10 Reasons to Augment Your SIEM With Behavioral Analytics

Security operations teams face a growing volume of alerts that lack context and precision. Many attacks now rely on compromised credentials, trusted users, and misuse of legitimate access. Traditional rules-based detection struggles to separate normal activity from real risk.

The 2025 Verizon Data Breach Investigations Report (DBIR) shows that a majority of breaches involve a human element, including phishing, social engineering, and stolen credentials. These behaviors often appear legitimate when viewed through logs alone.

Behavioral analytics addresses this gap by continuously modeling normal activity and identifying meaningful deviations. When paired with a SIEM, behavioral analytics adds context and prioritization. Instead of chasing isolated alerts, analysts can see how risk develops over time.

New-Scale Analytics applies machine learning and behavioral models to large volumes of telemetry to surface higher-fidelity detections. It reduces noise, highlights risk progression, and helps teams investigate faster with fewer manual steps.

Behavioral analytics adoption continues to grow as organizations look for detection methods that scale with cloud services, SaaS platforms, and automated systems. The technology establishes baselines for users, service accounts, devices, and software agents. When activity deviates from expected behavior, the user or entity's assigned risk score increases based on severity and persistence, helping teams prioritize investigation.

In practice, this means your security operations team can focus on behavior that signals real risk. The 10 reasons below outline where behavioral analytics strengthens a SIEM along the most common attack paths teams investigate.

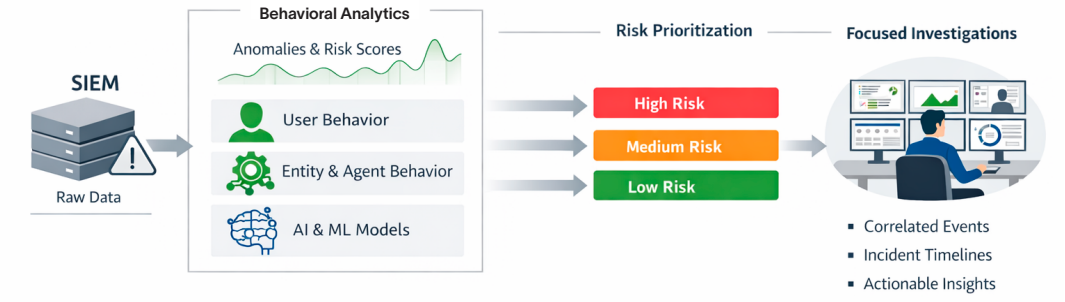

Figure 1.

Behavioral analytics adds context and risk-based prioritization to SIEM data, helping security operations teams focus investigations on activity that signals real risk.

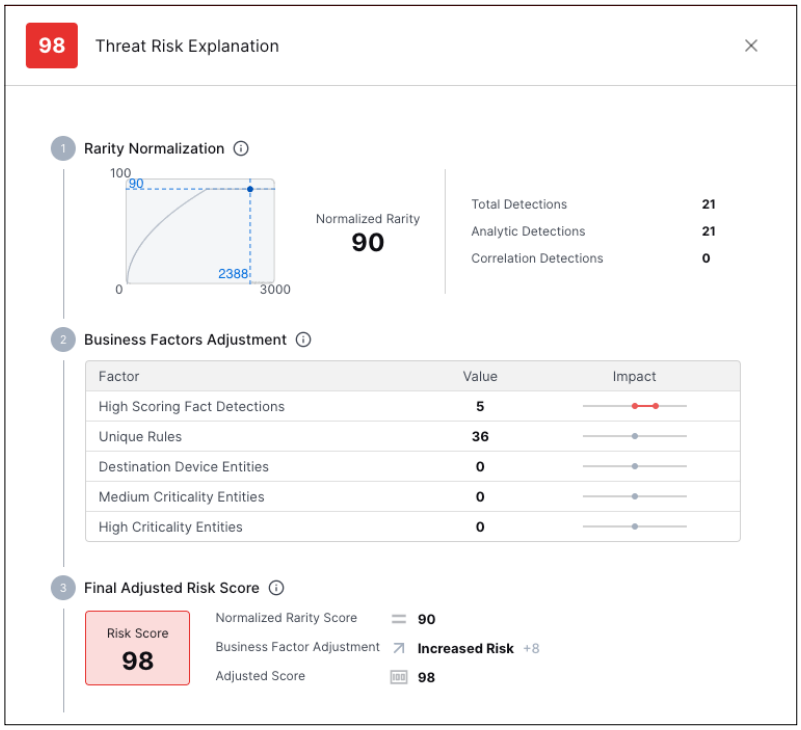

Figure 2.

Multi-layered risk scoring normalizes unusual activity signals, then adjusts the assigned risk score using business-relevant factors for prioritization.

1. Detect Compromised User Credentials

Stolen credentials remain one of the most common paths into an environment. Behavioral analytics identifies anomalies such as unusual login locations, impossible travel, or unexpected device use that indicate account compromise. These signals often surface before traditional controls generate alerts.

2. Detect Privileged User Compromise

Privileged accounts provide direct access to critical systems. Behavioral analytics continuously monitors these accounts for abnormal access patterns, unexpected privilege use, and deviations from historical behavior. This visibility helps teams detect compromise earlier and limit impact.

3. Protect Executive Accounts and High-Value Users

Executive and high-value users access sensitive data and business-critical systems. Behavioral analytics builds individualized behavior models for these users and monitors for unusual access, data usage, or account activity that could signal compromise or misuse.

4. Detect Compromised Systems and Unmanaged Devices

Unmanaged and personal devices increase risk and reduce visibility. Behavioral analytics monitors behavior rather than asset ownership. It identifies deviations in server access, account activity, and network behavior that point to system compromise.

5. Distinguish Malicious Activity From Legitimate Behavior

Insider threats and account misuse often blend into normal operations. Behavioral analytics helps teams identify risky actions that fall outside established behavior patterns, such as unusual access times, atypical data movement, or unexpected application use. As behavioral signals accumulate, the platform assigns a higher risk score to the affected user or entity, reflecting both severity and persistence rather than a single event.

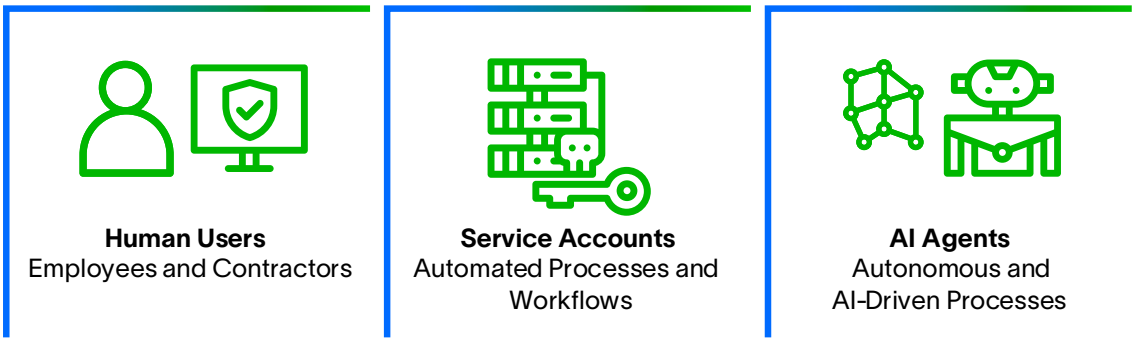

Figure 3.

Behavioral analytics applies the same monitoring and risk scoring principles to human users, service accounts, and AI agents, helping security operations teams detect misuse for all identity types.

6. Identify and Track Lateral Movement

Attackers rarely stop at initial access. Behavioral analytics connects activity across systems, accounts, and environments to reveal lateral movement early. By correlating related behaviors, teams can detect attack progression instead of investigating isolated events.

7. Detect Data Exfiltration and Misuse

Behavioral analytics monitors for abnormal data movement, including spikes in network traffic, suspicious email forwarding, and unexpected access to sensitive repositories. It also helps identify emerging risks such as sensitive data exposure through generative AI tools when usage deviates from normal patterns.

8. Add Context to Failed Logins and Account Lockouts

Failed logins alone generate noise. Behavioral analytics evaluates login failures in context, including timing, location, frequency, and related activity. This automated analysis reduces investigation time and helps teams assess risk faster.

9. Identify Service Account and AI Agent Misuse

Service accounts and non-human agents often have broad access and limited oversight. Behavioral analytics establishes baselines for these entities and monitors for deviations that signal misuse or compromise.

Agent Behavior Analytics (ABA) extends this visibility to automated processes, scripts, and AI-driven agents. It helps security operations teams detect abuse that traditional user-focused controls often miss.

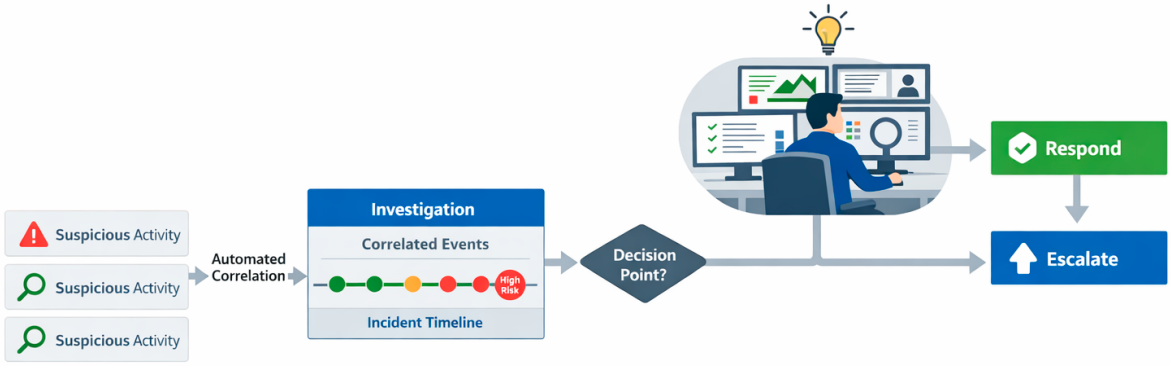

Figure 4.

Related activity is grouped and reviewed in a single investigation flow, helping security operations teams move from initial signals to informed response decisions with less manual effort.

10. Automate Detection, Triage, and Investigation

Manual investigation slows response. Behavioral analytics automates detection and prioritization by linking related activity into risk-driven, machine-built timelines. Analysts receive structured views of what happened, how risk developed, and where to focus next, reducing time spent on low-value tasks.

Upgrade Your SIEM with Behavioral Intelligence

Behavioral analytics adds the context and prioritization traditional SIEMs lack. New-Scale Fusion is designed to augment existing SIEMs and data lakes by applying behavioral models, automation, and risk scoring to your telemetry.

By automatically building incident timelines and correlating activity across users, agents, and systems, New-Scale Fusion helps security operations teams investigate faster and respond more effectively. Risk-based prioritization and machine learning guide analysts to the activity that requires action, so teams spend less time searching and more time stopping threats.

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). Learn more at www.exabeam.com.

exabeam™

Learn more at
www.exabeam.com →