Evaluation Brief

A Matchmaker's Guide to UBA Solutions

13 questions to find the UBA vendor that's right for you

So, you're searching for your User Behavior Analytics (UBA) soulmate? That's not just sweet, it's smart. UBA applies insight to the millions of network events your users generate every day to detect compromised credentials, lateral movement, and other stealthy, malicious activity earlier in the attack chain—providing your team with the time and context it needs to respond. It can save you time and find the attacks you're missing.

But finding the perfect UBA partner? Not as simple. Gartner predicts that by 2020, less than five stand-alone UBA solutions will remain in the market, with most vendors focusing on specific use cases and outcomes. Which means you need a partner who not only understands your unique needs and how to meet them, but is also in it for the long haul. (Don't we all?) To help you identify your dream UBA vendor, we've put together a list of questions to ask of your suitors.

Unified Data Collection

Is it a standalone solution or does it require another solution for data collection?

If you have a log aggregator in place today, most UBA vendors can support the integration. However, if you aren't currently centralizing log data for compliance, or if you might replace your log management tool down the line, make sure your UBA vendor can ingest data directly from a wide range of event sources.

Can the solution detect attacks in cloud services? How?

If your organization uses cloud services like Office 365, Salesforce, or Box, your attack surface now includes the sensitive data stored in them. Make sure your UBA vendor has direct API integrations to ingest authentication and admin actions. This allows you to detect subtle signs of compromised credentials, like: "Bob logged onto the Boston network at 9:15 AM. 30 minutes later, Bob authenticated to Office 365 from a French IP address." Merde!

Does the solution include the option to deploy endpoint agents? What do they help detect?

Most UBA vendors integrate with anti-virus and anti-malware endpoint solutions. However, this leaves gaps in detecting malicious behavior, such as lateral movement. And endpoint data for investigations? No such luck. Your UBA solution should be able to directly collect endpoint data and detect attacks that don't require malware to compromise your organization.

Will I need any new hardware to be deployed?

If you've deployed SIEM, you're all too familiar with a hardware footprint that grows faster than a beard in Brooklyn. If the UBA solution requires an appliance to run, consider how your log and network data will expand over the next few years. Will each branch office need a box, and does that provide coverage for traveling and remote workers?

Incident Detection

Are the underlying analytics run near real-time or only periodically?

There's clearly a right answer here. But some UBA vendors use dated logs and incidents in their demos and come apart during real POCs, so you still need to ask. Our suggestion? Run a POC shortly before getting a penetration test.

How does the solution use statistical models, baselining, and other forms of machine learning?

Machine learning, Bayesian analysis, artificial intelligence—there's a reason machines will one day rule us all. In the meantime, make sure your UBA vendor is taking advantage of this cutting-edge data science, as well as where they apply it and why. If it's just to spot anomalies in any data set, be prepared for continuous tuning in order to get the output you're expecting.

Will the solution detect attacker tools and activities? How?

Visualizing user behavior is no easy task, but without a clear view of the attacker behavior being detected, you'll wind up with more questions than answers. Look for vendors that both research attacker behavior non-stop and apply that knowledge in the form of targeted detections.

Can you write custom alerts to augment pre-packaged alerts?

Gartner recommends that tools applying UBA allow customers to add their own rules that fire in coordination with the built-in rules and models. And just like Oprah, when Gartner recommends something, you should probably get it.

Does it include deception technology for detection?

Deception technology extends beyond standard UBA log analysis by setting traps – such as honeypots, honey files, and honey credentials – designed to trick attackers into taking action and revealing high-risk user behavior in the process. Check if your vendor provides built-in deception technology—it's a great litmus test to determine if they understand how attackers work.

Investigation and Prioritization

How is additional context presented with the detected anomalies?

Generating high-quality alerts that show the users and assets involved is only half of the battle. Once you've validated an alert, you need to know if other users and machines are affected, and if the attacker moved laterally from there. Most investigations move from an alert to searching logs and checking endpoint data. Does your UBA vendor enable both, and if so, is it easy to make this pivot?

Can you build dashboards and analytics to augment pre-packaged analytics?

If you need to abide by an industry or vertical regulation, they likely recommend you track and monitor all access to network resources and critical systems. UBA solutions can tackle the tracking of that access, but make sure your vendor has a way to visualize and report on the data. That saves you time when reporting across the company and gives you peace of mind about your security posture.

Does it include the ability to search the data?

Whether you're investigating an incident or meeting a compliance request from an auditor, a powerful log search can save time and reduce headaches. If you don't have log search today or want to avoid "portal fatigue," check if your UBA vendor offers this, as it's ingesting the data already.

Does the solution include an integration with Security Incident Response Platform (SIRP) solutions?

Once you've validated the alert, determined everyone involved, and drawn up a timeline, it's remediation time. If you use a SIRP solution, such as IBM Resilient Systems or ServiceNow, make sure your UBA solution has an integration to help save you time and reduce that precious Time to Contain metric.

Let's talk UBA. Learn more and get in touch:

https://rapid7.com/solutions/user-behavior-analytics/