Are You Protecting Your Data or Chasing Threats?

In the face of rapidly evolving threats and rampant data growth, data-centric user behavior analytics is helping to answer the existential question: “Is our data safe?”

In this issue

- Are You Protecting Your Data or Chasing Threats? 2
- Research from Gartner: Market Guide for User and Entity Behavior Analytics 4
- About Varonis 23
Are You Protecting Your Data or Chasing Threats?

In the face of rapidly evolving threats and rampant data growth, data-centric user behavior analytics helps answer the existential question: “Is our data safe?”

“We don’t know if any data was stolen.”

Eight words that no CISO wants to hear after a security incident.

Those beginning their exploration of UEBA technologies often think they will be able to detect data breaches by simply sending more alerts to a central system for analysis. They quickly learn, however, that adding more hay to the haystack does not make it easier to find the needle.

The needle, in this case, is the answer to whether data is safe or not. To answer that question with certainty, you need the right telemetry and the right analytics.

Why Context Kills Noise

Here’s an alert you might get from a non-behavioral system:

- Upload to external email website exceeds 100MB

This is often followed by a security analyst spending hours or days trying to answer questions, like:

- Who is the user? An executive with access to thousands of sensitive files? The head of engineering who just put in her resignation this morning?
Were they using their normal computer?

Had they recently touched any files with personal information or critical intellectual property?

Is this business as usual, or unusual business?

An admin sending an unusually large ZIP file via a personal Gmail account soon after copying customer data from the corporate OneDrive is a hair-on-fire alert. A large upload to a photo sharing site by an HR specialist after accessing pictures of the holiday party means something fun to look at over lunch.

Wouldn’t it be better if security solutions figured this stuff out before demanding an analyst’s attention?

Yes! And that’s what effective UEBA solutions do. They learn behaviors and build context automatically, raising alerts only when the underlying evidence strongly suggests an anomaly. Alerts are packed with many of the answers to the questions an analyst needs to confidentially draw conclusions and close the case.

An organization’s threat surface isn’t static, so context must be built and refined over time. Users access different data sets on different systems, from different workstations, at different hours, from different places. This is where machine learning is essential – building and maintaining baselines of what normal behavior looks like based on the interactions between all users, systems, and data.

### A Data-Centric Approach to UEBA

UEBA only works well if it has enough of the right telemetry to analyze.

It’s difficult to predict who will attack you or what exploits they’ll use, but we all know what most attackers want: your data.

If data is the asset you want to protect most, you’ll need to understand precisely who is accessing your data and how. If you have critical data stored in files and emails, then file and email system activity is the focal point of the story – without it, you can’t answer the most important security question of all: “Is our data safe?”

Unfortunately, raw logs for file and email activity are frequently unavailable. When they are available, they are noisy and voluminous, like network traffic. If data protection matters, a data-centric technology designed to provide context about data usage, permissions, and data sensitivity – across as many of your core data stores as possible – should be the heart of your data security stack.

Source: Varonis
Security and risk management leaders considering UEBA are finding that the market keeps shifting away from pure-play vendors, toward a wider set of traditional security products that embed core UEBA technologies and features to benefit from advanced analytics capabilities.

**Key Findings**

- As evidenced by their use by midsize-to-large enterprises across a range of use cases, user and entity behavior analytics technologies have matured.

- UEBA capabilities are embedded in a wide range of adjacent security technologies, such as cloud access security brokers and identity governance and administration systems, whereas UEBA and security information and event management systems continue to converge.

- UEBA vendor hype and the misuse of the term “artificial intelligence” make it difficult for buyers to effectively compare vendor technologies and capabilities without a proof of concept.

- Buyers find that UEBA deployment time and ongoing operations can be more time-consuming and labor-intensive than what vendors promise, even for core threat detection use cases. Adding custom or edge use cases can be arduous, requiring expertise in data science and analytics.
Recommendations
IT security and risk management leaders involved with security operations should:

■ Initiate any UEBA project by clearly defining the use cases that need to be addressed, and by describing the desired output from the tool for each use case to ensure that the project is delivering value against key pain points.

■ Before buying another tool, determine whether existing tools in the organization have the required features, or whether they can be expanded (e.g., a SIEM solution).

■ Verify with a POC that the UEBA solution can ingest the data sources required for priority use cases, and whether use cases can be implemented “as is” with prepackaged analytics. Determine the expected level of effort for custom use cases.

■ Schedule at least 30 days for the POC process. This will provide the solution’s machine learning engine with the time needed to learn an organization’s data and construct baselines, using live or historical data, and for your organization to validate the UEBA solution and its outputs. More immediate results are possible, but they are unlikely to be driven by machine learning.

By 2022, 95% of all UEBA deployments will be “as a feature” of broader security platforms.

Market Definition
This document was revised on 23 May 2019. For more information, see the Corrections page.

UEBA solutions use packaged analytics to evaluate the activity of users and other entities (e.g., hosts, applications, network traffic and data repositories). They discover threats and potential incidents, commonly presented as activity that is anomalous to the standard profiles and behaviors of users and entities across time and peer group horizons. The most common use cases sought by enterprises are threat detection and response, as well as insider threat detection and response (mainly compromised insiders; sometimes malicious insiders).

Market Description
UEBA is a solution, as well as a feature, embedded in a particular tool. In this research, we will be covering both aspects:

■ Solution — Pure-play UEBA platform vendors, including vendors that also sell a SIEM separately, focus on broad range of use cases, for users, as well as entity behavior analytics.

■ Embedded — Vendors/domains embed UEBA features and technologies in their solutions (including SIEM vendors that embed UEBA features, but do not sell these UEBA features separately as a stand-alone solution). They usually cater to a more specific set of use cases. In this case, UEBA is for user and/or entity behavior analytics.

Strategic Planning Assumptions
By 2021, the user and entity behavior analytics (UEBA) market will cease to exist as a stand-alone market, and will have shifted to modern security information and event management (SIEM) systems with advanced analytics, as well as other tools embedding UEBA features.
Gartner defines UEBA (pure-play platform tools, as well as embedded UEBA), along the three dimensions of use cases, analytics and data sources (see Figure 1).

**Pure-Play UEBA Platforms Versus Embedded UEBA**

Gartner views the pure-play UEBA platform market as including solutions that:

- Solve multiple, distinct use cases, such as privileged user monitoring or data exfiltration, not just generically “monitoring for anomalous user activities.”

- Emphasize the use of advanced analytics, supported and enriched by basic analytic approaches, as required.

- Offer multiple ways to collect data, including natively from data sources, as well as from log management tools, data lakes and/or SIEM tools, without forcing buyers to deploy dedicated instrumentation agents.

- Can be purchased and implemented as stand-alone solutions, rather than be embedded in other solutions.

---

**Figure 1. The Three Pillars of UEBA**

The Three Pillars of UEBA

![Diagram of the Three Pillars of UEBA](image)

**Use Cases**
- Known threats
- Advanced persistent threat (APT) and zero-day
- Compromised user
- Malicious insider

**Data**
- Events and logs
- Network flow and packets
- User context
- External threat intelligence
- Human resources data
- Business context

**Analytics**

- Rule-based systems
- Statistical modeling
- Unsupervised machine learning
- Supervised machine learning
- Deep learning
- Ensemble networks
- Generative adversarial networks

Source: Gartner (May 2019)
ID: 36156
This definition purposely leaves aside “specialized” UEBA solutions and solutions that merely embed some UEBA feature set as part of their scope, such as data loss prevention (DLP) systems and cloud access security brokers (CASBs). Specialized UEBA and embedded UEBA vendors are noted in their respective sections below in this research — as doing user and/or entity behavior analytics (see Table 1).

<table>
<thead>
<tr>
<th>Category</th>
<th>Pure-Play UEBA Platforms</th>
<th>Other Solutions With Embedded UEBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Case</td>
<td>Perform behavior analytics for users, as well as entities.</td>
<td>Lack of available data can force UEBA to do behavior analytics only on users or entities.</td>
</tr>
<tr>
<td>Use Case</td>
<td>Service many use cases.</td>
<td>Cater to narrower set of use cases.</td>
</tr>
<tr>
<td>Analytics</td>
<td>Detect anomalies using various analytics approaches — primarily statistical models and machine learning — combined with rules and signatures. Delivered as prepackaged analytics used to create and compare user and entity activity against their profiles and their peers’ profiles.</td>
<td>Same as pure-play UEBA, although the scope can be users and/or entities.</td>
</tr>
<tr>
<td>Analytics</td>
<td>Offer advanced analytics capabilities that are not uniquely based on rules, such as clustering algorithms that offer dynamic peer grouping.</td>
<td>Same as pure-play UEBA, although peer grouping for certain use cases in embedded UEBA tools can/should be done manually.</td>
</tr>
<tr>
<td>Analytics</td>
<td>Correlate user and other entity activities and behaviors (through Bayesian network techniques, for example), and aggregate individual risky behaviors, to highlight anomalous activity.</td>
<td>Same as pure-play UEBA, although scope can be users and/or entities.</td>
</tr>
<tr>
<td>Data Sources</td>
<td>Ingest event data from user and entity activities natively from the data sources directly, or through an existing repository — log management SIEM or data lake.</td>
<td>Data ingestion mechanisms are usually ad hoc, involving users and/or entities only. They do not leverage an enterprise’s log management/SIEM/data lake for access to data.</td>
</tr>
<tr>
<td>Data Sources</td>
<td>The solution should not rely primarily on network data as a main data source, and should not rely primarily on its own agents to collect telemetry data.</td>
<td>Solution can be network-focused only (e.g., network traffic analytics [NTA]), and/or carry their own endpoint agents (e.g., employee-monitoring tools).</td>
</tr>
<tr>
<td>Data Sources</td>
<td>Enrich data about users/entities with contextual information. Support ingestion of structured, real-time event data, as well as structured/unstructured reference data from IT directories — e.g., Active Directory (AD) — or other sources of machine-readable information (e.g., HR databases).</td>
<td>Same as pure-play UEBA, although the scope of contextual data may be different depending on the use case. AD and Lightweight Directory Access Protocol (LDAP) seem to be the common context repositories leveraged by embedded UEBA tools.</td>
</tr>
<tr>
<td>Availability</td>
<td>Offer the above in a solution that can be purchased separately.</td>
<td>Cannot buy the embedded UEBA feature set outside the solution embedding it.</td>
</tr>
</tbody>
</table>

Source: Gartner (May 2019)
Table 1. Pure-Play Versus Embedded UEBA

Many of the attributes of a pure-play UEBA tool also apply to embedded UEBA — e.g., supervised or unsupervised machine learning; open versus closed analytics. However, tools that embed UEBA can also exhibit different attributes, mainly because they are often solutions addressing more-specific use cases, and because their embedded nature often precludes their availability outside the solution that embeds them.

Compared with a pure-play UEBA platform, solutions that embed UEBA feature sets also have access to:
- Fewer data sources
- More-tailored data via agents
- Fewer computing resources to run compute-intensive analytics (especially when the tool embedding the UEBA is delivered as an appliance)

This will offer an interesting twist. For the specific use cases they cater to, embedded UEBA could be running basic UEBA analytics (e.g., simple unsupervised machine learning), but having access to exactly the right data, be overall more effective than a pure-play UEBA solution. It is expected that the pure-play UEBA platform would offer more-sophisticated analytics as their core intellectual property (IP) than embedded UEBA tools. The implications are summarized in Table 2.

Table 2. The Implications of Pure-Play Versus Embedded UEBA

<table>
<thead>
<tr>
<th>Category</th>
<th>Pure-Play UEBA Platforms</th>
<th>Other Solutions With Embedded UEBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics</td>
<td>Applicability to many use cases requires a general-purpose set of UEBA features, with an emphasis on the sophistication of the analytics and the machine learning models.</td>
<td>A focus on a narrower set of use cases enables more specialized capabilities, centered on models addressing specific use cases and a lower sophistication of analytics.</td>
</tr>
<tr>
<td>Analytics</td>
<td>Customization of the analytics models is required for each use case.</td>
<td>Analytics models pretuned to the rest of the tool embedding the UEBA. Overall faster time to value for the specific use cases delivered by the tool embedding the UEBA.</td>
</tr>
<tr>
<td>Data Sources</td>
<td>Access to data sources from all corners of the enterprise.</td>
<td>Fewer data sources, usually restricted to the ones available through the agent or the solution embedding UEBA.</td>
</tr>
<tr>
<td>Data Sources</td>
<td>Information contained in each log can be limited by the data source, and might not have all data required for the central UEBA tool.</td>
<td>The amount and verbosity of raw data that can be generated by an agent, and fed to the UEBA can be specifically tailored.</td>
</tr>
<tr>
<td>Architecture</td>
<td>Allow a single UEBA tool for organization.</td>
<td>Require a separate UEBA feature set for each solution embedding UEBA capabilities.</td>
</tr>
<tr>
<td>Architecture</td>
<td>Easier integration to leverage capabilities of a log management SIEM or data lake.</td>
<td>Embedded UEBA point solutions often come with a requirement to deploy agents and manage data.</td>
</tr>
<tr>
<td>Architecture</td>
<td>Performance for stand-alone UEBA solutions is easier to scale, based on the required amount of data and the complexity of the analytics.</td>
<td>Form factor and architectural constraints for the solution may restrict resources available to perform the UEBA analytics.</td>
</tr>
<tr>
<td>Integration</td>
<td>Manual integration of the UEBA platform to the other tools driving each use case.</td>
<td>Core bundling of UEBA feature set is already done in the tool by the vendor.</td>
</tr>
<tr>
<td>Integration</td>
<td>Enable organizations to build a technology stack using a best-of-breed approach.</td>
<td>UEB A module embedded and unextractable, so clients can’t replace it with their own.</td>
</tr>
</tbody>
</table>

Source: Gartner (May 2019)
Market Direction

UEBA is near the bottom on the Trough of Disillusionment in Gartner’s latest Hype Cycle (see “Hype Cycle for Threat-Facing Technologies, 2018”), denoting a maturing of this technology. The paradox is to reconcile growing overall spending on UEBA technologies with the disappearance of a stand-alone UEBA market. The reasons include:

- The market shift to embedded UEBA, due to the proliferation of vendors offering UEBA features embedded in their solutions (see the “Embedded UEBA and UEBA as a Feature Are Becoming More Widespread” sections).

- The convergence of UEBA and SIEM (see the “UEBA and SIEM Continue to Converge Into a Modern SIEM” section).

- Client organizations’ observed behaviors. Many Gartner clients seem to be just waiting for their SIEM vendors to offer better analytics. During SIEM replacement cycles, there seems to be a preference for a SIEM with embedded UEBA (“modern SIEM”), or a full-stack bundle (a UEBA vendor that also happens to sell a SIEM). Fewer clients are considering replacing their SIEMs with a best-of-breed stack by mixing and matching SIEMs and pure-play UEBA platforms.

Gartner does not expect to track UEBA revenue beyond 2020, and expects the number of pure-play stand-alone UEBA solutions to continue decreasing. This trend has been confirmed since 2017, via acquisitions, pivots into specific markets or the development of a set of SIEM features to become a modern SIEM.

Furthermore, the term “UEBA” is likely to phase out eventually and be superseded by other acronyms that focus on a narrower use case (e.g., “user behavior analytics”), on an adjacent use case (e.g., “data usage/access/xxx analytics”) or just latch onto some new buzzword (e.g., artificial intelligence [AI] seems to get traction, although that term is meaningless today for UEBA vendors). Vendors themselves are elevating their messaging away from the technical aspects of UEBA features and moving into describing their value proposition aligned to one or more use cases.

Market Analysis

Changes Since the Last Market Guide for UEBA Update

Haystax was acquired by Fishtech Group in May 2018, ZoneFox was acquired by Fortinet in Oct 2018, and Interset was acquired by Micro Focus in February 2019.

UEBA and SIEM Continue to Converge Into a Modern SIEM

During 2018 and thus far in 2019, we saw a continuous blurring between SIEM tools and UEBA tools, as described in “Technology Insight for the Modern SIEM.” SIEMs have become better at analytics and can offer more-sophisticated use cases. At the same time, UEBA vendors have focused on better data management and operability, which makes them closer to a SIEM (although UEBA pure-play platforms often still lack robust case management for example).

Already half of the UEBA pure-play platform vendors tracked in this research also have a SIEM offering, usually provided as different modules for a more-complete threat detection technology. Likewise, most SIEM vendors now have advanced analytics capabilities, embedded in the SIEM or through a UEBA module. Their approach has been to:

- Develop this functionality organically
Integrate other UEBA solutions through an OEM arrangement

Partner with a UEBA vendor on a tightly coupled offering

**SIEM and UEBA Convergence**

This puts tremendous pressure on the remaining pure-play UEBA vendors to become SIEMs and instantly benefit from established SIEM budgets and identified buying centers, although in a competitive market (see Figure 2).

**Main Use Cases Are Solidifying, as New Ones Emerge**

UEBA solutions can support a variety of use cases. However, Gartner clients agree that the primary use case involves the detection of different categories of threats, achieved through visibility into and analysis of often-correlated user and other entity behavior. Gartner sees use cases such as monitoring for unauthorized data access and movement, suspect privileged user activities, and malicious or unauthorized employee activities. UEBA also monitors unusual cloud resource access and usage, and supports better detection from existing security technology investments — e.g., CASB and identity and access management (IAM).

**Figure 2. SIEM/UEBA Convergence**

![SIEM/UEBA Convergence Diagram](image)

Source: Gartner (May 2019)
ID: 36195
Finally, there is a set of typically non-cybersecurity-centric use cases, such as fraud or employee monitoring, for which UEBA solutions can sometimes be used. However, these often require non-IT and nonsecurity data sources, or specific analytics models derived from deep domain expertise. The five primary domains and use cases with which the stand-alone UEBA vendors and their users align are described in the sections that follow.

**Malicious Insider**

UEBA vendors targeting this use case monitor staff and trusted external parties only for unusual, bad or abusive behavior. Vendors in this domain do not monitor or analyze service accounts or other nonhuman entities to inform their analysis. Largely because of this, they are not oriented toward detecting advanced threats when hackers take over existing user accounts. Instead, they are oriented toward finding insiders engaged in malicious activities.

Essentially, malicious insider threats emanate from trusted users with malicious intent who seek to impose damages on their employers. Because malicious intent is difficult to assess, best-in-class vendors in this category analyze contextual behavioral information not readily available in log files. Vendors in this domain also optimally ingest and analyze unstructured information, such as email content, performance reviews or social media information, for employee behavior context.

**Compromised Insider and Advanced Threats**

The use case here is to rapidly detect and analyze bad activities once an attacker has infiltrated an organization and is moving laterally around the internal IT infrastructure. Advanced persistent threats (APTs) and unknown or not-yet-understood threats, such as zero-day attacks, are notoriously difficult to detect, and often hide behind legitimate users or service accounts. These threats usually have a complex operational model (see “Addressing the Cyber Kill Chain” or Mitre’s Adversarial Tactics, Techniques and Common Knowledge [ATT&CK] framework), or their behavior has not yet been recognized as bad. This makes them difficult to detect with simple analytics (e.g., pattern matching, thresholds or correlation rules).

However, many of these advanced threats force assets to behave differently than they usually do, often attached to unsuspecting users and identities — i.e., compromised insiders. UEBA techniques offer some interesting opportunities to detect these threats, improve signal-to-noise ratio, consolidate and reduce alert volume; prioritize alerts that remain, and facilitate efficient response and investigation. UEBA vendors that target this use case typically have tight two-way integration with organizational SIEM tools.

**Data Exfiltration**

The use case in this domain is to detect the exfiltration of data in organizations. Vendors focused on this use case typically enhance DLP or data access governance (DAG) systems with anomaly detection and advanced analytics, thereby improving their signal-to-noise ratio; consolidate alert volume; and prioritize alerts that remain. For additional context, they tend to integrate with, and rely more on, network traffic (e.g., web proxy) and endpoint data, because the analysis of these data sources can shed light on data exfiltration activities. Data exfiltration detection is used to catch insiders and external hackers threatening the organization.

**Identity and Privileged Access Management**

Stand-alone UEBA vendors in this domain monitor and analyze user behavior against already-established access rights with the goal of identifying excessive
privileges or abnormal access. This holds true for all types of users and accounts, including privileged users and service accounts. Organizations have also used UEBA to clean up dormant accounts and user privileges that are set higher than they need to be.

**Incident Prioritization**

In this use case, the goal is to help an organization prioritize the alerts that are being generated across the solutions in their technology stacks, and offer guidance on which incidents or potential incidents should be prioritized. UEBA tools and techniques are useful to understand what incidents are particularly abnormal or dangerous for a particular organization. In this case, the UEBA engine not only uses baselines and threat models, but usually enriches these with knowledge about the organization’s structure (e.g., criticality of assets, and people’s roles and access levels).

**Emerging Use Cases**

Some interesting edge use cases are being developed by forward-leaning organizations, notably to address insider threats. However, the real push comes from embedded UEBA vendors that are beginning to embrace UEBA features and capabilities, and can deliver on some unique insights. These will be reviewed in their corresponding sections below.

**Who Buys UEBA?**

In addition to large global organizations, stand-alone UEBA tools appeal to large accounts that have legacy SIEM without advanced analytics, that have invested to deploy their SIEM and to develop content for it, and are looking for overall better analytics.

Many buyers are simply waiting for their SIEM to include UEBA features. Forward-leaning organizations pave the way with pure-play UEBA and embedded UEBA tools, experiment, and contribute to the emergence of best practices.

Buyers typically have specific drivers for purchasing a tool, such as improving their external threat detection capabilities by augmenting their SIEM solutions, or requiring technology to support the build-out and operation of an insider threat detection program.

Different buying centers (see Figure 3) are looking at UEBA solutions, depending on organizations’ use cases:

- Security operations are primarily interested in improving the internal visibility for threat-detection-oriented use cases. That is, an external attacker has breached perimeter defenses and compromised an internal host and a user’s credentials, and is using them to move laterally through an organization.

- Buyers oriented toward risk management responsibilities — especially in finance or healthcare — are focused on monitoring users to detect prohibited or unauthorized activities by trusted insiders, such as employees, contractors and external third parties.

The two buyers may use the same tool to perform their jobs, but monitoring trusted insiders is generally performed by a team that is distinctly separate from security operations, due to the data sources typically involved and the insights generated. This raises privacy and regulatory issues for organizations, especially those operating in jurisdictions under tight regulatory schemes (e.g., Europe).

In some situations, buyers are interested in both use cases (e.g., those driven by a chief information security officer [CISO] with responsibilities for risk
management and security operations), or have vague use cases around improving the SRM team’s visibility of the IT environment. In any case, clear use cases and justification are required before moving forward on a UEBA project.

With the emergence of point solutions with embedded UEBA, many buying centers are purchasing solutions with UEBA capabilities (e.g., network security, identity, fraud). UEBA features are expected to eventually reach all corners of the enterprise.

**How Is UEBA Implemented and Delivered?**

Pure-play UEBA platform tools are generally deployed on-premises or offered as a cloud-based service (with some requiring both). Embedded UEBA solutions follow the form factor of the solution that is embedding them — on-premises, software, virtual appliance, appliance, or as a cloud-based service.

**Time to Value Is Often Underestimated**

Even among clients expressing interest to Gartner, there is a concern that UEBA solutions are expensive to acquire, implement, maintain and use. At a time when organizations are fighting portal fatigue, they unfortunately represent yet another console. The tools’ varying investments in time and resources depend on the use cases and types of analytics employed, and they usually represent a large commitment.

Contrary to many vendor claims, UEBA is not a set-and-forget tool that can be up and running in days. Gartner clients report that it takes three to six months to get a UEBA initiative off the ground and tuned to

---

**Figure 3. Different Buying Centers for UEBA Features**

[Diagram showing different buying centers for UEBA features]

*Source: Gartner (May 2019)*

ID: 361156
deliver on the initial simple use cases for which it was deployed. This jumps to 18 months for more-complex, insider-threat use cases in large enterprises.

The factors influencing the complexity of a UEBA implementation, and future effectiveness of the tool are:

- The complexity of the organization’s architecture, network topology and data governance posture.
- The availability of the right data at the right verbosity.
- The sophistication of the vendor’s analytics — i.e., whether it incorporates statistical models and machine learning, as opposed to just patterns and rules.
- How much of the analytics comes prepackaged — that is, the vendor knows which data to collect for the various use cases, and which variables and attributes are important to the analytics.
- How easy it is for the vendor to automatically integrate the required data, and whether the customer can easily access that information. For example:
  - If a UEBA solution uses a SIEM tool as its primary data source, then is the SIEM tool collecting the required data sources?
  - Can the applicable log events and organizational context information be forwarded to the UEBA solution?
  - If the SIEM tool is not already collecting and managing the data sources required for the UEBA, then how should it ingest that data?
- How focused the organization’s use case is, how many datasets the use case requires and how well the organization’s use case aligns with the vendor’s domain expertise.
- How much organizational maturity and involvement is required — for example, to write, develop, and tweak the rules and models; assign weights to variables selected for evaluation; and fine-tune the risk-scoring thresholds.
- How scalable the vendor’s solution and architecture are relative to the organization’s current and future requirements.
- Time to build baselines, profiles and identify groups. Vendors often need a minimum of 30 days (sometimes as much as 90 days) of data for their analytics, before they can establish a “norm.” Historical data can be used in batch mode to accelerate the training of the models. Interesting insights can be achieved more rapidly using rules, instead of using an impossibly fast machine learning engine.
- Level of effort to build dynamic peer grouping or account profiling (service/human) capabilities, which can vary a great deal between solutions. Many vendors overstate their features here, requiring organizations to manually define, tune and clean up the groups, rather than relying on the tools to do this automatically.

**Representative Vendors**

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.
This is not, nor is it intended to be, a list of all vendors or offerings on the market or a competitive analysis of the vendors’ features and functions (see Note 1). In addition, the providers below can often provide multiple UEBA-related services/products. This is also not a definitive list of each provider’s offerings.

**Market Introduction**

The UEBA market is a dichotomy, and the number of stand-alone UEBA solutions is consolidating. Although most of the vendors providing these tools offer a broader portfolio of solutions, including a SIEM, they still offer these stand-alone UEBA tools as platforms that can be procured independently of their other offerings. These vendors are mentioned in the “Stand-Alone UEBA Solutions” section below.

Similarly, several cybersecurity vendors providing tools that can benefit from more intelligence have decided to embed UEBA features and functionality in the fabric of their tools, by adding a layer of advanced analytics for user and/or entity behavior modeling. These vendors are organized by domain in the following sections.

**Stand-Alone UEBA Solutions**

Use cases for the stand-alone UEBA vendors cross the domains identified in this document, and vendors are defining and offering new models that cater to more use cases. However, organizations without data science teams should expect to need to rely on the vendors to support new use cases.

**Table 3. Representative Pure-Play Vendors**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product, Service or Solution Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay Dynamics</td>
<td>Risk Fabric</td>
</tr>
<tr>
<td>Exabeam</td>
<td>Advanced Analytics</td>
</tr>
<tr>
<td>Forcepoint</td>
<td>Ueba Behavioral Analytics</td>
</tr>
<tr>
<td>Gurucul</td>
<td>Risk Analytics</td>
</tr>
<tr>
<td>HPE (Aruba Networks)</td>
<td>IntroSpect</td>
</tr>
<tr>
<td>LogRhythm</td>
<td>Ueba</td>
</tr>
<tr>
<td>Micro Focus</td>
<td>Interset</td>
</tr>
<tr>
<td>Dell Technologies (RSA)</td>
<td>NetWitness Ueba</td>
</tr>
<tr>
<td>Securonix</td>
<td>Ueba</td>
</tr>
<tr>
<td>Splunk</td>
<td>UBA</td>
</tr>
</tbody>
</table>

**Source: Gartner (May 2019)**

Sample representative stand-alone, pure-play Ueba platform solutions (as defined in the Market Definition and Market Description sections and in Table 2 above) that have fully acquired or natively developed their Ueba (i.e., they are not OEMing the Ueba feature set of a third party) are shown in Table 3.

**Embedded UEBA and UEBA as a Feature Are Becoming More Widespread**

This section will address several areas that are active in embedding UEBA feature sets in their solutions. It is organized by technology domain.

**CASBs**

CASBs (see “Magic Quadrant for Cloud Access Security Brokers”) provide protection from a variety of threats to cloud-based SaaS applications by preventing unwanted devices, users and versions of applications from accessing cloud services through the use of adaptive access controls. Advanced CASB offerings can change cloud application functionality, based on signals observed during and after login. This is where
embedded UEBA capabilities come in for CASBs, by identifying anomalous behavior during the course of the cloud session. If excessively risky used behavior is observed, the CASB can take action, including restricting access or requiring stronger authentication of the user.

All of the market-leading CASBs include embedded UEBA capabilities. Furthermore, user behaviors can be correlated across multiple cloud services, strengthening the assurance of the detection of an event. CASB-based embedded UEBA is extremely critical, because the user actions/interactions analyzed by the CASB are not typically visible to central UEBA solutions. To get this visibility, UEBA point solutions need to use the APIs of the cloud providers to get user activity data. However, only approximately 15 of the top public cloud providers, including infrastructure as a service (IaaS) providers, such as Amazon Web Services (AWS), Azure and Google Cloud Platform (GCP), have APIs to get at this data. Market-leading CASBs can get this visibility via their proxy capabilities, and are not solely dependent on APIs. As an alternative to APIs, the UEBA point solution can partner with the CASB provider for access to this data, providing a “better together” story, with CASB vendors providing embedded UEBA for cloud-based activities.

Sample representative CASB vendors with embedded UEBA features include:

- Bitglass
- FairWarning
- Forcepoint
- Microsoft
- Netskope
- Oracle
- McAfee
- Symantec

Data-Centric Audit and Protection

Vendors that focus on improving the security of structured and unstructured data repositories — i.e., data-centric audit and protection (DCAP) — have also begun to add UEBA functionality to their products (see “Market Guide for Data-Centric Audit and Protection”). For example, some vendors provide user behavior analysis for monitoring unstructured data permission change, access and use in various repositories. Others apply user behavior analytics to structured data in databases being accessed via applications or directly by users, with the ability to block access or apply protection to the data, such as masking, tokenization and encryption.

Sample representative DCAP vendors with UEBA features include:

- Dataguise
- Datiphy
- Imperva
- Informatica
- SecuPi
- STEALTHbits Technologies
- Veritas Technologies
- Varonis
DLP

DLP (see “Market Guide for Enterprise Data Loss Prevention”) focuses on the detection of sensitive data exfiltration or misuse. DLP tools have a good track record in detecting data loss or misuse, assuming a properly evaluated and tested DLP policy is applied and in place. However, the deterministic, rule-based approach limits its application or prevention capabilities to avoid business friction. What DLP has accomplished has largely been through content awareness, with a lesser focus on context awareness, such as user, application, location, time, event rate and other external factors. DLP products need to be content-aware and context-aware to be effective. UEBA enables flexible rule creation to handle the gray areas between deterministic guardrail rules, without adding undue business friction and to heighten its focus on risker users or devices.

Sample representative DLP vendors with UEBA features include:

- Digital Guardian
- Forcepoint

Employee Monitoring

Employee monitoring (see “Market Guide for Employee-Monitoring Products and Services”) is the capability to record or reconstruct employee activity, usually to a standard admissible in court (if necessary). Content captured may include video footage of screen activity, screenshots, keystrokes and mouse captures. Employee-monitoring systems have traditionally orchestrated with a centralized employee risk function, which may include UEBA, as well as traditional rules triggers and manual intervention. Constant employee monitoring is likely to generate a prohibitive amount of material requiring human triage and review. Hence, UEBA is used to identify high-risk cases requiring human triage. Increasingly, vendors are encapsulating tuned UEBA within EM systems for streamlined operation.

Sample representative EM vendors with UEBA features include:

- Awareness Technologies
- Bottomline Technologies
- CANDA Solutions
- Dtex Systems
- Forcepoint
- Fishtech Group (Haystax)
- ObserveIT
- Teramind
- Veriato

Endpoint Security

Endpoint detection and response (EDR; see “Market Guide for Endpoint Detection and Response Solutions”) and endpoint protection platform (EPP; see “Magic Quadrant for Endpoint Protection Platforms, 2018”) solutions provide deep instrumentation and telemetry into the endpoint OS. This includes processes and network ports. This data is then analyzed for indications of system compromise or attack. In most cases, this deep visibility also includes data on what user is logged in and the actions they initiated on the endpoint. For example,
what applications the user ran, at what time and what they may have typed in at the command line. This identity-related telemetry can be analyzed to provide embedded UEBA capabilities.

Like pure-play UEBA solutions, EDR solutions use a combination of traditional techniques, such as signatures, static file analysis and behavioral analysis, and machine learning capabilities (or the more hyped AI) to differentiate their detection methods. Most pure-play UEBA solutions simply don’t have enough visibility into user behaviors at the endpoint. This is the critical gap that embedded UEBA within EDR solutions can provide. Likewise, EDR solutions don’t see interactions outside the endpoint (for example, in SAP or other applications) that UEBA solutions analyze.

Gartner expects more EDR/EPP vendors to experiment with embedded UEBA moving forward.

Sample representative EDR/EPP vendors with UEBA features include:

■ Cybereason
■ Cylance
■ Rapid7

Fraud

Online fraud detection (see “Market Guide for Online Fraud Detection”) solutions detect aberrant activity, which indicates a compromise of a customer account, through a human actor, malware or man-in-the-machine/browser interception. Modern fraud systems attempt real-time detection through the analysis of multiple data elements, including device characteristics and, more recently, transactional and nontransactional user behavior. UEBA is highly preferable to device characteristic measurement, because it is far harder for a fraudster to spoof dynamic human behaviors in comparison to spoofing static attributes, such as browser canvas. Most fraud solutions use a mixture of UEBA, transactional analysis, and device characteristic measurement, with more advanced systems also mapping the entity relationships in identity link graphs. Online fraud detection systems are becoming more tightly coupled with authentication and identity verification systems.

Sample representative vendors for fraud detection with UEBA features include:

■ BioCatch
■ Bottomline Technologies
■ Featurespace
■ IBM Trusteer
■ Kaspersky Lab (see Note 2)
■ Mastercard (NuData)
■ LexisNexis Risk Solutions (ThreatMetrix)
■ TransUnion (iovation)

IAM and Access Management

IAM (see “Identity and Access Management Primer for 2019”) has evolved to incorporate UEBA techniques and features to enrich its fundamental value propositions. Gartner has observed a trend in evolution among access management vendors to integrate with pure-play vendors and embed some UEBA features in their own products.

Access management vendors (see “Magic Quadrant for Access Management, Worldwide”) have largely
leveraged UEBA for authorization and adaptive access management use cases. Adaptive access is an IAM-specific instance of a continuous adaptive risk and trust assessment (CARTA) approach. “Technology Overview for Adaptive Access Control” defines adaptive access control as an instance of context-aware access control that balances trust against risk at the moment of access, using a combination of trust elevation and other dynamic risk mitigation techniques. For example, risk scores can be used to dynamically adapt the level of access of a user, or to ask a user to reauthenticate using multifactor authentication (MFA). Identity analytics capabilities for adaptive access should be preferred capabilities for choosing an access management solution.

Sample representative access management vendors with UEBA features include:

- CA Technologies
- IBM
- Microsoft
- Okta
- Ping Identity
- OneLogin

IAM and Identity Governance and Administration

Identity governance and administration (IGA; see “Magic Quadrant for Identity Governance and Administration”) vendors use UEBA to enable behavioral and identity analytics use cases, such as anomaly detection, dynamic peer group analysis, login analysis and access policy analysis.

Stand-alone UEBA vendors, mainly Gurucul and Securonix, pioneered identity analytics innovation, providing rich identity governance features coupled with the feature set of their UEBA behavioral analytics engines. As with access management, Gartner has observed a trend in evolution among IGA vendors to integrate with pure-play vendors and embed UEBA features in their own products.

Identity analytics moves the IGA market toward more predictive and prescriptive analytics, allowing dynamic risk evaluation for workflow approvals, for example. A lower-risk access request approval can be automated, without requiring manual approvals from managers or application owners. Access requests can be validated in real time against these scores, transforming traditionally compliance-focused IGA platforms into risk-oriented “governance on the fly” engines (see “IGA Best Practices: Prioritize Analytics When Adopting IGA”). Identity analytics can compute risk indicators as spikes in login activity, unusual login behaviors, rogue or outlier access, abandoned and dormant accounts, access to sensitive unstructured data, or separation of duties (SOD) violations.

Sample representative IGA vendors with UEBA features include:

- Brainwave GRC
- CA Technologies
- IBM
- SailPoint
- Saviynt
IAM and Privileged Access Management

Privileged access management (PAM; see “Magic Quadrant for Privileged Access Management”) is another subdomain of IAM, focused on providing visibility and control into administrative access of IT systems. Because of the critical nature of these privileged accounts, most leading PAM vendors provide embedded UEBA capabilities. Because of their role in governing the use of administrative accounts, PAM solutions have telemetry on how, why, when and where administrative accounts were used. This data can be analyzed for indications of abnormal administrator behavior or malicious intent using embedded UEBA capabilities.

Leading PAM solutions with embedded UEBA can detect suspicious activity and common administrator threat scenarios, such as privileged credential abuse that bypasses PAM controls. More-advanced, agent-based components running on Microsoft Domain Controllers can provide further protection from attacks on Windows domain controllers, such as “golden ticket” or “pass the hash.” Many UEBA projects start by focusing on administrative credentials, because they are often targeted by attackers to gain credentialed access into critical systems.

Acknowledging the risk of highly empowered IT accounts, some IaaS cloud providers are providing their own embedded UEBA capabilities. Offerings such as AWS Macie analyze a combination of administrative behaviors and sensitive data access to provide alerts.

Another use case for UEBA in PAM products is passive biometrics, in which machine learning can baseline an individual user’s keystroke cadence and mouse movement profile and attempt to identify when an account is being used by a different human.

Sample representative PAM vendors with UEBA features include:

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- One Identity
- Thycotic

NTA

NTA vendors (see “Market Guide for Network Traffic Analysis”) use a combination of machine learning, advanced analytics and rule-based detection to detect suspicious activities on enterprise networks. NTA tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior, essentially focused on entity behavior analytics. Some NTA tools also gather context on users from integration with AD or other LDAP and IAM solutions deployed in organizations. This way, the tool can infer conclusions, such as “this user was on this device that was behaving anomalously.”

In addition to monitoring north/south traffic that crosses the enterprise perimeter, NTA solutions can also monitor east/west communications by analyzing network traffic or flow records that it receives from strategically placed network sensors. This way, they can link IP addresses to user IDs, attribute specific network traffic to specific users, and enrich the level of understanding of the network traffic, feeding visibility into potential anomalies. Although they may not do user behavior analytics at the transaction level,
they still perform entity behavior analytics at the network traffic level, and can further reconcile network information back to the user owning that transaction. Many solutions can further orchestrate natively or through a security orchestration, automation and response (SOAR) solution to block malicious activity through other technologies, such as enterprise firewalls, EPPs, and secure web gateways (SWG).

Sample representative NTA vendors with UEBA features include:

- Awake Security
- Cisco
- Darktrace
- ExtraHop
- Fidelis Cybersecurity
- FireEye
- HPE (Aruba Networks)
- Lastline
- Plixer
- Vectra

SIEM

SIEM tools’ natural extension is to always offer better analytics (see “Magic Quadrant for Security Information and Event Management” and “Critical Capabilities for Security Information and Event Management”). SIEM vendors are embedding UEBA features as described in the section on the convergence of SIEM and UEBA.

Furthermore, emerging companies developing newer UEBA platforms are usually building these on top of their own data lakes, and offering functionality sets that make them resemble modern SIEM, as described in “Technology Insight for the Modern SIEM.”

Sample representative SIEM vendors with UEBA features include:

- Dell Technologies (RSA)
- Exabeam
- FireEye
- IBM
- LogRhythm
- McAfee
- Micro Focus
- Microsoft
- Rapid7
- Securonix
- Splunk

Market Recommendations

The following has been consistent advice from Gartner clients that have been more successful with their UEBA deployments for the past three years. This list is not exhaustive, but rather offers pointers on attributes to increase the success of UEBA initiatives:

- Check whether your SIEM vendor already offers UEBA features and advanced analytics in its tool’s
latest release — for example, IBM offers a free UEBA module focused on users.

Evaluate UEBA vendors with domain expertise that aligns with your primary use case. This includes improving security operations via anomaly detection, helping to prioritize and enable more-efficient response and investigations; monitoring the use of privileges established in IAM systems; and pinpointing data exfiltration and leakage.

Avoid selecting a UEBA tool based on its ability to detect novel and interesting insights during the POC; instead, select a tool that delivers on your initial requirements, and demonstrates the ability to scale and evolve with your needs.

When implementing a UEBA tool, take a deliberate, phased approach. Start small with a narrow set of well-defined use cases and a limited set of data. Address “quick wins” early to benefit from the momentum of tactical successes.

Operationalize UEBA tools by integrating them with a SIEM (or buy one embedded in a SIEM or from a vendor that sells a SIEM and can build a bundle), a SOAR, or a service desk tool that provides ticketing and workflow capabilities. Use current tools to continue monitoring developer and privileged user behavior, because UEBA anomaly detection is less reliable for these unpredictable users.

Consider the inclusion of network and endpoint data to gain additional visibility into user and application activity beyond what is present in log files.

Augment your UEBA capabilities by ingesting nonstructured behavioral information, such as email, HR data and records, or social media activity, to provide fuller context for user behavior analysis. Few tools can offer that functionality, so be prepared for longer project timetables and the inability to fully automate the inclusion of all required data sources.

Promote cultural change and executive-level interest in security and risk at your organization by using UEBA dashboards as one of the inputs to present security and risk postures and indicators in a meaningful way to senior SRM managers. This type of information presentation can be and has been used to promote organizations’ continued investment in UEBA solutions.

Note 1

Representative Vendor Selection

The 10 pure-play UEBA platform vendors were selected because they met Gartner’s inclusion criteria, and were not eliminated by the exclusion criteria noted above. The other vendors (an additional 76 entries) were selected because they offer embedded UEBA feature sets in their respective solutions for the domains identified.

Note 2

Kaspersky Lab

In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky Lab’s software from their systems. Several media reports, citing unnamed intelligence sources, made additional claims. Gartner is unaware of any evidence brought forward in this matter. At the same time, Kaspersky’s initial complaints have been dismissed by a U.S. District of Columbia court.

Kaspersky has launched a transparency center in Zurich where trusted stakeholders can inspect and evaluate product internals. Kaspersky has also committed to store and process customer data in Zurich, Switzerland. Gartner clients, especially those who work closely with U.S. federal agencies, should consider this information in their risk analysis and continue to monitor this situation for updates.

Source: Gartner Research, G00361156, Gorka Sadowski, Neil MacDonald, Jonathan Care, Henrique Teixeira, 21 May 2019
Varonis Data Security Platform is the Most Reviewed Solution in the UEBA
Market on Gartner Peer Insights, as of July 1, 2019.

Varonis is trusted by more than 6,700 customers worldwide, and as of July 1, 2019 is the most-reviewed solution in both the User and Entity Behavior Analytics (UEBA) Solutions and File Analysis Software markets on Gartner Peer Insights, with overall ratings of 4.7 out of 5 stars and 4.5 out of 5 stars respectively.

Here are a few recent reviews from real customers:

**“Simplification For Operational Efficiency! Security Perfection”**
Senior VP of IT, Healthcare, $50M - $250M
File Analysis, 5 stars
**Overall Comment:** “Exceptional, this solution integrates with our overall security roadmap. This solution allows us to focus limited resources on critical security projects while still remaining compliant and mindful of other security threats.”

**“Great Product With Great Relationships.”**
Infrastructure & Operations, Finance, $50M - $250M
UEBA, 5 stars
**Overall Comment:** “My overall experience with Varonis has been great. My Sales Team and Professional Services have been absolutely incredible. They work hard to make sure we have what we need when we need it...”
**Submitted: 5/3/19**

**“Completely Satisfied 1 Year In”**
Security & Risk Management, Finance, $500M - $1B
File Analysis, 5 stars
**Overall Comment:** “They seem to be the real deal for today’s data security landscape.”
**Submitted: 4/25/19**

**“Invaluable Tool For Tracking File Operations And Threats.”**
Systems Admin, Energy & Utilities, $50M
UEBA, 5 stars
**Submitted: 4/29/19**

About Varonis

A pioneer in user behavior analytics, Varonis drastically reduces the time to detect and respond to cyberattacks – spotting threats that traditional security products miss.

With a data-centric approach to threat detection, Varonis:

- Correlates and analyzes telemetry from file and email systems, Active Directory, DNS, and network devices
- Delivers context-rich insights about users, roles, devices, and data
- Makes forensics intuitive and conclusive with lightning fast search and built-in incident response playbooks

Varonis is trusted by more than 6,700 customers worldwide and, as of June 12th 2019, is the most-reviewed user and entity behavior analytics solution on Gartner Peer Insights.