REVEAL SECURITY ANALYTICS PLATFORM

Designed to deliver radical clarity into your cyber risk.

Gurucul provides a radically clear view of cyber risk through a dynamic security analytics platform purpose-built for real-time threat detection and incident response. From a single interface, you get prioritized insights about true threats and fine-grained context to expedite your response.

Designed to be ready Day One, the platform has unmatched versatility in deployment options, data ingestion, and customization so it adapts to your enterprise.

REVEAL is a dynamic security analytics platform that fills the gap where SIEM and XDR tools have failed so you can focus on battling threats, not the tools that should help you find them.

The REVEAL Security Analytics Platform helps enterprises uncover true threats and quantify cyber risk.

It provides real-time prioritized and actionable insights so you can spend more time on what's most important, eradicating threats.

Business Challenges

Security teams seeking clarity about their risk are increasingly faced with a data problem. Traditional SIEMs cannot cover their entire IT estate or scale to accommodate data ingestion, querying, and analysis. They must accept undue risk or seek an alternative.

Here are three signs a SIEM is maxed out and unfit for threat detection and response at scale:

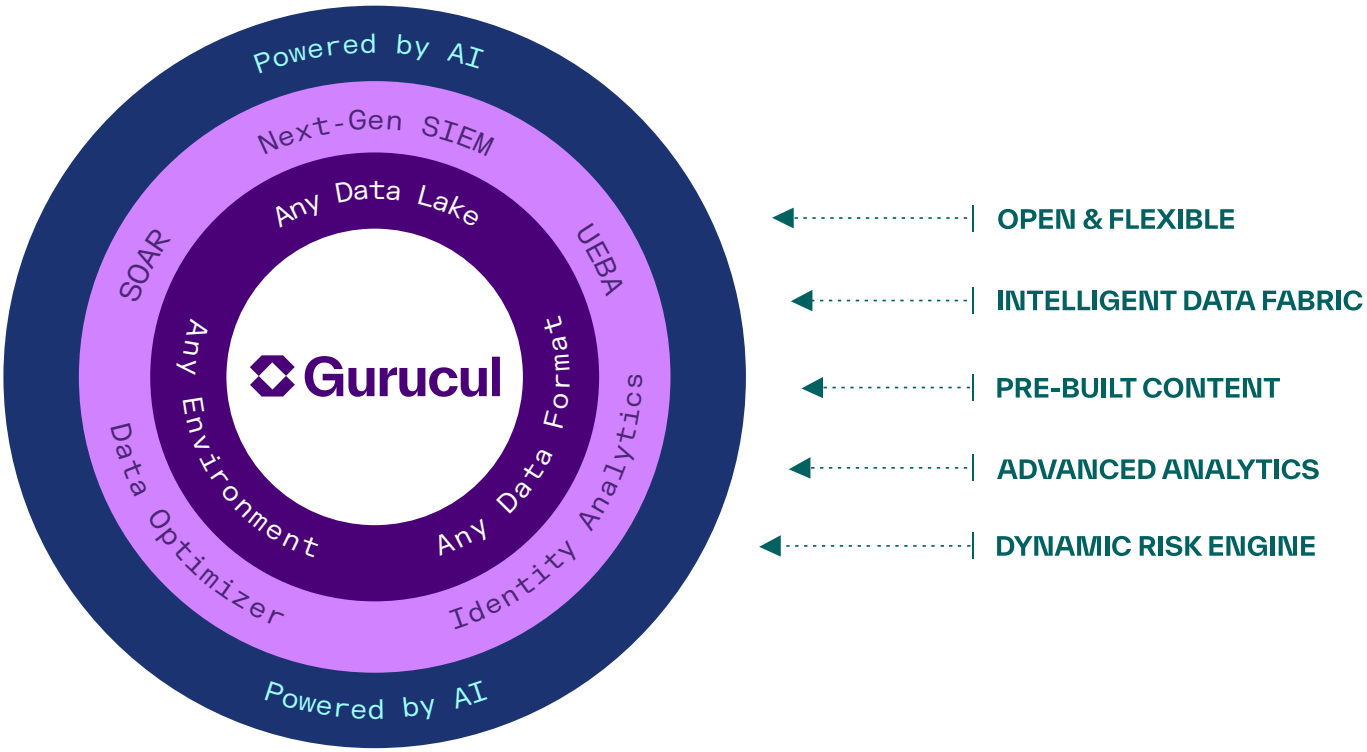
- It is inflexible and cannot conform to unique business demands, compliance requirements, risk tolerance, and existing processes.
- It generates endless false positives and is incapable of producing accurate and actionable insights in real time.
- It treats risk generically and is unable to quantify and prioritize threats across the enterprise.

These challenges lengthen the Mean-Time-To-Detect (MTTD) and Mean-Time-To-Respond (MTTR) by days, weeks and even months.

Gurucul

Introducing the REVEAL Security Analytics Platform

Gurucul developed a cloud-native platform that presents a stark contrast to failing SIEMs. It is designed to deliver results on Day One because it offers unmatched versatility in deployment, data ingestion and customizations.



Platform Design Principles

Data science is at the core of the platform's design, which is built to derive actionable insights from noisy structured and unstructured data.

Open and Flexible

Don't compromise or conform

Our cloud-native platform is open and completely adaptable, so you don't have to compromise on what your business needs or conform your security operations workflow. The platform supports whatever IT estate you have – on-premises, multi-cloud, or hybrid - and easily integrates with anything in your technology stack.

Most SIEMs today are inflexible. They can't be deployed into every IT estate or integrate with every tool. Many can't scale, which causes data ingestion failures and slow query and search times.

Gurucul's Advantages vs. SIEM

- Deploys anywhere and easily integrates into your tech stack.
- Delivers a ubiquitous experience in every IT environment and supports existing business processes.
- Performs at scale with rapid query and search response
- Auto scales to meet the most demanding compute requirements.

Intelligent Data Fabric

Ensure full visibility

Gurucul's intelligent data fabric gives you full visibility and coverage for your data, even nonsecurity data. It automatically ingests, interprets, enriches, reduces and routes data. Because it optimizes your data from source to destination, it can eliminate the need for third party data distribution platforms.

Gurucul's Advantages vs. SIEM

- Data ingestion is automatic. This eliminates the time wasted writing parsing rules and the expense incurred outsourcing to third parties or acquiring data distribution tools.
- Data is analyzed and enriched as soon as it is ingested.
- We can build any data pipeline within days and we provide you with a drag-and-drop interface to build them on your own.

Purpose-built Content

From ingestion to high-fidelity detections in seconds

Our content library has more than 10,000 modules that are fully enabled out of the box for fast time to value. The content can be easily modified to suit your unique needs.

Gurucul's Advantages vs. SIEM

- Modify content as needed with built-in wizards or a simple drag-and-drop interface.
- Eliminate time and money wasted on purchasing, downloading, and installing content.
- It doesn't require a special skill or proprietary vendor knowledge to use or modify the content.

Advanced Analytics

Turn data into actionable insights

Analytics are at the heart of Gurucul's platform. Our massive library of pre-tuned ML models has been developed and refined for more than a decade to drive high-fidelity detections, decrease false positives and find zero-day threats on Day One. Analytics can be applied to telemetry from any source to improve detection coverage.

Gurucul's Advantages vs. SIEM

- No data science expertise required to easily customize models with a drag-and-drop interface or build and import your own.
- Models can be chained together to automatically link and visualize the sequence of threats in one screen for high-fidelity detections.
- Models can easily be aligned to any compliance framework, like MITRE or PCI-DSS, using model category tags. Tags make it simple to maintain existing model maps, map new models to existing categories and add new categories.

Dynamic Risk Engine

Quantify and prioritize what matters for surgical response

Our dynamic risk engine quantifies and prioritizes risk in real time so you can respond before damage is done. As part of the platform's open and flexible design, you can customize risk models with dragand-drop ease to align to your risk tolerance.

Gurucul's Advantages vs. SIEM

- Risk models are dynamic and customizable giving you flexibility in how and what you score.
- A single consolidated and normalized risk score is generated for any user, entity, application or asset group across every transaction and entitlement.
- Elevate and assign the right case to the right person at the right time to ensure operational efficiency.

Artificial Intelligence

Streamline hunting and investigation to combat sophisticated threats

Gurucul's entire REVEAL platform is powered by AI, enabling it to learn from the ML models and perform complex tasks unmanageable by humans. Our generative AI engine broadly benefits security teams by working across the threat detection and response lifecycle to reduce MTTD, investigation time, and MTTR without compromising data privacy.

The REVEAL platform is powered by secure, native AI. It works behind the scenes improving detections using adversarial AI counter techniques to combat sophisticated threats. Unlike many SIEMs today that simply bolt on ChatGPT, our AI lets you leverage your own enterprise data and securely access external publicly-sourced data.

Gurucul's Advantages vs. SIEM

- Native, secure AI that doesn't expose your data to the public cloud.
- Simple UI empowers security teams to natural language queries to expedite investigations.
- Our AI securely queries both public and enterprise data.

Solving real world business problems

The platform was purpose-built to solve pressing cybersecurity issues. It can be customized to handle nearly any use case, including the most common.

Cloud Monitoring & Detection

Cloud Monitoring and Detection involves tracking and reviewing the performance of cloud-based applications and infrastructure to ensure optimal performance, availability, and security.

Problems it solves:

- Identify potential misconfiguration issues before they escalate, ensuring business continuity.
- Detect unauthorized access and underprivileged or dormant accounts.
- Detect multi-cloud attack campaigns"
- Identify performance bottlenecks

SOC Transformation

SOC transformation helps to build resilience and create efficiencies in daily operations. It involves restructuring and optimizing the SOC, streamlining operations, improving threat detection and response, and maximizing the value of cybersecurity investments.

Problems it solves:

- Slow and ineffective manual workflows.
- Noisy false positives that detract attention away from actual threats.
- Lack of visibility across the security landscape.

Cyber Threat Detection & Response

Cyber threat detection and response requires the use of advanced technologies and strategies to stay ahead of sophisticated attackers. It requires continuous monitoring, timely alerts, and rapid response actions to address breaches or vulnerabilities.

Problems it solves:

- Basic correlation rules won't detect unknown and Zero Day threats.
- Lack of threat context increases false positive noise.
- Cumbersome investigations increase MTTR.

Privileged Access Monitoring

Unsecured privileged access is a common cause of many breaches. If an attacker has access to a single account, they can easily steal data, modify system settings or install unwanted apps.

Problems it solves:

- Unnecessary and over privileged accounts and entitlements.
- Access misuse and violations.
- Unusual or unauthorized privilege escalation.

Insider Threats

A malicious or negligent insider poses significant risk to the integrity, confidentiality, and availability of information. Understanding and identifying the potential for insider threats is crucial for implementing an effective risk management strategy.

Problems it solves:

- Privileged access misuse and account compromise.
- Data collection and exfiltration.
- Predict flight risk and disgruntled users.

Fraud Detection & Mitigation

Fraud is not just a banking concern. It impacts many industries including insurance, finance, e-commerce, retail, health care and telecommunication to name a few. A successful anti-fraud program requires realtime advanced analytics to accurately detect activities that indicate fraudulent activity and take swift corrective actions.

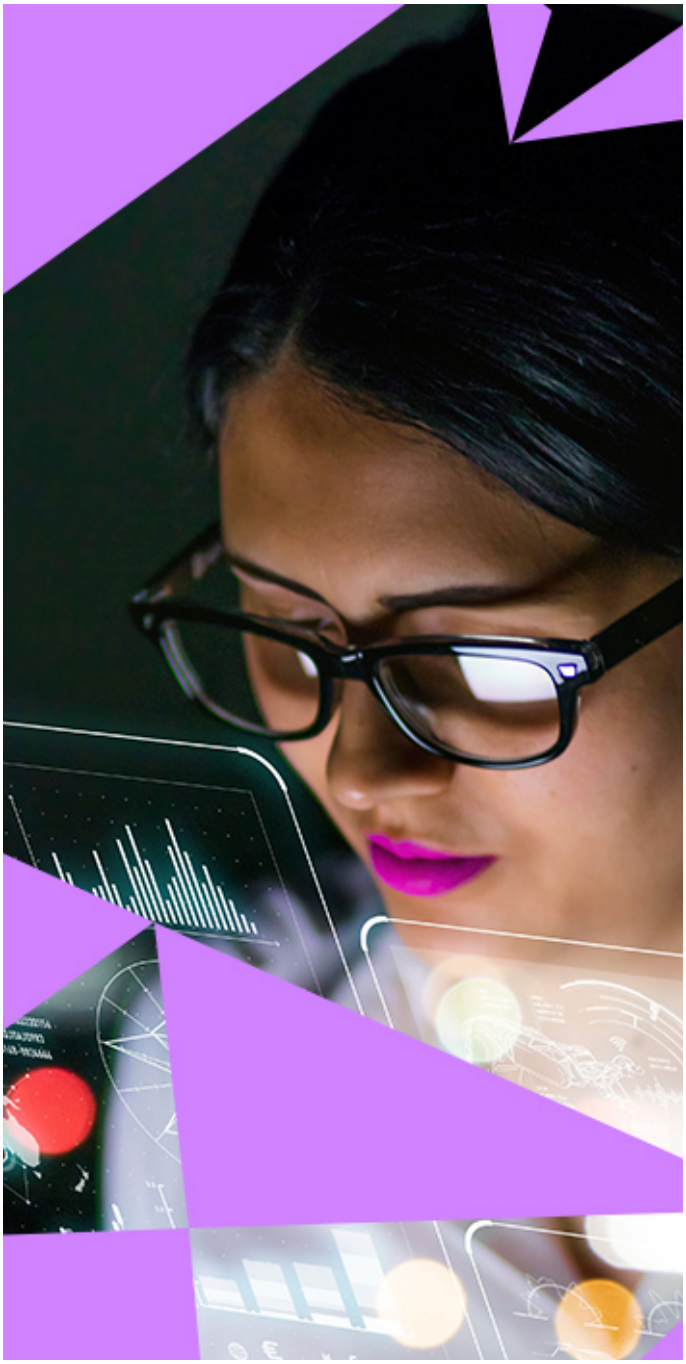
Problems it solves:

- Lack of fraud activity correlation across siloed systems.
- Account takeover and login fraud.
- Credit Card fraud

Conclusion

Managing today's complex threat environment requires a radically clear view of cyber risk. Gurucul's dynamic security analytics platform is purpose built to help you find true threats and respond in real time. It's designed to be ready Day One and has unmatched versatility in deployment options, data ingestion, and customization so it adapts to your enterprise.

- **Open & Flexible**: Purpose-built for adaptability means no compromise
- **Intelligent Data Fabric**: Ensure full visibility with ML powered data processing.
- **Purpose-built Content**: Go from ingestion to high-fidelity detections in seconds
- **Advanced Analytics**: Turning data into actionable insights.
- **Dynamic Risk Engine**: Quantify and prioritize what matters for surgical response.
- **Powered by AI**: Streamline hunting, investigation, and combat sophisticated threats.



About Gurucul

Gurucul is the only cost-optimized security analytics company founded in data science that delivers radical clarity about cyber risk. Our REVEAL security analytics platform analyzes enterprise data at scale using machine learning and artificial intelligence. Instead of useless alerts, you get real-time, actionable information about true threats and their associated risk. The platform is open, flexible and cloud native. It conforms to your business requirements so you don't have to compromise. Our technology has earned us recognition from leading industry analysts as the most Visionary platform and an Overall leader in product, market and innovation. Our solutions are used by Global 1000 enterprises and government agencies to minimize their cybersecurity risk. To learn more, visit Gurucul.com and follow us on LinkedIn and Twitter.

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