User and Entity Behavior Analytics
Use Cases
**Introduction**

"Security and risk management leaders should leverage user and entity behavior analytics to improve their organization’s threat detection capabilities across a variety of use cases."

Gartner Market Guide for UEBA, - December 2016

Hacker innovations continue to rise unabated alongside leveraging compromised accounts, while traditional signatures, rules and patterns within defenses offer minimal capability to detect them. Security leaders face a perpetual challenge to keep up with the accelerating pace of risk on an ever-expanding access risk and threat plane, often within a hybrid environment of on-premises and cloud. A large component of this challenge includes the growing state of big data to analyze for security insights. While big data is the source of critical indicators for a prospective attacker’s access and activity, its burgeoning scale has far eclipsed the ability for humans to hunt through it in any realistic manner.

Within the domain of advanced security analytics, the clear benefit of user and entity behavior analytics (UEBA) to leverage models over rules has been observed by the majority of industry analysts. Drawing from the context of big data, and driven by machine learning models to deliver invaluable visibility and risk scoring, UEBA provides the most realistically effective approach to comprehensively manage and monitor identity-based risks and unknown threats across all of an organization’s environments. User and entity behavior analytics quickly identifies anomalous activity, thereby maximizing timely incident or automated risk response. The range of UEBA use cases is what makes the solution extensible and valuable. For organizations to effectively face these challenges, customers must assure the use cases offered by a vendor align with their specific needs and varied requirements today and into the future.

**A comprehensive set of use cases for user/entity behavior analytics should include:**

<table>
<thead>
<tr>
<th></th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Account Compromise, Hijacking and Sharing</td>
</tr>
<tr>
<td>2</td>
<td>High Privileged Access Abuse</td>
</tr>
<tr>
<td>3</td>
<td>Data Exfiltration, DLP and IP Protection</td>
</tr>
<tr>
<td>4</td>
<td>Insider Threat Detection and Deterrence</td>
</tr>
<tr>
<td>5</td>
<td>Self-Audit and ID Theft Detection</td>
</tr>
<tr>
<td>6</td>
<td>Cyber Fraud Detection and Deterrence</td>
</tr>
<tr>
<td>7</td>
<td>Trusted Host and Entity Compromise</td>
</tr>
<tr>
<td>8</td>
<td>Stateful Session Tracking</td>
</tr>
<tr>
<td>9</td>
<td>Step-up Authentication (Adaptive Authentication)</td>
</tr>
<tr>
<td>10</td>
<td>Anomalous Behavior and Watch Lists</td>
</tr>
<tr>
<td>11</td>
<td>SIEM and DLP Risk Intelligence</td>
</tr>
<tr>
<td>12</td>
<td>Hybrid Infrastructure</td>
</tr>
</tbody>
</table>

While it is common to start with one or two use cases for a UEBA deployment, a customer roadmap of future projects across departments is advised. The advent of analytics features within solution silos is expected. At the same time, however, the contextual value of big data for security analytics between multiple solutions, making APIs and the democracy of data of critical importance, must be recognized. Today’s SOC analysts may be engaged mainly with incident reviews, yet tomorrow, the advantages of automated risk response between security solutions can become a primary requirement. As current innovations expand with widening adoptions, security leaders will deepen their understanding of how advanced security analytics improve detection and response. As well, they will see added benefits of step-up multi-factor authentication deployments and self-audits to leverage the unique context from users not found today within most traditional SOCs. This white paper explores a comprehensive and optimal set of use cases for UEBA.

© 2017 Gurucul. All rights reserved.
User and Entity Behavior Analytics
Maximizing Timely Unknown Threat Detection and Response

**UEBA** is the detection and response side of advanced security analytics using machine learning models to detect unknown risks and threats via predictive risk scoring early in the kill chain as a best use case scenario. Utilized in both on-premises and hybrid cloud environments, user and entity behavior analytics use cases are focused on detection of risks and threats beyond the capabilities of signatures, rules and patterns. Using machine learning models to detect anomalous behavior for users and peer groups, while minimizing false positives, these use cases result in predictive risk scores driving alerts, responses and case tickets. To assure optimal and comprehensive capabilities, UEBA vendors’ use cases should draw from the context of big data, utilizing proven and mature machine learning models.

This solution framework should include data ingestion 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 applications/SaaS, authentication, physical ID badge systems, file storage and endpoints). This level of advanced solution should also support an open customer choice for big data with Hadoop, Cloudera, Hortonworks, ELK-Elastic and MapR. Models should run on top of a customer choice for big data to compute and store, to avoid reading and storing data multiple times. In simple terms, use your data lake with advanced security analytics on top.

The types of analytics residing within an advanced security analytics platform are:

**User and Entity Behavior Analytics**
UEBA’s threat analytics deliver systematic analysis to deter, detect, and prevent insider threats, compromised accounts and data exfiltration, with multiple machine learning models for specific use cases. Identity is a threat plane that modern threats compromise, hijack and misuse for data breaches. Machine learning clustering and outlier analysis with dynamic peer groups uniquely uncover and risk score these holistically, minimizing false positives and enabling prompt, targeted remedial or automated risk responses.

**Identity Analytics (IdA)**
IdA’s access analytics involves detecting access risks, access outliers, excess access, shared high privileged access (HPA) accounts, as well as orphan and dormant accounts. In addition, it reduces the attack surface area for identities with machine-learning-based intelligent roles, replacing roles defined by manual processes and legacy rules. Identity analytics also reduces identity management manual processes, improves and often automates provisioning, and also cleanses identity as an access plane for compliance and audits. The key to IdA deployments is bidirectional API integration with identity access management solutions to access data for machine learning and provide risk-scored identity analytics.

© 2017 Gurucul. All rights reserved.
The robust capabilities of these collective analytics solutions employ advanced machine learning to harness the vast ocean of data – big data. This delivers the invaluable context of a given identity’s access and activities which continually verifies the status of their behavior: legitimate or anomalous. To date, the only solution set capable of addressing all the challenges described above, leveraging machine learning, is through mature UEBA and IdA. When these two are integrated jointly within the cloud environment, targeting the challenges residing there, CSA is the resulting solution. When UEBA and IdA are applied to the challenge of privileged access entitlement abuse, privileged access analytics (PAA) is the associated solution.

The depth and range of advanced security analytics use cases fundamentally defines the areas of expertise and functionality for vendors providing UEBA, IdA, PAA and CSA. A number of vendors offer only a limited selection of use cases, often only with the UEBA domain, while only a few others are more inclusive and comprehensive in their offerings. Use cases are organized in three categories: UEBA, IdA and CSA, with PAA use cases overlapping within these groupings. Some of these use cases are correlated and/or parented with use cases in other solution categories. A good example is the privileged access abuse case, which requires both UEBA and IdA. The scope of this white paper addresses the specific use cases of user and entity behavior analytics. White papers for identity analytics and cloud security analytics are also available. An optimal list of use cases for UEBA is found below.
One of the Top 10 OWASP (Open Web Application Security Project) vulnerabilities is related to the 'Broken Authentication and Session Management' scenario. Here, attackers exploit vulnerabilities through attacks such as Pass-the-Hash (PtH), Pass-the-Token (PtT), Brute Force and Remote Execution to gain access to user credentials (passwords or hash). Such attacks can be detected using the underlying machine learning algorithms tuned to inspect various parameters like timestamp, location, IP, device, transaction patterns, high-risk event codes and network packets, to identify any deviation from the normal behavior of a particular account and the corresponding transactions. This facilitates detection of any potential account compromise or hijacking scenarios based on the anomalous behavior patterns such as: abnormal access to high-risk or sensitive objects, abnormal number of activities, requests in a short time frame, activity from terminated user accounts, or dormant accounts, PtH attacks and session replay attacks. Anomalies identified via clustering machine learning models and outlier analysis inconsistent with a user or peers’ normal behaviors are given risk scores based on advanced security analytics, to drive alerts, actions and case tickets. Self-audits (reviewed below) may also support this use case.

**Benefits**
- Detects anomalous behaviors beyond known threat signatures, rules and patterns for account compromise, hijacking and sharing
- Provides 360-degree visibility for user accounts, access and activity for on-premises, cloud and hybrid environments
Data Exfiltration and IP Protection

UEBA identifies data exfiltration and protects intellectual property by ingesting data sources such as DLP and data classification to learn important data locations, access and application activity. Risk scoring DLP alerts are a primary benefit of UEBA machine learning to reduce alert fatigue and prioritize ‘find-fix’ resources. Analysis by UEBA includes on-premises and cloud applications for a 360-degree view of data access and activity. This approach helps customers prioritize DLP alert investigations, as well as identify and monitor even the low severity DLP alerts associated with departing users or high-risk users. UEBA solutions traditionally provide out of the box (OOTB) machine learning models which can identify known patterns such as: sensitive documents downloaded and copied to USB, large amounts of source code checked out from source code repositories and file uploads to cloud storage, emails to personal accounts, access to competitor and/or job websites, etc. Solution customers have also extended UEBA alerts beyond SOC analysts to project managers, given their depth of context and relevance regarding employees, data and projects. Self-audits can also provide deterrence for data access and unsanctioned activity.

Benefits

- Baselines data access and activity for anomalous events through self-learning and self-training machine learning models
- Supports customized and unique DLP and data classifications, metadata models and big data infrastructure support to each company
- Significantly reduces DLP alerts, time to investigate and false positives through predictive risk scoring

High Privileged Access Abuse

This use case identifies high privileged access (HPA) abuse by leveraging the combination of accounts, access and activity data. Typically, accounts and access data is ingested from IAM, PAM and/or directory services platforms to identify HPA accounts and discover any non-HPA accounts granted high privileged entitlements. Additionally, the activity data is ingested from enterprise level audit or log sources (e.g., SIEM or log aggregators) or obtained directly from the target data sources. Once HPA accounts are identified, UEBA can detect suspicious behavior and misuse such as: using HPA to assign special or elevated privileges to the user’s own account followed by an activity, transactions outside the window of password value checkout and check-in timeframe. This also includes access to resources and transactions outside normal behavior profiles, abnormal access to classified or sensitive documents, multiple concurrent sessions from the same account, different IPs, devices, locations, etc.

Benefits

- Discovers privileged access and provides visibility on who has the ‘keys to the kingdom’
- Reduces high privileged access account abuse and eliminates shared HPA accounts
- Reduces access risks before abuse with risk scored HPA accounts and entitlements
Insider Threat Detection and Deterrence

Advanced UEBA insider threat detection and deterrence leverages research drawing from extensive insider threat databases of real-world incidents to develop, test and refine machine learning (ML) behavior models. Identifying high-risk profiles with abnormal behaviors in conjunction with data risk monitoring, machine learning and statistical analysis, reveals anomalies in data that humans could not otherwise recognize or detect. As a force multiplier, ML far surpasses human capabilities and software engineering for managing large volumes and varieties of data. True machine learning also has the ability to find high-order interactions and patterns in data for complex problems such as insider threats, compromised accounts and data exfiltration. It does this by leveraging useful and predictive cues that are too noisy and highly dimensional for human experts and traditional software to detect. A 360-degree dashboard provides visibility of an identity’s accounts, access and activity for on-premises and cloud hybrid environments. A self-audit feature may support this use case adding deterrence and increasing security awareness for users. Both access and activity are risk scored for anomalous events with results visible to employee managers and SOC analysts.

Benefits

• Delivers insider threat detection machine learning models from big data analysis to detect anomalies and apply predictive risk scores
• UEBA dashboard highlights insider threats first and in common risk groups, plus watch lists
• Provides unique insider threat deterrence to users and detection for managers through self-audit features

Self-Audit and ID Theft Detection

A self-audit feature deputizes users into a collaborative relationship with security analysts to provide context and relevance not available to SOC teams. This multiplier of ‘eyes on glass’ applies to employees, business partners and suppliers, agents in hub-spoke organizations, and in some cases, customers. All of these parties are likely to have one or more accounts with access entitlements to critical applications and data. A frequently issued (usually weekly) self-audit report provides visibility for access, devices, locations and risk-scored anomalous behavior providing both detection and deterrence for end users. A case in point: a self-audit was implemented by a company where an employee was out of office on a Wednesday due to a sick child. This employee never logged into her accounts on that day. A self-audit report sent to this individual on the following Friday showed account activity on Wednesday when the employee knew they had not logged in. Further investigation by security analysts discovered the account had been compromised for over three-and-a-half years, where the employee had high privileged access (HPA) to critical applications and data.
Cyber Fraud Detection and Deterrence

UEBA addresses cyber fraud use cases for treasury, accounting, payments and areas concerning funds transactions. Here, the UEBA solution would provide a flexible data model open to attributes from commercial or homegrown treasury and accounting systems to be considered for behavioral analytics from machine learning models. UEBA solutions have been deployed for merchant solutions to monitor for cyber fraud and account compromise. A real-world scenario: in April 2016, SWIFT acknowledged attackers had obtained valid credentials for operators to create and approve SWIFT messages. Over 11,000 financial organizations that use SWIFT daily to transfer billions of dollars were jeopardized by this cyber fraud. SWIFT and supporting vendors issued patches and made recommendations to detect fraudulent use. However, the substantial volume of data is too overwhelming and the signals are too fine-grained for analysis by humans. Ingesting data on access and activity from treasury, accounting and payments areas within organizations, UEBA allows organizations to integrate their cyber fraud models and risk frameworks providing significant benefit of leveraging existing investments and security models in alignment with business context. The use of self-audits may also support this use case.

Benefits

• Supports the ingestion of data sources from treasury, accounting and payment systems through an open metadata model
• Detects anomalies with predictive risk scoring and feedback for false positives and negatives powered by machine learning behavior models
• Improves accuracy reflected in risk scores for data quality and relevance through risk weightings that can be customized for attributes
Trusted Host and Entity Compromise

It is well known that one of the widely used tactics to execute cyber-attacks is to compromise trusted hosts connected to an organization’s network infrastructure. In addition to monitoring anomalous user behavior with UEBA, it is critical for organizations to monitor closely all the endpoints (devices and hosts) connected to the network. UEBA builds an anomaly timeline for an entity based on the high-risk anomalous events and activities performed from the respective device and hosts. UEBA correlates a wide range of parameters associated with an entity, including: endpoint security alerts, vulnerability scan results (Common Vulnerability Scoring System [CVSS]), risk levels of users and accounts used, targets accessed, packet level inspection of the requested payloads, and more. This correlation facilitates detection of any anomalous activities or events to determine predictive risk scores.

Benefits
- Provides risk-based dashboard for closely monitoring high-risk entities and investigation using detailed anomaly timeline based on users, accounts, alerts and activities associated with the entity
- Detects advanced persistent threat (APT) attacks and attack vectors and predicts data exfiltration by performing entity-centric anomaly detection

Stateful Session Tracking

In this use case, UEBA builds and tracks the user session state, even when a user navigates across heterogeneous resources or applications using different accounts and devices at different times. Leveraging machine learning, UEBA dynamically builds session correlation attributes used to build session context in order to link any subsequent activities based on a confidence factor. This enables the identification of valid IP switching due to transitions between wired and wireless networks, a workstation and a handheld/mobile device, or accessing enterprise resources from various onsite locations or remotely over VPN. UEBA’s ability to track user sessions across these various parameters ensures a significant reduction in false positives while simultaneously delivering greater visibility into the sequence of events. It also provides the capability to drill down on specific activities performed by a user or entity while performing an investigation. This analysis also expedites the detection of session replay and hijacking attacks, highlighting any anomalous activity from a user session or concurrent sessions from the same account.

Benefits
- Provides greater visibility into user activities across multiple resources or applications via with stateful session tracking
- Provides drill-down and raw log views for deep event analysis at the source
- Reduces false positives due to common scenarios like IP, account and device switching while performing day-to-day activities
- Detects session replay and hijacking attacks
Step-up Authentication (or Adaptive Authentication)

The use of passwords to authorize users is core to the problem of identity compromise and misuse. Deploying multi-factor authentication takes time, resources and expenses and can impede high-productivity users in low-risk environments. The concept of step-up authentication (also known as adaptive authentication) leverages the UEBA risk score of an identity or entity to determine the levels of authentication for access. A low-risk score may result in a simple password challenge while a high-risk score may result in three authentication challenges (e.g., password, access code and answering questions). Mature UEBA solutions support bidirectional integration with industry standard adaptive authentication solutions by using ready-to-use connectors and API interfaces. The net effect raises security awareness to end-users when they have high-risk situations. In addition, there is an increased chance of disrupting external intruders that have compromised the account at the password level only and may not have compromised the end-user’s smartphone where an access code is provided. Even with step-up authentication, an account may still be compromised or hijacked and the use of UEBA for detection is advised.

Benefits

- Creates a closed-loop for step-up authentication with API integration between risk analytics and authentication solutions
- Raises security awareness with end users via authentication challenges when their identity shows high-risk behaviors
- Combines step-up authentication with self-audit as key parts of an increased security awareness program

Anomalous Behavior and Watch Lists

UEBA addresses anomalous behavior with watch lists to quickly profile and maintain an eye on unknowns and apply escalating predictive risk scores. Machine learning behavior models are designed to deliver feedback on false positives and negatives and then update self-learning and self-training models to adapt to time-based norms and conditions unique to each customer deployment. For example, a database administrator may create a script that runs several commands with security implications at 2 a.m. each evening. This user is an innovator, working to improve the enterprise’s productivity. However, machine learning models will see these commands during non-business hours as an anomaly and risk score accordingly. Feedback from the models can note the situation is benign. Nonetheless, the database administrator should be put on a watch list. Watch lists also come pre-defined within UEBA for common high-risk groups like new hires, departing users, terminated users, and high-risk users. These groups should be easily accessed in dashboard drop-down menus to analyze risk scores, anomalies, accounts, access, activity and timelines. UEBA also supports explicitly adding or removing identities within watch lists.
SIEM and DLP Risk Intelligence

UEBA addresses the alert fatigue issue of SIEM (security information and event management) and DLP (data loss prevention) solutions by aggregating the risk scores at the user and entity level, rather than generating a huge number of alerts at the transaction or event level. This allows SOC analysts to focus on the high-risk identities and the associated anomalies detected by UEBA. The result is a significant reduction in the number of alerts. This use case employs bidirectional integration via APIs enabling SIEM and DLP data ingestion into UEBA as it provides risk scores back to these systems to allocate ‘find-fix’ resources. SIEM, AD and DLP solutions provide critical data sources for additional context related to identity profile information and the corresponding access grants (accounts, entitlements), also including the activity and alerts data ingested from on-premises and cloud applications in hybrid environments. While SIEM and DLP solutions work with known variables and identifiers via open queries, rules, patterns and signatures, UEBA detects the unknown via robust machine learning behavior models. Leveraging clustering and outlier algorithms, the models identify anomalies for predictive risk scoring. UEBA examines the data from an identity-based perspective analyzing user or entity behavior against itself and peer groups using baseline norms. As companies migrate to the cloud for applications and data, the role of UEBA becomes more essential for security events and data protection.

Benefits

• Provides ready-to-use data connectors for popular SIEM and DLP solutions to speed connectivity and data ingestion
• Delivers risk scored SIEM and DLP events and alerts to focus ‘find-fix’ resources through machine learning behavior models
• Provides bidirectional integration via APIs, enables data ingestion into UEBA, as well as the export of risk scores to SIEM and DLP solutions
Hybrid Infrastructure

This use case addresses hybrid infrastructure by providing UEBA platforms for both on-premises and cloud applications, removing the need for any large data transfers between environments. These transfers can be expensive and impede the use of important data for advanced security analytics. The threat and identity analytics would run on-premises and provide ready-to-use data connectors for common on-premises applications and platforms as data sources. The cloud analytics portion of the solution is an API-based cloud access security broker (CASB) that integrates with SaaS cloud applications, along with IaaS, PaaS and IDaaS, via APIs. The CASB API architecture enables direct data collection from cloud data sources while providing users a transparent access experience from any location on any network. Proxy-based CASBs are a data source into cloud analytics for shadow IT use, cloud DLP, and more. Threat, identity and cloud security analytics share combined processes and models to provide 360-degree visibility for identity, accounts, access and activities in hybrid environments.

Benefits

- Enables organizations to avoid data transfer charges between on-premises and cloud (if data collection was only in one location)
- Improves the context of data inputs from on-premises and cloud for each identity or entity through user and entity behavior analytics
- Ensures organizations can migrate applications and data from on-premises to cloud with peace of mind

Capital Markets

Use Cases

Trading Surveillance

Enterprises engaged in trading transactions face a unique challenge to assure the inviolability of trades is assured. To support that objective, a number of advanced security analytics use cases are aligned to address the various challenges these enterprises face.

- **Pre-Trade Surveillance** - Pre-Trade Surveillance, prevention of regulatory and compliance violations. Pre-validation to ensure both customer and personal (employee) trades fall within acceptable risk, limit, and price volatility thresholds. Monitor trade order manifests to ensure they are consistent with past requests and identify outliers.
- **At-Trade Surveillance** - Monitoring trade transactions as they occur with near real-time analysis, based on data ingestion. Identifying anomalous patterns in order flow (spoof trading, order entry) to manipulate volumes and security prices.
- **Post-Trade Surveillance** - Comparing trade transactions to historical trading behavior baseline and reviewing order/trade ratios. This process can be run across instruments and/or traders. The process uses supervised learning and rules based on previous abuse and known non-compliant trading patterns. Both customer and in-scope personal (employee) trades are reviewed. Instances of potential illegal insider trading can be identified during this process.
- **Cross-Asset Class, Cross-market Surveillance** - Monitoring multiple market classes across geographies for potential abuse. This type of surveillance monitors for events in one class of asset or geography that impacts another class of asset (equities versus bonds, oil, gold, silver, etc.).
• **Trade Communication Linking** - Monitor voice, chat, and email for market manipulation. Link communications to trading patterns to establish patterns of communications before trades occur.

• **Social Media Monitoring** - Monitor social media feeds to map social media accounts of key employees. Generate an alert when someone posts information that could be considered a compliance violation (market manipulation).

• **Misreporting** - Detect payments to a vendor by unrelated third parties, misclassification or over/under valuation of commodities and double invoicing.

• **Unusual Trading and Transactions** - Detection of repeated importation and exportation of the same high-value commodity (carousel transactions) or trades of commodities that do not match the business involved.

• **Consumer Account Breaches** - Monitoring of customer accounts for unusual account activities including slow drip attacks, account changes, and link this information with consumer reporting agencies (fraud detection agencies) such as credit freezes, and unusual account activity.

• **Fraudulent Consumer Account Detection** - Identity validation – Detection of accounts with suspicious combinations of SSN, name, address and phone. Validate information is not the same or similar to an unusually large number of other accounts. Flagged accounts require additional validation prior to allowing transactions.

• **Personal Trading Checks** - Pre-validation to ensure personal trades fall within risk, limit, and price volatility thresholds. Ensure trades are consistent with past behavior.

• **Insider Trading Surveillance** - Monitoring of personal trading of key employees to identify outlier behavior. Correlate personal trading pattern with available insider information.

---

**Capital Markets Use Cases – Process Flow**

**Inputs**
- **Operational Systems**
  - Trading Systems
  - Accounting
  - Compliance
- **Compliance**
  - Employee Monitoring & Oversight
- **Communications**
  - Phone
  - Social Media
  - Email
  - Chat / SMS

**Policies & Thresholds**
- Machine Learning
- Big Data

**Outputs**
- **Mobile / Web Dashboard**
- **Custom Reporting**
- **Case Management**
- **Cases, Alerts, Escalation**
- **Behavioral Analytics**
- **Pattern Detection**
- **Workflow Management**

© 2017 Gurucul. All rights reserved.
Depending on their roles and responsibilities, different members with an organization have varied use and interaction with user and entity behavior analytics use cases.

- **End User** - With the self-audit feature, end users have the opportunity to view their risk-scored behavior for self-analysis. They can view devices, access, activity, and risk-scored anomalies through convenient and regular reporting. This enables them to participate in a collaborative partnership with the organization to protect assets. They also provide rich context not found within a SOC to quickly identify anomalous behavior and feedback on any false positives to improve machine learning model accuracy. The self-audit feature is also used with business partners and customers, and in some cases has been monetized.

- **Department Leaders** - Taking a risk-based approach to an identity’s access management and processes, department leaders gain assurance that the sensitive intellectual property their teams work with is secure from excess access and access outliers. This heightens departmental productivity, allowing the team to focus more effectively on organizational goals and objectives and eliminates rubber-stamping of certifications and access cloning. In addition, the self-audit fosters a sense of engaged understanding of security requirements and best practices and a sense collective commitment and involvement among group members to help protect the ‘crown jewels’ of an organization because of their shared investment in the organization’s success.

- **SOC Analyst** - Through UEBA normalized risk scoring, analysts detect insiders, account compromise, data exfiltration and external intruders. Context-aware analysis facilitates multi-level analyst reviews with data masking through workflow based on role-based access controls. Process empowerment is available through canned machine learning models as well as case and ticket management internally, or interfacing with solution applications such as Remedy, ServiceNow, and SFDC plus email or SMS alerts.

- **Data Scientist** - They are enabled by advanced security analytics solutions offering vendor agnostic capabilities to create custom machine learning models without coding in a step-by-step process requiring only a minimal knowledge of data science. As an open solution, advanced security analysts and data scientists can adjust risk weightings within existing machine learning models, add or update attributes to the metadata model, and ingest desired attributes from any data source with a flex data connector. Customers may have confidential and unique data not open to vendor data scientist reviews, or private use cases which they prefer not to discuss. For these scenarios, data scientists are able to build custom machine learning models in test environments, compare model profiles and risk scoring to select the most optimal model(s) for production deployment. These advanced security analytics solutions with custom capabilities also support an open choice of big data for customers, including Hadoop, Cloudera, Hortonworks, MapR and Elastic/ELK. Data science teams and architects can use their data lake of choice to extend machine learning model use cases.
Having a broad selection of user and entity behavior analytics use cases provides customers with the assurance that their advanced security analytics requirements will be addressed. Assuring a vendor can support these use cases across both on-premises, cloud, and in hybrid environments, as well as being vendor agnostic, provides the strongest assurance that solution objectives are achieved. The overall benefits of user and entity behavior analytics use cases include:

- **Empowered security capabilities and quality** - The mature capabilities of UEBA provide robust and optimal advanced security analytics across a range of on-premises and hybrid environments, scoring the gray areas of unknowns and minimizing false positives. The result is improving the focus of ‘find-fix’ resources, and optimizing the time of security analysts, efficiency in the SOC, making operations and people more productive.

- **Extended and optimized, discovery, monitoring and visibility** - This includes the baseline ability to view the full context of a user’s access and activities, both legitimate and anomalous. A mature solution also includes analytics for hybrid environments, providing a combined 360-degree view for identity, and risk-scored behavior anomalies, driven by machine learning, as part of a newly recognized state-of-the-art UEBA standard along with its empowered ability in interface with IdA and CSA for increased efficiencies.

- **Improved productivity and cost savings** - By having holistic visibility across all an organization’s environments, users and devices, SOC teams’ efficiencies are maximized, delivering cost savings. In addition, as enterprises migrate to cloud applications, the ability to expand platforms without adoption of additional solutions helps to minimize costs.

- **Self-audit capabilities** - With the self-audit feature, the rich context of users is leveraged in a collaborative relationship with SOC teams and managers to quickly identify anomalous behavior with a low false positive rate via high-risk-scored ad hoc reports or via a regular reporting schedule. In addition, self-audits provide security and deterrence. They also apply to many use cases, including insider threat.
The depth and range of use cases fundamentally defines the areas of expertise and functionality for user and entity behavior analytics vendors. This factor represents an important qualification when choosing a solution partner. Having a broad selection of use cases provides customers with the assurance that their advanced security analytics requirements will be addressed comprehensively today and into the future. Assuring a vendor can support these use cases across on-premises, cloud and in hybrid environments, as well as being vendor agnostic, provides the strongest assurance that objectives are achieved. Big data provides rich context that drives machine learning models. A key to its success is the democracy of data from solution silos and open APIs for data collection and leveraging risk scores for automated response. Behavior analytics centers on identity with a 360-degree view of accounts, access and activity for users, entities and peers to detect anomalous behavior and outliers. Both big data and identity are horizontal planes that slice through solution silos and organization charts. This perspective with defined uses cases makes for a successful journey.

[NOTE: For a comprehensive overview of advanced security analytics uses cases – which include UEBA, IdA, CSA, custom use cases, and more – please refer to “Borderless Behavior Analytics – Who’s Inside? What’re They Doing?” by Gurucul CEO Saryu Nayyar (Chapter 9). For more information on the book go to: http://borderlessbehavioranalytics.com]