ANOMALIX

ANOMALIX
WHITE PAPER
IdGenius Overview



IdGenius Overview

The traditional Identity and Access Management space has been dominated by reactive business drivers: gathering data on a periodic basis, setting up rules to add or remove access if a job role changes, generating reviews and reports for periodic audits, etc. The proliferation of user access across multiple, disparate systems combined with the increased sophistication in potential attackers makes controlling entitlements and permissions more important than ever before. IdGenius is designed to detect anomalous behavior and take action in near real time, provide more intelligent targets for access reviews and provide a "point in time" view of any user's access giving visibility into historical user access data.

Identity Analytics Features:
Fast, Scalable Data Collection – Anomalix IdGenius enables vast data collection through a heterogeneous engine that will span the breadth and depth of required identity and security related information and data

User Behavior Analytics – Dynamic user profile and peer group enhancements that provide real-time and historical user behavior context to empower business decisions

Real-Time Risk Based Policy Enforcement – Detect real threats in real-time and take action. By filtering through the 99% of false positive events and alerts, Anomalix provides the ability to identify suspicious and anomalous threats, internally and externally, and react based on risk to organizational resources

Identity and Security Dashboard – IdGenius provides an intuitive User Interface that maximizes the user experience. The Genius Dashboard (charts, graphs and organized data points) quickly identifies Identity and Security related Anomalies with respect to Authentication, Authorization, Geo-location, Vulnerability, Access Requests, Policy Violations and Enforcements, Peer Group Behavior and Security Investigation

Advanced Threat Monitoring – IdGenius improves threat detection cycles by over 1000% when compared to SIEM capabilities alone. Most SIEM tools do not enable real time capabilities with organizational, risk-based policy enforcement to predict user behavior and plan for an automated response or manual response

Dynamic Analytical Models – IdGenius provides dynamic analytical models that can be adjusted and refined by clients to enable the following:

- Visibility into Operational Risk Models
- Reduce Operational Risk
- Reduce Operational Costs
- Improve Security and Audit Readiness
- Improve operational efficiency

- Fraud Prevention
- Identity Validation
- User Access Propensity Tracking
- Risk Mitigation

IdGenius: Actionable Identity Analytics IdGenius Identity Analytics takes inputs from the following types of systems in order to understand the sensitive data and information in your environment:

- SSO
- IAM
- VPN
- RDBMS Logs
- Application Logs
- Server Logs
- GRC
- DLP
- PAM

IdGenius Security Analytics builds upon the Identity Context and enables further visibility across security events within the enterprise that include:

- HTTP Transactions
- Firewalls
- Gateways
- Proxy
- DLP
- Virtual Machines
- SIEM (ArcSight, Log Rhythm, QRadar)
- Malware (FireEye, Palo Alto, Wildfire)
- External Threats (FS-ISAC, Google CIF)
- Cloud (AWS CloudTrail, Mobile Device Logs, Box)
- Endpoints (App Logs, Security Logs, DB Logs, Server Logs)
- Custom APIs (Java, JavaScript, REST, SysLog)

Historical User Profile Information – IdGenius gives a Timeline view of individual user access, allowing you to view a snapshot of what users have access to at a given point in time. This removes the process of trying to forensically reconstruct a user profile based on logs and reviewing access requests.

IdGenius: Identity Analytics Security – Identity and Privileged User Analytics starts by collecting Identity data from HR repositories, (PeopleSoft, Workday, Active Directory, etc.) LDAP repositories and Contractor/1099 Worker Databases (any RDBMS) or existing IAM implementations. IdGenius will use this to establish an identity profile for all users with access to sensitive company resources.

Once collected, IdGenius can then establish a baseline of who has access to sensitive information. The next step is to build a baseline of "normal" user activity based on time, geography, transactions, and session information. That baseline is continuously gauged against a peer group of users to further identify the "normal" baseline for a user given their respective responsibilities through credential modeling.

IdGenius builds a dynamic baseline of user behavior through profiles of when, where, and how users employ credentials to access sensitive company resources. Once it detects anomalous behavior, IdGenius will reference Risk-Based Policies to determine if real-time action is warranted.

IdGenius: Security Analytics IdGenius – enables true Dynamic & Polymorphic Threat Detection by continuing to build upon User Behavior Analytics profile through a multidimensional lens. IdGenius provides continuous Machine Learning, Graph Analysis and Behavior Analytics. Since anomalies don't always pose risk, Advanced Threat Monitoring is improved exponentially with actionable line of sight through the kill chain.

Anomalix Inc. is a privately held company that offers Identity-centric security solutions. Anomalix has over 50 customers across industry verticals with more than triple digit YTY growth since 2013. Anomalix solutions (products & services) enable organizations to understand user behavior and act upon anomalous activities through risk-based policy enforcement. Anomalix offers highly sophisticated and discrete analytical solutions to address Identity and Access Governance and Cyber Security challenges. By establishing a baseline of "normal" user behavior across peer groups, Anomalix enables its customers to filter through the "99%". Specifically, the 99% of false positive alerts that organizations allocate precious resources to investigate while outsider and insider threats go undetected. Anomalix offers solutions that enable:

- Identity Analytics
- Security Intelligence
- Privileged User Analytics
- Insider Threat Monitoring
- Data Exfiltration Intelligence
- User Behavior Analytics
- Qualitative Risk Modeling
- Real-time risk-based access policy enforcement
- Advanced threat protection and monitoring



Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144