Considering Microsoft Sentinel for SIEM?

What You Don't Know Will Hurt You

When cyberattacks are as sophisticated and hard to detect as they are today, effective defense starts with the right security information and event management (SIEM) solution SIEM is essential for driving threat detection, investigation, and response (TDIR). But choosing the right SIEM isn't simple.

Many outdated, mediocre SIEM solutions flood the market. They overwhelm security analysts with excessive data and irrelevant alerts, blinding teams to real threats. Enterprise technology giants often bundle SIEM as an add-on within larger ecosystems, treating it as an afterthought rather than a core cybersecurity capability that protects the entire architecture. Microsoft Sentinel is a prime example of this approach.

The Problem With Microsoft Sentinel

Microsoft Sentinel promises robust SIEM capabilities, but its limitations—especially outside the Microsoft ecosystem—pose serious risks. Sentinel struggles with manual processes, slow investigations, limited visibility, and constant maintenance. Basic analytics deliver minimal impact, and low-fidelity detections lead to a high number of false positives. Over time, this can result in audit failures, compliance risks, financial losses, and reputational damage—along with the steep costs of data loss, containment, and remediation following an incident.

And once Sentinel is embedded, it's not easily replaced. This makes its limitations a serious concern for CISOs, CIOs, CTOs, and even CFOs and COOs who manage costs and efficiency.

Here's a detailed overview of how organizations can get persuaded into adopting limited SIEM solutions like Microsoft Sentinel, why this hinders them in the short and long term, and how Exabeam can mitigate these shortcomings.

Why Do Organizations Choose Microsoft Sentinel?

One reason is executive mandate. Microsoft strategically promotes Sentinel's cost advantage to the CFO, positioning as a natural extension of existing Microsoft investments. This messaging influences purchasing decisions by suggesting it maximizes committed spend, even though it often overlooks hidden long-term costs. System integrators may promote it as "free," though this ignores hidden costs.

Other companies prefer consolidating their tech stacks from multi-vendor, best-of-breed ecosystems to a platform, possibly due to vendor fatigue or executive and budgetary pressures to streamline and do more with less. In these scenarios, generalist platform providers like Microsoft are mistakenly perceived as offering sufficient security, eliminating the need for best-of-breed solutions.

But this consolidation comes at a price. Limited integration with other vendors, inefficient observability, and recent security breaches have raised concerns about Microsoft's reliability. Gartner has reported that when security solutions lack support and compatibility with other systems and integrations, it leads to observability inefficiencies and more complex tech infrastructure.

For example, in July 2023, multiple US government agencies were breached by state-sponsored cyberterrorists through a vulnerability in Microsoft's cloud services. Later, in November 2023, Microsoft disclosed another significant nation-state attack targeting its corporate systems. These incidents, carried out by advanced persistent threat (APT) groups, exposed critical vulnerabilities within Microsoft's cloud and security infrastructure and raised serious concerns about the effectiveness of its security capabilities. And when it comes to meeting regulatory requirements—like GDPR, PCI DSS, and SOX—limited integration with best-of-breed solutions is a major liability, introducing costly compliance risks.

Why Integration Matters in SIEM

A successful SIEM must integrate across all environments to ensure full visibility. Yet, an IDC study commissioned by Exabeam on the state of TDIR found that most organizations struggle with achieving this visibility. Microsoft Sentinel's limited integration capabilities make it harder to see the entire attack surface. In contrast, the Exabeam New-Scale Security Operations Platform is a modern, cloud-native, cloud-scale SIEM that integrates with nearly 700 vendor products. It's vendor neutral, open, and designed for full detection, connected insights, and consolidated workflows.

Powered by AI, the New-Scale Platform not only identifies threats that others miss but also simplifies investigation by automatically building detailed timelines and risk profiles. The Exabeam and IDC study also found that 35% of organizations struggle to understand "normal behavior"—a critical challenge for effective TDIR. By learning and understanding what normal behavior looks like for users and devices, the platform uncovers hidden threats—like compromised credentials—that other tools miss. This removes blind spots, accelerates response, reduces analyst fatigue, and lowers operational costs.

Bearing this difference in mind, the only reason to select a SIEM tool like Microsoft Sentinel would be its supposed cost effectiveness. But is it actually as economical as they present it to be?

The Hidden Costs of Microsoft Sentinel

Sentinel operates on a pay-as-you-ingest model. The more data processed, the higher the cost. Playbook actions also contribute to these expenses, as do third-party integrations and log storage. Organizations seeking enhanced performance through the Premium plan face additional costs, while the commitment tier offers discounted rates for a preset daily data consumption limit. However, exceeding this limit incurs further charges, and transitioning to another tier requires a formal request and added payment. Even "free" data ingestion has its limits, and retention requirements essential for regulatory compliance add further costs.

While Microsoft Sentinel allows certain types of Microsoft data to be ingested for free—such as Azure activity logs, Office 365 audit logs, Azure Active Directory (AD) Identity Protection, and Microsoft Defender alerts—only organizations that pay for premium Microsoft 365 licensing receive a "data grant." This grant allows up to a minimal 5MB per user per day of data ingestion from additional Microsoft audit logs, cloud security, information protection, and threat hunting sources. However, this represents just a small portion of the data a typical SOC needs to ingest daily. All other data sources, particularly from non-Microsoft products, result in additional costs.

These costs are often difficult to predict, making budgeting and forecasting a challenge for finance leaders. Large enterprises, which utilize an average of 75 different security tools across their environments, face even greater complexity and costs when trying to ensure all relevant data is ingested and monitored. Additionally, while Microsoft allows certain types of data to be ingested for free, full log storage comes at an added cost, often priced per gigabyte retained. Regulatory requirements frequently mandate data retention for extended periods, such as six months for certain standards or up to six years for HIPAA compliance—further driving up expenses.

Microsoft Sentinel also has notable feature gaps that can lead to additional unexpected costs. Many organizations find they must purchase supplemental solutions to address limitations in Sentinel's core offerings, including more advanced analytics, third-party integrations, and comprehensive compliance support. Worse, these costs can escalate rapidly as data volumes grow and security demands increase.

In contrast, Exabeam offers transparent pricing. Compliance capabilities are built in, reducing uncertainty and ensuring you meet regulatory demands without surprise fees. This predictability enables better financial planning and cost control.

Where Microsoft Sentinel Falls Short

With Microsoft Sentinel, it's not just pricing that's opaque. Microsoft struggles with:

- **Visibility:** Limited integrations and poor support for custom correlations restrict visibility and increase the risk of costly breaches. Pre-built correlation rules often fail to trigger for data from non-Microsoft vendors, reducing detection accuracy and leaving gaps in threat coverage.
- **Complexity:** Non-Microsoft log connectors are not prioritized, requiring security teams to build custom parsers using Microsoft's proprietary Kusto Query Language (KQL). Creating and maintaining these parsers and correlation rules demands specialized skills, often leading to additional costs for external services and support. The complexity compounds when managing integrations with non-Microsoft tools or compensating for gaps in Microsoft's built-in analytics—further straining resources and increasing operational overhead.
- **Automation:** Sentinel's SOAR capabilities are fragmented, requiring additional Azure Logic Apps and programming for orchestration and automation. This disjointed approach adds complexity, delays responses, and incurs unpredictable costs.
- **AI and analytics:** Sentinel's AI features, including Security Copilot, are expensive and limited to Microsoft's ecosystem. Pre-built UEBA models are minimal, and while additional models can be created with BYOML, this process is complex, costly, and requires specialists. Budget must also be allocated for Microsoft's BYOML products like Azure Databricks and Azure Machine Learning Studio.

Exabeam, on the other hand, offers:

- Over 9,500 prepackaged parsers and 350 vendor collaborations for integration with nearly 700 vendor products
- A vendor-neutral Common Information Model (CIM) for streamlined log management and faster insights. Microsoft, by contrast, tweaked an open-source model (OSSEM) and rebranded it as ASIM, which introduces limitations in flexibility and customization.
- AI-driven threat analysis that simplifies investigation and reduces manual queries—cutting operational costs. Automated timelines dramatically reduce investigation times, avoiding hundreds of queries and saving hours or even days of analyst time. This is especially crucial in detecting the first instance of suspicious behavior.
- Built-in, transparent SOAR capabilities with automated playbooks, reducing complexity and minimizing support costs. Unlike Sentinel, Exabeam SOAR features are unified and part of a full TDIR approach, not standalone products that incur separate costs.
- More anomaly detection models for Microsoft products than Sentinel itself—10 times as many anomaly-based detection models and eight times as many UEBA models—ensuring deeper, broader detection with less manual effort.

Sentinel's lack of integration with non-Microsoft solutions means the timelines it generates are often incomplete. Integrating extra tools—like Microsoft Defender and Azure Logic Apps—incurs additional costs, increasing the total cost of ownership.

Microsoft's limited and complex UEBA models require additional investments for customization and integration. Meanwhile, Exabeam offers advanced UEBA models and robust multi-vendor integration prebuilt. Exabeam also supports rule chaining in any order, saving countless hours for SOC teams and eliminating the need to create multiple ordered rules to cover various event combinations.

Another advantage of Exabeam is the detection grouping logic in Threat Center. This advanced feature simplifies investigations by providing comprehensive context about related security alerts without forcing analysts to pivot between systems. This reduces mean time to detect (MTTD) and mean time to respond (MTTR), significantly enhancing efficiency and accuracy.

Exabeam has long led the industry in embedding UEBA and SOAR directly into SIEM tools and TDIR workflows—ensuring a unified, efficient approach to threat detection and response.

Does Microsoft Sentinel Differentiate Itself With Generative AI?

Microsoft has made significant investments in generative AI (GenAI), leveraging its exclusive access to OpenAI products and introducing Microsoft Security Copilot. This solution integrates chat functions across multiple products, promising to address visibility gaps within Microsoft's ecosystem. However, its effectiveness is worth scrutinizing. Microsoft's track record of limited integration with other vendors and its history of exploitable vulnerabilities raise important concerns.

As with other Microsoft security add-ons, Security Copilot's pricing is unpredictable and can escalate quickly. The computing capacity for running a Copilot workload is measured in Security Compute Units (SCUs) per hour. At approximately $4 per SCU per hour, running Copilot continuously—24 hours a day, 365 days a year—can exceed $35,000 annually. This doesn't account for additional costs to use Copilot with other products, such as Microsoft 365 and CoPilot Pro, which can add another $30 per user per month. These unpredictable expenses make it difficult for organizations to forecast and control AI-related costs. By contrast, Exabeam includes AI capabilities as part of its core platform, with no extra charges.

The Exabeam approach to GenAI is intentional and focused on real-world impact. To lower barriers to entry—especially in a market facing a cybersecurity talent shortage—Exabeam employs natural language processing (NLP) and AI to simplify querying. Users can search data using natural language, with backend conversions visible for validation.

Additionally, Exabeam leverages machine learning-based AI to analyze investigation timelines and scenarios. GenAI then enhances these analyses by providing clear, coherent explanations. This ensures consistent, reliable interpretation, regardless of analyst experience or location.

Exabeam Nova expands on the capabilities of Exabeam Copilot, delivering a more intelligent, action-oriented approach to security operations. Integrated directly into the Threat Center TDIR workbench, it automatically generates detailed investigation

summaries, enabling analysts to assess and respond to threats faster. Using multiple APIs, advanced threat classification, and real-time data enrichment, Exabeam Nova distills complex detections into clear, actionable insights. Analysts gain a unified, context-rich view of alerts and cases without manually piecing together information. With features like proactive entity extraction, chronological attack timelines, and recommended remediation steps, this AI-driven agent empowers security teams to reduce alert fatigue and improve overall threat detection, investigation, and response efficiency.

While there are valid use cases for GenAI, it's not a universal solution. As companies promote AI for its own sake, it's imperative to evaluate what it truly delivers and how intelligently it's integrated into a product.

SIEM Built by Cybersecurity Professionals, for Cybersecurity Professionals

The New-Scale Platform stands apart because it's built by security experts for security professionals. Unlike enterprise software mega-vendors, Exabeam is a pure-play cybersecurity company. The Platform is state-of-the-art, cloud-native, and scalable—purpose-built for one goal: delivering TDIR excellence. Continuous innovation ensures the platform evolves with the industry, adding new features and capabilities every month to stay ahead of emerging threats.

The strength of Exabeam comes from its deep understanding of how security teams operate and the challenges they face. Solutions are designed to be user friendly, persona based, and workflow oriented, ensuring seamless integration into security operations. Exabeam also aligns with industry frameworks and best practices, such as MITRE ATT&CK®, offering guided process maps and prepackaged use cases to improve threat coverage and achieve strategic security outcomes.

The results speak for themselves. One leading SOC service provider reported a 70% reduction in log onboarding times—shrinking a process that once took months down to days. They also saw a 60% decrease in false alerts, a 50% improvement in mean time to acknowledge (MTA), and an 80% reduction in customer inquiries related to normal and abnormal behaviors.

Exabeam prioritizes transparency in pricing. New-Scale SIEM includes features that enable organizations to track consumption, making pay-as-you-ingest pricing more predictable, understandable, and fair.

In cybersecurity, knowledge is power. That means having complete, relevant data and insights at your fingertips, and understanding the budget and resources needed to manage risk effectively. Exabeam excels on both fronts, whereas Microsoft Sentinel falls short in versatility and visibility. In today's dynamic threat landscape, it bears repeating: What you don't know can hurt you—and it certainly will.

If you're using Microsoft Sentinel and struggling with limitations, Exabeam can augment your current deployment for improved value. And if you're ready to fully transition, Exabeam makes the process straightforward. Do you know how much a SIEM is truly costing your organization? If your vendor can't provide a complete and transparent answer, it's time to talk to one who can. Contact us today.

	Exabeam	Microsoft Sentinel
Notable Capability Differentiators		
EPS	1M+	1M+
# Integrations	549	85
# Pre-built Rules	1,800	450
# Pre-built Models	750	11
# MITRE ATT&CK® Techniques	101	87
# Parsers	7,937	<500
Detection Content		
Behavior-based Models to Detect Abnormalities	795+ Behavioral Models	61+ limited UEBA capabilities; may require custom rules or integration with external UEBA solution
Detection Rules to Detect Known Threats	1800+	Extensive pre-built rules for Microsoft products and services; 51+ limited rules for non-Microsoft data sources
Integrated Commercial-grade Threat Intelligence	✓	After setting up Sentinel, users may need to integrate threat intelligence manually; it doesn't come pre-configured.
Detection Content Mapped to Use Cases	✓	✓
Investigative Automation		
Automatically Generated Threat Timelines	✓	~
ML-based Alert Prioritization	✓	Built-in prioritization based on severity and other factors
Pre-built Watchlists for Risky Users and Entities	✓	Limited watchlist functionality; may require custom queries
Granular Risk-based Scoring	✓	Limited risk scoring capabilities

	Exabeam	Microsoft Sentinel
Log Management		
Self-service Data Collection Interface	✓	✓
Search Query Builder Assistant	✓	✗
Up to 10 Years of Searchable	✓	Depends on storage
Data Without Rehydration		Configuration
Deployment Architecture		
Fully Cloud Native	✓	✓
Integrated SIEM + UEBA + SOAR	✓	Not natively built

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 →