eBOOK

Optimizing SecOps Costs in 3 Steps

Maximize Security Value, Minimize Costs

Expanded connectivity demands advanced protection

Balancing risk reduction and the cost of cybersecurity challenges every CISO. Data costs associated with security information event management (SIEM) systems are frequently at the center of this balancing act.

If SIEM data ingestion is not properly managed, the costs can be unpredictable and can become excessive. Unfortunately, it can be difficult to determine which logs are worth the cost of ingestion from a security point of view, and the ongoing task of managing ingestion costs is tedious and difficult.

SIEMs aren't inherently expensive. But they can be costly if you don't pay attention to the value of the data you're ingesting and how you're storing and managing it. Organizations who use Microsoft Sentinel in conjunction with Ontinue's SecOps Cost Optimization capabilities can eliminate the guesswork – and can reduce your security data costs by 50%.

Organizations can also control the TCO of Sentinel over the life of their Microsoft security program if they review several key aspects of their data management:

Consider your data ingestion priorities:
Think about the log sources and look closely at those you're monitoring for detection and response telemetry, versus those you ingest for compliance purposes.

Store and manage Sentinel data where it makes sense:
Storing everything in log analytics can provide the most flexibility and, as the name implies, analytical capability. But it's overkill for many log sources. Knowing which logs to store in more cost-effective locations can save your organization significant cost while maintaining security efficacy.

Ingest only the data you need into Sentinel:
It's key to monitor all security-relevant signals. However, ingesting every possible log source can be expensive and get noisy as well, slowing down operations without adding security value.

Incorporate cost-monitoring into your regular routine:
As data usage and workflows evolve, it's critical to keep a watchful eye on data costs. Changes to your environment, updates to security controls, and the incorporation of new controls into your security posture can all impact your data ingestion costs. You can't just "set it and forget it."

By continually monitoring the signals that Sentinel ingests and analyzing their respective cost and security value, you can improve threat detection and response while keeping your security data costs under control. The reality, however, is that few organizations have the time to devote to manually tracking data ingestion rates at a granular level, or the expertise to evaluate how to tune them.

Controlling SecOps costs through Sentinel optimization

Modern MXDR providers are responsible for optimizing all aspects of their customers' security programs, and that includes optimizing security cost. For Microsoft security customers, data ingestion costs often make up a significant portion of the overall cost of a security program. As the MXDR service of choice for Microsoft security customers, only Ontinue ION has a suite of unrivaled capabilities that enable customers to predict, optimize and manage Microsoft Sentinel spend – while upholding security.

Ontinue ION ensures you get the most security value for every dollar you spend, whether you're considering adopting Microsoft Sentinel or want to optimize your existing implementation. ION helps you understand your Sentinel costs and optimize your data ingestion to ensure your TCO doesn't outpace the security value your solution delivers.

Here's how it works:

1. Optimize

During the onboarding process, we provide an optimized estimate of your projected costs. This estimate is based on your environment and the telemetry required for continuous threat detection and response with the Ontinue ION MXDR service. Our Sentinel experts configure Sentinel ingestion optimized for security and value based on your key requirements and budget.

2. Manage

As part of the Ontinue ION MXDR service, your designated Cyber Advisor regularly analyzes your data ingestion costs against the security relevance of the log sources and provides optimization recommendations for your environment. With regular tuning of Microsoft Sentinel ingestion, your organization gains the highest cost efficiencies.

3. Monitor

The Ontinue ION platform provides a convenient dashboard for continuous visibility into Sentinel cost and data usage, allowing you to easily identify and respond to spikes and dips in cost over time. Ontinue Cost Anomaly Detection delivers active monitoring and alerting on deviations in Microsoft Sentinel costs based on user-defined thresholds—so organizations can respond to data spikes before they turn into unexpected bills at the end of the month.

Key questions to ask about your data

While you may be tempted to ingest as much data as possible, as previously discussed, it's neither feasible nor advisable. Instead, consider these questions to help your team focus on the data that matters to your security operation.

What data should be ingested into Sentinel?

Monitoring all security-relevant signals is key, but ingesting every possible log source gets expensive and noisy. Ingest only the signals that add security value.

Why are we ingesting the data that we are?

To manage data effectively, you need to understand what you're currently monitoring or plan to monitor. What sources are you monitoring for detection and response telemetry? What are you ingesting for compliance purposes?

How are we storing and managing our Sentinel data?

Storing everything in log analytics can provide the most flexibility and analytical capability, but in some cases it's not necessary. Microsoft provides other ways to store logs that, if used judiciously, can save significant money without affecting security efficacy.

How do we manage costs on a day-to-day basis?

As data usage and workflows evolve, it's critical to keep a watchful eye on data costs. Take an active role in managing your costs.

Are we taking advantage of all free data sources that apply to our organization?

Microsoft offers multiple free alert and log sources in Sentinel. Make sure you understand what they are, their insights and limitations, and take advantage of them where possible.

Are we in the right pricing tier?

By paying attention to your data usage and ensuring you're in the pricing tier that matches your needs, you can save a great deal of money.

Putting our Microsoft expertise to work

Managing Microsoft Sentinel costs is key to getting the most out of the Microsoft Security product portfolio. You need to maximize the security value of your data without letting costs spiral out of control.

That's why Ontinue has developed the suite of SecOps Cost Optimization capabilities to help you evaluate, manage, and monitor your Sentinel costs. Only Ontinue has the expertise to ensure you get the most value out of every dollar you spend on the Microsoft Security product portfolio.

Request a SecOps Cost Optimization demo

Ready to see how you can lower your Sentinel costs? We're here to show you.

REQUEST A DEMO

LEARN MORE

Ontinue

Ontinue ION is the MXDR service of choice for Microsoft security customers that want to accelerate MTTR, proactively reduce risk, and reduce costs. ION combines a cloud-native platform, AI-driven automation, and designated security and Microsoft expertise to get faster at detection and response, prevent threats, and optimize Microsoft security tools.