# Choosing A User Behavioral Analytics Software

Using analytics remains your organization's best bet at data protection and breach prevention. User Behavioral Analytics software focuses on the behavior of the user. Specifically, these track the user's network activity, including the files they have accessed.

User Behavioral Analytics is closely related to Security and Information Event Management (SIEM). The latter focuses on analyzing events that have been captured by the system and correlates these to pre-defined system rules. This focus on the perimeter systems is, in effect, the biggest flaw of this protocol. It fails to pick up on insider manipulation or abuse in your network.

On the other hand, User Behavioral Analytics focuses less on the system and more on the specific user activity. It learns the user's patterns in a bid to zero in on a user whose behavior is different from that of a legitimate user.

Picture 1 of Choosing A User Behavioral Analytics Software

## What to Watch Out for When Choosing a User Behavioral Analytics Software

Your User Behavioral Analytics software provides you with a unique opportunity to neutralize unknown threats within your existing security infrastructure. The key capabilities to look for when choosing a User Behavioral Analytics Software include:

### Real-time Alerts

As part of your security infrastructure, you want to rapidly respond and neutralize any threats to your system. As such, you want software that can quickly scan through your files, user activities, networks, and endpoints for any threats.

Other than real-time alerts, you want software that creates an automatic timeline for any security incidents. It should be able to stitch together any events across your IT infrastructure, including information from all IP addresses.

### Hacker Detection Algorithm

Intrusion detection is a must-have when choosing a User Behavioral Analytics Software. This is mainly since there has been an increase in ransomware and threats to customer databases and business processes.

Other than detecting the initial suspicious behavior, you also want software that has lateral movement detection. Specifically, you want to detect everything the attacker does after that initial penetration. To be safer, you want

software that can track malicious entry into your system through different IP addresses, hardware, and credentials.

Overall, you want a software that protects your system from external threats and one that protects you from industrial espionage as a result of internal threats.

## Process Large User Files and Email Activities

User files are user credentials, including their usernames and passwords. These will often be attacked using a privilege escalation technique where the hacker grants themselves additional privileges into your system using stolen credentials. The amount of said files within your system depends on the size of your organization.

Still, you want an analytical software that processes each of these regardless of their number. Additionally, it would help if you considered software that can process Personal Identifiable Information (PII) to ensure that criminals do not impersonate any of your genuine users.

As part of processing all files and email activities, the software should have dynamic peer groupings. This capability should come in handy when grouping similar users and entities, as this should help the software analyze the collective behavior of your typical user.

## Advanced Visibility of Threats Against Application

Soon as you deploy your software, you want to have a complete overview of your organization's threats. Mainly, you want infrastructure in place that can correlate connected threats and attacks. This holistic view across all threats or attack chains should help you circumvent any threats and respond promptly.

Additionally, you want software that is threat intelligence. This should include the publishing of up-to-date information about your threat levels. Besides, you should benefit from the excellent repository of known threats to protect your system in the future.

## Threat-hunting

Ideally, security teams deal with the existing threats and prepare for the same. This could include tweaking the business's response range, including training on phishing awareness and updating or patching known vulnerabilities.

Still, for more excellent protection, you should consider software that embarks on threat-hunting for you. This should help your organization understand the sophistication of possible attacks. In hindsight, this proactive approach is at the root of behavioral analytics. Overall, while choosing a User Behavioral Analytics software, you want to look for software that integrates threat-hunting into your protection.

Risky or abnormal user behavior puts your data and IT infrastructure at risk. As a business owner, you want a multi-faceted approach to your security. Specifically, you want software that continuously picks up on foreign and camouflaged threats in real-time. Additionally, you want software that can constantly process all user information within your system and provides you with extensive visibility. The objective of the User Behavioral Analytics software you go with should be to help you come up with an incident response plan that helps prevent further damage or threat to your data and IT infrastructure. Overall, behavioral analytics is a proactive security solution that is, in effect, a cross-functional response tactic that your business will benefit from.