Devo Behavior Analytics

Uncover Anomalous Behavior and Elevate SOC Effectiveness with AI-powered User and Entity Behavior Analytics (UEBA)

SOLUTION BRIEF

INTRODUCTION

The threat landscape is more complex than ever, with the attack surfaces expanding rapidly. Attackers have grown in their abilities and use of advanced methods and tools to launch attacks that slip in past traditional SOC technologies, move laterally through networks, and cause extensive damage.

It's extremely difficult and time consuming for analysts to uncover anomalous attack behaviors across users, devices, and domains. The traditional approach of SOC teams relying on rules-based alerts provides no way to easily uncover anomalous behavior — and attackers know this. Alerts inherently lack the context analysts need to effectively prioritize and best spend their precious time.

Devo Behavior Analytics, a cloud-native UEBA solution, elevates SOC effectiveness by identifying sophisticated threats, elevating threat hunting effectiveness, and accelerating proactive response.

Powered by an extensive library of out-of-the-box machine learning models, and offering self-service customization, Behavior Analytics uncovers anomalous user and entity behavior throughout your organization, delivering next-level risk context across the entire MITRE ATT&CK framework and rapid time to value.

Security analysts can correlate events and anomalous behavior in a single view and quickly understand and prioritize the most serious cyberthreats, enabling them to optimize their time, make better decisions, and swiftly mediate sophisticated attacks.

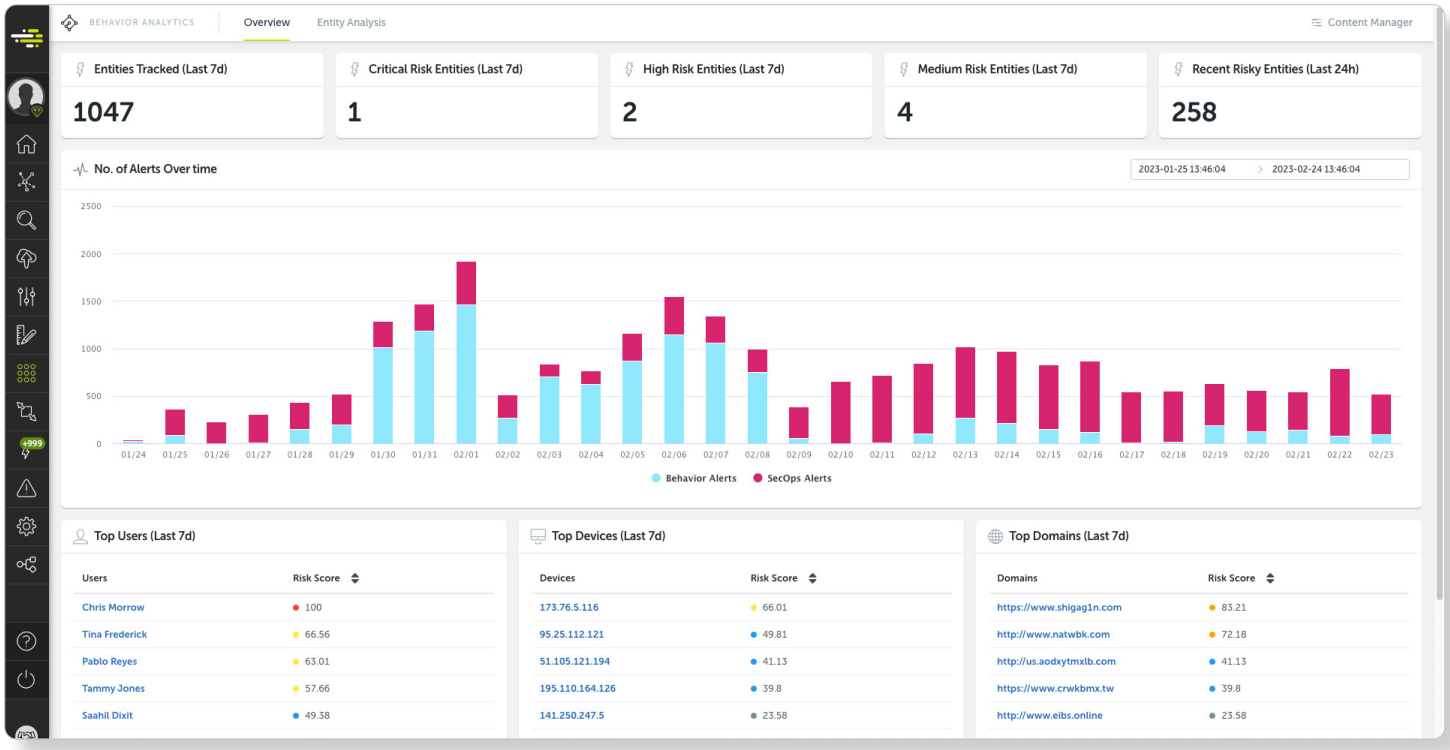

Figure 1: Behavior Analytics elevates SOC effectiveness by uncovering and investigating anomalous behavior across your entire organization

Go beyond traditional SIEM solutions and uncover anomalous activity they miss

Make use of dozens of behavior models to identify abnormal and anomalous behavior across your entire organization, stopping compromised users and systems in their tracks.

Accelerate investigations by focusing on riskiest entities

Risk-based scoring helps SOC teams prioritize their time and guides analysts to focus on the most serious threats to deliver sustained protection against complex cyberattacks.

Visibility of the most advanced threats across the entire attack chain

Behavior Analytics leverages the MITRE ATT&CK framework to deliver clear and actionable context to security teams, enabling faster investigation and response.

Easily tune use cases to your organization's infrastructure and network

Behavior Analytics allows users to easily enable and configure dozens of use cases to their environment to reduce false positives and focus on truly risky behavior.

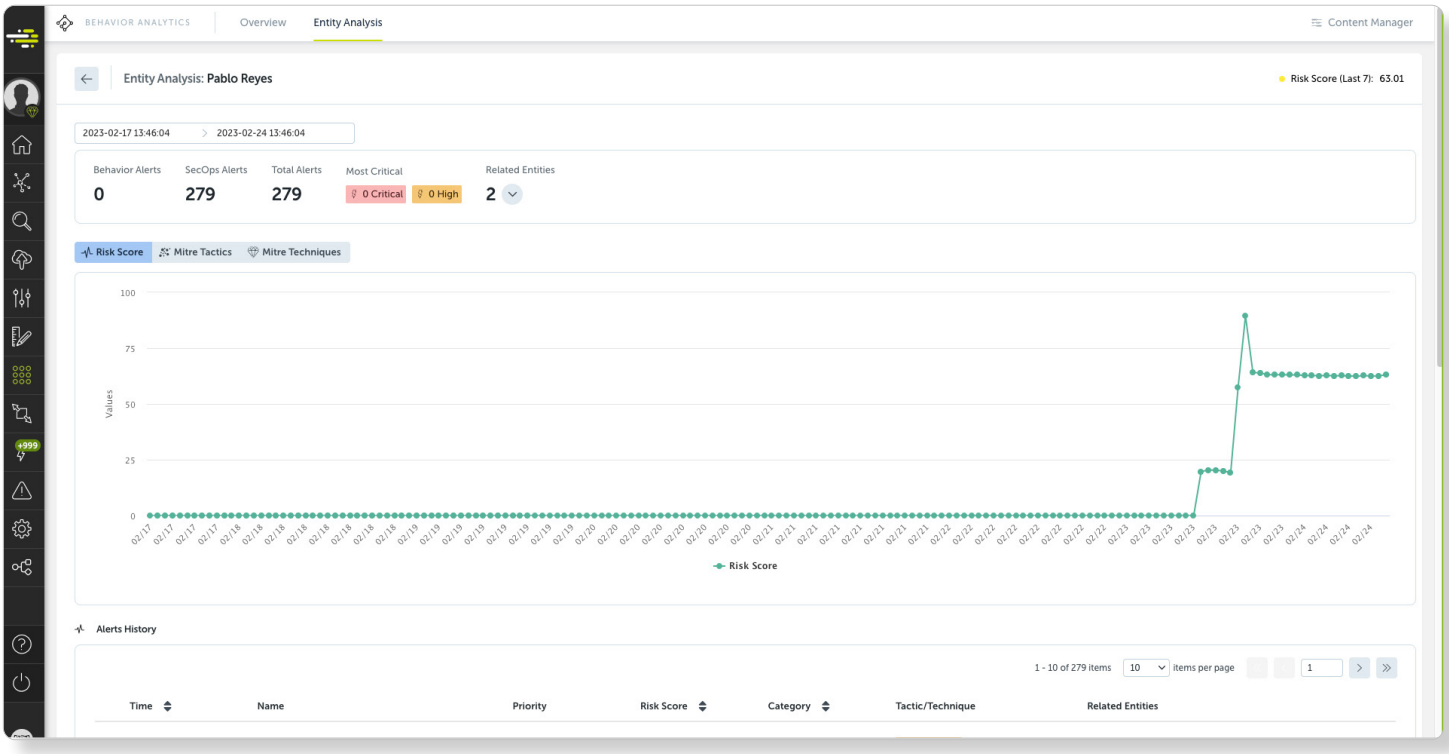

Figure 2: Risk-based scoring powers accurate detection of anomalous behavior

WHAT MAKES DEVO BEHAVIOR ANALYTICS DIFFERENT?

Visibility of anomalous activity across your entire enterprise, powered by broad data source coverage

Behavior Analytics supports a wide variety of data sources including Cloud (Azure, GCP, AWS, Microsoft 365, Google Workspace), Firewall, Authentication, Proxy, Endpoint, and VPN, allowing you to detect anomalies across a broad attack surface.

Rapid time to value with self-service configuration

Other vendors require extensive hours and reliance on support services to get up and running, involving constant handholding to avoid numerous false positives. Behavior Analytics offers an extensive out-of-box library of behavioral models with easy-to-use customization that doesn't require professional services.

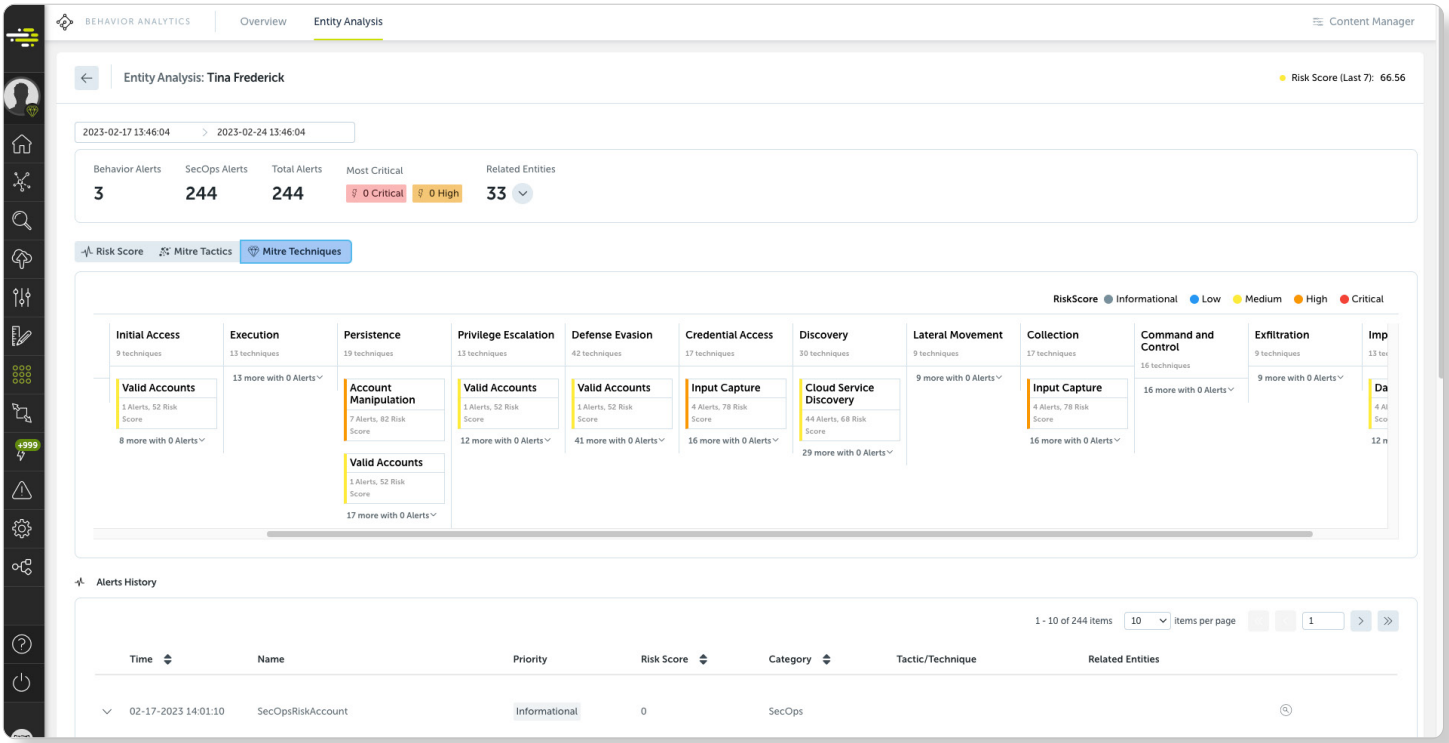

Figure 3: View clear and actionable intelligence on anomalous threats across the entire MITRE ATT&CK chain

Superior risk assessment to drive improved resource prioritization

By applying AI-driven risk modeling to prioritize alerts, Behavior Analytics delivers superior visibility of entities across your environment, enabling you to visualize your risk levels in context of the MITRE ATT&CK framework and make smart resource decisions for risk mitigation.

Seamless integration with other Devo capabilities — A 'native' UEBA solution

Behavior Analytics integrates seamlessly with other Devo capabilities such as Devo SOAR to correlate behavior findings into cases to reduce MTTR.

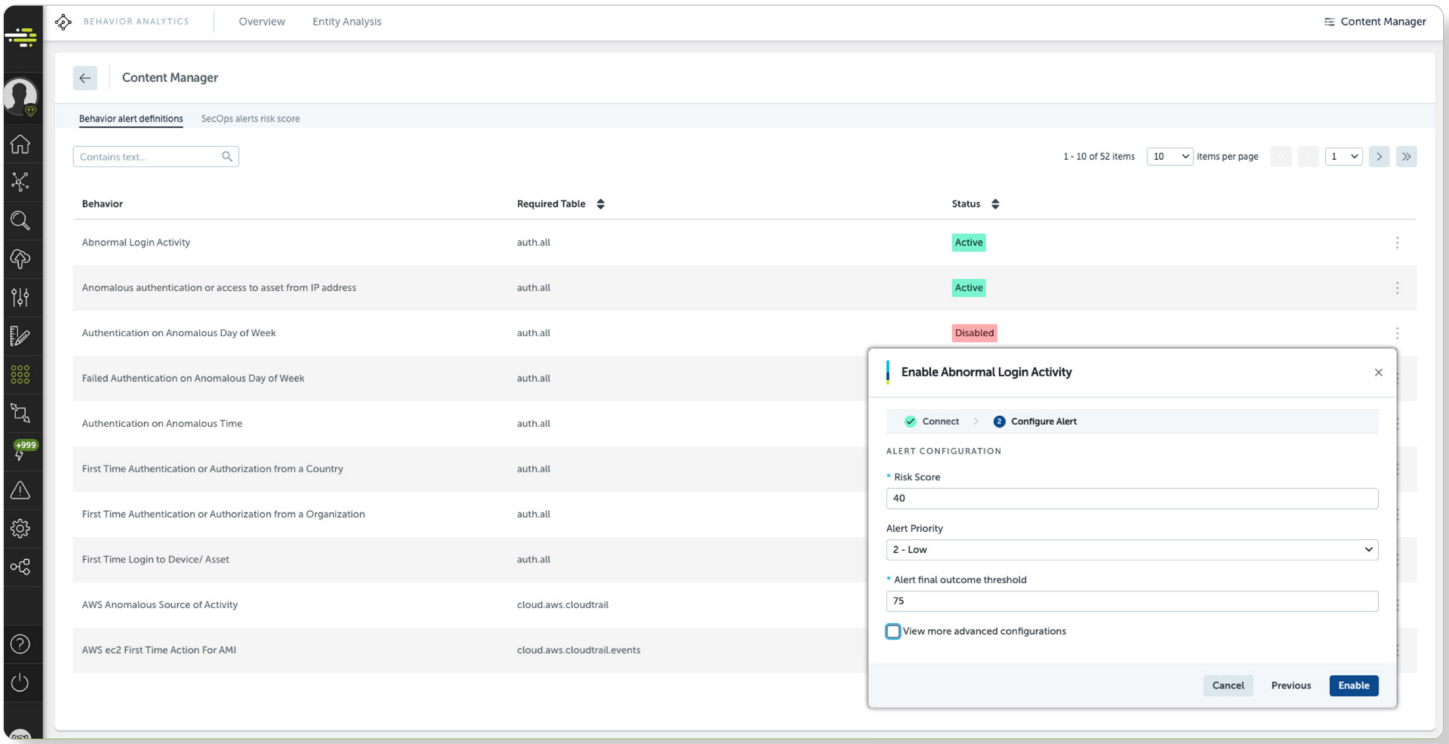

Figure 4: Easily configure dozens of use cases for your particular environment to uncover the most pressing cyber threats

BENEFITS

Improve Security Posture

Behavior Analytics bolsters The Devo Platform, the highly scalable and performant security analytics solution, and gives analysts a detailed view of entity risks in a single location. Analysts can quickly drill down and attain a deep understanding of riskiest entity behavior to drive rapid threat remediation.

Empower Analysts

Analysts can correlate events and behavior across multiple sources in a single view, quickly identify and prioritize the riskiest entities throughout the organization and provide critical context for triage and investigation.

Reduce Compliance and Reputation Risk

By discovering insider threats and sophisticated attacks other vendors miss, Behavior Analytics helps you to avoid expensive regulatory violations and potential damages to your organization's reputation and brand.

Uncover anomalous activity across users, devices, and domains with Devo Behavior Analytics

- Detect advanced threats
- Optimize investigations
- Save analyst time
- Accelerate response

Are you ready to learn more about Devo Behavior Analytics?
Contact your sales representative or visit Devo.com

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.