GURUCUL

Secez services
www.secez.com

Corporate Overview

www.secez.com | enquiry@secez.com | +91-120-2423448

Table of Contents

COMPANY PROFILE

Gurucul was established in 2010. Gurucul has pioneered the concept of user behavior analytics and has been researching, developing and deploying the Gurucul Risk Analytics platform successfully since 2010. Gurucul spends over 50% of its annual spend on Research & Development, and this has allowed for a significant investment in machine learning behavior algorithms and big data. Gurucul software today includes more than 1000 Machine Learning models to detect insider threats, access misuse and fraud with a deep focus on enterprise and cloud.

The company is a global cyber security company that is changing the way organizations protect their most valuable assets, data and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time behavior based security analytics and intelligence technology combines machine learning behavior profiling with predictive risk-scoring algorithms to predict, prevent and detect breaches, insider threats, privileged access abuse, fraud and more. Gurucul technology is used by Global 1000 companies and government agencies to fight cyber fraud, IP theft and account compromise.

The company was founded by seasoned entrepreneurs with a proven track record of introducing industry-changing enterprise security solutions. Gurucul's mission is to help organizations protect their intellectual property, regulated information, and brand reputation from insider threats and sophisticated external intrusions. Gurucul is backed by an advisory board comprised of Fortune 500 CISOs, and world-renowned experts in government intelligence and cyber security.

The company is headquartered in Los Angeles, CA and has development and support operations in Pune, India. To learn more, visit gurucul.com and follow us on LinkedIn and Twitter.

WHAT WE DO

Gurucul is a leader in behavior based security analytics. We like to say, **"You can steal an identity, but you can't steal behavior."**

We take unlimited data feeds from structured and unstructured security sources – SIEMs, firewalls, Identity and access management systems, AD/LDAP, Intrusion Detection Systems, NetFlow and more. We can also gather context from your business applications – like SAP, EPIC, Salesforce or even your own proprietary applications on virtually any platform. **All we need are transaction logs. It's that simple.**

We aggregate, correlate and analyze that data using our enterprise risk engine, providing a 360-degree view of users and entities: what they're doing, where, when, and with what entitlements.

We generate a single risk score for every user and entity in your organization using behavior analytics. Why is that important? **It's important because you can focus on the highest risk a eas in your organization. This enables you to automatically orchestrate downstream actions and apply automated risk-based controls.**

GURUCUL LEADERSHIP

Saryu Nayyar
Chief Executive Officer &
Co-Founder

Saryu Nayyar is a recognized visionary in the Information Security and Risk industry. Having held leadership roles with Oracle, Sun Microsystems, Ernst & Young, Disney, and Vaau (acquired by Sun), Saryu has over 10 years of experience in assessment, strategy, design and implementation of information security, identity and access management, and risk solutions. Saryu has served clients in several industries including telecom, retail, energy, automotive, pharmaceutical, food and beverage, entertainment, financial services, and insurance. Recognized as a thought leader, Saryu has published several white papers in the information security space.

Leslie K. Lambert, former CISO for Juniper Networks and Sun Microsystems, has over 30 years of experience in information security, IT risk and compliance, security policies, standards and procedures, incident management, intrusion detection, security awareness, and threat vulnerability assessments and mitigation. She received CSO Magazine's 2010 Compass Award for security leadership and was named one of Computerworld's Premier 100 IT Leaders in 2009. An Anita Borg Institute Ambassador since 2006, Leslie has mentored women across the world in technology. Leslie is also serving on the board of the Bay Area CSO Council since 2005.

Leslie K. Lambert
Chief Security and
Strategy Officer

Nilesh Dherange
Chief Technology Officer

Nilesh Dherange is responsible for development and execution of Gurucul's technology vision. Nilesh brings a wealth of experience in inventing, designing, and building software from inception to release. Nilesh has been a technologist and leader at three startups and at one of the largest software development companies in the world. Prior to founding Gurucul, Nilesh was an integral member of a company that built a Roles and Compliance product acquired by Sun Microsystems. Nilesh was also a co-founder and VP of Engineering for BON Marketing Group where he conceptualized and created BON Ticker — an innovative patented bid management system which used predictive analytics to determine advertising bids for PPC marketing campaigns on search engines like Google, Yahoo, MSN etc. Nilesh holds a B.A in Social Science, B.E in Computer Engineering from University of Mumbai and M.S in Computer Science from University of Southern California.

Craig Cooper has served in several information security and risk management roles including CISO for a Fortune 500 Financial Services organization. While in this role, Craig defined and implemented an ISO standards-based Information Security program. Craig has led, developed, and delivered multiple Identity and Access Management Strategies and Roadmaps for several organizations. Craig has written for several trade magazines and has had been a speaker with Burton Catalyst, Gartner, and ISSA.

Craig Cooper
Chief Operating Officer

Jasen Meece
President, Business Development

Jasen Meece is responsible for overseeing sales, business development, channel and partnership programs, and their respective go-to-market strategies. With over 20 years of experience in the security industry, he brings deep expertise and acumen in building high-growth sales organizations at scale, spanning both enterprise and mid-market sectors. Prior to Gurucul, Jasen served as a Managing Partner, Cloud Identity at IBM. Prior to IBM, he was a Managing Director in KPMG's Information Protection practice, where he helped implement cyber risk mitigation programs for several global organizations. He was previously President of Qubera Solutions (acquired by KPMG) and has held executive sales positions at Oracle, Sun Microsystems (now Oracle) and Sabre Corporation.

BOARD OF ADVISORS

Gary Eppinger
GLOBAL VP, CISO AND PRIVACY OFFICER, CARNIVAL CORPORATION

Gary B. Harbison
CISO, MONSANTO

Jason Clark
INVESTOR, CISO ADVISOR AND BOARD DIRECTOR

Jerry Archer
CSO, SALLIE MAE

Joe Sullivan
CISO, CLOUDFLARE, INC.

Renee Guttmann
CISO, ROYAL CARIBBEAN CRUISE LINES

Robert D. Rodriguez
CHAIRMAN AND FOUNDER, SINET

Teri Takai
SR. ADVISOR, CENTER FOR DIGITAL GOVERNMENT, EX-CIO DOD, STATE OF CALIFORNIA

AWARDS

Gurucul's innovation and thought leadership has been recognized with many prestigious industry awards, including:

- 2018 ASTORS Homeland Security Award: Best User & Entity Behavior Analytics (UEBA) Solution
- 2018 SC Media Reboot Leadership Awards: Thought Leader – Saryu Nayyar, Gurucul CEO and Founder
- 2018 Fortress Cyber Security Awards: Best Analytics, User and Entity Behavior Analytics (UEBA) Product
- 2018 Infosec Awards: User Behavior Analytics – Most Innovative
- 2018 Cybersecurity Excellence Awards: Most Innovative Cybersecurity Company – Finalist
- 2018 Cybersecurity Excellence Awards: User and Entity Behavior Analytics – Finalist
- 2017 Homeland Security Awards: Best User & Entity Behavior Analytics Solution – Gold Award
- 2017 CDM – Best Product: Leading UEBA Vendor Wins Award for Second Consecutive Year Based on Continued Innovations
- 2017 CSO50 Award: Company Receives CSO50 Award for Developing and Implementing Security Initiatives

To view the full list of Gurucul awards, click here.

Gurucul Risk Analytics (GRA)

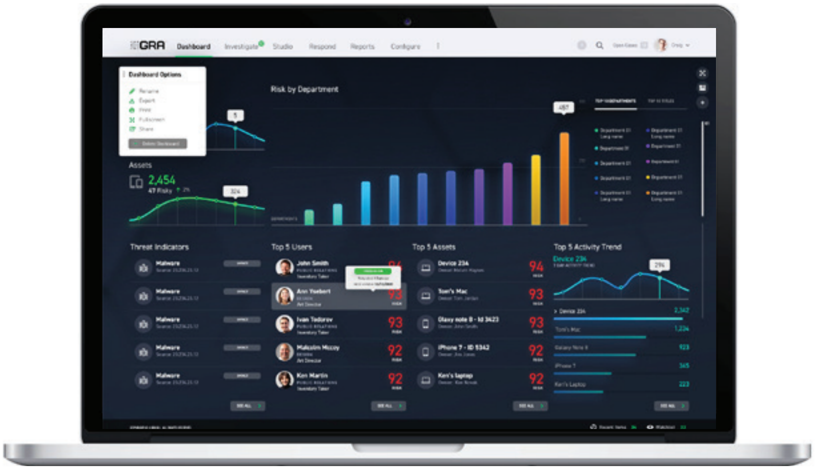
Gurucul Risk Analytics (GRA) is a behavior based security analytics and intelligence platform on open choice of big data. Gurucul Risk Analytics (GRA) is built ground up on HDFS (Hadoop) with 254 attributes leveraged in over 1000 machine learning models. GRA does not rely on signatures, rules or patterns. It is intended – from the ground up – to identify zero-day threats and is designed to provide both contextual and situational awareness.

Gurucul Risk Analytics detects and stops malicious behavior before cyber criminals or rogue insiders can do harm. GRA is the only security analytics platform that can ingest all data sources out-of-the-box. It can ingest any data from any source, including proprietary business applications, to give you the most accurate 360-degree view of a user's or entity's behavior. Data ingestion is available via flat file, database, API, message or streaming inputs with ready to use data connectors for common enterprise systems and platforms (i.e., HR, IAM, PAM, SIEM, AD, databases, networks, vulnerabilities, DLP, threat intel, Cloud Apps/ SaaS, authentication, physical ID badge systems, file storage and endpoints).

Gurucul Risk Analytics leverages a comprehensive risk engine which performs continuous risk scoring based on historical and current behavior. GRA provides real-time risk prioritized alerts for incident analysis. The dynamic risk scores can be used to trigger automated risk-response workflow for enterprise and cloud.

Gurucul Risk Analytics leverages Gurucul Data Mine™, an open source big data backend. Gurucul Data Mine™ is used to correlate, link and store data from applications, platforms, NetFlow, threat intelligence, and other security solutions. GRA uses this contextual information for machine learning, behavior analytics and deep learning.

GRA supports an open choice for big data with Cloudera, Hortonworks, MapR or a customer's own implementation of Hadoop. An open metadata model enables customers to tune the analytics engine using various parameters such as selection of attributes, risk score weightages, etc., in order to align with their business patterns and security requirements. Customers may also develop and integrate their own machine learning models within GRA.



Gurucul Risk Analytics consists of three products as follows, each with their own use cases:

User and Entity Behavior Analytics (UEBA)

Gurucul User and Entity Behavior Analytics (UEBA) uses machine learning models on open choice big data to detect unknown threats early in the kill chain. UEBA provides the most realistically effective approach to comprehensively manage and monitor user and entity centric risks. UEBA quickly identifies anomalous activity, thereby maximizing timely incident or automated risk response.

The range of Gurucul UEBA use cases is what makes the solution extensible and valuable. It focuses on the detection of risks and threats beyond the capabilities of signatures, rules and patterns. Gurucul UEBA use cases include:

- Insider Threat Detection and Deterrence
- Account Compromise, Hijacking and Sharing
- Privileged Access Abuse
- Data Exfiltration, DLP and IP Protection
- Adaptive Authentication
- SIEM and DLP Risk Intelligence
- Self-Audit and ID Theft Detection
- Trusted Host and Entity Compromise

Using big data, Gurucul provides risk-based behavior analytics delivering actionable intelligence for security teams with low false positives. Gurucul leads the market in demonstrating UEBA results where others cannot. We consume the most data sources out-of-the-box and leverage the largest machine learning library. Additionally, we deliver a single unified prioritized risk score per user and entity. Find threats – unknown unknowns – quickly with no manual threat hunting and no configuration. Get immediate results without writing queries, rules or signatures.

Identity Analytics

Gurucul Identity Analytics (IdA) comprehensively manages and monitors identity-based risks and threats across an organization's siloed environments. Using big data, Gurucul provides a holistic 360-degree view of identity, access, privileged access, and usage in the cloud, on mobile and on-premises. IdA reduces the access plane by detecting and removing access risks, access outliers, and orphan or dormant accounts. This improves an organization's security posture by significantly decreasing the number of accounts that can be compromised or abused.

Identity Analytics delivers the data science that improves IAM and PAM, enriching existing identity management investments and accelerating deployments. IdA surpasses human capabilities by leveraging machine learning models to define, review and confirm accounts and entitlements for access. It uses dynamic risk scores and advanced analytics data as key indicators for provisioning, de-provisioning, authentication and privileged access management.

The impact of machine learning with Identity Analytics can radically reduce accounts and entitlements. Machine learning models provide 360-degree visibility for an identity, accounts and access, with the ability to compare to peer groups using baselines to determine normal and anomalous access. The objective is to clean up the access plane to enable access only where it should be provided.

Cloud Security Analytics

Gurucul Cloud Security Analytics (CSA) utilizes API-based cloud access security broker (CASB) architecture to deliver advanced security analytics for SaaS cloud applications – including IaaS, PaaS, and IDaaS. The flexibility of this approach enables Gurucul to ingest data directly from applications on cloud provider platforms as well as consume data feeds from CASB proxy gateways. CSA leverages cloud infrastructure and platform data alongside cloud application activity data for a complete view of user/entity behavior analytics and identity access intelligence.

Gurucul Cloud Security Analytics provides cloud API data connectors out-of-the-box as well as delivering the capability for developing custom connectors. Get visibility into cloud applications and infrastructure including: Amazon AWS, Box, Concur, Dropbox, Google Cloud, G-Suite, IBM, Microsoft Azure, Microsoft Office 365, Okta, Oracle, Ping, SalesForce, SAP, ServiceNow, Splunk Cloud, and Workday.

Gurucul Cloud Security Analytics works on its own for cloud-only deployments and joins seamlessly with Gurucul UEBA and Gurucul Identity Analytics on-premises for hybrid environments. Having Cloud, UEBA and Identity Analytics holistically integrated is essential for a comprehensive hybrid environment risk analytics implementation. With Gurucul, you get full hybrid visibility of identities, accounts, access and activity for on-premises and cloud.

Who isn't moving some portion of their business to the cloud? A continually expanding range of users are accessing on-premises and cloud applications from desktops, mobile phones, and tablets 24/7. It has become fundamentally impossible for humans to effectively manage and assure the security of all their data. Only Gurucul provides full 360-degree visibility and context of users accessing applications and data both in the cloud and on-premises.

Gurucul Fraud Analytics

Gurucul Fraud Analytics provides a holistic risk-based approach for fraud detection of both internal and external users, using award-winning machine learning algorithms and an open big data architecture. Its data science architecture creates a unique risk score for each internal user, customer or provider entity, using context-driven sensors from public and private data and transactions. It ingests both structured and unstructured data and aggregates risk context for intelligent predictive fraud detection.

Gurucul Fraud Analytics can link data from a multitude of sources to provide a contextual view, and highlight anomalous transactions, based on historic user and community profiles. Its analyzes online and offline activity: public records, contact center interactions, point of sale transactions and ATM transactions. Gurucul Fraud Analytics mines and normalizes data, and then creates a risk score for fraud and abuse. It's used for real-time decision making or batch scoring of an event. It can also provide scores and risk factors for other systems to use in a decision.

> *"The most successful fraud detection and prevention strategies make use of machine-learning techniques."*
>
> – Gartner Market Guide for Online Fraud Detection, February 2018

Gurucul SaaS

Gurucul SaaS delivers behavior based security analytics and intelligence as a service. Powered by Gurucul Risk Analytics, Gurucul SaaS leverages over 1000 machine learning models to find hidden insights, without explicit rules and policies typically found in SIEM and log aggregation platforms. In any machine learning model, the quality, quantity and depth of data impacts the accuracy and usefulness of the predictions. Gurucul can collect the data right from the source — cloud or enterprise — and will keep it on line for three years. Combining Gurucul Data Mine™ and the power of Gurucul Machine Learning will provide your organization with an unprecedented view of cyber risk and compliance reporting, and enable you to take action all from a cloud-based SaaS offering.

COMPETITIVE DIFFERENTIATION

Gurucul's behavior based security analytics and intelligence platform answers the question: **Is anomalous behavior risky?** This is what Gurucul does and why we're different than everyone else in this space. We don't waste your time with alerts on anomalous activity that isn't risky. We use context to determine whether behavior is risky. Context is critical.

Telling you what's happening is not helpful. Telling you when something bad is happening is the Gurucul difference. That's information you can act on. We deliver actionable intelligence for security teams with low false positives. This is extremely hard to do without our technology. Instead of getting 30,000 SIEM alerts of unknown context you cannot possibly investigate, we give you 30 true positives. That's a manageable number your security team can process.

So, how do we do it?

Largest Machine Learning Library

We have the largest machine learning library on the planet – over 1300 machine learning models. More behavior models equals better coverage. We provide essential value with out-of-the-box algorithms that learn anomalous behaviors immediately upon deployment. With Gurucul, you'll see results as soon as we're deployed. Our customers have been able to find compromised accounts on day 1, which is why they move forward with us. Gurucul delivers results.

Gurucul STUDIO™

We are the only security analytics company to enable you to customize our machine learning models or quickly build your own with Gurucul STUDIO™ – no coding required. Create custom machine learning models without coding and minimal knowledge of data science. Gurucul STUDIO™ provides a step-by-step graphical interface to select attributes, train models, create baselines, set prediction thresholds and define feedback loops. STUDIO™ as part of Gurucul Risk Analytics (GRA) supports an open choice for big data and a flex data connector to ingest any on-premises or cloud data source for desired attributes. Step outside the black box and create custom models for your own predictive security analytics needs.

Pure Play Analytics

We are a pure play analytics vendor. We don't deliver light-weight, siloed analytics on point data feeds like privileged access management products and SIEMs. Our analytics is powered by robust machine learning models built by data scientists. Our competitors use signatures, patterns, rules and policies which can only detect known behavior patterns. ***What about the unknowns?*** Our models go beyond detecting known or common patterns, so you can detect unknown threats.

Big Data Lake Agnostic

We are big data lake agnostic – we work on your choice big data platform: Hadoop, Hortonworks, Cloudera, Amazon EMR, etc. If you don't have a data lake, we will give you ours for free: Hadoop.

Gurucul Miner™

Investigate incidents quickly with Gurucul Miner™. Only Gurucul offers natural language contextual search using big data to mine linked users, accounts, entitlements, structured and unstructured data, along with risk score and peer group analytics. From a single console, you can use any query you like to investigate incidents and correlate data across channels. You can save and export results for reporting and compliance purposes. **Our contextual search reduces case resolution time by 67%**.

Unlike traditional threat hunting tools and SIEMs, Gurucul Miner™ uses artificial intelligence capabilities to uncover all behavior patterns and data relationships that map to the search profile. It conducts natural language searches across any combination of structured and unstructured data to provide a 360-degree view of user and entity behaviors based on HR/profile attributes, events, accounts, access permissions, devices, cases/tickets and anomalies.

Cost Effective

Our platform is cost effective. **We don't charge you for data, period.** One of the issues with competitive solutions and SIEMs is that these vendors charge based on the volume of data analyzed. We want you to build your behavior based security analytics as big as possible. You need to be able to bring in lots of different kinds of data. You need to partner with a vendor like Gurucul that does not charge based on the quantity of data. This is one of the reasons enterprises choose Gurucul. We don't charge you for data. We want to ingest at much data as possible to give you a 360-degree view of all your users and entities. We'll run our analytics engine on your data lake or ours – whichever you prefer.

Enterprise Risk Engine

Our Enterprise Risk Engine is our "secret sauce". It consumes all your data out-of-the-box. We can ingest data from any source – SIEMs, CRMs, Electronic Medical Records, Identity and Access Management systems, end points – you name it, we ingest it into our enterprise risk engine. If you have proprietary business applications – we can take that data and aggregate it with your other data sources to give you the most accurate 360-degree view of a user's (or entity's) behavior.

Our Enterprise Risk Engine ingests all your data feeds in real-time and generates a single risk score for every user and entity in your environment. We provide intelligent prioritized risk scores based on user and entity behavior – so you can make smart decisions quickly. All you have to do is investigate high risk users and entities. It's that easy.

> *"Gurucul really stood out because the analytics engine was the most powerful. The machine learning algorithms are the strongest. We saw results very, very quickly."*
>
> – William Scandrett, CISO, Allina Health