GURUCUL

Cloud Analytics Platform™

DATA SHEET

Cloud Analytics Platform

New challenges exist with the advent of the cloud. Organizations have low visibility into who has access to applications and information, who is using the applications, from where, and what devices, as well as how that use is being conducted. Auditability for the business is constricted. To meet these challenges, cloud applications require both identity analytics (IdA) and user and entity behavior analytics (UEBA). IdA reduces the attack surface for accounts, unnecessary access rights and privileges. UEBA identifies, predicts and prevents breaches. Machine learning data science provides full insight to cloud applications with contextual views of an identity, its access, and associated activity. Hundreds of attributes modeled in machine learning algorithms result in predictive security analytics to provide comprehensive risk-based security monitoring through Gurucul Risk Analytics (GRA).

> ***"CAP discovered a terminated employee downloading data from the corporate Salesforce account from the employee's new job."***
>
> NETWORKWORLD

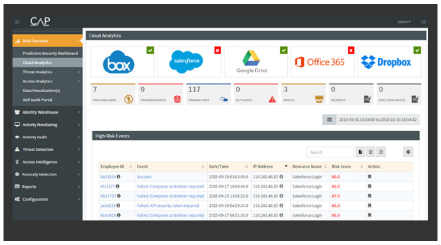
Why consider Gurucul's Cloud Analytics Platform (CAP)?

- Predict, detect and deter insider threats and cyber fraud for cloud applications via an API-based CASB solution
- Prevent data exfiltration with risk-scored timelines from predictive security analytics
- Detect high privileged account abuse, account hijacking and anomalous activity
- Identify anomalies and improve access control and data governance with real-time access analytics
- Enhance certifications with user, account, and entitlement risk determined by behavior analytics
- Reduce excess accounts and access entitlements to minimize identity risk and exposure
- Leverage for hybrid deployments of on-premises and cloud behavior analytics

What are CAP features and benefits?

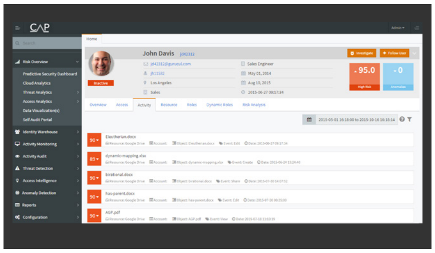
- Full contextual visibility into cloud applications for identities, access and activities
- Cloud-to-cloud ready-to-use connectors for popular SaaS applications
- Risk-scores highlight compromise, hijacking, insider threats, and data leakage
- Manage accounts using identity analytics and risk-based certifications
- Proactive and actionable alerting for anomalous behavior and risk scores
- Customizable dashboards, configurable policies and risk model optimization
- Work-centric UI with case management, or input to third-party solutions

Visualization value from CAP



Employee ID	Event	Date/Time	IP Address	Resource Name	Risk Score	Action
ke11554	Success	2015-09-19 03:03:50.0	216.240.46.30	Salesforce Login	86.0	
kf11577	Failed: Computer activation required	2015-09-17 19:00:46.0	216.240.46.30	Salesforce Login	86.0	
kb13757	Failed: Computer activation required	2015-09-25 13:08:25.0	216.240.46.30	Salesforce Login	87.0	
jw14228	Failed: API security token required	2015-09-20 04:29:33.0	216.240.46.30	Salesforce Login	86.0	
kb14818	Failed: Computer activation required	2015-09-27 06:52:38.0	216.240.46.30	Salesforce Login	86.0	

Predictive security dashboards provide a focused starting point for cloud applications.

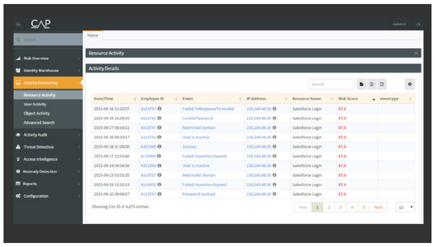


John Davis jd42312
jd42312@gurucul.com
jh11532
Los Angeles
Sales
Sales Engineer
May 01, 2014
Aug 10, 2015
2015-06-27 09:17:34

2015-05-01 16:18:00 to 2015-10-16 16:18:14

90 Eleutherian.docx — Resource: Google Drive · Account: · Object: Eleutherian.docx · Event: Edit · Date: 2015-06-27 09:17:34
89 dynamic-mapping.xlsx — Resource: Google Drive · Account: · Object: dynamic-mapping.xlsx · Event: Create · Date: 2015-06-24 13:24:40
90 birational.docx — Resource: Google Drive · Account: · Object: birational.docx · Event: Share · Date: 2015-07-30 14:07:52
90 has-parent.docx — Resource: Google Drive · Account: · Object: has-parent.docx · Event: Edit · Date: 2015-07-20 00:35:00
90 AGP.pdf — Resource: Google Drive · Account: · Object: AGP.pdf · Event: View · Date: 2015-07-18 11:10:19

Risk-scored cloud activities for terminated employees.



Date/Time	Employee ID	Event	IP Address	Resource Name	Risk Score	eventtype
2015-09-16 13:32:07	kb13757	Failed: InResponseTo Invalid	216.240.46.30	Salesforce Login	87.0	
2015-09-19 14:09:05	ka12741	Invalid Password	216.240.46.30	Salesforce Login	87.0	
2015-09-27 08:34:12	kb13757	Restricted Domain	216.240.46.30	Salesforce Login	87.0	
2015-09-10 08:33:17	ka12741	User is Inactive	216.240.46.30	Salesforce Login	87.0	
2015-09-18 01:29:06	kd11945	Success	216.240.46.30	Salesforce Login	87.0	
2015-09-27 23:53:46	kc15095	Failed: Assertion Expired	216.240.46.30	Salesforce Login	87.0	
2015-09-14 04:50:56	kd11945	User is Inactive	216.240.46.30	Salesforce Login	87.0	
2015-09-23 03:51:35	kb13757	Restricted Domain	216.240.46.30	Salesforce Login	87.0	
2015-09-19 13:32:13	kb14852	Failed: Assertion Expired	216.240.46.30	Salesforce Login	87.0	
2015-09-20 09:09:07	kb13757	Password Lockout	216.240.46.30	Salesforce Login	87.0	

Showing 1 to 10 of 4,875 entries

Cloud resource activity monitoring by risk scores or events.

What makes CAP more effective?

- GRA's 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 self-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 metadata framework
- Inclusion of identity management and privileged 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 self-training

About Gurucul

Gurucul is changing the way enterprises protect themselves against insider threats, external intruders and cyber fraud on-premises and in the cloud. The company's user and entity behavior analytics (UEBA) and identity analytics (IdA) 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.