OpenText Behavioral Signals

Detect, investigate, and respond to threats that may be hiding in your enterprise before your data is stolen

Benefits

- **Detect threats** with speed and at scale
- **Prioritize leads** to focus your efforts
- **View risky entities** with the intuitive dashboard that shows the greatest potential risks

All organizations have important assets to protect—customer information, intellectual property, critical infrastructure controls, or all of the above. Unfortunately, existing approaches to protecting these assets from advanced threats frequently fall short, leaving security teams to contend with rigid, rules-based analytics, fragmented security ecosystems, and a never-ending barrage of alerts, most of which are false alarms. Meanwhile, these teams are expected to flawlessly protect against critical threats like data exfiltration and unauthorized network access.

Detect threats with speed and at scale

OpenText™ Behavioral Signals is uniquely positioned to find the threats that matter for enterprises with valuable data to protect, limited security or financial resources, and significant surface area to monitor. Unlike other solutions, Behavioral Signals goes beyond traditional rule- and threshold-based detection to assess the potential risk of a user or entity based on mathematical probability and online unsupervised machine-learning models. This approach, combined with the software's native big-data architecture, allows your security team to detect threats with speed and at scale.

Detect. Investigate. Respond.

OpenText™
Behavioral Signals

Threat detection use cases

Behavioral Signals is effective in the following scenarios:

Insider threats

- At-risk or high-risk employees
- Account or privileged account misuse
- Terminated employee activity

Data breaches

- Data staging
- Data, network, or USB exfiltration
- Unusual data access or uploads

Advanced threats

- Compromised accounts
- Internal recon
- Unusual traffic or applications
- Abnormal processes
- Infected hosts
- Malicious tunneling
- Bot detection

IP theft

- Interactions with dormant resources or files
- High-risk IP or data access
- Lateral movement

Prioritize leads

Using machine learning, OpenText™ Behavioral Signals distills billions of events into a prioritized list of high-quality leads to focus and accelerate the efforts of your security operations center. The software's machine learning models, combined with a highly intuitive user interface, accelerate threat detection and investigation, drastically reducing attacker dwell time.

With this unsupervised machine learning—a type of AI that doesn't need pre-labeled datasets—Behavioral Signals' algorithms extract available entities (users, machines, IP addresses, servers, etc.) from log files and observe events involving these entities to determine expected behavior, a measurement called "unique normal." As new information comes through the analytics process, events are evaluated against previously observed behavior to assess potential risk.

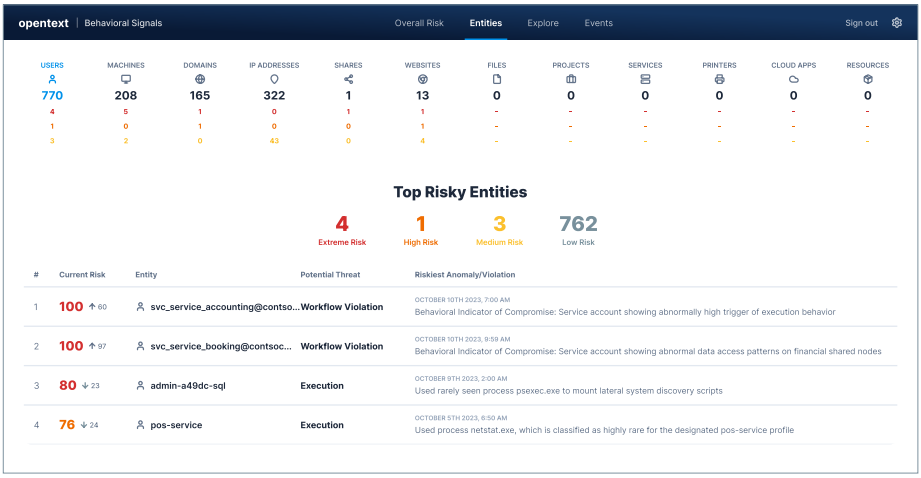
The process of baselining and scoring used by Behavioral Signals boosts the efficiency and speed at which security teams detect, triage, investigate, and respond to threats. Its risk assessments can be used to initiate actions via automation, orchestration, and alerting solutions that execute faster-than-human actions as risks are found. Behavioral Signals also provides downloadable reports summarizing immediate organizational risks.

View risky entities

As a security practitioner, your primary mechanism for interacting with Behavioral Signals is the intuitive, web-based dashboard. This dashboard allows users to quickly and easily determine which entities represent the greatest potential risk. As risky entities are identified, the dashboard allows you to explore a timeline of events so that the potential risk can be understood in the context of the generated alerts and, if desired, the raw events that produced them.

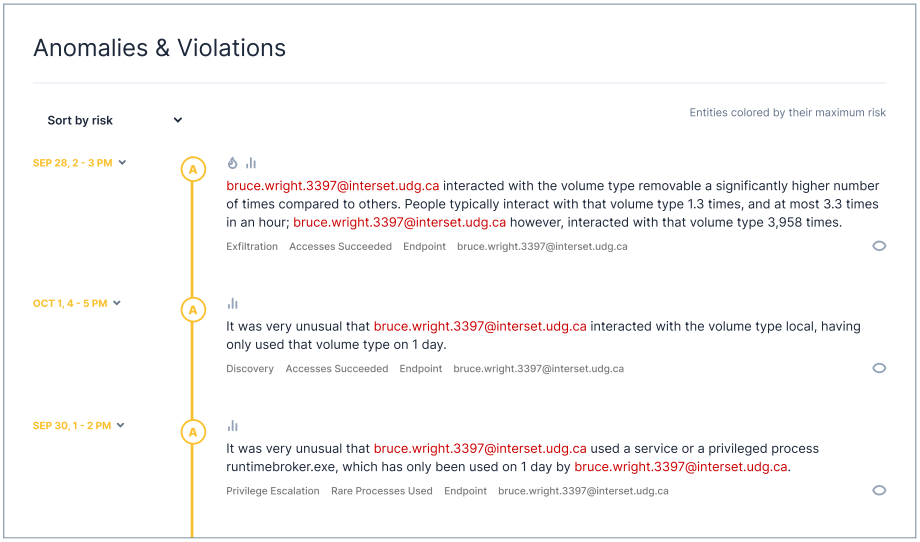
The screenshots below show a drilldown from the list of riskiest users to the raw events.

1. View all entities with analytics, grouped by entity type. The screenshot shows a list of users in order of risk score from highest to lowest.

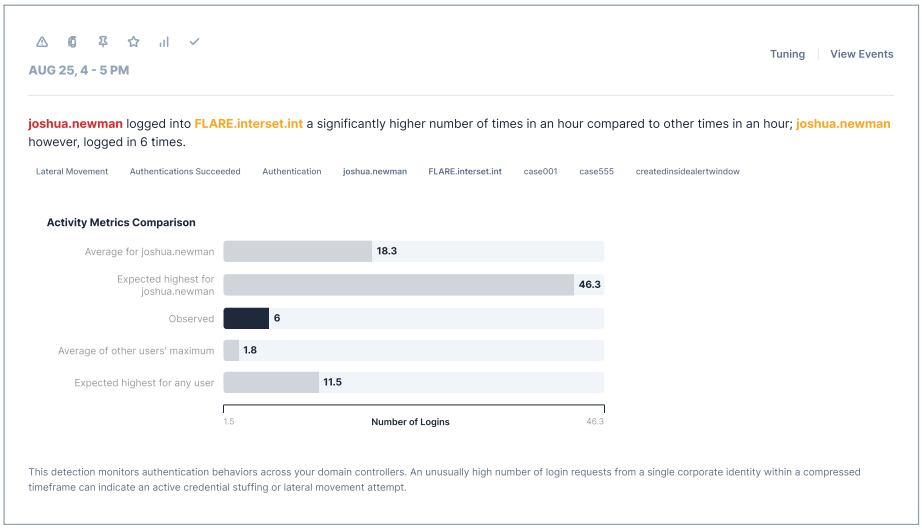


2. When any entity is viewed, its risk score over time is displayed in a timeline view. This perspective shows not only the change in risk score, but also broadly characterizes the types of behavior that drove it.

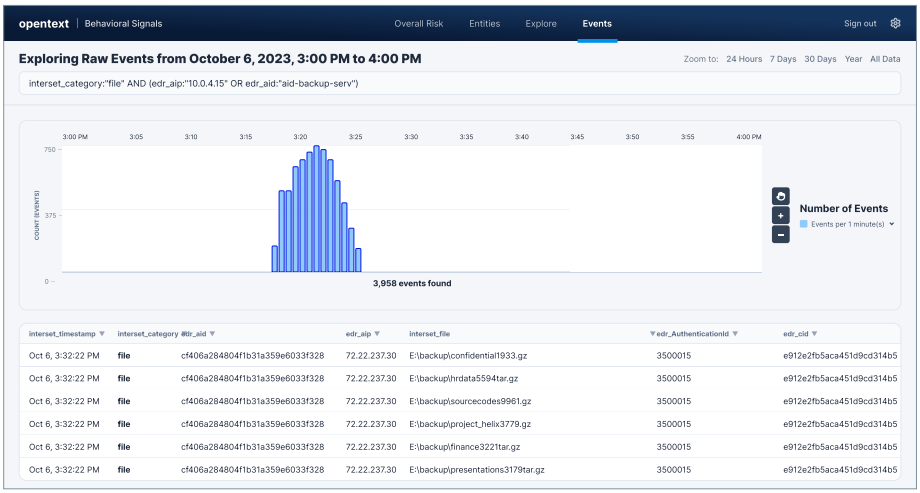
3. When viewing an entity, a display of the alerts associated with it can be seen below the timeline view. They can be filtered by associated entities and types of risk, displayed in chronological order, and linked to the timeline view to show a narrative of the unfolding behavior in the context of other events.



4. Clicking on any of the alerts allows for examination that shows the event in context of the user's baseline and other relevant entities in the enterprise. The risk associated with the alert is displayed, and the model that triggered the alert is described in detail. Note that the user's baseline is compared to itself as well as to other similar entities. These similar entities are identified through statistically determined peer groups.



5. The raw events that triggered an alert are only a click away. In addition to seeing the actual contents of the log file responsible for the analytics, users can enter additional queries using this interface.



Learn more about OpenText Behavioral Signals.