TRACE3

Innovation Research Team

360VIEW

Trend Report

9/15/2016

SIEM-Centric User Behavior Analytics (SCUBA)

New Hotness in Security

Executive Summary

In today's enterprise, it is apparent that current security technologies are not enough to stop an ever-increasing barrage of cyber-attacks. Many companies are now making the assumption that they will soon be breached or have already and current signature-based threat detection is not a sufficient defense as it leaves the enterprise perpetually one step behind. Couple this with the problem of separating the signal from the noise in a continually growing cacophony of alerts and this quickly becomes an untenable task for even the most experienced security analysts.

User Behavior Analytics (UBA) has recently emerged to solve these problems by using machine learning to detect both external and insider threats overcoming the shortfalls of signature-based security. UBA analyzes data from various sources to establish baseline behavior and then detects anomalies from this baseline indicating possible threat actors. This study considers the products, features, predictions and recommendations for enterprises seeking to adopt SIEM-centric UBA.

Report Scope

Based on the variety of data sources being analyzed, UBA has diverged into three distinct, but often overlapping, approaches: Network-centric UBA, Agent-centric UBA and SIEM-centric UBA. The scope of this report is the analysis of the SIEM-centric segment of the UBA space, specifically exploring the functionality of five leading products we have selected as the "New Hotness". The remaining two UBA approaches will be covered in forthcoming reports.

This study was conducted from the customer's point of view, gathering feedback from actual users, product demonstrations, published information and direct information from each solution vendor. It analyzes each solution on the three components found to be most critical to customer purchasing decisions:

- Data Analytics
- Data Integration
- Data Presentation & Visualization

The accompanying comparison matrix presents each products' capabilities to support these success factors.

Did You Know...

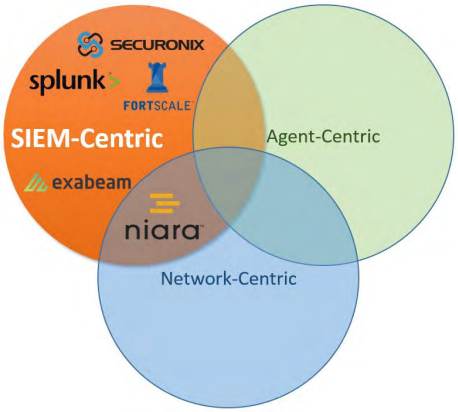
- 59% of employees steal proprietary corporate data when they quit or are fired. [1]
- The average time to detect a malicious or criminal attack is 170 days [1]
- 88% of networks are susceptible to privileged account hacks. [2]
- Cyber security incidents have surged 38% since 2014. [3]
- Privilege misuse is #3 out of nine attack patterns found in 96% of all breaches. [3]
- As many as 75% of breaches go undiscovered for weeks or months. [4]
- Large enterprises can receive 500,000 to 1,000,000 alerts a day across multiple security monitoring systems. [5]
- 55% of all attacks are carried out by malicious insiders or inadvertent actors. [6]

Trends

Solutions Selection

The five SIEM-centric UBA "New Hotness" products selected are:

- Exabeam
- Fortscale
- Niara
- Securonix
- Splunk (UBA)



It is worth noting that E8 Systems, Bay Dynamics and Red Owl were also serious contenders but not included in the study due to study size constraints and not through any deficiencies found in their products.

There is a burgeoning array of UBA solutions on the market today. Many are actually traditional signature-based IDS solutions that have been re-branded as UBA with buzzwords like "machine-learning" or "deep-learning" sprinkled throughout their marketing literature.

For this study we have focused on those products that are not only true UBA solutions but are also full featured and with an established customer footprint. We could have selected several other products that fit this criteria but we limited our study to the five that were mentioned the most favorably and frequently in our customer interviews.

Solution Comparison Summary

	exabeam	FORTSCALE	niara	SECURONIX	splunk>
Ease of Install	YES	NO	YES	NO	NO
Ease of Operation	YES	YAP	YES	YAP	YAP
Ease of Customization	YES	YES	YES	YAP	YES
Supervised Learning	YES	YES	YES	YES	YES
Unsupervised Learning	YES	YES	YES	YES	YES
Adaptive Feedback	YES	NO	YES	YES	YES
Data Lake Integration	YES	NO	YES	YES	NO
Big Data Store	YES	YES	YES	YES	YES
Open API	YES	YES	YES	YES	YES
Non-SIEM Data Sources	NO	NO	YES	NO	YES

The five selected solutions were compared on 57 criteria (see accompanying Comparison Matrix). Not surprisingly, many of the criteria were completely supported by all 5 vendors as these solutions were preselected for this study based on their completeness. However, when discussing SIEM-centric UBA features with current and potential customers ten key features were repeatedly identified as driving selection and purchasing decisions.

As depicted to the left, these key features are:

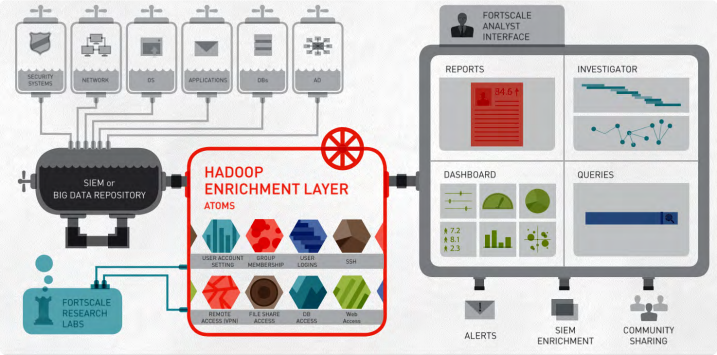
- Ease of Install - Can the solution be installed, configured and deployed with no vendor assistance?
- Ease of Operations - Can the solution's day to day operations, investigation and analysis be accomplished without the need of specialized training and with minimal clicks?
- Ease of Customization - Can the solution be customized automatically, or with only minimal in-house manual intervention, account for changing or unique operational constraints?
- Supervised Learning - Does the system support building predictive models from known input and response data?
- Unsupervised Learning - Does the system draw inferences from datasets of input data without labeled responses?
- Adaptive Feedback - Does the system factor analyst input into the machine learning for continual training?
- Data Lake Integration - Does the solution integrate with enterprise data lakes (e.g., Hadoop) as a data source?
- Big Data Store - Does the solution store results, baselines, alerts or other artifacts in a scalable, unstructured data store (e.g., Hadoop) for future analysis?
- Open API - Does the solution publish an API that can be integrated with other visualization products?
- Non-SIEM Data Sources - Can the solution be extended to ingest data from non-log or non-SIEM data sources (e.g., network traffic)?

Exabeam

The Exabeam Security Intelligence Platform helps security teams detect and respond to credential-based threats. The product includes applications for User Behavior Analytics (UBA), threat hunting, and ransomware detection. Exabeam connects to any SIEM or log management system and connects individual events into coherent user sessions, linking activity across multiple accounts, devices, and IP addresses.

It then uses these sessions to create baselines of normal activity for each user on the network. New activity is compared to baselines to determine if a user is acting in an unusual and risky manner, and users with high risk scores are presenting to SOC analysts. The product automatically creates investigation timelines, reducing incident response activities from days to seconds. Finally, the product's threat hunting capabilities enable proactive searching for users that match any combination of activity and attributes.

Fortscale



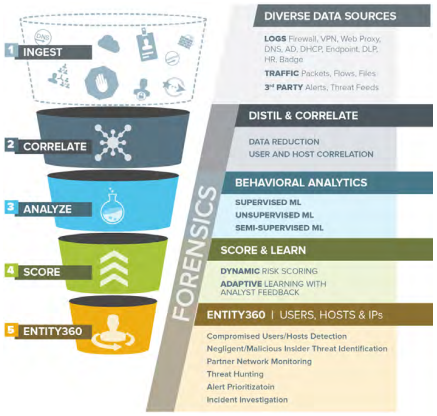
Fortscale is a machine learning system that detects abnormal account behavior indicative of credential compromise or abuse. Fortscale's UBA is a Hadoop based solution that enables processing, visibility into, and analysis of the appropriate timeframes (days, weeks, months, quarters, or years) to identify behavioral changes that occur over long periods of time and throughout lengthy attack campaigns.

Fortscale SMART Alerts are triggered when the system identifies a threat, based on a collection of anomalies or indicators that together cross a statistical threshold that is unique for every user in your system. SMART Alerts are designed to provide analysts with specific semantic context about the threat that has been discovered, giving analysts a major head start on understanding the state of their network during stressful incidents. Using Fortscale's Investigations interface, analysts can drill down into any SMART Alert to pull up the indicators that together created the Alert in the first place.

Fortscale's insider threat detection engine analyzes authentication and contextual data from a number of sources and models "normal" or baseline user and entity behavior. It then identifies when deviations in behavior occur without the need to write any rules.

Niara

Niara's behavioral analytics platform automates the detection of attacks and risky behaviors inside an organization and boosts the power of security teams by providing analytics-driven visibility for accelerating alert prioritization, incident investigation and threat hunting efforts. Key capabilities include the detection of compromised users and hosts, negligent employees, and malicious insiders.



Niara ingests logs from the security infrastructure (e.g. AD, firewalls, web proxy, VPN, DLP, IDS, DNS) and combines them with network flows and packets. Behavioral analytics models are then applied on correlated users and hosts across multiple dimensions: authentication, access to high value resources, exfiltration, remote access, cloud application usage, Internet activity and physical access. The broad range of data sources and behavioral models enable Niara to build Entity 360 risk profiles with high fidelity. Unsupervised machine learning models establish behavioral baselines and flag unusual activity. These results are combined with supervised machine learning models and adaptive learning techniques to reliably link anomalous and malicious activity, thereby reducing false positives. Niara aids investigations by integrating its analytics with layered forensics to make its results explainable, verifiable and actionable.

The Niara solution:

- Detects compromised users/hosts and negligent/malicious Insider threats (i.e., privilege escalation, command and control, file downloads, internal reconnaissance, lateral movement, abnormal resource access, SaaS usage, data transfer activity) and accelerates incident investigations.
- Assists less experienced security personnel by reducing alert white noise and automating labor-intensive data collection and correlation.
- Assists experienced security personnel by providing analytics driven visibility for threat hunting activities.
- Leverages existing security investments by ingesting data from other tools, integrating with existing consoles and performs historical assessments of new "zero-day" alerts from other systems.

Securonix

Securonix Enterprise is a behavior-based threat prediction, detection and prevention engine that mines, enriches, analyzes, prioritizes, and transforms machine data into actionable intelligence. Using signature-less anomaly detection techniques that track user, account, and system behavior, the platform detects insider threats and cyber-attacks that typically go unnoticed by signature-based technologies while reducing the number of alerts and incidents that warrant investigations.

Securonix aggregates user, account, application and device data to create a unified view from which to learn each entity's normal behavior patterns and track its risk posture with signature-less anomaly detection algorithms. This is paired with known threat indicators and third party intelligence to identify high risk, abnormal, and fraudulent activities from within or outside the organization. The system provides investigators with one screen to investigate any identified threat, security event, user, account, or system.

Some key capabilities of Securonix include:

- High-Risk Entity Dashboard - provides a unified and prioritized view of high-risk insider and cyber-threats across users, accounts, hosts, endpoints in the enterprise.

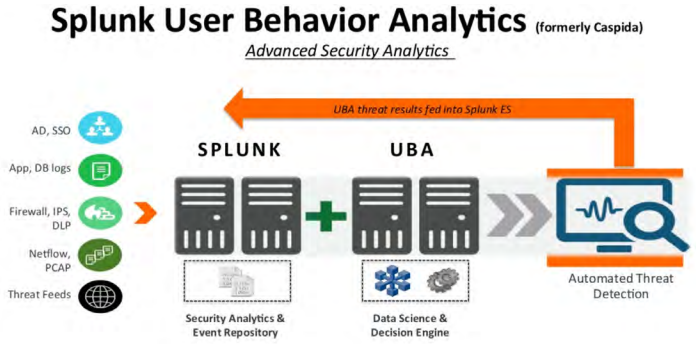
• Multi-Entity Investigation Workbench - tool for analysts to visually investigate the threats and attacks,identify similarities and anomalies between all entities in the organization.

• Advanced Correlation of 3rd Party Intelligence - combines event analytics with fifteen 3rd party intelligence providers to correlate events in the network with known bad threat actors and suspicious network events such as remote access to sensitive data from abnormal geographical locations.

• Data Encryption and Masking - secures, encrypts, and masks PII (Personally Identifiable Information) data, to align with data security and privacy requirements.

Splunk (UBA)

Splunk User Behavior Analytics (UBA) helps organizations find known, unknown and hidden threats using machine learning, behavior baselines, peer group analytics and advanced correlation to find lurking advanced persistent threats, malware infections and insider threats. Splunk UBA addresses security analyst and hunter workflows, requires minimal administration and integrates with existing infrastructure to locate hidden threats.



The entire lifecycle of security operations — prevention, detection, response, mitigation, to the ongoing feedback loop — must be unified by continuous monitoring and analytics to provide context aware intelligence. Splunk Enterprise, Splunk Enterprise Security (ES) and Splunk UBA work together to:

• Extend the search/pattern/expression (rule) based approaches in Splunk Enterprise and Splunk ES with threat detection techniques to detect threats with sophisticated kill chain visualizations

• Provide security teams with machine learning, statistical profiling and other anomaly detection techniques that leverage the readily available data at massive scale in Splunk Enterprise

• Combine machine learning methods and advanced analytics capabilities to enable organizations to monitor, alert, analyze, investigate, respond, share and detect known and unknown threats regardless of organizational size or skillset.

Trace3 Research's Take

Predictions

There are four key predictions that can be made for the SIEM-centric UBA space today:

1. UBA will augment or replace signature-based detection solutions. Signature-based solutions continue to fall behind current attack strategies as exhibited by the growing number of breeches in environments with signature-based protection. UBA offers a compelling alternative that is becoming the obvious replacement or at least can do the heavy lifting while signature-based solutions are switched to cheaper open-sourced solutions.

2. There will be a continued effort by the various vendors to increase the number and variety of behavior data they can consume, baseline and analyze. This will mean that the intersection between network, agent and SIEM-centric UBA tools will increase until the distinctions blur and disappear. Said another way, the three UBA approaches will merge to become just generic UBA that gather data from a growing set of sources with network, agent and SIEM data being table stakes.

3. UBA will merge with SIEM and DLP spaces. It is difficult to determine what this superset will be called but it is likely to just be called SIEM and will include UBA, DLP, IDS and other current security use cases.

4. Larger incumbent SIEM vendors will acquire the leading UBA vendors. Today several of the larger SIEM vendors just OEM their SIEM products' UBA features from emerging firms such as HP Arcsight and Securonix. We have already seen the first of these with Splunk acquiring Caspida and this trend will continue. To quote Gartner "by 2017, at least four UEBA technology companies with revenue less than $50 million will be acquired by SIEM, DLP or other large technology vendors supporting security use cases." [5]

Recommendations

Trace3 recommends the following:

1. Larger enterprises should layer a UBA solution on top of their existing SIEM solution in order to provide threat protection that can keep up with today's morphing and growing attached threat.

2. If the enterprise is already using a signature-based IDS solution we are not recommending that they discard this in lieu of a UBA solution unless keeping both solutions is cost prohibitive. We are seeing a growing number of UBA customers switching to open source signature-based security solutions and using the cost savings to implement UBA solutions.

3. In a perfect world with infinite budgets, a combination of network, agent and SIEM-centric UBA solutions would be optimal. However, given real-world budget constraints, we recommend enterprises evaluate and rank which UBA strategies are the most critical and select a solution that not only covers the most important area but, if possible, also overlaps secondary needs also.

4. Since this market is shifting and consolidating quickly, Trace3 recommends that after selecting and implementing a UBA solution that enterprises continue to monitor the space as IDS, DLP and SIEM features continue to merge. There may come a point when a super-product emerges that better protects the enterprise's full threat surface, but until then keeping abreast of UBA's ongoing evolution is mandatory.

5. Any of the five solutions analyzed will be a welcome addition to an enterprise security team with no showstoppers discovered. However, subtle nuances between solutions' underlying features will help hone product selection.

Appendix

Featured Use Cases

Security Information and Event Management (SIEM)

New Hotness: Splunk Enterprise by Splunk, LogRhythm

Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

User Behavior Analytics

New Hotness: Security Analytics Platform by Niara, Exabeam

User Behavior Analytics uses logs, network traffic and/or endpoint agents to set behavioral baselines for users and systems from which to identify anomalies and potential threats.

Other Materials *(available upon request)*

SCUBA Comparison Matrix

Compares features and capabilities of five SIEM-Centric UBA products: Exabeam, Niara, FortScale, Securonix and Splunk UBA

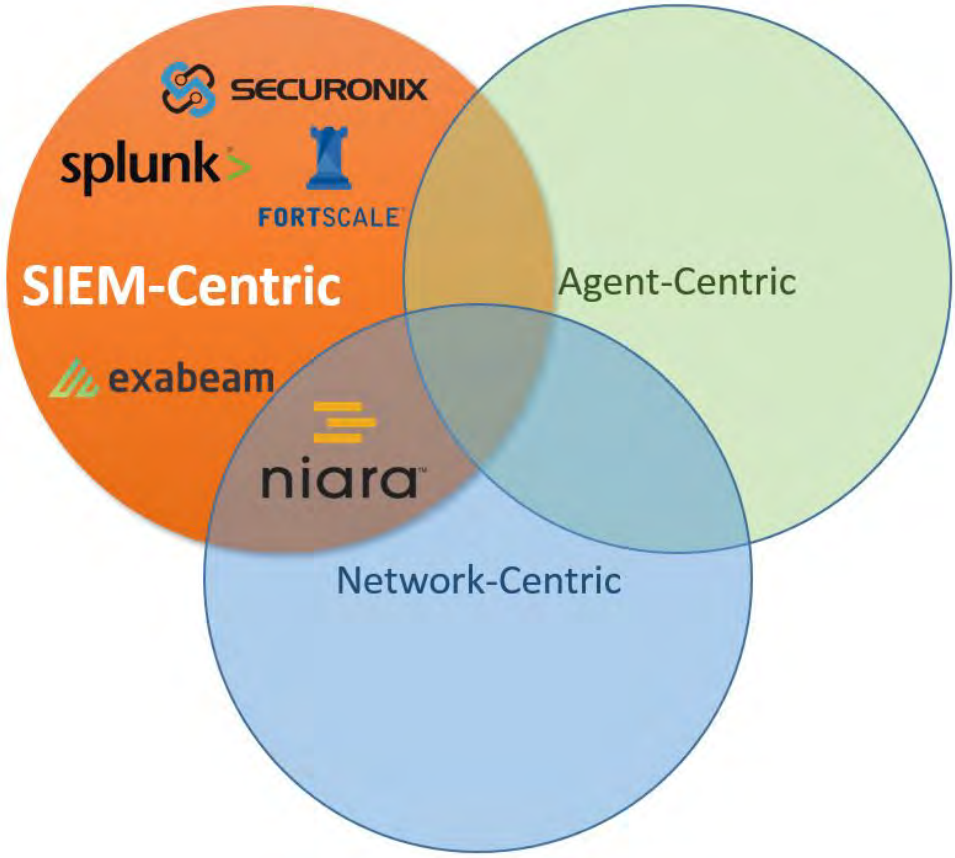
SCUBA Comparison Summary

Comparison of 10 key features among the five SCUBA solutions.

Sources

1 - Heimdal Security – *10 Surprising Cyber Security Facts That May Affect Your Online Safety* – Andra Zaharia – 2016
2 - CyberArk – *88 Percent of Networks Susceptible to Privileged Account Hacks* – Chris Brook – 2015
3 - CyberArk – *Fast Facts: Noteworthy Cyber Security Statistics* – Amy Burnis – 2015
4 - Swimlane - *10 Facts Every Cyber Security Professional Should Know* – Cody Cornell – 2015
5 - Gartner – *Market Guide for User and Entity Behavior Analytics* – Avivah Litan – 2015
6 - Security Intelligence – *The Threat is Coming from Inside the Network: Insider Threats Outrank External Attacks* – Nick Bradley – 2015

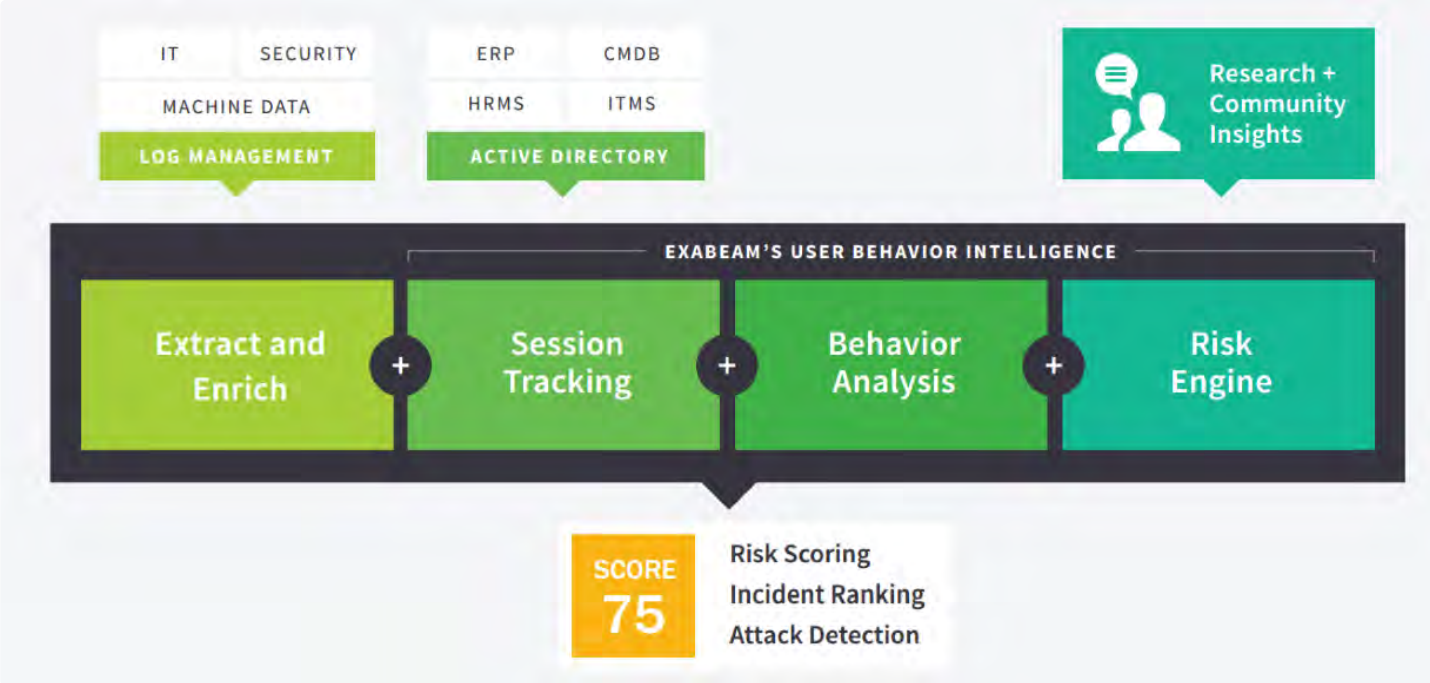
Solutions Selection



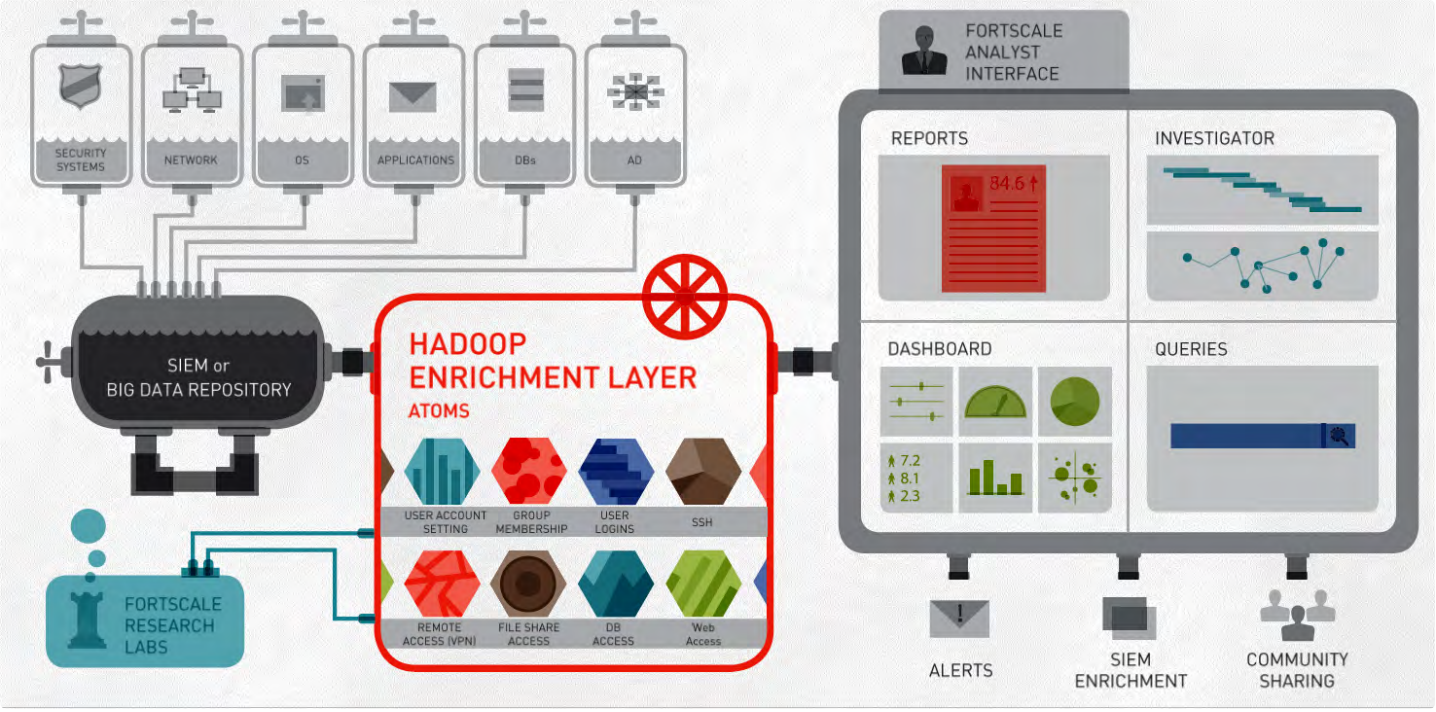
Solution Comparison Summary

	exabeam	FORTSCALE	niara	SECURONIX	splunk>
Ease of Install	YES	NO	YES	NO	NO
Ease of Operation	YES	YES	YES	YES	YES
Ease of Customization	YES	YES	YES	YES	YES
Supervised Learning	YES	YES	YES	YES	YES
Unsupervised Learning	YES	YES	YES	YES	YES
Adaptive Feedback	YES	NO	YES	YES	YES
Data Lake Integration	YES	NO	YES	YES	NO
Big Data Store	YES	YES	YES	YES	YES
Open API	YES	YES	YES	YES	YES
Non-SIEM Data Sources	NO	NO	YES	NO	YES

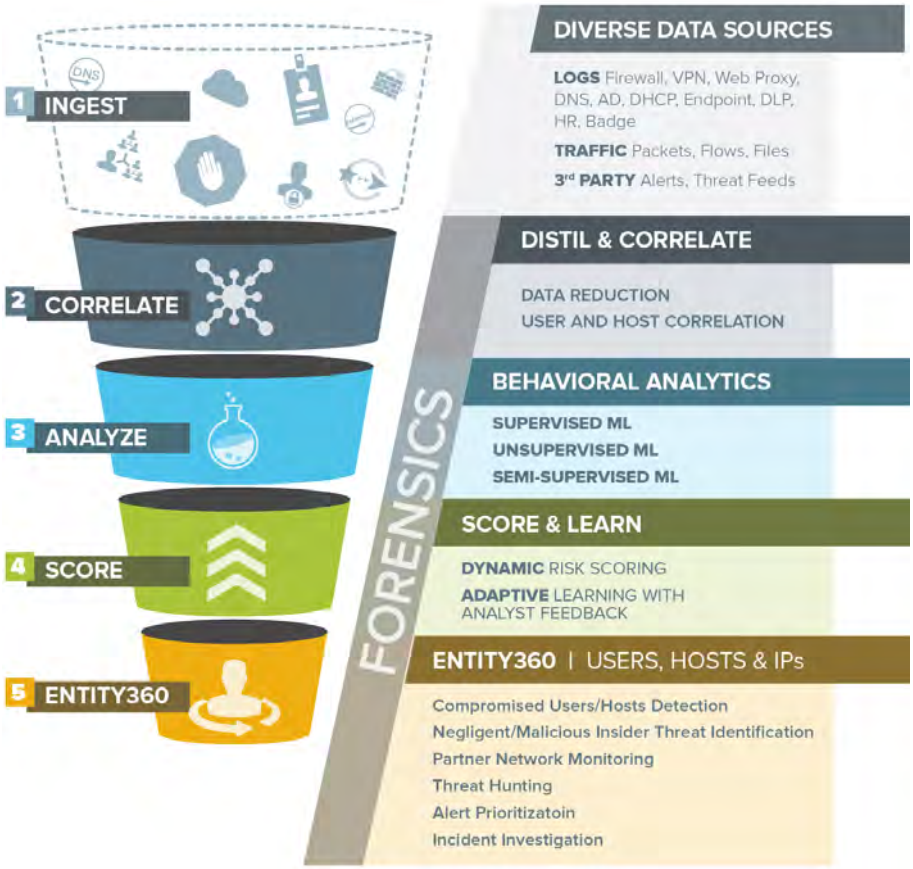
Exabeam



Fortscale

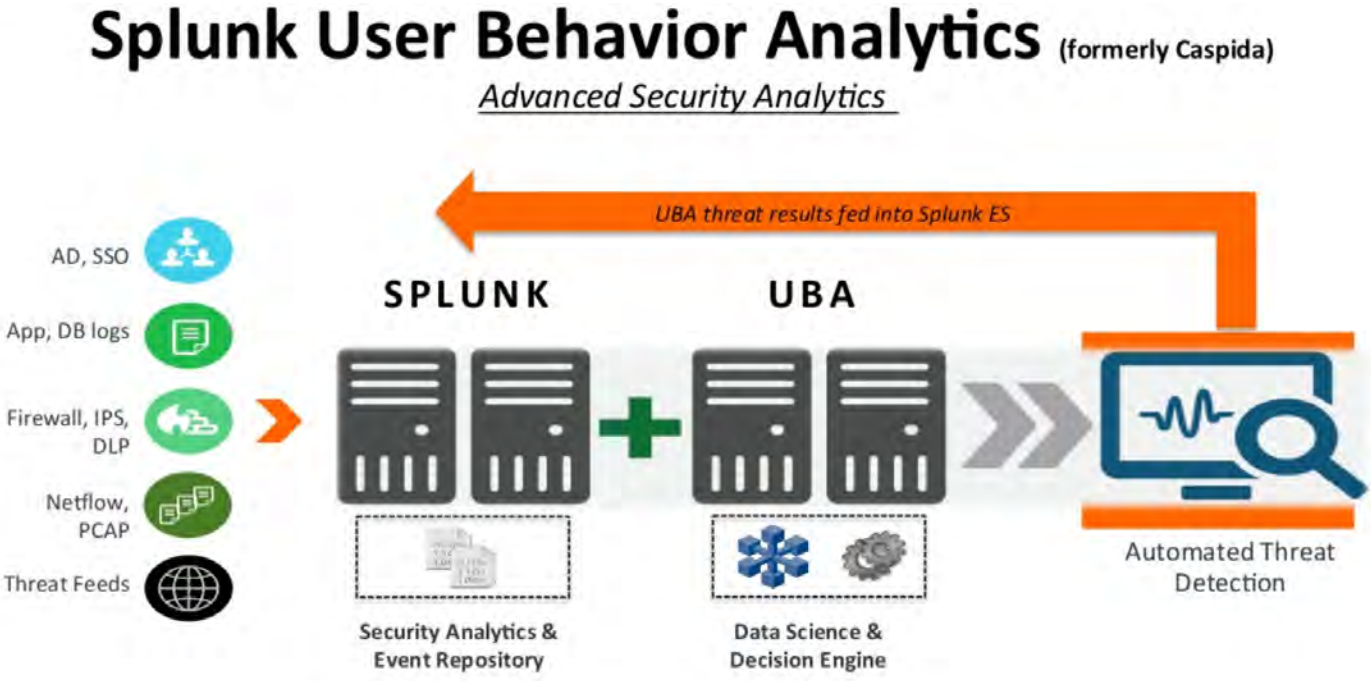


Niara



Securonix

Splunk (UBA)



(end of report)