GURUCUL AI-POWERED NEXT GEN SIEM

DATASHEET

Smarter Security for the Modern SOC.

Give your security operations team the platform to cut through noise, respond faster, and outsmart threats that rule-based tools were never built to catch. One AI-native engine unifies SIEM, UEBA, SOAR, ITDR, and data pipeline management, enhanced by a 24/7 AI Analyst that turns signal into decisive, defensible action.

40%+
Reduction in SIEM costs

70%
Fewer false positives with Behavioral AI

58%
Faster threat investigations

5000+
Out-of-the-box ML detection models

THE PROBLEM

Security Operations at a Breaking Point

Security teams are overwhelmed by data, alerts, and rising ingestion costs that force real compromises in visibility and control. Traditional SIEMs cannot scale, prioritize genuine threats, or manage costs while disjointed tools, manual processes, and outdated detection techniques slow response times and burn out analysts.

According to the Cybersecurity Insiders Pulse of AI SOC report, 96% of organizations lack complete visibility, and 62% cite alert fatigue as a key contributor to analyst burnout, prompting 78% to seek smarter SIEM alternatives.

THE SOLUTION

Gurucul Next-Gen SIEM Amplified by AI

Gurucul's AI-powered Next-Gen SIEM is purpose-built to address the limitations of traditional security platforms and meet the demands of modern SOCs. Cloud-native and modular by design, it supports flexible deployment across SaaS, cloud, on-premises, and hybrid environments.

Generative and agentic AI give analysts a natural-language co-pilot and automate repetitive tasks across the entire threat lifecycle, keeping them in control of critical decisions with transparent human-in-the-loop feedback. Native Data Pipeline Management (DPM) optimizes data ingestion and reduces storage costs while maintaining full visibility without compromising the budget.

HOW GURUCUL SOLVES IT

Five Pillars, One Unified Platform

Intelligent Data Management

Native Data Pipeline Manager enables pre-ingestion normalization, enrichment, shaping, filtering, and routing to or from any data lake, ensuring optimized data flow aligned with detections.

Advanced Security Analytics & Model Customization

Over 5,000 ML detection models pinpoint external, insider, and identity-based threats with continuous risk prioritization and daily threat content updates. Gurucul Studio's wizard-driven, low-code interface lets security teams build, customize, and share ML models without data science expertise, adapting rapidly to emerging threats.

Virtual AI SOC Analyst

Automates alert triage, investigation, and escalation around the clock. Extracts IOCs, enriches data, scores risk, and delivers MITRE-aligned reports so analysts can focus on what matters most.

Universal Federated Search

Search any data, in any format, in any location from a single console, boosting compliance, deepening investigations, and eliminating costs tied to data rehydration and movement.

Native SOAR and Agentic AI

Built-in orchestration and response capabilities stream case management and incident response. Agentic AI orchestrates enrichment, correlation, and response 24/7 while preserving analyst oversight.

COVERAGE

Built for High-Priority Use Cases

COST REDUCTION

Cut SIEM Costs by 40% or More

Lower data ingestion and storage expenses and consolidate point tools with native Data Pipeline Management, saving 40 to 87% on SIEM-related costs.

THREAT DETECTION

Faster, Smarter Detection

Reduce false positives by up to 70% and accelerate threat detection with a 40-60% shorter mean time to detect (MTTD) using 5,000+ ML behavioral models.

ANALYST PRODUCTIVITY

Free Your Analysts to Focus

Reduce investigation time by up to 58% and give analysts back up to 50% of their time, freeing them from repetitive triage so they can focus on strategic initiatives.

VISIBILITY

Enhanced Coverage Without Added Cost

Gain more than 40% additional visibility through full data control and native pipeline management without incurring added infrastructure expense.

SECURITY POSTURE

Stronger Defense Across Every Vector

Leverage 5,000+ ML models to expand SOC coverage, reduce false positives, and cut mean time to respond (MTTR) by 83% across external, insider, and identity threats.

DATA INDEPENDENCE

Own Your Data, Your Way

Maintain complete control over data and architecture with a bring-your-own-data-lake (BYODL) approach, supporting cloud, SaaS, or on-prem deployments without vendor lock-in.

PLATFORM CAPABILITIES

Key Capabilities of Gurucul Next-Gen SIEM

Behavioral-Informed Detections Instead of Static Rules

Replaces more than 85% of static rules with 5,000+ ML behavioral models. The dynamic risk engine assigns priorities based on 240 attributes and detects both known and unknown threats, including zero-day exploits and identity-based attacks.

Agentic AI

Orchestrates a network of AI agents to automate enrichment, correlation, and response across the full threat lifecycle, accelerating SOC workflows while preserving analyst oversight and decision authority.

Gen AI Co-pilot

Delivers real-time guidance, investigation summaries, and next-step recommendations, enhancing analyst efficiency and decision-making during active incidents.

Modular Architecture

License only what you need, when you need it. Start anywhere and scale as your SOC matures with flexible deployment across SaaS, cloud, on-premises, and hybrid environments.

Open and Extensible Design

No black boxes. Deep customization across detections, workflows, and integrations to fit unique environments. Over 10,000 pre-built content items and 98% MITRE ATT&CK framework coverage out of the box.

Agentless and Optional Agent

Lightweight, flexible deployment enables enhanced monitoring and data discovery when endpoint agents are needed, at enterprise scale, without a mandatory agent rollout.

Privacy and Compliance Controls

Granular RBAC, data masking, and user-level monitoring align with SOC 2, GDPR, HIPAA, PCI DSS, NIST 2.0, and CISA frameworks.

Proven Cost Savings

Gurucul's unified platform reduces ingestion and storage costs by 40-87%, eliminates tool sprawl, and streamlines workflows, enabling teams to ingest more data without incurring additional expense.

Rule-based tools fire at the end, after the damage. Gurucul's behavioral engine scores risk from step one contained before exfiltration, investigations compressed up to 83%, with a human in command.

HOW IT WORKS

Anatomy of an Attack — Worked at Every Step

1	**Alert Overload**	Thousands of low-fidelity alerts flood the queue.	**Gurucul AI** Correlates signals, scores risk in real time, and surfaces only what genuinely warrants attention.
2	**Threat Investigation**	Analysts spend hours piecing together fragmented data from disconnected tools.	**Gurucul AI** AI SOC Analyst automates triage, extracts IOCs, enriches context, and delivers an evidence-backed narrative.
3	**Identity Threat**	Compromised or over-provisioned accounts move laterally without triggering rules.	**Gurucul AI** UEBA and ITDR chain anomalies into one attack timeline mapped to MITRE ATT&CK.
4	**Data Exfiltration Attempt**	Sensitive data staged for exfiltration via cloud or personal email channels.	**Gurucul AI** Behavioral analytics detect clipboard, screenshot, and GenAI-channel misuse other tools miss.
5	**Response**	Manual playbooks delay containment, extending the window for damage.	**Gurucul AI** Agentic AI runs adaptive playbooks, isolates accounts and hosts automatically, before data leaves.

BY THE NUMBERS

How Does Gurucul Next-Gen SIEM Compare?

Feature	Gurucul NGSIEM	Other NGSIEM	Traditional SIEM
Cloud, Data Lake and Deployment Agnostic	●	◐	–
Cost Reduction with Native Data Pipeline Management	●	◐	–
AI Agent-Driven Visibility and Automated Data Ingestion	●	◐	–
Fully Customizable AI/ML Analytics	●	◐	◔
High-fidelity Detections with ML Model Chaining	●	◐	–
Dynamic Risk Prioritized Alerting and Case Management	●	◐	◐
Universal Federated Search	●	◔	–
Agentic AI-driven Alert Triage and Investigations	●	◔	–
Auto Triage with AI SOC Analyst	●	◔	–
Automated Response with AI Agent-Generated Playbooks	●	◔	–
Seamless Interoperability and Orchestration	●	◐	◐
Migration In As Little As 4 Weeks	●	◐	◔
Natural Language Threat Querying with SME AI Co-pilot	●	◐	◔

VALIDATED BY ANALYSTS | **2025 Gartner® Magic Quadrant™ Leader, SIEM · KuppingerCole Overall Leader, Intelligent SIEM · 4.9/5 Gartner® Peer Insights™ ·** a decade of behavioral AI, in production worldwide

COMPLIANCE - MAPPED | **SOC 2 · CISA · NIST 2 · GDPR · HIPAA · PCI DSS** with granular RBAC, PII masking & retention controls

PROOF IN THE FIELD

Real Customers. Real Results.

Global security teams trust Gurucul to modernize their SOC and detect threats that other platforms miss.

HEALTHCARE · FORTUNE 50

Healthcare Insurer

Rapidly detected and responded to insider threats, enforced geo-compliance policies, and uncovered repeat data exfiltration attempts with no endpoint agents deployed.

APPAREL · GLOBAL

Global Sportswear Company

Built a stable, scalable insider threat program that reduced false positives, protected critical IP, and accelerated response through robust XSOAR integration.

Replaced a legacy UEBA/SIEM

BANKING · GLOBAL

Banking & Financial Services

Identified and prevented insider threats while scaling effortlessly, handling 15TB of daily data ingestion across 250,000 users in more than 20 countries.

> "Gurucul is a real game changer. Next-Gen SIEM technology. I really like their threat hunting platform and reduction in false positives. With flexible UI, out-of-the-box integrations, customized models, and prioritized risk scoring."
>
> **MANAGER, IT SERVICES COMPANY**

OUTCOMES

Business Impact & Benefits

- Cuts SIEM and data ingestion costs by 40 to 87% through native pipeline management
- Eliminates tool sprawl by unifying SIEM, UEBA, SOAR, ITDR, and DPM on one platform
- Replaces over 85% of static detection rules with adaptive ML behavioral models
- Detects both known and unknown threats including zero-day exploits
- Automates regulatory compliance and audit readiness across major frameworks
- Reduces mean time to respond (MTTR) by up to 83%
- Returns up to 50% of analyst time from manual triage back to strategic work
- Delivers 40%+ more visibility without added infrastructure or storage cost
- Migrates existing SIEM environments in as little as four weeks
- Supports any deployment model without proprietary data lake lock-in

EXPANDED COVERAGE

Out-of-the-Box Use Cases & Compliance

Cloud infrastructure monitoring | Threat detection & response | Insider threat prevention | Incident response automation | AI-powered threat hunting | Compliance management | Any Data Lake (Snowflake, Databricks, S3) | Any Cloud (AWS, GCP, Azure)

See Gurucul Next-Gen SIEM in action.

Unified. Automated. Smarter security for every team.

REQUEST A DEMO →

ABOUT GURUCUL

Gurucul is the cost-optimized security analytics company founded in data science that delivers radical clarity about cyber risk. Our AI-native platform analyzes enterprise data at scale using machine learning and AI — so instead of useless alerts, you get real-time, actionable intelligence about true threats. As the original pioneers of behavioral analytics, Gurucul is trusted by Global 1000 enterprises and government agencies to minimize cyber risk.

Gurucul | 222 North Pacific Coast Highway, Suite 1310 | El Segundo, CA 90245 | 213-259-8472 | sales@gurucul.com |