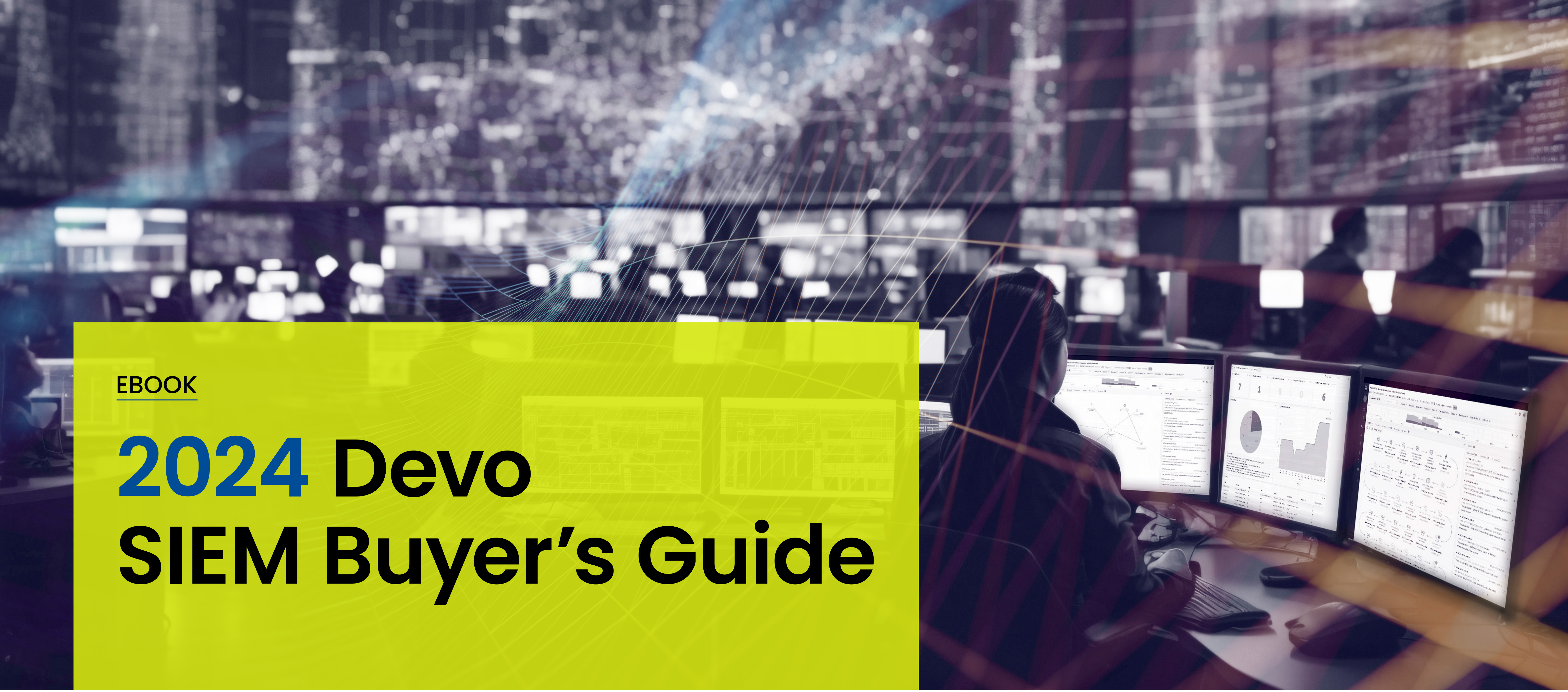


EBOOK

2024 Devo SIEM Buyer’s Guide

DEVO

INTRODUCTION

The role of SIEMs, a mainstay in security operations centers (SOCs) for over 15 years, has undergone significant expansion. This evolution is in response to the rising sophistication of attacks, the increasing complexity of technology, broader compliance mandates, and the disastrous consequences of data breaches and ransomware. The shift to hybrid and multicloud environments, coupled with SaaS adoption and the rise of mobile and remote work, has further exacerbated these challenges by inundating SOCs with a deluge of security data.

Traditional SIEM solutions designed without a data-at-scale mindset struggle with diverse data sources and an increasing volume of events. **Their inability to simultaneously ingest and analyze these vast amounts of data leads to vulnerabilities that attackers can exploit.**

As the attack surface expands and budgets shrink, the conventional strategy of incremental enhancements, such as upgrading hardware and increasing computing power, is inadequate. And until the underlying data problem is solved, the potential of AI will remain out of reach for SOCs due to its need to train models on extensive datasets.

It's clear that traditional SIEMs have been stretched well beyond their limits, both in terms of performance and cost-effectiveness.

As a result, a new breed of SIEM—**the security data platform**—has emerged, offering a more advanced, scalable, and efficient solution to provide accurate and timely detection and handle the vast and varied nature of modern security data.

‹ Previous Section   Next Section ›

This Guide Covers Three Key Concepts

1. How to distinguish a security data platform from its older, less sophisticated predecessors
2. How to recognize the signs that it's time to move toward a security data platform
3. How to compare and evaluate solutions to choose the right one for your needs. As examples, we'll compare Devo Security Data Platform to four distinct market categories in the SIEM space:

Traditional SIEM deployed in the cloud

E.g., Elastic, IBM, LogRhythm, Splunk

Cloud-provider SIEM + a data lake

E.g., Google Chronicle, Microsoft Sentinel

SIEM bundled with other vendor-specific tools

E.g., Crowdstrike, Palo Alto Networks

SIEM optimized for a single use case

E.g., Exabeam, Securonix

Previous Section   Next Section

Traditional SIEMs Can't Keep Pace. The Security Data Platform Drives SOC Success.

Traditional SIEMs force enterprises to make compromise after compromise. But the hard truth remains that too much compromise increases the risk of having your critical data compromised. Look no further than the 2023 cyberattacks, including MGM, Clorox, and the abuse of the zero-day exploit in Progress Software's MOVEit enterprise file transfer tool, to see the stark reality of being unable to detect attackers quickly and respond before the damage is done. Traditional SIEM technology does not work at scale against modern attacks, limiting your team's ability to respond with speed to halt these disruptive attacks.

The types of compromises organizations make regarding security data include:

How much security data they collect	If the SOC doesn't collect all relevant security data, it won't have the context and supporting information to identify and detect malicious activity.
Which log sources they ingest	Being too selective on security data sources creates a situation where the SOC can't correlate and substantiate attacks because relevant data isn't analyzed.
How long you store the data	Not storing security data long enough means the SOC may miss attacks from patient attackers that stage their campaigns over many months.
What types of analytics are performed on data	Constraints on the analytical techniques used for performance reasons means the SOC may be unable to detect sophisticated attacks because the SIEM cannot perform the required analysis.

Make the wrong choices, and you will miss an important attack indicator.

The pragmatic answer is to address the root cause of the issue and implement a platform that can keep pace with modern attacks and increase the team's ability to respond effectively and efficiently. **The answer is a security data platform**.

Previous Section   Next Section

THE VALUE OF A SECURITY DATA PLATFORM

Previous Section Next Section

According to Gartner, security information and event management (SIEM) technology is used for threat detection, investigation, compliance, and security incident management by collecting and analyzing (both near-real-time and historical) security events, along with many other events and contextual data sources. But as security data has grown exponentially, traditional SIEM doesn't cut it.

To keep pace with today's requirements and ensure the ability to handle tomorrow's, SIEMs must take a security data-first approach. This means simultaneously ingesting and analyzing these vast amounts of security data to ensure threats are detected in time. The only way to do this is to build a SIEM on a security data platform.

The key characteristics of a security data platform are:

1. **Ingests all data at any scale:** The ability to ingest all data at any scale is a fundamental requirement of a security data platform, as it directly addresses the challenges of managing vast and varied data streams and ensures reliability as security data grows. Supporting all quantities and forms of data is crucial to fuel robust security analytics and intelligence, which is essential for enterprises dealing with diverse adversaries.

2. **Real-time alerts and analytics:** Receiving real-time alerts and analytics from the security data platform provides a significant advantage for enterprises, enabling them to detect and respond to security threats instantly. This immediacy is vital in a landscape where even a five-minute delay can lead to substantial data breaches or system compromises, negatively impacting corporate assets and reputation.

3. **Unrestricted real-time and historical data access:** Access to all data over any time period without lag ensures security teams can stay ahead of attackers. It makes it possible to understand all threats, even those that began over a year ago. It also allows security teams to seamlessly use their data without ever needing first to ask, "Do I have access to that data?" This empowers enterprises to be proactive in their security strategies, hunt for potential threats, and leverage security data to adapt defenses as new challenges arise.

4. **A broad set of analytics and use cases:** The security data platform should offer a wide spectrum of tools and functionalities to tackle various security challenges. This versatility ensures that the platform can be customized to meet an enterprise's specific use cases, whether for basic threat detection or advanced predictive analysis.

5. **No operational responsibilities:** Gone are the days of dedicating multiple people to keep the SIEM available and operating efficiently. The security team should focus on deriving value from the security data platform rather than maintaining it. Modern security data platforms must handle operational responsibilities, providing transparent scale and always-on availability. This reduces hardware, software, and personnel costs and allows enterprises to focus their scarce resources on strategic activities.

All paths do not lead to the security data platform

Traditional SIEM issues are well understood, so many vendors are positioning themselves as the solution. The reality is these alternatives require the same kinds of compromises as traditional, on-prem SIEMs. Let's take a look at the general categories of market entrants:

1. **Traditional SIEM deployed in the cloud** (*E.g., Elastic, IBM, LogRhythm, Splunk*): Traditional SIEM providers have a long history, but their legacy architectures can't operate in today's cloud environments, leading to performance and scalability issues and requiring significant ongoing back-end data management resources in terms of equipment and personnel.

2. **Cloud-provider SIEM + a data lake** (*E.g., Google Chronicle, Microsoft Sentinel*): These solutions are better suited when all telemetry resides within the cloud provider's walled garden. The proprietary nature of these systems locks you into their solution, which is challenging in an increasingly multicloud world. The SIEMs provide delayed alerts due to batch processing of log records and use a general-purpose data warehouse unsuited for real-time analytics, causing latency in detecting attacks and handling threats – effectively giving your attackers a head start. Finally, the pricing model drives up costs to collect, store, and analyze third-party data.

3. **SIEM bundled with other vendor-specific tools** (*E.g., Crowdstrike, Palo Alto Networks*): Broad security platform vendors offer the convenience of a single-vendor solution but aren't built for organizations with a heterogeneous infrastructure. Additionally, their offerings are relatively new to the market and don't have a track record of SIEM success or scale. They are built on open-source search capabilities with known limitations and offer limited analytic capabilities.

4. **SIEM optimized for a single use case** (*E.g., Exabeam, Securonix*): These SIEMs typically started as a UEBA offering and have expanded into SIEM, and as a result, these tools are not well suited to satisfy a wide breadth of use cases, cannot support real-time analytics, and suffer from scale and reliability issues.

You need a purpose-built security data platform

The Devo Security Data Platform is powered by HyperStream, a proprietary, real-time data analytics engine. Providing limitless visibility by ingesting data from any source at any volume, HyperStream drives the integrated security capabilities of our platform – including advanced SIEM, SOAR, and UEBA.

Previous Section Next Section

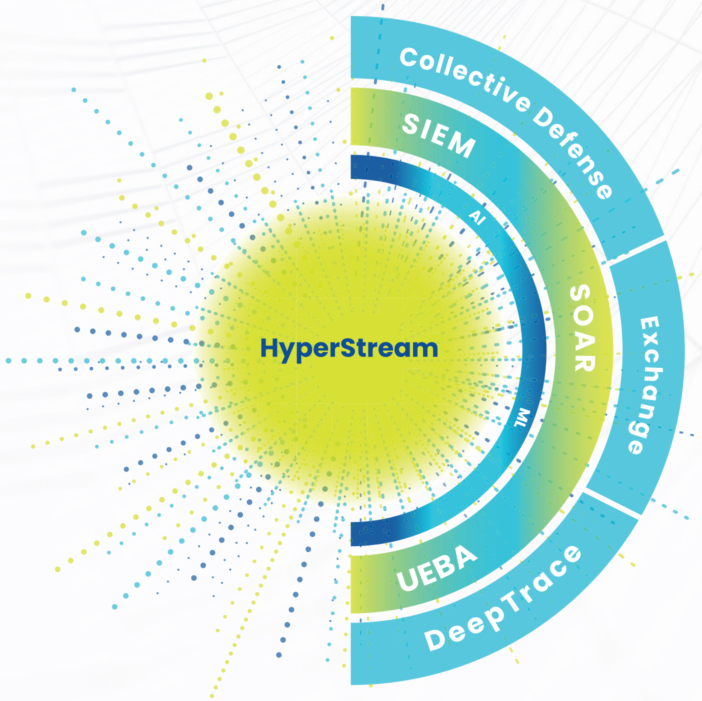
HyperStream enables innovation not available from any other SIEM, including:

a. **Autonomous investigations and threat hunting:** Devo DeepTrace uses AI to automate much of the investigative process for analysts, asking hundreds of thousands of questions in minutes to autonomously construct traces detailing an attacker's actions. It assembles the answers and timeline so analysts can get to the decisions and remediation work more quickly.

b. **Community-based intelligence sharing:** Devo Collective Defense uses ML to securely analyze alert data across the Devo community and identifies insights, trends, and Indicators of Compromise (IOCs) that are made available to Devo customers.

c. **Community-driven content marketplace:** Devo Exchange provides on-demand access to an ever-growing library of curated security content created by Devo, our partners, customers, and the greater security community.

Only Devo's Security Data Platform provides the security data-first architecture and capabilities that modern SOCs require. HyperStream handles data at any scale and unlocks greater efficiency for your team with advanced automation and AI-powered capabilities.



Previous Section   Next Section

SIEM vs. XDR vs. SOAR

SIEM vs. XDR: SIEM and XDR (extended detection and response) provide value in different but complementary ways. SIEM had its genesis in compliance and has evolved to serve as a broader threat detection and operational risk platform. XDR focused on endpoint threats and now provides a platform for deep threat detection and response across multiple environments, adding network and cloud telemetry. The solutions are not mutually exclusive. Rather, XDR solutions provide another robust security data source for SIEMs.

SIEM vs. SOAR: While SIEMs ingest various log and event data from on-premises and cloud data sources, SOARs (security orchestration, automation, and response) automate response path workflows to reduce the time required to handle alerts and investigations. The SIEM is the brain that provides the triggers, and the SOAR is the muscle that completes the work. Optimally, the SIEM and SOAR are integrated within a common platform to provide the best outcomes and user experience.

EVALUATION CRITERIA

Several criteria warrant consideration as you move forward in your journey to select a data-driven security analytics platform. These include:

Data ingestion at scale

Analytics across real-time use cases

Full suite of integrated capabilities

Flexible open architecture

Previous Section Next Section

Data Ingestion at Scale

Can the platform ingest more than 1 PB per day?

When evaluating data ingestion at scale for a security data platform, one of the critical factors is ensuring full visibility of all log data. Threats target an incredible variety of attack surfaces. Thus, you need a solution that can ingest any kind of event in any format and look for threats. You can't secure what you can't see.

The complexity and volume of security data continue to increase exponentially and show no signs of stopping. Centralizing all of this log data is essential for continuous monitoring and comprehensive analysis to maintain a robust security posture. Security teams need a unified view of their entire digital ecosystem, making it easier to identify patterns, anomalies, and potential threats that might be dispersed across various systems and clouds.

Look at data volume and accessibility

To evaluate the platform's scalability technically, look at how your SIEM stores data, indexes it, and the compression ratio of ingest to storage. Index-free access is one of the biggest advantages of a security data platform over its traditional predecessors. Indexing on ingest limits your access to the data until indexing is complete - which delays being able to use the data. The Devo Security Data Platform gives you access immediately, putting you closer to the attacker.

Pay attention to data storage efficiency, as you want more hot, searchable data. To identify low and slow attacks, you should be able to search year-old data as quickly and easily as data from last month. Access to historical data also pays dividends for compliance use cases. Similar to comparing the efficiency of two engines by looking at their power-to-weight ratio, you can compare SIEM efficiency and ability to scale by their compression ratio - how much data is stored compared to how much they ingest.

Here’s how SIEM providers stack up:

Traditional SIEM deployed in the cloud	Traditional SIEMs use various standard ingestion methods, most of which are fairly straightforward. However, they need to index data before it can be queried or alerted on, adversely impacting performance and mean time to detect (MTTD). In addition, the fixed data schema creates problems when log data formats change, negatively affecting data indexing. This can cause data gaps and break alerts until data is re-indexed, dramatically impacting a traditional SIEM’s agility.
Cloud-provider SIEM + a data lake	Data ingestion for cloud-provider SIEMs is relatively easy as long as the data comes from that same cloud provider. Other third-party sources require jumping through hoops, such as sending data via Syslog in a standard format like the common event format (CEF). Any non-CEF data must be converted to CEF before ingestion. This is a problem for custom application logs that change frequently, resulting in significant maintenance overhead and challenges in performing real-time analytics.
SIEM bundled with other vendor-specific tools	Security-platform vendor SIEMs are newer to the market, so they tend to have better scalability than traditional SIEMs. However, they still suffer from fixed data schemas, negatively impacting data indexing and searching. Also, consider the accuracy of the information coming from the system. Since data analysis tends to be on security platform logs, you may not see the full picture. Like cloud-provider SIEMs, they are optimized to work with data sources from their own ecosystem but don’t integrate as well with third-party sources.
SIEM optimized for a single use case	The UEBA platforms didn’t re-architect as they became SIEMs, resulting in scalability and stability issues. These tools tend to use cloud-provider native tools, inheriting the limitations of general-purpose ingestion and indexing capabilities, which are not optimized for security detection or reporting.

The Devo Security Data Platform is the ideal choice

The Devo Security Data Platform, powered by HyperStream, ensures you have the data you need at any scale. Devo ingests data with zero data transformation from any source, at any volume – with **proven success at 1PB per day peak ingest**. The proprietary HyperStream technology uses a nested file storage approach that enables a 10x data compression ratio, which uses less disk space and makes searching much faster. With Devo, you are better equipped to perform analytics that produce accurate results, enabling more effective decision-making and faster response times.

Understanding SIEM licensing

SIEM licensing typically falls into two categories: ingest-based and resource-based.

- Ingest-based licensing charges organizations based on the volume of data they ingest into the SIEM. This model offers predictability as costs scale with data volume growth.
- On the other hand, resource-based licensing depends on CPU, memory, and storage usage, providing potential cost savings but demanding careful resource management.

Understanding SIEM packaging is equally vital. SIEM vendors offer three main models: all-inclusive, pay-by-module, and discounted modules for certain data sources.

- The all-inclusive model provides organizations with SIEM, SOAR, and UEBA functionalities without tradeoffs, simplifying adoption and adaptation to evolving needs.
- Conversely, the pay-by-module approach lets you customize capabilities but can lead to considerable cost increases as you adopt new modules.
- Discounts on modules for specific data sources, often seen with Cloud Service Providers (CSPs), can create sticker shock when extending capabilities beyond the CSP’s offerings.

The key is to choose a vendor whose licensing aligns with your organization’s needs. Ingest-based models encompassing all functionality offer the best value for your investment. These models provide pricing predictability and allow organizations to scale their SIEM without the complexities associated with resource-based models.

< Previous Section   Next Section >

Analytics in Real-Time Across Use Cases

Does the platform reduce mean time to respond (MTTR) by 93%?

A key differentiator of a security data platform is its ability to conduct analytics without indexing data on ingest, which is essential for zero-lag streaming alerts and sub-second analytics. This enables analysts using the platform to stay ahead of attackers by storing the data raw as soon as it comes in, utilizing your compute resources on ingestion far more efficiently and enabling you to easily handle large spikes in incoming data. Even better, security data is available for analysis immediately, enabling instant identification and response to threats as they occur. In today's security world, even a 15-minute delay can make a critical difference between stopping an intrusion or letting it spread.

Is your data being parsed?

Contrast this approach with traditional SIEMs, which parse data on ingest. This entails receiving the raw log or event, putting it in a queue, breaking the data into a set of predefined fields, and finally indexing the data to make it searchable. This approach results in a delay between when the raw data is received and when it is parsed and indexed, creating "dead time," typically between 15 and 30 minutes, where no alerts or searches can occur. Another drawback of parsing on ingest is that large spikes of incoming data cause CPU contention and slow search performance—usually at the exact time you need to know what's happening.

Can you find anomalous activity as it's occurring?

With the data in the security data platform available immediately, solutions should incorporate integrated real-time behavioral analytics to identify anomalous activities, a key indicator of potential security threats. You want your SIEM to analyze and interpret vast amounts of diverse data to detect unusual patterns identifying sophisticated attacks, including those from insiders. Behavioral analysis is necessary for detecting known threats and uncovering subtle, unusual activities that could signify more complex, hidden, or emerging threats.

Can you quickly look back a year?

Many organizations face determined and patient attackers, meaning any SIEM must assess security data aggregated and analyzed from across the entire environment over extended timeframes. This extensive data analysis enables the platform to discern threat trends and pinpoint threat actor actions, providing a more in-depth understanding of the full scope of an attack.

Some SIEM vendors can't offer the same search performance for data 30, 90, 120, and 365 days old, if they can even store data for that length of time. If the SIEM stores older data in cold storage, it is largely meaningless from a detection standpoint. Slower search performance over a shorter timeframe of security data means slower investigations and longer response times.

Here's how others stack up:

Traditional SIEM deployed in the cloud	Traditional SIEM tools were not built with analytics in mind, so they tend to have bolted-on, inflexible analysis modules that don't provide real-time analysis. Their index-on-ingest approach also impacts accuracy, the scale of data that can be analyzed, and search performance.
Cloud-provider SIEM + a data lake	Cloud-provider SIEMs leverage general-purpose analysis capabilities, which are neither real-time – as data lakes do more batch-oriented analysis – nor optimized for security use cases.
SIEM bundled with other vendor-specific tools	Security-platform vendors take advantage of more modern architectures but leverage open-source analytics capabilities that aren't optimized for security detection.
SIEM optimized for a single use case	The UEBA platforms didn't re-architect as they became SIEMs, resulting in scalability and stability issues at scale. These tools tend to use cloud-provider native tools, inheriting the limitations of general-purpose ingestion and indexing capabilities, which are not optimized for security detection or reporting.

The Devo Security Data Platform is the ideal choice

The Devo Security Platform provides real-time analytics at scale. Devo's proprietary HyperStream technology makes data immediately searchable as soon as it hits the platform, so there are no delays between an event and when you can alert or search on it. Lightning-fast query performance means shorter query times, resulting in faster detection and investigations.

Built-in ML models detect anomalous behaviors, including insider risk, compromised credentials, cloud security, and network - going beyond other vendor's security analytics offerings. And the analytics are based on real-time data, not data collected 30 to 60 minutes prior. The whole point of security analytics is to detect attacks at machine speeds, not after a lengthy delay.

If you have the internal skills, Devo allows you to BYOML (Bring Your Own ML), supporting the use of custom-built models. Additionally, the availability of up to 400 days of always-hot searchable data makes it easier and faster to go back and conduct investigations to see the first occurrence of a threat in your environment.

‹ Previous Section   Next Section ›

Fully Integrated Capabilities

Are all features integrated to accelerate the analyst workflow?

Many organizations have dozens of security tools to manage, all with disparate user experiences, data models, and capabilities. It's hard for SOC analysts to ensure they're using the right tool at the right time to detect attacks. A security data platform should provide integrated capabilities to collectively enhance the platform's effectiveness in managing and responding to cyber threats.

How can you investigate attacks?

One of the fundamental capabilities SOC analysts need from a platform is the ability to build an attack timeline to construct the sequence of events during a cyberattack, providing a clear and detailed understanding of how an attack unfolded - at machine speed. This capability is invaluable for immediate response and future prevention strategies, as it helps identify the attack vectors used and the vulnerabilities exploited.

Can you automatically respond to threats?

A platform with broad security device support and AI-powered decision automation enables more efficient threat response and mitigation. SOAR capabilities allow for the automation of routine tasks and the orchestration of complex workflows across different security tools, streamlining security operations. AI-driven decision automation further speeds the response process, enabling faster and more accurate decision-making in the face of complex threats.

Do you have access to threat intelligence?

Integrated, out-of-the-box threat intelligence can help increase the productivity of experienced and junior analysts. Enriching log data with contextual information, such as a threat's origin, nature, and potential impact, enables faster and more informed decision-making.

< Previous Section   Next Section >

Can you identify gaps in coverage?

A platform that leverages the MITRE ATT&CK® framework to provide a clear and concise visualization of areas where the organization's security measures may be lacking allows for targeted improvements and strengthening of defenses. Integrating the MITRE ATT&CK framework also ensures that the platform's analytics are grounded in an industry-standard list of cyber threat tactics and techniques, enhancing its ability to identify and categorize threats accurately.

Can you optimize analyst workflows?

A platform that consolidates all necessary information and tools into a single, integrated user interface addresses the challenges of managing security in a piecemeal fashion. This integration is crucial for enabling analysts to work efficiently and effectively, reducing the time and effort required to switch between different tools and interfaces. A unified UI ensures that analysts have immediate access to all the data and tools they need, streamlining the analysis and response process.

Here’s how others stack up:

Traditional SIEM deployed in the cloud	Traditional SIEM providers take a piecemeal approach to their suite, offering modules to provide additional capabilities. This can be helpful if a customer doesn’t want an integrated experience but increases the learning curve for analysts, hinders their workflow, and requires additional management for every incremental tool.
Cloud-provider SIEM + a data lake	Cloud providers do not have all of the integrated capabilities of stand-alone platforms, nor are the capabilities particularly integrated, forcing a disjointed experience for SOC analysts. Additional modules and integrating data from third parties can also be very pricey in these offerings.
SIEM bundled with other vendor-specific tools	Security-platform vendors provide an integrated experience, given their platforms were built to provide multiple security functions. Yet these tools were built as an adjunct to their core security offerings so they could check a box, not as the primary capability. The flagship products get the bulk of the resources and new features because they pay the bills, while the SIEM functionality lags behind competitors.
SIEM optimized for a single use case	Single use case SIEMs started with detection and have lagged in adding capabilities. Organizations must determine if the focus on detection outweighs the missing capabilities of a broader suite.

The Devo Security Data Platform is the ideal choice

The Devo Security Data Platform offers comprehensive security capabilities in an integrated platform. In addition to SIEM, SOAR, and UEBA, Devo provides features that increase SOC performance and efficiency.

- **Devo DeepTrace** augments SOC analysts by autonomously investigating threats leveraging attack-tracing AI. DeepTrace asks hundreds of thousands of questions to build full attack traces in minutes, automatically giving analysts full visibility over the attack timeline and accelerating context-based decision-making.
- **Devo’s MITRE ATT&CK Adviser Application** has hundreds of rules built-in that map against the MITRE ATT&CK framework, providing a clear, visual indication of an organization’s security posture while pinpointing gaps in controls.
- **Devo Collective Defense** offers out-of-the-box, integrated threat intelligence that leverages knowledge of threat activity and trends across the Devo user community. Collective Defense is operational on day one and doesn’t require any manual setup, scripting, or coding.

Previous Section   Next Section

Flexible, Open Architecture

Does the SIEM play well with others?

When evaluating a security data platform, flexibility in data handling and an open architecture are crucial. These capabilities significantly enhance the platform's efficiency and adaptability in managing cybersecurity threats.

Does it support structured and unstructured data?

The most powerful platforms can handle structured and unstructured data without requiring data transformation or normalization. This is vital for a couple of reasons. First, it simplifies the data ingestion process, as data from various sources can be ingested in its original format. This reduces the workload and complexity of pre-processing data, ensuring that information is available for analysis more quickly and with less overhead. An open API capable of ingesting data at scale from all types of data sources further enhances a platform's ability to collect comprehensive security data. Second, by accommodating diverse data types and formats, the platform ensures comprehensive coverage of potential data sources, which is essential for thorough threat detection and analysis.

Can you seamlessly adjust your data ingestion?

Requiring data transformation and normalization causes problems with data ingestion. For example, migrating to a new firewall vendor or even upgrading to a new software version can affect the format of the data, which breaks the parser and results in lost data. This approach also leaves you with only the processed version of the data— not the original raw data. Once that occurs, you can never go back and parse the data differently or look for something your parser may have ignored. This can lead to dangerous oversights in your security posture.

Can you leverage knowledge from the security community?

Integrating community-sourced threat intelligence and detection methodologies can tap into a wider community's collective experience and expertise, leading to more effective and timely identification of new and evolving threats. You want access to a content marketplace that provides access to the SIEM vendor's content and content developed by other organizations that may see different attacks and face different adversaries.

‹ Previous Section Next Section ›

Does your SIEM play well with other technologies?

Your SIEM cannot operate in a vacuum. It must play well with the rest of your security ecosystem. And that security ecosystem is a two-way street. Your SIEM must be able to ingest data from firewalls, EDR, IPS/IDS, and your cloud environments. But it also must work seamlessly with the SOAR platform you use today and any other solutions you might adopt down the road.

Can you work with any cloud platform?

Support for workloads in any cloud platform is critical for companies with multicloud and hybrid cloud strategies. A platform that can cost-effectively aggregate data and operate seamlessly across different cloud environments provides significant advantages in terms of flexibility and scalability. For businesses that leverage multiple cloud services or plan to migrate between clouds, a cloud-agnostic security data platform is essential. This ensures consistent security monitoring and management across all cloud platforms, which is crucial for maintaining a strong and unified cybersecurity posture in a multicloud environment.

‹ Previous Section Next Section ›

Here's how others stack up:

Traditional SIEM deployed in the cloud	Traditional SIEMs have been around for decades and have well-established technical alliances. However, a library of connectors can't address a traditional platform's scalability and analytical limitations.
Cloud-provider SIEM + a data lake	Cloud providers are relatively new entrants into the SIEM market and, as such, lag in terms of partnerships. They also do not support multicloud environments, for obvious reasons. Additionally, generic data storage and analytics technology limits integration with other SOC tools.
SIEM bundled with other vendor-specific tools	Security-platform vendors typically compete with their partners, so although the partner list is long, the depth of integration can be limited and the partnerships are at arms-length, given that the platform vendor may acquire a competitor before long.
SIEM optimized for a single use case	Single use case SIEMs tend to be limited in terms of their API capabilities and technical partner program, and the general inflexibility of its platform doesn't lend itself to deep integrations.

The Devo Security Data Platform is the ideal choice

As an independent software vendor, Devo provides a truly open architecture and deep integrations with technical partners without worrying about competing with its own products and services. This independence provides enterprise SOCs with a full suite of integrated tools and a means to extend the security data platform's capabilities as needed.

a. Devo has a fully extensible API, and the Devo Exchange content marketplace provides access to Devo-created content and allows partners and customers to build and share custom alerts and applications.

b. HyperStream technology provides Devo's customers with the flexibility and scale to ingest data from virtually any source (cloud providers, on-prem sources, hybrid environments, etc.) in structured or unstructured formats without requiring transformation or normalization, making the data instantly available for analytics and reporting.

c. By indexing data at query time and NOT on ingestion, HyperStream preserves the original event in case you want to parse it differently in the future. This also makes Devo the most change-tolerant solution since changing data format does not impact ingestion.

d. Devo doesn't alter your raw data, so you can always extract the data in exactly the format and fidelity. Given most of your security data will be archived and stored for at least five years, having the raw data offers unique data integrity.

‹ Previous Section   Next Section ›

CONCLUSION:
THE DEVO SECURITY DATA PLATFORM IS THE IDEAL CHOICE

Previous Section

In today's rapidly evolving digital landscape, enterprises are navigating an increasingly complex environment. The surge in cloud adoption, alongside the proliferation of applications, has led to a substantial increase in the volume and variety of security data. This data explosion presents significant challenges for organizations striving to maintain a strong security posture.

In addition to these challenges, there is a pressing need to optimize operations—doing more with less. Enterprises are under constant pressure to enhance their security controls while simultaneously managing constraints in time, resources, and budget. This balancing act requires a strategic approach to security data management, one that can accommodate the growing complexity and scale of modern enterprise environments.

SIEM migration projects are both a significant investment and a commitment of resources. And it's not like you can put your SOC on ice while the migration happens, so you only want to migrate when you have a reason to.

Organizations are recognizing the limitations of traditional SIEM platforms. These rigid and inflexible systems struggle to keep pace with the dynamic requirements of modern enterprises, especially given rapid technological advancements and evolving cyber threats. There is a growing need for organizations to rethink their approach to SIEM. This reevaluation presents an opportunity to implement a strategic security data platform that meets current needs and has the scale and open architecture to handle future demands.

Your organization is counting on you to find the attackers before they cause damage and compromise data. To do that, you need a security data platform that ingests security data at scale, regardless of its source, and easily handles changes in data sources or schemas. Your team needs the ability to analyze data and detect attacks in real time to eliminate the blind spots in your environment and reduce your risk. Your team needs a platform with an open architecture that facilitates collaboration and the ability to adapt to dynamic attacks, not a product that perpetuates a siloed operational model. You need a platform that provides a broad set of integrated capabilities, allowing for more efficient and effective security operations.

With Devo, organizations can effectively address the challenges of managing security data in today's complex environments, ensuring robust protection against an ever-evolving array of cyber threats.

DEVO

Devo
3 Center Plaza
Suite 302
Boston, MA 02108

Devo unleashes the power of the SOC. The Devo Security Data Platform, powered by our HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence global enterprises need to defend expanding attack surfaces. An ally in keeping your organization secure, Devo combines the power of people and AI to augment security teams, leading to better insights and faster outcomes. Learn more at www.devo.com.

< Previous Section