14 Behavioral Analytics Use Cases Security Operations Teams Should Evaluate

User and entity behavior analytics (UEBA) plays a central role in modern security operations. Instead of relying only on known indicators or static rules, behavioral analytics evaluates how users, entities, and agents normally operate, then identifies deviations that signal risk. This approach helps security teams detect activity that appears legitimate on the surface but indicates misuse, compromise, or abuse over time.

As environments evolve, UEBA must extend beyond human users. Service accounts, automated processes, and AI agents now perform critical work and often operate with elevated access. This guide outlines 14 behavioral analytics use cases that security operations teams should evaluate when assessing their ability to detect, prioritize, and investigate identity-driven risk across people, systems, and agents.

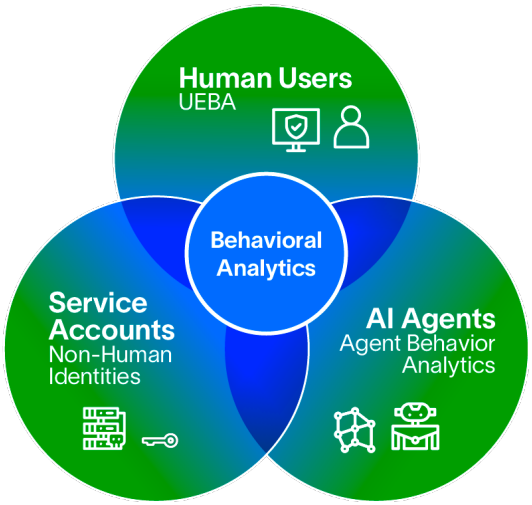

Figure 1.

Behavioral analytics evaluates risk across human users, service accounts, and AI agents using the same core behavioral principles.

As identity has expanded, behavioral analytics has had to evolve, as well.

Figure 2.

Identity in security operations has expanded from human users to service accounts and AI agents, all of which require behavioral analysis.

Use Case Coverage Map

Identity Type	Detection Use Cases Covered	Investigation Use Cases Covered
Human Users	Credential misuse, insider threats, account sharing, privilege abuse	Activity timelines, breach forensics, third-party alert investigation
Privileged Users	Privileged account misuse, executive asset access	Scope analysis, access history, impact assessment
Service Accounts	Abnormal service account behavior, dormant accounts, unauthorized account creation	Long-term behavior review, misuse investigation
AI Agents	AI agent misuse, abnormal automation, unexpected access patterns	Agent activity timelines, human-agent interaction review

Table 1.

Behavioral analytics use cases span both detection and investigation, depending on how teams identify and analyze identity-driven risk.

Detection Use Cases

1. Compromised User Credentials

Behavioral analytics identifies abnormal authentication and access patterns that suggest stolen or misused credentials. Indicators include unexpected login locations, device changes, or access sequences that deviate from established behavior. Early detection reduces dwell time and limits downstream impact.

2. Privileged User Compromise

Privileged users access sensitive systems as part of normal operations, which makes misuse harder to spot. Behavioral analytics detects deviations in how privileged accounts authenticate, move laterally, or access data, even when activity appears technically valid.

3. Executive Asset Access

Executives are frequent targets due to access to sensitive financial and strategic information. Behavioral analytics builds behavior profiles for high-risk users and assets, then flags unusual access patterns that may indicate account takeover or fraud.

4. Insider Threats

Not all threats originate externally. Behavioral analytics surfaces risky activity by insiders, whether intentional or accidental, by identifying behavior that falls outside normal access patterns and peer activity.

5. Account Lockouts

Account lockouts consume investigation time and administrative effort. Behavioral analytics evaluates activity leading up to a lockout to help distinguish between user error and potential credential misuse.

6. Suspicious Account Creation

Attackers may create new accounts to maintain persistence. Behavioral analytics monitors account creation behavior and flags deviations from expected provisioning patterns and access norms.

7. Account Sharing

Shared credentials reduce visibility and accountability. Behavioral analytics identifies concurrent or conflicting usage patterns that suggest multiple individuals accessing the same account.

8. Service Account Behavior

Service accounts often operate continuously and hold broad privileges. Behavioral analytics establishes baselines for service account activity and highlights deviations that may indicate misuse or compromise.

9. Dormant Accounts

Inactive accounts increase risk when they remain enabled. Behavioral analytics tracks inactivity over time and highlights credentials that no longer align with expected usage patterns.

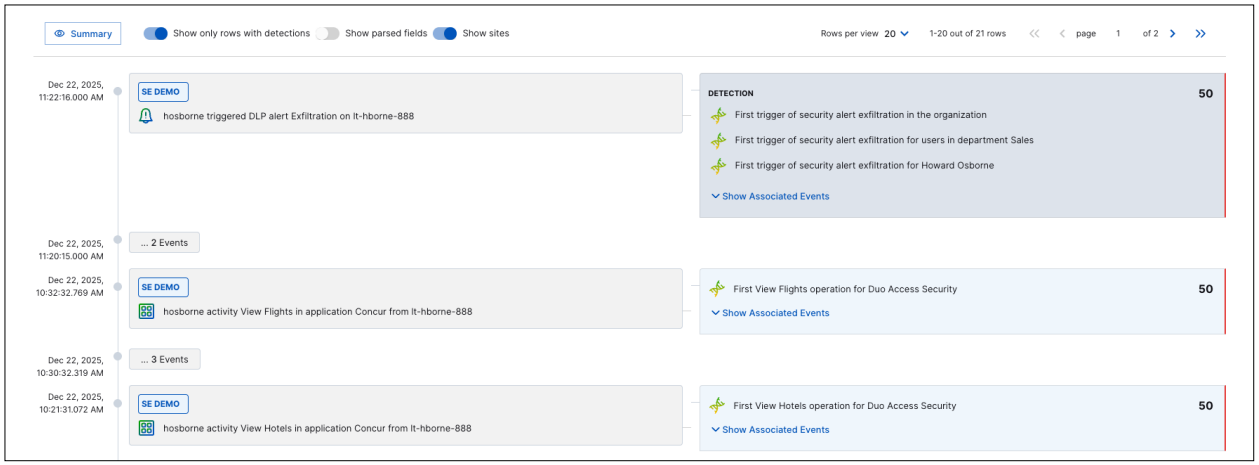

Figure 3.

Behavioral analytics correlates detections and activity into timelines that help you understand scope, sequence, and impact during investigations.

Investigation Use Cases

10. Third-Party Alert Investigation

Alerts from endpoint, network, and data tools often lack identity context. Behavioral analytics enriches these alerts with user, asset, and behavior data to accelerate investigation and triage. Once a signal is identified, behavioral analytics helps teams understand how activity unfolds over time.

11. User Activity Investigations

Legal and HR investigations often require historical activity reviews. Behavioral analytics provides consolidated timelines that show authentication, access, and movement without manual data collection.

12. Breach Forensics Review

Post-incident reviews require reconstructing attacker behavior across systems. Behavioral analytics automates timeline creation, helping teams understand scope, sequence, and impact.

13. Red Team Testing and Training

Red Team exercises test detection and response readiness. Behavioral analytics visualizes attack paths during simulations, helping teams identify gaps and improve investigative consistency.

14. AI Agent Security

As organizations adopt AI agents and automated workflows, security teams need visibility into how these agents behave and what access they use. Traditional tools often treat agent activity as background noise, making misuse difficult to detect.

Agent Behavior Analytics (ABA) applies behavioral baselining to AI agents, identifying deviations that indicate misuse, drift, or compromise. This includes unexpected access patterns, unusual privilege use, or activity outside an agent's intended role. Evaluating AI agent behavior alongside human and service account activity gives security operations teams a more complete view of identity-driven risk as AI adoption expands.

Conclusion

Behavioral analytics provides a practical foundation for detecting and investigating threats that evade rule-based controls. By evaluating how users, entities, and agents behave over time, security operations teams gain earlier visibility into risk and reduce the effort required to investigate complex incidents.

As identities expand to include service accounts and AI agents, the importance of behavioral analytics continues to grow. When evaluating solutions, teams should assess whether these 14 use cases are supported in practice and whether behavioral insights translate into faster investigations, clearer prioritization, and reduced operational overhead.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at
www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

© 2026 Exabeam, LLC. All rights reserved.