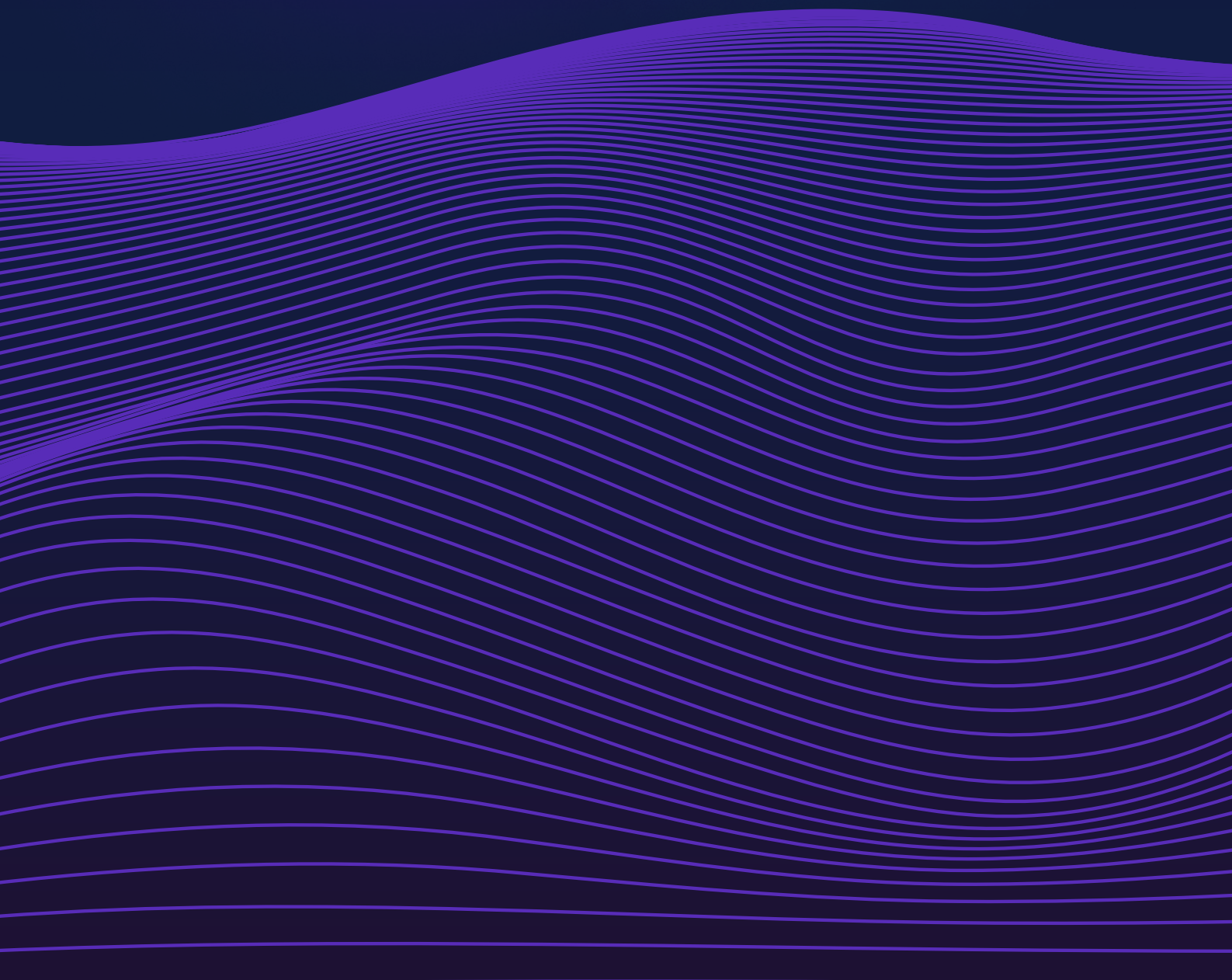
observo.ai

Whitepaper

The Easiest Way to Add or Evaluate a New SIEM

This paper will discuss how an AI-Powered Observability Pipeline, like Observo AI, can give you the freedom to choose the right mix of tools to protect your organization from cyber threats and continue to earn the trust of your customers.



INTRODUCTION

Organizations face an ever-growing array of threats that can compromise their data, operations, and reputation and erode the trust of their customers. To mitigate these risks effectively, organizations rely on robust Security Information and Event Management (SIEM) solutions. A comprehensive SIEM serves as the cornerstone of an organization's security infrastructure, helps manage risk effectively, and enhances its overall security posture.

Whether you are selecting a SIEM for the first time or considering adding or switching to a new SIEM, you must consider how your needs may evolve over the next several years.

This paper will discuss how an AI-Powered Observability Pipeline, like Observo AI, can give you the freedom to choose the right mix of tools to protect your organization from cyber threats and continue to earn the trust of your customers.

THE VALUE OF THE RIGHT SIEM

SIEMs are powerful tools responsible for enabling the detection of threats, efficient management of logs, insightful data visualization, proactive incident response, and adherence to regulatory requirements and industry standards. Moreover, a well-implemented SIEM empowers organizations to manage risk effectively, generate insightful reports, and maximize their security posture. Comprehensive SIEM platforms have many of these core features:

Detect Threats

A SIEM's primary function is to detect and protect against potential security threats in real time. By aggregating and correlating data from various sources, including network devices, servers, endpoints, and applications, an SIEM can identify suspicious activities, unauthorized access attempts, malware infections, and other security incidents. Many use AI to study patterns to surface these threats.

Log Management

SIEM solutions streamline log management processes by collecting, normalizing, and centralizing logs from disparate sources. This centralized approach enhances visibility into the organization's IT environment, enabling security teams to analyze logs efficiently and identify anomalies that may indicate security breaches or compliance violations. Examples include security event logs, firewall logs, VPC flow logs, Windows/Linux event logs, SSO logs, and others.

Data Visualization

Data visualization is crucial for turning raw

security data into actionable insights. SIEM platforms offer advanced visualization tools and dashboards that enable security analysts to visualize security events, trends, and patterns intuitively. By seeing how the environment is changing, security teams can make data-driven decisions and gain a comprehensive understanding of the organization's security posture.

Respond to Incidents and Alerts

A SIEM automates the detection, prioritization, and remediation of security incidents. By correlating security events in real-time and generating alerts, SIEM solutions empower security teams to respond to potential threats, minimizing the impact of security breaches and reducing incident response times.

Compliance with Legal Requirements and Industry Standards

Compliance with regulatory requirements and industry standards is a top priority for many organizations. SIEM solutions help organizations maintain compliance by providing real-time monitoring, audit trails, and reporting capabilities that align with regulatory mandates such as GDPR, HIPAA, PCI DSS, and SOC 2.

Improve Security Posture

> Ultimately, the goal of a SIEM solution is to enhance the organization's overall security posture.

By integrating advanced threat detection, incident response, and compliance management capabilities, SIEM platforms help organizations detect and respond to security threats more effectively, reduce the risk of data breaches, and safeguard critical assets. This helps you retain your customers' trust.

THE PERILS OF VENDOR LOCK-IN WITH SIEM TOOLS

Vendor lock-in is real. Vendor lock-in occurs when organizations become overly dependent on a particular SIEM vendor's technology, making it challenging to switch to alternative solutions. Vendor lock-in can restrict organizations' flexibility, limit innovation, and increase reliance on a single vendor for security needs. It can be hard to change, and vendors know that. SIEM vendors are aware of the challenges associated with switching solutions, and they may leverage this knowledge to retain customers and increase prices.

Some SIEM vendors may have little incentive to innovate or improve their products, knowing that customers face significant barriers to switching solutions. This lack of competition can result in stagnant product development and higher prices for customers. This is commonplace with established SIEM vendors resting on the laurels of their past success.

At the same time, most companies are seeing an annual increase of 25-50% or more in telemetry data for Security and DevOps teams. The exponential growth of data further exacerbates the challenges of vendor lock-in. As organizations generate increasing volumes of security data from diverse sources, the complexity and cost of managing this data within a single SIEM platform can become unsustainable. This can also force organizations

to deal with daily-ingest limit overage fees, which can get expensive very quickly. When it's time to renegotiate license renewals, these teams often face steep cost increases corresponding with this increase in data.

Ultimately, the only leverage organizations have regarding vendor lock-in is the option to switch SIEM vendors. By exploring alternative solutions, organizations can exert pressure on vendors to get better pricing and influence feature development if several customers have the same requirements.

WHY SWITCHING SIEMS CAN BE DIFFICULT

Selecting a new SIEM solution requires careful evaluation of functionalities, performance, scalability, and vendor support. Evaluating multiple vendors and conducting thorough proof-of-concept tests can be time-consuming and resource-intensive. SIEM platforms typically require that specialized agents or collectors are deployed across potentially thousands of applications, servers, and other endpoints: This can be a huge undertaking and derail evaluating a new SIEM because organizations don't know whether a new SIEM will meet its requirements given its unique data and environment.

Transitioning to a new SIEM solution requires thorough testing, configuration, and validation to ensure compatibility and functionality. This process can be time-consuming, particularly when migrating large volumes of data and reconfiguring integrations with existing security tools and workflows. A lack of proactive planning and preparation can prolong the SIEM migration process, leading organizations to recommit to their current vendor to avoid gaps in security coverage. The cycle starts over again and the lock tightens.

AI-POWERED OBSERVABILITY PIPELINE MAKES IT EASY TO EVALUATE AND SWITCH TO A NEW SIEM

> Observo AI enables organizations to leverage existing data without adding new agents or collectors.

Re-use all of the data you have. By transforming data from any source, including existing SIEM agents, Observo ensures seamless integration with new platforms, enabling organizations to preserve historical data.

You don't need to add new agents. Unlike traditional SIEM migration approaches that require deploying additional agents and collectors, Observo AI eliminates the need for agent-based data collection. By leveraging its AI-powered capabilities, Observo AI streamlines data ingestion, parsing, normalization, and transformation, for a faster more seamless migration. Observo AI de-couples data ingestion, optimization, and enrichment from the detection and analytics layer which provides a great deal of flexibility.

Observo AI transforms data from any source, including your existing agents, into the schemas used by any SIEM platform. Observo AI converts data from diverse sources into formats compatible with the target SIEM platform's schemas. This flexibility ensures seamless data integration and facilitates interoperability

between disparate systems, simplifying the migration process.

Add new sources as you go for a more complete picture of your enterprise security. Observo AI allows organizations to add new data sources incrementally as needed. This approach enables organizations to adapt to evolving security requirements and incorporate additional telemetry data sources without disrupting ongoing operations. If you aren't analyzing all of the right data, you may have security blind spots. Observo AI makes it affordable and effortless to add new sources that otherwise may seem too verbose or incompatible to analyze with any SIEM.

Create a bake-off to evaluate a new SIEM. Observo AI helps you evaluate new SIEM solutions by forking data from the existing SIEM platform and routing it to the new SIEM in real-time. This enables organizations to compare the efficacy, performance, and functionality of different SIEM solutions in a controlled environment. Compare alerting, feedback, and investigative capabilities with the existing SIEM platform.

> By ensuring feature parity (or superiority) between the two environments, organizations can make informed decisions about adopting a new SIEM.

When you are ready to make a change, stop sending data to the incumbent tool and only send data to the new one. By redirecting data streams from the incumbent SIEM platform to the new SIEM in real-time, Observo AI ensures uninterrupted security monitoring and incident response, minimizing disruption and downtime.

Use Observo AI to control data volume to give you leverage in negotiating your next SIEM license agreement. Observo AI optimizes data to control data volume and reduce uninteresting data sent to the SIEM platform. Observo AI can reduce data volume sent to the SIEM platform by up to 80% or more, minimizing storage costs and improving SIEM performance. By prioritizing relevant data and summarizing normal data, Observo AI ensures that only actionable security insights are sent to the SIEM platform, enhancing operational efficiency, reducing storage overhead, and providing organizations with leverage in negotiating license agreements with SIEM vendors.

Make new SIEM more effective - faster incident response times. Observo AI adds a lot of valuable context to data in the stream which improves how quickly they can identify and resolve critical issues. By enriching data with sentiment analysis, which identifies anomalies and separates them from run-of-the-mill alerts, security teams can prioritize which items need immediate attention. Solving the problem of alert fatigue makes sure your teams focus on what matters most.

Summarize "normal data" that is not interesting to downstream SIEM tools. Observo AI summarizes normal data that is not relevant to downstream SIEM tools, reducing storage overhead and improving data analysis efficiency. By prioritizing security-relevant data and summarizing routine events, Observo AI enhances SIEM performance and facilitates more accurate threat detection and incident response.

Creating a security data lake for long-term retention gives you the flexibility to switch SIEMs without losing archival information. Creating a security data lake ensures continuity and flexibility during SIEM migrations. Observo AI can rehydrate data on demand so organizations can retrieve and format archived data for analysis and reporting in any downstream tool. Observo AI enhances compliance, forensic investigations, and historical analysis, even after transitioning to a new SIEM platform. Most SIEM queries are on data from the last 48 hours. Storage cost for block storage in the SIEM index can be 100 times more expensive than storing in Parquet in low-cost cloud storage. Bloated indexes also require a lot more compute expenses. Consider the needle in a haystack puzzle - the bigger the haystack the longer it takes to find the needle - adding more resources can speed up the search, but it costs more money - the same is true with trying to search through a large SIEM Index.

A better approach is to save a copy of full fidelity data in a security data lake and drop data from the SIEM index after a month or even 1-2 weeks.

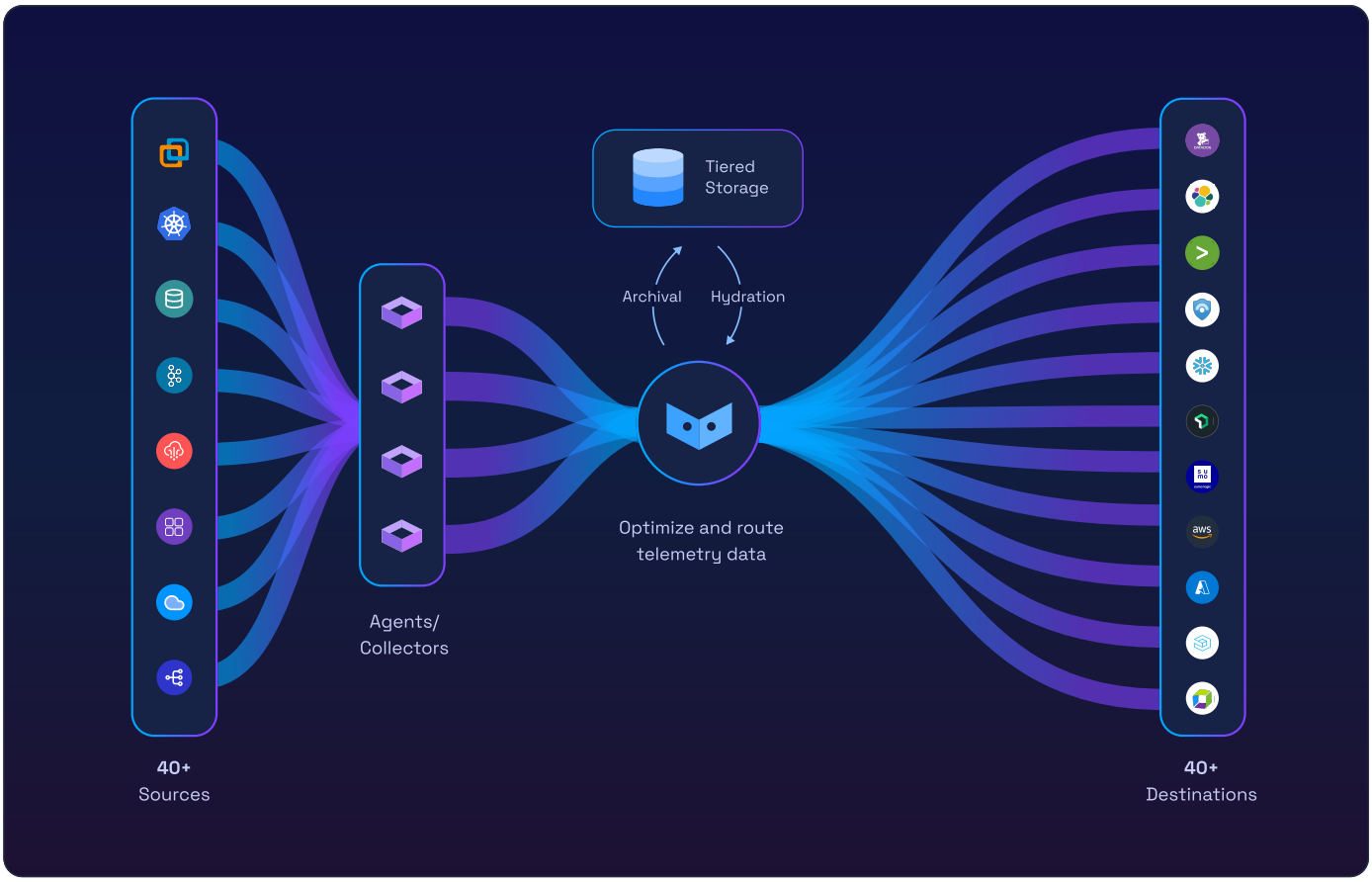
> Observo AI can always retrieve, rehydrate, and send any older data back to your SIEM for later investigation on-demand, no matter which SIEM(s) you use.

Make your security data lake searchable and stay in compliance with PII. Another advantage of using Parquet format is that is is fully searchable and Observo AI lets you use natural queries to look for relevant data - this means you don't need to have a data scientist to understand the complexities of how the data is stored so anyone can draw insights and with a single click resend a subset of data to your SIEM.

Observo AI also protects PII data by detecting it and automatically masking or hashing it even when it's in an unexpected location. Protecting this information not only helps you stay in compliance with regulations and industry standards, it also helps you maintain the trust of your customers.

Focus security team on threat detection and response. Observo AI helps teams focus on the work that is in their actual job description. It eliminates the need to write and maintain scripts to do some of this same work manually. Automating data handling and filtering puts time back in the hands of your security team and makes them much more productive.

USING OBSERVO AI TO ROUTE DATA TO MULTIPLE SIEM AND OBSERVABILITY PLATFORMS



Different teams may want to use different tools. Observo AI provides organizations with the flexibility to route data to multiple SIEM and Observability platforms, catering to the diverse needs of security and IT teams. By supporting disparate tools and platforms, Observo AI enables organizations to leverage best-of-breed solutions and address specific security and operational requirements.

Observo AI ensures that the most important security data is routed to higher-cost SIEM platforms, maximizing the value of investment in premium security solutions. By directing lower-value data to lower-cost tools and platforms, you get all of the signals you need from your data while staying within your tight budget.

Whenever your needs change, switch downstream tools on the fly. The Smart Routing features of Observo AI enable organizations to adapt quickly to changing security requirements and operational priorities.

CONCLUSION

SIEMs are very valuable tools for improving security, but with escalating data growth they can become very expensive very quickly. Vendor lock-in with SIEM platforms is real and can leave you with escalating costs, a lack of innovation, and no flexibility to change with the needs of your business. Without the right tools, switching SIEM platforms can be challenging - expensive, labor-intensive, and time-consuming.

An AI-Powered Observability Pipeline, like Observo AI can make it much easier to evaluate a new tool and make switching seamless. Use the data you have now without having to add agents or collectors across thousands of endpoints. Observo AI gives you the flexibility to use multiple SIEM and Log Management platforms to address both security and observability objectives. Observo AI gives you the power to use whichever tools best fit your needs. Take back control of your SIEM licenses, save as much as 50% on total security costs, and improve the security of your organization.

If you think we can help elevate your observability efforts with our industry-leading AI-powered observability pipeline, contact us at **info@observo.ai**