Gurucul Risk Analytics™

A root of modern threat involves compromise or misuse of identities. Users have multiple accounts and entitlements often in excess providing an opportunistic environment for cyber crime, insiders and advanced attacks. CIOs desire widespread data access and enablement while CISOs contend with declarative defenses and controls. The outcome is data breaches and escalating costs as preventive defenses decline in effectiveness. The volume of security data needs data science.

Winner of Best Behavior Analytics / Enterprise Threat Detection Trust Award

SC MAGAZINE AWARDS 2016 WINNER Honored in the U.S.

* Honored in the U.S. and Europe

Why consider Gurucul Risk Analytics (GRA) ?

- Analyze access and its abuse with identity-centric behavior analytics from big data
- Model good behavior to expose unknown bad through peer groups, clustering and outliers
- Leverage predictive security analytics to risk-score incidents and drive 'find-fix' focus
- Optimize resources and time with machine learning algorithm compute cycles
- Reduce and manage the account surface area with risk-based access controls
- Provide behavior analytics for on-premise and cloud app hybrid deployments
- Detect insider threats, account hijacking and abuse, plus data exfiltration

GURUCUL | 222 N. SEPULVEDA BLVD., SUITE 1322, EL SEGUNDO, CA 90245 | 213.259.8472 | INFO@GURUCUL.COM | WWW.GURUCUL.COM

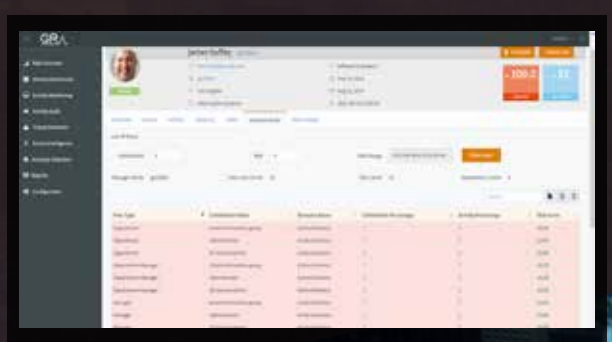
What are the core components and features?

- Gurucul Risk Analytics has three components to address access, threats and cloud use, uniquely combining data science for user and entity behavior analytics (UEBA) and identity analytics (IdA)

Access Analytics Platform™ (AAP)

Access Analytics Platform™ (AAP) provides risk-based compliance and provisioning

- Real-time 360⁰ contextual view of identities, access and activities
- Identity analytics and roles from behavior analytics machine learning
- Radical reduction of accounts and access entitlements using behavior-based access
- High privilege access detection, plus obsolete, orphan and unused access reporting
- Risk based certifications and dynamic access provisioning reduces effort and errors
- Access outliers based on usage and dynamic peer group analytics



Cloud Analytics Platform™ (CAP)

Cloud Analytics Platform™ (CAP) provides visibility into cloud access and anomalies

- Full contextual visibility into cloud apps for identities, access and activities
- Cloud-to-cloud ready to use connectors for popular SaaS applications
- High Privilege Access (HPA) anomaly detection with detailed insight into outlier access
- Risk scores highlight compromise, hijacking, insider threats, and data leakage
- Manage accounts using identity access intelligence and risk-based certifications
- Leverage for hybrid deployments of on-premise and cloud behavior analytics

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

"Hands down, the most sophisticated example of behavior analytics..."

SC Magazine
July 2015

GURUCUL | 222 N. SEPULVEDA BLVD., SUITE 1322, EL SEGUNDO, CA 90245 | 213.259.8472 | INFO@GURUCUL.COM | **WWW.GURUCUL.COM**

Threat Analytics Platform™ (TAP)

Threat Analytics Platform™ (TAP) provides behavior-based predictive risk scoring

- Risk-scored time line to predict, detect and deter insider and advanced threats
- Identity based threat plane behavior analysis for account hijacking and abuse
- Proactive and actionable alerting for anomalous behavior and risk scores
- High privilege access anomaly detection for misuse, sharing, or takeover
- Customizable dashboards, configurable policies and risk model optimization
- Work-centric UI with case management, or input to third-party solutions
- Self-audit portal deputizes users for risk awareness to detect identity theft

What makes Gurucul Risk Analytics more effective?

πβαε Core architecture is built on PIBAE™
(Predictive Identity-based Behavior Anomaly Engine)

- Behavioral machine learning algorithms based on 254 attributes to profile identity
- Self-learning and training algorithms are contextually aware for transaction scoring
- Dynamic peer groups improve clustering and outlier machine learning accuracy
- Awareness to time-based norms such as accepted workflows and operational changes
- Built for scale with big data foundation and flexible meta data framework
- Inclusion of identity management and privilege account management data sources
- Out of the box algorithms learn anomalous behaviors immediately upon deployment
- Fuzzy logic and linked data analysis automates mapping of activity and accounts to identities
- Big data architecture ingests historical data to speed self-learning and training

What are the outcomes and reviews?

- On the second day of using GRA, a manufacturing firm discovered two hijacked research accounts
- GRA reduced the number of accounts and entitlements by 83% for a financial firm, plus defined intelligent roles and provided dynamic access provisioning using behavior-based risk context
- GRA often finds high privilege access abuse and anomalous behavior in unexpected areas as unknown unknowns
- The common occurrence of departing employees and contractors accumulating data and information prior to exfiltration
- Terminated accounts with access to cloud applications

What are the deployment options?

- GRA appliances come pre-loaded, ready to rack and provision on-premise
- GRA virtual machine images can be provisioned on existing servers or private cloud
- CAP is cloud-based with connectors for popular SaaS apps with your cloud provider
- GRA can be bare-metal deployed on existing hardware leveraging your data lake
- GRA is also provided as a managed security service with 24/7 service and support
- Maintenance, support, training and professional services are available

What are the use cases for user behavior analytics and identity access intelligence?

- Security Investigations and Risk Analytics
- Identity Access Management (IAM) and Privilege Account Management (PAM)
- Data Exfiltration, Data Loss Prevention (DLP) and Insider Threats
- Cloud Access Security Intelligence (CASI)
- Online Fraud Detection (OFD)

Awards

SC Magazine Awards 2016 Winner Honored in the U.S.
SC Magazine Awards 2016 Europe Winner
Best of Breed User Behavior Analytics Solution 2016 CDM
2014 2015 SINET 16 Innovator
Gartner 2014 Cool Vendor
CIO Review 20 Most Promising RSA Security Solution Providers - 2015
Editor's Choice CDM
Computer Technology Review MVP Awards Most Valuable Product

About Gurucul

Gurucul is changing the way enterprises protect themselves against insider threats, external intruders and cyber fraud on-premise and in the cloud. The company's user behavior analytics and identity access intelligence technology uses machine learning and predictive anomaly detection algorithms to reduce the attack surface for accounts, unnecessary access rights and privileges, and identify, predict and prevent breaches. Gurucul technology is used globally by large enterprises in finance, banking, insurance, manufacturing, hi-tech, pharmaceutical and retail.

GURUCUL | 222 N. SEPULVEDA BLVD., SUITE 1322, EL SEGUNDO, CA 90245 | 213.259.8472 | INFO@GURUCUL.COM | WWW.GURUCUL.COM