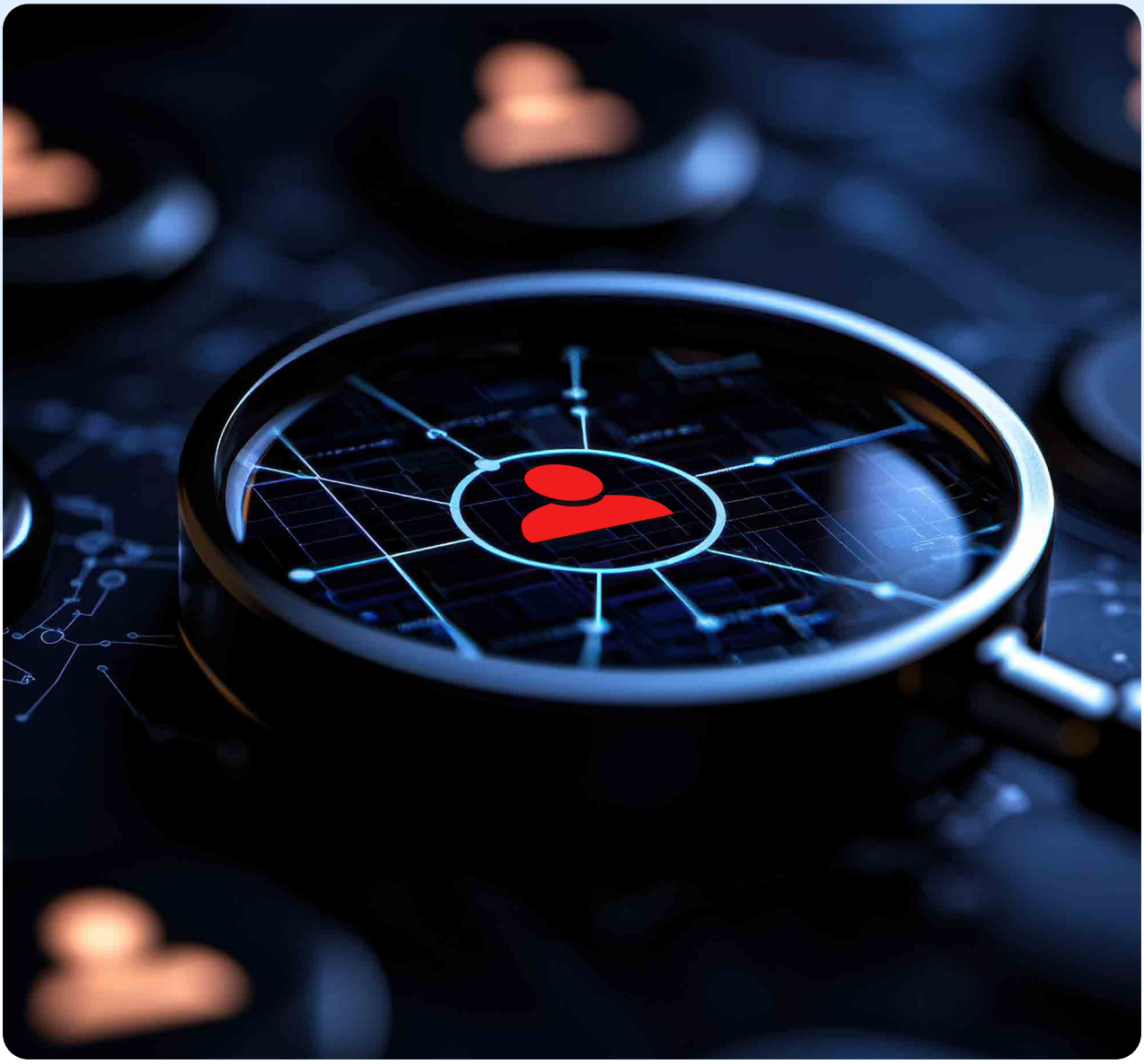
ManageEngine
Log360 Cloud

DATASHEET

User and entity behavior analytics in Log360 Cloud



Overview

Security teams today face an overwhelming volume of alerts, making it difficult to identify the few that truly matter. Traditional detection mechanisms fall short when it comes to identifying insider threats, compromised accounts, and other stealthy attacks that hide behind legitimate credentials.

Log360 Cloud's user and entity behavior analytics (UEBA) applies machine learning and behavioral analytics to user and entity activity, empowering your security operations center to detect unknown threats, reduce investigation time, and respond more effectively. By combining intelligent anomaly detection, risk scoring, focused watchlists, and insightful dashboards, UEBA transforms vast data into actionable intelligence, all within a unified cloud platform.

Uncover hidden threats with behavior-driven anomaly detection

Use case: Detecting credential misuse, lateral movement, and insider threats

Traditional signatures and static rules miss many threats that mimic legitimate activity. Log360 Cloud's UEBA uses machine learning to establish baselines and detect time-, count-, and pattern-based anomalies, catching what others miss.

Spot the early signs of account takeover	Security teams can detect when legitimate user accounts are behaving out of character, like accessing systems at odd hours, logging in from unfamiliar geolocations, or executing unusual commands. These early indicators help stop potential compromises before damage is done.
Expose compromised or misconfigured assets	UEBA spots anomalies in machine behavior that hint at unauthorized changes or lateral movement. Analysts can quickly correlate actions to the responsible endpoint and prioritize investigation.
Catch hidden data movement and misuse	When sensitive files are downloaded in bulk, transferred through unexpected channels, or accessed by unusual users, UEBA flags the behavior instantly. This helps organizations prevent data exposure, whether it's caused by insiders, attackers, or misconfigured systems.
Keep privileged access in check	Admins and users with elevated rights are monitored continuously. Any deviation from their normal activity profile, from launching suspicious processes to modifying critical configurations, is detected as an anomaly. This reduces the risk of privilege abuse.
Map risky behavior across your environment	Log360 Cloud's UEBA brings context to suspicious behavior by correlating activity across users and assets. Security teams gain visibility into how threats unfold across multiple touchpoints, empowering faster, more confident decision-making.

Enhance visibility and accelerate threat investigations with contextual behavioral insights

Use case: Prioritizing investigations with clear risk context and actionable data

Security teams face alert overload and fragmented data that slow down investigations. Log360 Cloud's UEBA consolidates behavioral anomalies into intuitive dashboards that highlight overall risk posture, trends, and high-priority users or entities. Analysts can quickly zoom in on suspicious activity backed by detailed event context, enabling them to focus on what matters most.

- Visualize anomaly volumes, risk distributions, and top contributing behaviors over time for a holistic view.
- Drill down into individual users or assets to review detailed anomaly histories and trigger explanations.
- Maintain and monitor dynamic watchlists of privileged, high-risk, or flagged subjects for ongoing vigilance.
- Leverage customizable alerts to ensure timely response to critical anomalies.

Highlights of Log360 Cloud's UEBA

Proactive anomaly detection

Leverage a rich library of predefined anomaly rules to detect suspicious activity across users, devices, and network assets, including signs of account compromise, privileged access misuse, policy violations, and potential data exfiltration. Fine-tune detection by enabling up to 20 active rules or crafting custom ones tailored to your environment.

Insight-rich dashboards

Visualize anomaly trends, risk distribution, and high-risk individuals or systems across interactive dashboards. Drill down into user or entity activity, anomaly types, and contributing events to accelerate investigation.

Behavioral rule customization

Adapt detection logic to your organizational risk profile. Create custom rules based on time-based, count-based, or pattern-based behavior anomalies to spotlight the threats most relevant to your operations.

Focused threat monitoring

Use watchlists to continuously track users and entities under investigation, privileged roles, or systems managing sensitive data. Prioritize based on risk scores and recent anomalies.

Real-time insights and reporting

Receive real-time alerts when critical anomalies are detected. Generate detailed reports with contextual summaries and exportable visuals to support audits, compliance, and internal audits.

Cloud-native approach

Log360 Cloud's UEBA is designed for quick deployment, effortless scaling, and seamless integration, helping security teams stay agile without added infrastructure or overhead.