Four Ways to Augment Microsoft Sentinel With the Exabeam Microsoft Sentinel Collector

Security teams often start with Microsoft Sentinel for visibility into activity within their Microsoft environments. As your environment grows, you may feel that Sentinel alone doesn't provide the behavioral context, consistent investigations, or automation you need for faster outcomes. The Microsoft Sentinel Collector from Exabeam augments Microsoft Sentinel by sending its telemetry into the New-Scale Security Operations Platform. Once there, the data is modeled, risk scored, organized into timelines, and supported by intelligence and automation so you can pinpoint high-risk activity sooner and reduce manual effort.

This guide outlines four practical ways the Exabeam Microsoft Sentinel Collector strengthens your team's work and helps you get more value from your existing investment in Microsoft Sentinel.

1 Broader Visibility Throughout Your Environment

Many investigations extend beyond Microsoft services. Analysts need to understand how identities, devices, cloud platforms, and SaaS applications interact, not only what Sentinel observes. The Microsoft Sentinel Collector augments Sentinel by bringing Sentinel telemetry into the New-Scale Platform where it is aligned with additional data sources for a unified view of activity.

Within the platform, prebuilt parsers, a security-specific Common Information Model (CIM), and continuous behavioral modeling organize data into consistent structures so your team can understand how activity relates from one system to another. This lets you follow key behaviors even when telemetry originates outside the Microsoft ecosystem.

What this means for you:

- Visibility that spans multi-cloud and hybrid environments, not just core Microsoft services
- Behavioral models that update as normal user and entity activity changes
- Less manual tuning and log engineering through consistent normalization and context enrichment
- Better alignment between the data you ingest and the threats you are working to uncover, which helps improve threat coverage over time.

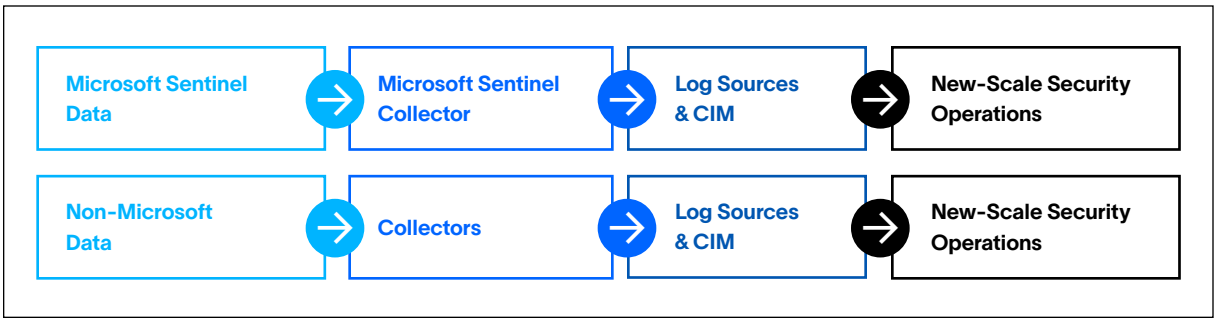

Figure 1.

The Microsoft Sentinel Collector sends Sentinel telemetry into the New Scale Platform where it is normalized and modeled alongside other security data.

2 Flexible Correlation Supported by Behavioral Intelligence

Sentinel correlation rules work well for known patterns. Many teams add behavioral analytics to find unfamiliar, slow-moving, or subtle activity that traditional rules miss. The Microsoft Sentinel Collector applies New-Scale Analytics to Sentinel data, building behavioral profiles that update as patterns change and organizing related evidence into timelines that surface anomalous activity.

Microsoft also offers user and entity behavior analytics (UEBA) capabilities. Sentinel UEBA builds baselines from a defined set of eligible sources and a per-activity lookback window. Exabeam builds broader, continuously updated profiles and doesn't restrict behavioral modeling to short windows or predefined source lists.

Even more, New-Scale Analytics turns behavioral analytics into risk-scored, evidence-grouped response objects. It calculates an entity's risk trajectory from those objects, giving analysts a clear view of how unusual actions accumulate and why the activity requires attention.

What this means for you:

- Broader use case coverage informed by continuous profiling rather than short lookback windows
- Detection logic that adapts to changing behavior and new attack techniques
- A single interface to write, test, and monitor correlation rules and behavioral detections
- Dynamic risk scoring that focuses analyst attention on activity with the greatest potential impact

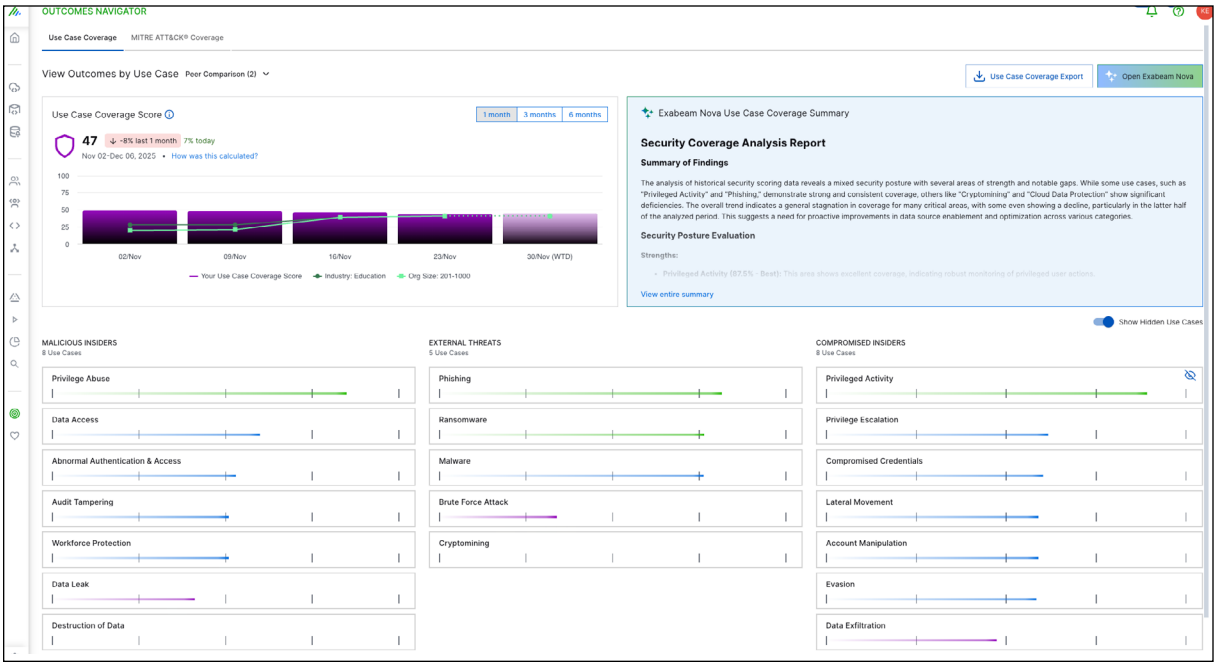

Figure 2

Outcomes Navigator shows coverage scores, category-level use cases, and Exabeam Nova-generated insights to help your team identify strengths and find opportunities for improvement.

3 Automated Timelines That Accelerate Investigations

Investigations often slow down when analysts switch between searches, tabs, or tools. The New-Scale Platform removes this friction by placing Sentinel events into clear, structured Threat Timelines. Activity from Sentinel and your broader environment is normalized, scored, and arranged in chronological order so you can follow what happened without stitching logs together manually.

These Threat Timelines live in Threat Center, the unified workbench where analysts review detections, examine evidence, escalate events, and manage cases. Threat Center brings timelines, incidents, investigation context, and tasks into one place, so your team works faster and avoids the repetitive steps that delay investigations.

What this means for you:

- Faster investigations because Sentinel events flow directly into structured timelines rather than requiring multiple searches
- A consistent investigation process supported by the unified view of timelines, cases, and evidence in Threat Center
- Reduced manual effort because related events, risk context, and behavioral signals are organized for you
- Analysts of any experience level benefit from predictable, repeatable workflows instead of ad hoc investigative paths.

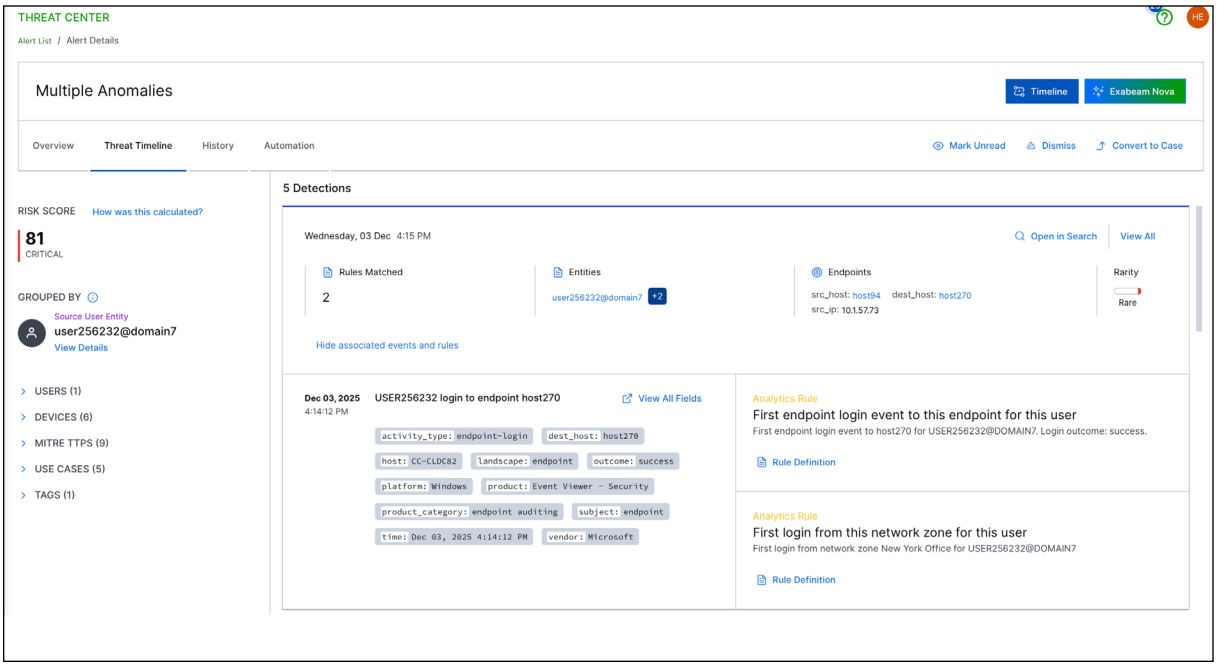

Figure 3

Threat Timelines organize correlated detections, risk scores, entities, and analytics rule matches into a time-ordered view so analysts can understand what happened and take the next steps quickly.

4 Automation Management for Faster, More Consistent Response

After a detection, analysts often spend too much time on repetitive steps such as tagging, enriching, routing, or closing events. The Automation Management app within the New-Scale Platform introduces structure and consistency to these tasks. The Microsoft Sentinel Collector feeds Sentinel telemetry directly into Automation Management, allowing your team to build, test, and execute repeatable workflows without custom scripts or separates security orchestration, automation, and response (SOAR) tools.

Automation Management includes prebuilt playbooks, a no-code and low-code workflow editor, and OpenAPI Standard (OAS) support, so your team can orchestrate investigation and response with Sentinel data, threat intelligence, and context from behavioral models. When paired with Exabeam Nova, the platform's coordinated system of AI agents, Automation Management becomes even more effective. The Exabeam Nova Investigation Agent, Threat Scoring Agent, and Analyst Assistant Agent surface context, recommend next steps, and streamline repetitive tasks that playbooks can then automate.

What this means for you:

- Workflows built with no- and low-code automation let your team reduce manual effort without engineering overhead.
- Prebuilt playbooks provide ready-to-use response patterns for common tasks.
- SOAR is built directly into the New-Scale Platform, reducing tool switching and accelerating coordinated response.
- Exabeam Nova boosts efficiency by recommending next steps, scoring high-risk activity, and supplying investigation details that automation can act on.
- OAS support makes it easy to connect additional security and IT systems so automation scales with your environment.

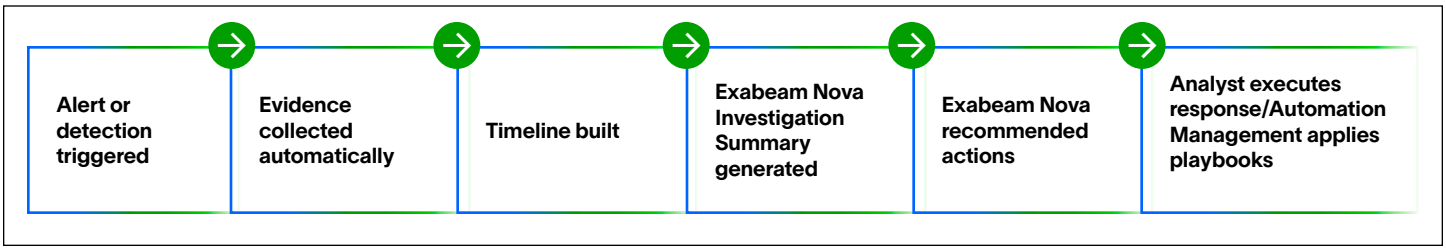

Figure 4.

Exabeam Nova and Automation Management work together to collect evidence, build a timeline, generate an investigation summary, recommend next steps, and help your team move from alert to response with fewer manual steps.

Conclusion

Microsoft Sentinel provides valuable visibility into Microsoft ecosystems. The Exabeam Microsoft Sentinel Collector augments Sentinel by sending its data into the New-Scale Platform where analytics, automation, timelines, and structured workflows help your team detect high-risk activity sooner and work more consistently. When you combine Microsoft Sentinel with the New-Scale Security Operations Platform, you strengthen investigations, reduce manual effort, and move toward more repeatable and efficient security operations.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at
www.exabeam.com →