture exists to solve.

> **From MarketsandMarkets perspective,** the defining characteristic of next-generation SIEM platforms is not simply improved analytics, but the ability to combine detection, investigation, enrichment, and response within a unified AI-driven operational framework. Organizations are increasingly prioritizing platforms that reduce operational complexity while improving security outcomes.

Legacy SIEM vs. AI-Native SIEM

Legacy SIEM Key Gap		AI-Native SIEM Advantage
Limited across hybrid environments	70%+ report limited visibility	Unified telemetry across environments
High false positives	50%+ are false positives	AI correlation and prioritization
Manual workflows	25–30% on manual triage	Automated enrichment and guided response
Average breach lifecycle	~241 days to identify + contain	Real-time analytics and faster MTTR
Tool Sprawl	20–30 security tools	Converged SIEM + XDR + SOAR + UEBA + NDR
Human Capacity Constraint	4,400+ alerts/day	Autonomous triage and scalable operations
Detection Rules	Static rules miss unknown threats	Behavioral analytics + ML anomaly detection

Source: IBM Cost of a Data Breach, 2025; Mandiant M-Trends, 2025; CrowdStrike Global Threat Report, 2026; MarketsandMarkets Analysis, 2026

WHAT DEFINES AN AI-NATIVE SIEM?

- **Unified telemetry** across endpoint, network, cloud, identity, and application environments.
- **Behavioral analytics and machine learning** for anomaly detection and threat prioritization.
- **AI-assisted investigation and enrichment** to reduce analyst workload.
- **Automated response orchestration** that accelerates containment and remediation.
- **Platform convergence** that unifies SIEM, XDR, SOAR, UEBA, NDR, and threat intelligence into a common operational framework.

From Visibility to Autonomy

AI-native SIEM architectures extend beyond detection by combining data, analytics, automation, and response into a continuously improving security operations model.

Source: MarketsandMarkets Analysis

AI-NATIVE SECURITY OPERATIONS STACK

From Data Collection to Autonomous Security Operations

1. SECURITY DATA PIPELINES

Ingest, normalize, enrich, and route data across the enterprise and cloud.

- High-throughput ingestion
- Data normalization
- Enrichment & correlation
- Reliable delivery

2. SECURITY DATA LAKE

Centralized repository for structured and unstructured security data at scale.

- Massive scale
- Flexible storage
- Historical analytics
- Cost optimization

3. CONVERGED SIEM+XDR+SOAR +NDR

Unified platform combining detection, investigation, response, and network visibility.

- Unified detection
- End-to-end response
- Automation & orchestration
- Extended coverage

4. AI SECURITY COPILOTS

AI-powered assistants that augment analysts with guided, automated support.

- Natural language interface
- Guided investigations
- Threat summarization
- Analyst productivity

5. AGENTIC AI

Autonomous AI agents that reason, decide, and act across the security lifecycle.

- Autonomous reasoning
- Decision & action
- Workflow orchestration
- Continuous learning

6. AUTONOMOUS SOC

Self-optimizing operations that continuously detect, investigate, respond, and adapt.

- Continuous protection
- Adaptive response
- Minimal intervention
- Business resilience

DATA FOUNDATION → INTELLIGENCE • AUTOMATION • AUTONOMY

Source: MarketsandMarkets Analysis

The six layers represent a progression of maturity, not discrete tools. Data pipelines and lakes enable scalable analytics; converged platforms unify visibility; and AI copilots and agentic AI add intelligence and automation, culminating in autonomous SOC operations.

MARKETSANDMARKETS KEY OBSERVATION

The future of security operations will not be defined by how much data organizations collect, but by how effectively they transform telemetry into actionable intelligence. AI-native SIEM architectures represent this shift by combining visibility, analytics, automation, and response into a unified operating model designed for modern threat environments.

Against this backdrop, vendors are reimagining SIEM architectures around AI-native principles. Platforms that combine unified telemetry, behavioral analytics, automation, and response orchestration are increasingly emerging as the foundation of modern security operations.

How Security Operations will Evolve Beyond Traditional SIEM?

The next evolution is **Agentic AI and platform convergence**. Leading enterprises now seek unified platforms that integrate SIEM, XDR, SOAR, UEBA, NDR, and threat intelligence into a single operational layer. Emerging AI agents can autonomously triage alerts, gather context, recommend remediation, and execute approved workflows with human oversight. Combined with **Zero Trust** strategies that require identity-centric visibility and continuous verification, AI-native SIEM is becoming the new foundation for modern SOC operations. The future of SIEM is no longer log management—it is autonomous detection, continuous validation, and machine-speed response

The Next Frontier of AI-Native Security Operations

How Security Operations Will Evolve Beyond Traditional SIEM

01 AGENTIC AI

AI agents autonomously understand context, determine next actions, and execute security workflows with minimal analyst intervention.

Impact:
Scalable, adaptive, and continuously improving security operations.

02 AUTONOMOUS INVESTIGATIONS

From alert triage to enrichment, correlation, and containment, investigations become increasingly automated and self-directed.

Impact:
Reduced MTTR, greater analyst efficiency, and faster response outcomes.

03 IDENTITY-CENTRIC SECURITY

Identity becomes the primary security control layer, with authentication, behavior, privilege, and risk continuously evaluated.

Impact:
Stops identity-based attacks at the source.

04 ZERO TRUST ANALYTICS

Continuous verification and behavioral analytics replace perimeter-based trust models across users, devices, applications, and workloads.

Impact:
Never trust, always verify.

OUTCOME:

Autonomous, Identity-Aware, and Continuously Adaptive Security Operations

The future SOC combines AI-driven decision making, automated investigations, identity intelligence, and continuous trust validation into a unified operating model.

MARKETSANDMARKETS PERSPECTIVE

These four trends represent the next stage in the evolution of AI-native security operations. As organizations continue to modernize security architectures, the focus will shift from improving detection alone to enabling autonomous investigations, identity-aware decision making, and continuous risk validation. Together, these capabilities will define the future operating model of modern SOCs.

Sources: CrowdStrike Global Threat Report 2025; IBM X-Force Threat Intelligence Index 2025; Google Cloud Security Forecast 2025; CISA Zero Trust Maturity Model 2.0; MarketsandMarkets Analysis 2026.

Future Outlook

The future of security operations will be shaped by the convergence of autonomous investigations, identity intelligence, and continuous trust validation. Organizations that establish strong data foundations and adopt AI-native operating models today will be better positioned to scale security outcomes without a proportional increase in operational complexity. In this environment, AI-native SIEM will increasingly serve as the foundation for intelligent, adaptive, and continuously evolving security operations.

The next section explores how Seceon operationalizes this vision through its AI-native SIEM platform.

How Seceon Supports Bridging the Gap with AI-Native SIEM?

Seceon's **aiSIEM platform** is helping organizations transition from legacy SIEM to **AI-native, outcome-driven security operations** by combining threat detection, analytics, investigation, and automated response in one unified platform. Instead of relying on static rules and fragmented tools, Seceon uses AI/ML-driven correlation, behavioral analytics, and contextual intelligence to detect real threats faster while reducing operational noise.

Security Challenge

Traditional SIEMs Fall Short

- Legacy SIEMs are slow, complex, and miss critical threats, leaving blind spots across the network and endpoints.
- Teams drown in 500+ daily alerts with 40% false positive rates.
- High deployment complexity and slow scaling across hundreds of devices.
- Heavy reliance on manual rules and skilled analysts slows response and remediation.

43% Miss Critical Threats

20% False Positive Rate

Seceon's aiSIEM Solution

AI-Powered Real-Time Defense

- Real-time AI/ML-driven detection with full coverage of NetFlow, logs, servers, endpoints, and cloud assets.
- Intelligent filtering, policy tracking, automated alerts, cutting noise by 90%.
- aiSIEM scales across 400+ assets within hours, not weeks.
- Automated threat correlation, behavior-based threat models, and actionable remediation.

99.7% Detection Rate

90% Noise Reduction

Source: Seceon

How Seceon Adds Value?

✓ **95% - REDUCED MTTD**
While traditional SIEM takes hours or days, Seceon aiSIEM detects threats in seconds, cutting MTTD by 95%

✓ **50% -CUT OPERATIONAL COSTS**
Seceon aiSIEM automates threat response, cutting SOC costs by up to 50% versus legacy SIEM

✓ **100%- INFRASTRUCTURE COVERAGE**
Seceon aiSIEM provides complete visibility across all logs, endpoints, cloud, and networks

Source: Seceon

THE SECEON PERSPECTIVE: Enabling AI-Driven, Scalable Security Operations

AI-Native XDR for Unified, Scalable, and Outcome-Driven Securityc

SECEON

Organizations are transitioning toward AI-native security operations, and platforms must provide unified visibility, behavioral analytics, automated response, and scalable deployment models. Seceon's aiSIEM platform is designed to address these requirements through a converged approach to detection, investigation, and response.

The value of AI-native SIEM lies not only in faster threat detection but in its ability to reduce operational complexity by consolidating analytics, automation, and response into a unified operating mode. Seceon has built the Open Threat Management (OTM) Platform, an AI/ML-powered architecture that operationalizes this vision at enterprise scale.

The OTM Platform encompasses Seceon's core product suite: aiSIEM, aiSIEM CGuard 2.0, aiXDR-PMax, and aiMSSP — each purpose-built to address a dimension of the modern security operations challenge, yet unified into a single, coherent ecosystem.

SECEON'S aiSIEM PLATFORM

Seceon positions aiSIEM as an AI-native detection-and-response platform that consolidates SIEM, XDR, behavioral analytics, automated response, and threat intelligence into a single operational layer.

Architecturally, this reflects the **platform convergence** thesis: rather than stitching together discrete SIEM, UEBA, NDR, and SOAR tools, the platform correlates raw network telemetry (NetFlow) with traditional log sources, applies behavioral analysis and threat-context enrichment, and drives automated responses through a unified pipeline.

Its vendor-agnostic integration model is designed to ingest data from diverse devices and systems, addressing the cross-environment visibility gap left by legacy, log-centric SIEM.

Seceon aiSIEM: Full-Spectrum Network Visibility NetFlow + Traditional Log Sources

Seceon aiSIEM

Raw Network Monitoring

- Collects NetFlow from endpoints, switches, firewalls, cloud services & hybrid infrastructures.
- Detects abnormal traffic patterns traditional logs might miss — IPv6 exploits, lateral movements.

Vendor-Agnostic Integration

- Ingests data from 900+ devices and systems for unified threat detection across all assets.
- Eliminates blind spots caused by single-vendor reliance.

SOC Performance & Metrics

- Tracks alert response across analysts and playbooks, highlighting bottlenecks and patterns.
- Role-based dashboards guide SOC improvements and enable predictive threat mitigation.

Behavioral Analysis

- AI/ML models correlate NetFlow and event data, detecting anomalies with behavioral baselines.
- Real-time risk scoring adapts continuously lateral movement, MitM, ransomware detection.

Threat Context Enrichment

- Aggregates telemetry, vulnerability data & threat intelligence from endpoints, networks & cloud.
- Enriched, high-confidence alerts with actionable context for faster threat prioritization.

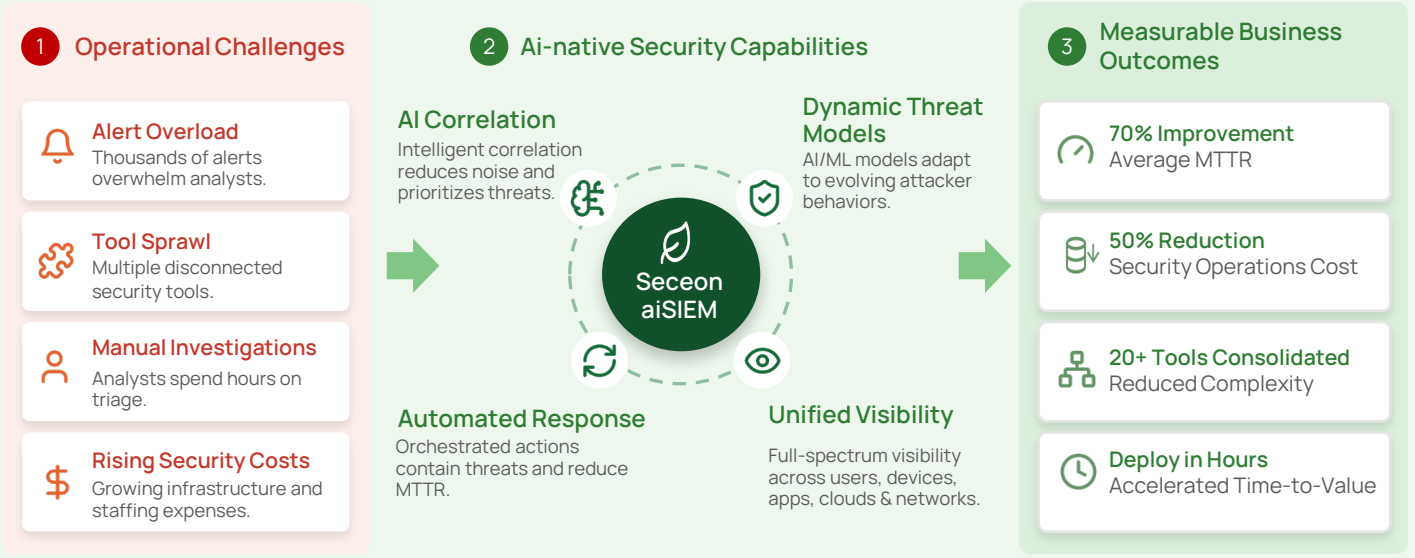
Autonomous Threat Response

- Automatically triggers EDR/XDR actions or SOC alerts, containing threats in real time.
- Reduces risk exposure by isolating threats, blocking malicious activity, detecting lateral movement.

Source: Seceon

How Seceon aiSIEM Creates Measurable Security ROI?

The strongest ROI driver in AI-native SIEM platforms is not a single feature but the consolidation of analytics, investigation, automation, and response into a unified operating model. Organizations increasingly measure success through reduced operational complexity, faster response times, and improved security outcomes rather than through tool count or log volume alone.



Source: Seceon

BUSINESS IMPACT Reduce operational overhead, improve analyst productivity, accelerate threat detection, and scale security operations without proportional increases in cost.

DEPLOYMENT OPTIONS

SaaS
Seceon Cloud – Fully managed, instant onboarding

Self-Hosted
Seceon Cloud – Fully managed, instant onboarding

Kubernetes-Ready
Deploy in your own environment

Multi-Tenant
Built for MSSPs managing multiple clients

SUPPORTED INTEGRATIONS

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

SIEM & SOAR Ecosystem
Splunk, Microsoft, ServiceNow, Jira, Slack, Teams

Native Integration
with aiSIEM and aiXDR-DMAX

How does aiSIEM impact?

- ✓ Reduce analyst workload through AI-driven investigations.
- ✓ Consolidate fragmented security tools into a unified platform.
- ✓ Improve detection and response efficiency while lowering operational costs.

Source: Seceon

Seceon aiSIEM CGuard 2.0 Key Capabilities

Seceon aiSIEM CGuard 2.0
Revolutionizing Cloud-Native Security with Unified AI-Driven Protection

Comprehensive Cloud-Native Application Protection

Cloud Workload Protection
Runtime defense for VMs, containers & serverless

Multi-Cloud
Native Coverage for AWS, Azure, GCP & private clouds

Posture Management
Auto-fix misconfigurations & compliance gaps

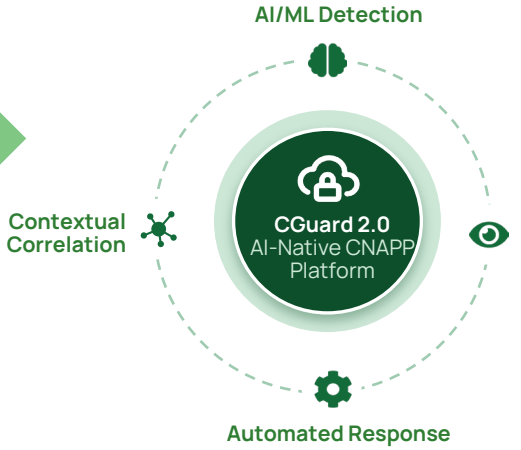
Infrastructure-as-Code
Scan Terraform, CloudFormation & K8s manifests

WHY CGUARD 2.0 MATTERS FOR CLOUD SECURITY

CLOUD ENVIRONMENTS

- **Cloud Workloads** VMs, containers, serverless
- **Cloud Identity** Users, roles, service accounts
- **Cloud Infrastructure** Networks, storage, databases
- **Compliance & Policy** Regulations, standards, governance

CGuard 2.0 CAPABILITIES



OUTCOMES

- **Unified Visibility** Across workloads, identities, infrastructure & apps
- **Continuous Monitoring** Real-time detection across multi-cloud environments
- **Automated Response** Reduce MTTR with policy-driven automation
- **Policy Enforcement** Ensure compliance & reduce risk exposure

PROVEN BUSINESS IMPACT

85%	80%	60%	900%	95%
False Positive Reduction	SOC Cost Reduction	Faster Threat Detection	Ready Integrations	Threat Detection Accuracy

TRANSFORM YOUR SECURITY ARCHITECTURE TODAY

RAPID DEPLOYMENT
Deploy comprehensive security in weeks, not months

COST OPTIMIZATION
80% SOC cost reduction through unified platform

SUPERIOR PROTECTION
85% false positive reduction with AI-driven detection

CHANNEL PARTNERSHIP
Exclusive channel-first go-to-market model

Source: Seceon aiSIEM Cguard 2.0 Platform, and MarketsandMarkets Analysis

> Organizations increasingly require cloud-native security platforms that combine visibility, analytics, automation, and compliance management. CGuard 2.0 addresses this requirement through cloud workload protection, cloud identity security, automated response, and multi-tenant deployment capabilities.

Seceon - Applied Use Cases: Seceon aiSIEM Platform

Seceon's role in modern security transformation is most evident in environments where organizations must manage high-volume, distributed, and multi-tenant operations with real-time visibility and rapid response. The following case studies illustrate how Seceon helps address critical requirements such as unified telemetry across endpoints, networks, and cloud, AI-driven threat correlation, automated response, and scalable security operations.



Englewood Health
Deployed Seceon aiSIEM to Modernize Healthcare Cybersecurity Operations

CHALLENGE:

Englewood faced growing cybersecurity pressure from ransomware threats, insider risks, the expansion of IoMT/medical devices, and strict compliance mandates such as HIPAA. Legacy security tools created fragmented visibility across clinical systems, networks, identities, and cloud applications, while manual investigations slowed response times and increased operational burden. The organization required a modern SIEM platform capable of improving detection speed, simplifying compliance, and reducing security overhead.

SOLUTION:

Following a modernization initiative, Englewood Health selected **Seceon aiSIEM** to unify telemetry, automate threat detection, and strengthen SOC efficiency. Seceon's platform delivered centralized monitoring across endpoints, networks, cloud systems, identities, and healthcare applications while applying AI-driven analytics and behavioral threat detection to surface actionable alerts.

KEY CAPABILITIES LEVERAGED:

- Unified telemetry across healthcare IT, cloud, endpoints, and identities
- AI/ML-driven behavioral analytics and anomaly detection
- Real-time threat detection and automated response workflows
- Continuous compliance reporting for HIPAA and regulatory needs
- Integrated SIEM, XDR, SOAR, and threat intelligence capabilities

This enabled Englewood Health to transition from fragmented monitoring to a more unified, intelligence-driven security operations model.

ABOUT ENGLEWOOD HEALTH: Englewood Health is a leading not-for-profit healthcare organization HQ in Englewood, New Jersey, serving communities across northern New Jersey and the New York metropolitan area. The organization operates an acute-care hospital, physician network, outpatient facilities, and specialized clinical services, managing a complex healthcare ecosystem that includes electronic health records (EHRs), connected medical devices (IoMT), cloud applications, and critical patient-care systems.

OUTCOME:

With Seceon aiSIEM, Englewood significantly improved cyber resilience and operational performance.

The organization achieved:

- **60% lower security overhead**
- **70% reduction in manual investigations**
- **90% faster detection and response workflows**
- Improved audit readiness and compliance visibility
- Stronger protection for patient data and connected environments

KEY TAKEAWAYS FOR SECURITY LEADERS

This Healthcare case highlights how Seceon helps regulated organizations modernize beyond legacy SIEMs by combining AI-native detection, automated response, unified visibility, and compliance readiness into a single platform. For the broader SIEM market, it reinforces the shift toward solutions that deliver measurable outcomes—not just alerts.

- Helps reduce common SIEM challenges such as alert fatigue, false positives, and delayed investigations
- Provides unified visibility across endpoint, network, cloud, identity, and OT environments
- Enables scalable deployment models for enterprises, MSSPs, and regulated industries
- Helps lower operational complexity and improve SOC efficiency
- Reflects growing demand for SIEM platforms focused on measurable security outcomes

For more Seceon's Customer Success Stories, click on **Customer Success Stories**

Source: Seceon Case Studies

Conclusion -The Future of SIEM is AI-Native, Unified, and Autonomous

Enterprise security has reached a defining inflection point. Traditional SIEM platforms, once essential for centralized log management and rule-based monitoring, are no longer sufficient for today's distributed, cloud-first, and high-speed threat landscape. Rising data volumes, fragmented toolsets, alert fatigue, and increasingly sophisticated attacks have exposed the limits of legacy architectures. The future of security operations belongs to platforms that combine intelligence, automation, and unified visibility at scale.

Generative AI and emerging Agentic AI capabilities enable faster threat detection, fewer false positives, automated investigations, and stronger response outcomes across modern environments. Seceon exemplifies this shift by combining unified telemetry, AI-driven correlation, automated workflows, and scalable deployment models to help enterprises and service providers modernize security operations with greater efficiency, resilience, and measurable business value.

Looking ahead, Several Key Trends Will Continue To Shape The Future of SIEM:

RISE OF AGENTIC AI IN THE SOC

Autonomous AI agents will increasingly triage, investigate, and respond with minimal analyst intervention

CONVERGENCE OF SECURITY FUNCTIONS

SIEM, XDR, SOAR, UEBA, NDR, and identity analytics will continue merging into unified security operations platforms

AUTONOMOUS INVESTIGATIONS

AI-assisted investigations are evolving toward autonomous triage, enrichment, and response workflows that reduce analyst workload and accelerate incident resolution.

SECURITY DATA PIPELINES & LAKES

Modern security operations increasingly depend on security data pipelines and open data architectures that improve scalability, retention, analytics, and cross-domain visibility

IDENTITY-CENTRIC ZERO TRUST OPERATIONS

Identity signals, access behavior, and continuous verification will become core pillars of modern SIEM strategy

The Path Forward: Strategic Priorities for CISOs

- ✓ Modernize security data architecture
- ✓ Reduce tool sprawl through platform consolidation
- ✓ Adopt AI-assisted investigations and response
- ✓ Build toward autonomous SOC operations
- ✓ Prioritize identity-centric security models

> "The future of security operations will not be defined by how much data organizations collect, but by how effectively they transform telemetry into actionable intelligence and measurable outcomes. Organizations that modernize their security operations today will be best positioned to build resilient, scalable, and increasingly autonomous security programs."

The defining question for security leaders is no longer whether AI belongs in security operations, but how organizations can safely operationalize autonomous decision-making.

AI-native SIEM provides the foundation for autonomous security operations by combining visibility, analytics, automation, and response into a unified operating model.

Contact

Sayali Saste
Associate Manager – MarketsandMarkets
sayali.saste@marketsandmarkets.com

Vidhu Rawat
Team Lead – MarketsandMarkets
vidhu.rawat@marketsandmarkets.com



About MarketsandMarkets

Founded in 2009, MarketsandMarkets (MnM) was built on a forward-looking vision: to identify and monetize the next wave of business opportunities embedded within global disruption. While others discussed megatrends like AI, 3D printing, IoT, and robotics, MnM saw a deeper insight—the unrealized revenue potential these shifts could unlock across industries.

MnM anticipates a USD 25 trillion revenue transformation in the B2B economy by 2030—driven not just by technology, but by macroeconomic shocks, policy shifts, climate pressures, and geopolitical flashpoints. Today, MnM tracks both emerging innovations and global dislocations—including landmark disruptions such as the 2025 US reciprocal tariffs—to help clients decode complexity, quantify exposure, and seize asymmetric growth opportunities ahead of competitors.

Over the past 13+ years, MnM has worked with 10,000+ clients across 30+ sectors, delivering over USD 140 billion in revenue impact. We've evolved from a market research publisher to a growth-enablement partner, powered by a 'GIVE Growth' philosophy and a 1,500+ strong team driven by outcome, not output.

Our commitment to strategic foresight and execution has earned us recognition from Forbes as one of America's Best Management Consulting Firms, and we remain the only India-origin firm on that prestigious list. What makes us a blue-ocean partner is our proprietary platform: Knowledge Store™—an AI-enabled, primary-research-driven market intelligence engine built to empower CXOs, strategy teams, and growth leaders to identify hidden inflection points and future profit pools in real-time.