Forgepoint

2025 Q2 Report

/ Forgepoint Forward /

What's Ahead in Security Log Data Management

Table of Contents

> *The architecture has collapsed: the ecosystem utilizes 18 different tools and costs hundreds of dollars per GB. How will you start to automate or improve the decision-making capabilities of a human when you're dealing with billions of events? Something must change: a disruptor needs to come in because the market is broken."*

George Webster

CEO, Ziggiz

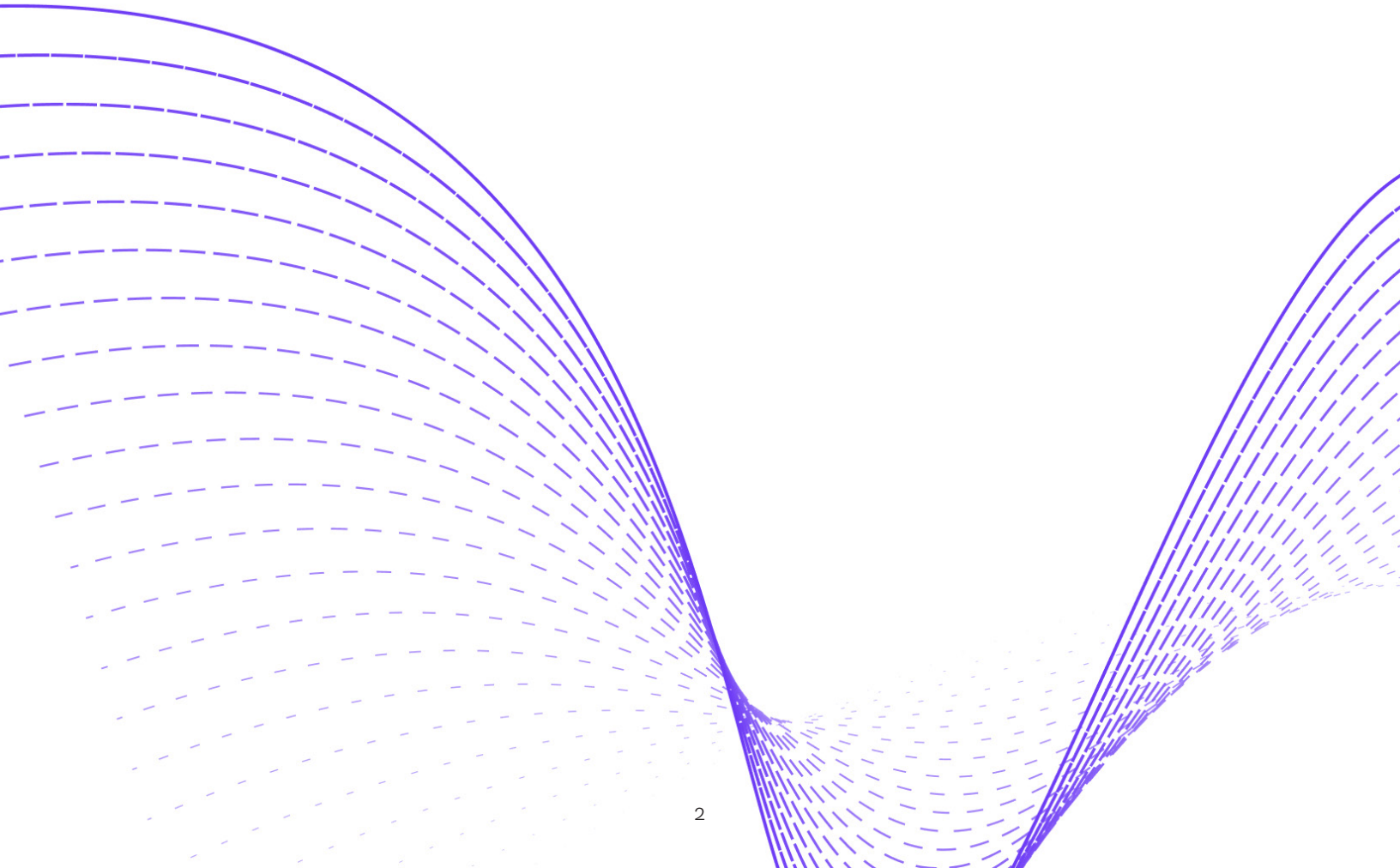
Introducing Forgepoint Forward

In today's rapidly evolving digital landscape, the role of cybersecurity has never been more critical. Modern companies navigate a complex threat environment, often relying upon big tech partners and legacy solutions, but still face critical security gaps. These gaps represent risks and opportunities – the linchpins of cybersecurity innovation, software development, and economic progress.

As longtime investors, operators, and company-builders with decades of experience in cybersecurity, the Forgepoint Capital team has the privilege of collaborating with a deep network of CISOs, CIOs, CEOs, industry experts, and national security leaders. These individuals are at the forefront of defending against cyber threats, implementing robust security postures, and fostering organizational and industry resilience.

What follows is the third edition of Forgepoint Forward, a series of quarterly reports on the most critical emerging spaces in cybersecurity. Forgepoint Forward presents our findings from extensive research and interviews with experts across our network- including our Global Advisory Council. Our goal is to highlight investment trends and market projections, as well as startups involved in promising areas, to identify key opportunities for entrepreneurs and the cybersecurity community.

We would like to extend our thanks to everyone in our community who shared their insights and contributed to this report. A full list of contributors can be found at the end of this report under Acknowledgements.



The State of Security Log Data Management

Log data is indispensable for security analytics and threat detection in the modern Security Operations Center (SOC). Security logs provide analysts a granular view of an organization's security posture via timestamped records of security events, system changes, and user access.

This information is generated across web and mail servers, complex IT and OT environments, on-premise and cloud environments, and various Endpoint or Network Detection and Response (EDR or NDR) tools. Log data is used in various security activities including event correlation, incident monitoring and response, suspicious user activity detection and monitoring, and compliance and audit report generation.

Faced with a rising number of disparate event sources, companies must manage an explosion of application, system, error, and security logs. Security logs have traditionally been sent to Security Information and Event Management (SIEM) platforms which enable security teams to query and analyze security data in real time. However, several factors are causing companies to reconsider the efficacy of SIEMs for log data management, including the expanding volume of security log data, costly SIEM platform prices, vendor lock-in, and high technical requirements for SIEM data analysis.[1]

Challenges

1) The explosion of log data has made managing data with SIEMs more challenging.

Companies have invested in more servers, firewalls, and data sources in response to increased demand for digital products and services. Subsequently, their desire to capture more data and perform advanced analytics has grown. The resulting boom of semi-structured data has made it more difficult for companies to comb through, normalize, and analyze billions of logs. One SIEM provider we spoke with reported an average of 20% YoY growth in the number of security logs ingested. The amount of data large enterprises ingest grows when they adopt new tools, move to the cloud, or pursue other technological changes.

This trend has also created overlaps between cybersecurity data storage and big data infrastructure. Enterprises typically place long-term data in 'cold storage' lakes such as Databricks or Snowflake for audit and compliance purposes and send active data to 'hot storage' SIEMs for correlation and analysis. However, it is not always clear where to route data in this mixed infrastructure format. For example, companies may send more security logs to generalized data lakes to circumvent the climbing costs of SIEMs. At the same time, despite their relative cost efficiency, non-security centric data lakes introduce barriers to scalability and accessing and running analytics with important data. The trade-off between cost savings and detection and analysis capabilities complicates data storage decisions.

As companies demand faster and more effective processing for a growing amount of data, there is an emerging need to automatically identify important data in-transit and reduce the volume of data sent to the SIEM.

2) SIEM costs are skyrocketing.

The cost of storing data in SIEMs is increasing alongside the explosion of data volume and variety and an acceleration of data processing speed. Most SIEMs are licensed largely based on the rate and volume of data ingested and the cost of processing—and based on our conversations with CISOs and senior executives, prices have steepened exponentially. Installation costs, infrastructure costs to handle SIEM bandwidth, and the costs of 24/7 staffing for real-time monitoring and response further compound this issue.[2]

For more reading, take a look at Forgepoint's Threat Intelligence Portfolio Spotlight #15, "How can companies strike a balanced approach to log management," which dives into the role of rising costs in leading to budget cuts and diminished security capabilities.[3]

With the post-COVID scramble to adopt cloud-native data storage and technologies, cloud storage and its associated logging configuration expenses can also be costly.

For some organizations, it is no longer financially viable to simply capture as much log data as possible in the SIEM. Instead, they must make critical decisions about what data should be filtered out during transport across both on-premise and on-cloud environments. Unfortunately, many organizations with tighter budgets are forced to exclude critical data, which can lead to a weaker security posture.

With the post-COVID scramble to adopt cloud-native data storage and technologies, cloud storage and its associated logging configuration expenses can also be costly.

For some organizations, it is no longer financially viable to simply capture as much log data as possible in the SIEM. Instead, they must make critical decisions about what data should be filtered out during transport across both on-premise and on-cloud environments. Unfortunately, many organizations with tighter budgets are forced to exclude critical data, which can lead to a weaker security posture.

> *"Organizations often sacrifice critical network visibility to reduce SIEM costs and inefficiencies. By eliminating the need to ingest network traffic into a SIEM, companies can regain full visibility, reduce costs, and benefit from extended data retention required for effective compliance, threat detection and response."*

Ricardo Villadiego

CEO & Founder, Lumu Technologies

This further underscores the need for companies to manage log volume by filtering relevant data during transport across both on-premise and in cloud environments.

3) Vendor lock-in makes it difficult to move on from expensive SIEMs.

SIEMs are notoriously difficult to rip and replace given the technical challenges and risks associated with downtime and configuration. Companies that run vendor-specific agents across servers and networks find breaking away from SIEMs even more difficult.

This has put innovation on the back burner as enterprises seek log management solutions which integrate with their current SIEM. Unsurprisingly, enterprise adoption of emerging log management technologies remains slow.

4) Security analysts require highly specialized skills to analyze log data.

Security analytics conducted at the SIEM level often require technical skills such as mastery of specialized programming languages like Search Processing Language (SPL) for Splunk. An industry-wide skills shortage and mounting alert fatigue and pressure on short-staffed SOCs have made effective security analytics even more difficult. These issues have ignited a call for SIEMs to support non-vendor specific rule languages and general-purpose analytics languages (SQL, Python) to construct detection rules.[4] Vendor-specific languages that incorporate transferable working knowledge from other widely used languages may also alleviate these problems.

Keep in mind that unformatted data also must be enriched by highly technical analysts. Tools that normalize data and unify a format between SIEMs and data lakes are invaluable to security analysts.

> *"The cost for cyber logs sent to the SIEM can be 10x higher than the cost in the retention realm, where the operational or business intelligence log is simply retained for auditors and not analyzed for security benefit."*
>
> 
>
> David Emerson
>
> CTO, SolCyber

Opportunity for SLDM Startups

These issues have opened a window of opportunity for startups we categorize as Security Log Data Management (SLDM) providers. These startups provide intermediary routing platforms which ingest data from multiple feeds, aggregate it, enrich it with intelligence, and transfer it to hot or cold storage based on tool-led or user-led routing rules.

1) Cost Benefit

The key benefit these providers offer is cost efficiency. Enterprises are eager to circumvent staggering and unsustainable projected SIEM costs and may spring for new solutions that correlate data and control the volume of data sent to the SIEM. Primarily serving the need to better manage data flows, these startups have positioned themselves for success by using cost reduction as an entry point into the market.

2) Improved Data Analysis Timing and Accessibility

Timing and accessibility are also important aspects of managing security log data. We see an opportunity for startups to bring capability-driven impact to their customers in this area. For example, some enterprises seek the ability to easily construct pipelines and routing rules while others look for innovative ways to enrich log data and shift analytical workloads away from the SIEM for specific use cases. SLDM platforms that provide better telemetry normalization across disparate tools, real-time data lookups, and cybersecurity-focused routing recommendations are likely to garner attention.

> *"The externalization of configuration is beneficial– it serves as an abstraction layer. You can now make security-focused decisions about what is being routed into security infrastructure. It is simpler and more delegable for the security team."*

David Emerson

CTO, SolCyber

3) User Interface / User Experience (UI/UX)

User interface / User Experience (UI/UX) is another critical opportunity for market entrants. Security analysts want practical ways to analyze data at the node or pipeline level with visualizations that are more intuitive and user-friendly than raw data in the SIEM. They prefer solutions that prioritize the most important queries to run on the infrastructure. They also want plug-and-play, easy to manage solutions that enable data security without requiring a data engineer's skillset.

What enterprises want from SLDM tools:

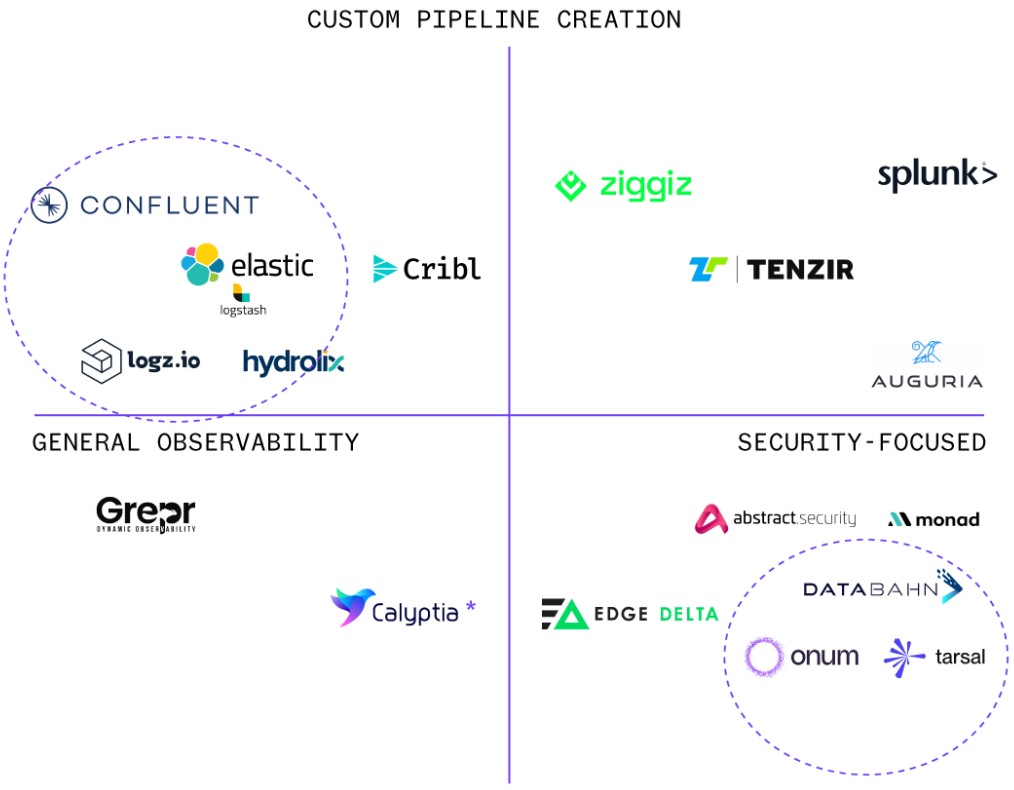
- Easy-to-manage tools that require less training and technical expertise compared to specialized analysts who code pipelines

- The ability to intelligently route logs between the SIEM and other data storage to optimize cost efficiency

Startups that meet enterprise needs across these three areas will help optimize SOCs and security team data management processes. We have mapped the current SLDM startup landscape below, categorized by commercial focus or target functionality.

SLDM Market Map

Teams that want to leverage both observability and security logs in a single pipeline may look to the left side of the matrix.



Larger enterprises with larger security teams often require highly customized pipeline creation.

Customers with less mature security teams may gravitate toward low-code pipeline creation with inbuilt identification logs beneficial for threat detection or analytics.

*acquired

The most appropriate quadrant for a buyer to focus on depends on the size of the enterprise and how they use log data. Larger enterprises tend to have bigger security teams with more time and resources to dedicate to coding pipelines and often require highly customized routing schema for complex infrastructure. As such, they may gravitate towards solutions in the two upper quadrants which enable more custom pipeline creation. Large enterprises with security teams that value security-specific tools might look to the solutions in the top right quadrant, while sophisticated teams that want to leverage both observability and security logs in a single pipeline may find solutions in the top left quadrant sufficient for their data management needs.

Down-market customers with less mature security teams may gravitate toward low-code or no-code pipeline construction tools to make the best use of their time, such as those in the two lower quadrants. They are also more likely to benefit from built-in guidance which helps them identify logs that can be used for threat detection or other security-focused analytics.

Trends

1) SIEMs are on SLDM Product Roadmaps

Some SLDM providers such as Edge Delta, Hydrolix, and Cribl are developing data storage solutions that can compete with legacy SIEMs. However, the maturity of legacy SIEM platforms and vendor lock-in difficulties have kept these startups from directly challenging legacy players.

It is not clear if there is an opening for these startups to displace legacy SIEM vendors. That said, the best opportunity for SLDM startups expanding into log storage and/or data lakes would likely be to target down-market customers without a SIEM or data lake solution.

> *Large companies often have years of investment in Splunk. Displacement is possible, but it is going to be expensive from a time investment perspective. It requires two platforms to run at the same time- use cases have to be moved over to a new platform one at a time."*

Jerry Kowalski

CISO, Jefferies

Meanwhile, legacy SIEM and data providers like Splunk, Elastic, and Confluent have begun to enter the SLDM space by adding and/or improving their routing capabilities. These legacy companies also offer these toolsets at a discount while adapting their licensing models to address customers' cost concerns. These measures, which are largely in response to the popularity of Cribl, create increased competition from trusted providers and may endanger newer SLDM entrants. Splunk notably engaged in a lawsuit against Cribl over alleged intellectual property theft in violation of the Digital Millenium Copyright Act (DMCA) and tortious interference in 2022, with mixed results. In 2024, a jury ruled that Cribl's use of Splunk's Enterprise software reverse engineer the Splunk to Splunk (S2S) protocol was lawful fair use under US copyright laws, but also that Cribl had violated the Splunk Enterprise copyright and general terms contract in other instances. Splunk sought $155M in damages but was only awarded $1.[5]

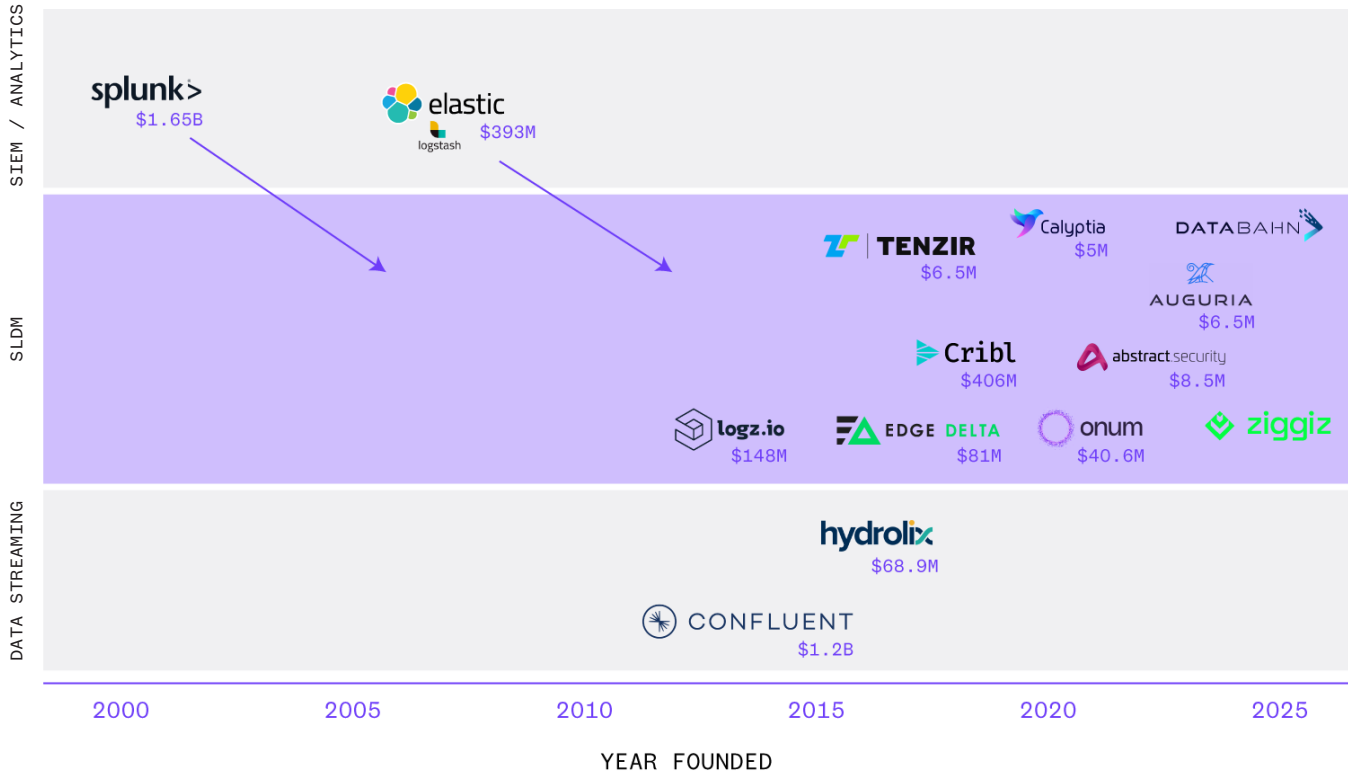
Startups will avoid eroded market share if they can pivot to differentiators beyond just log filtering. Persistent customer concerns about vendor lock-in may push larger enterprises toward a more agnostic and modular security architecture that utilizes both legacy SIEM for storage and separate SLDM or data management at the pipeline.

> *Logging strategy should be abstracted from the SIEM layer because the SIEM should be a customer of the logging facility, and only one of many tools ingesting logs."*

David Emerson

CTO, SolCyber

SLDM Total Amount Raised



2) Room for disruption amid Cribl's dominance

Cribl, now valued at $3.5B, has taken the lead in mindshare among newcomers in the SLDM space, if not in market share[6]. A significant number of enterprises looking for SLDM solutions have evaluated or are currently evaluating Cribl to reduce log data storage costs.

However, there are emerging concerns about Cribl's licensing model being too similar to legacy vendors and increases in pricing. The company also does not bring as much security context as compared to competitors, having originated as a generalized data routing platform. This may create an opportunity for other startups to enter this space and ultimately command market share. Other SLDM startups appear to be centering around stronger security-focused analytics and recommendations, customizable routing capabilities, cheaper price points, and more intuitive drag-and-drop style UI/UX. Differences in user interfaces correspond to different target audiences; certain platforms are oriented for larger teams of more technical security data analysts (Cribl, Tenzir and Auguria), whereas others create an integrated security focus in data routing and management and can be utilized by a smaller SOC with less specialized security experts (Databahn and Abstract Security).

While we believe there is an opportunity for new entrants and smaller players to gain traction and grow, Cribl's tool can still be augmented given the company's revenue and funding. Cribl is also quite far ahead in the number of destinations and integrations offered and appears to have mastered a tool which is simple and easy-to-use for security teams looking to build pipelines more efficiently.

3) Opportunity for small business and mid-market lift

We see the most opportunity for lift in the small business and mid-market segments: that is, customers with lower security budgets and smaller teams than enterprises but more sophisticated SOCs than SMBs. According to Gartner, the budget and expertise required to uphold a SIEM makes it especially expensive for midsize enterprises, who, with "low-maturity security operations and few, if any, staff specifically responsible for security operations, are especially challenged to maximize value from SIEM solutions."[7] As SLDM startups expand into the SIEM space, their target customers might be those without SIEM infrastructure in place because, as previously mentioned, vendor lock-in makes ripping and replacing existing SIEMs cost-ineffective.

> *"The effort to move SIEMs at a 5,000-person enterprise takes multiple years and millions of dollars. This amount of spent time and money for moderate cost savings does not make sense– the SIEM is a very difficult product to pull out [and replace]."*
>
> 
>
> Ramin Safai
>
> CISO, Point72 Ventures

> *"From working with hundreds of thousands of SMBs and the MSPs who serve them, it became obvious the industry needed a better SIEM solution that eliminates unnecessary data and alerts, streamlines complexity, and cuts out unpredictable costs. In this era of mounting threats and vulnerabilities, focus is everything: on just the data you need, paying only for what you've used."*
>
> 
>
> Chris Bisnett
>
> CTO and Co-Founder, Huntress

The mid-market end user is a professional with some security expertise who is open to guidance from a vendor on efficiently routing high-priority log data. While Fortune 100 teams typically have full capabilities to write SQL and Python to build in-house SLDM management solutions for acute needs, SMBs commonly rely upon plug-and-play options to solve problems around log collection processes and log traffic- and not as often for problems around log volume.

Companies like Edge Delta who cater to SMBs solve these issues by either providing pipelines products that pre-process log data and route optimized datasets or take care of all infrastructure through comprehensive platforms for analytics and single-lever pricing models.[8]

What Executives Want: Areas for Opportunity

1) Data Normalization Capabilities

Logs are largely unstructured- they are contained in diverse formats across different sources and vendors, making data normalization a time-consuming task. Data normalization pre-presentation layers can optimize time and ease of viewing for security analysts and a range of users across data science and security functions. For data scientists using an SLDM solution primarily for data management, effective normalization is particularly important.

Currently, most data management systems are incredibly linear, fragile, and expensive. They are heavily dependent on how the data is structured, formatted, and stored, necessitating assurance that data is collected properly and in the right forms.

> *"How do you know your data is going to be pulled in the right search format and optimized? What happens when data changes? You can have hundreds of sources of data that translate into thousands of different feeds of data. A configuration change or schema change would break every observability tool or report. Every single step in that ladder would have to be changed."*

George Webster

CEO, Ziggiz

Traditionally, high-capacity telemetry normalization is limited to the SIEM where there are more information processing capabilities than in the pipeline stage. However, normalizing data earlier in the pipeline allows real-time data querying en route to the SIEM. This presents an important opportunity that SLDM startups can take advantage of in several ways.

The Open Cybersecurity Schema Framework (OCSF)[9] offers an emerging standard for security telemetry that is gaining massive traction. It is an open-source effort to provide a standard security event schema for security log producers and consumers.[10]

OpenTelemetry (OTel) is a newer open-source observability framework developed by the Cloud Native Computing Foundation (CNCF) which provides a unified, vendor-neutral set of libraries, APIs, and agents to facilitate data ingestion and transport.[11]

Pipeline solutions that format data according to OCSF or OTel standards can help security engineers increase efficiency by automating repetitive tasks like data parsing, monitoring, and replay. The OCSF is a step in the right direction and the newest version 1.3.0, released in August 2024, handles diverse event types and security data sources. However, it is not comprehensive and there is room for adaptation going forward- there are concerns that the variety of data evolves too often and too quickly to establish a universal standard. Regardless, security leaders are excited about how these standards can optimize their workloads and promote efficiencies by making it easier to correlate information across disparate tools and derive value from data.

> *Standards like OTel and OCSF provide a certain comfort level that you can change tools or have ten tools because you have a standard way of collecting data. Organizations are deploying OTel and OCSF everywhere right now- the more vendors that start to use it, the less work I have to do in terms of creating a standard."*

Jerry Kowalski

CISO, Jefferies

While some startups have centered their data normalization solutions around OCSF standards, others marry security data with contextual information from other sectors, enabling their customers to develop custom schema. For example, those building machine learning models can work with data in more raw formats, while security analysts may need normalized data to befit threat detection.[12]

2) Predefined schema vs. customizable (codable) security pipelines

A core task for any security analyst is analyzing data and deciding what they need versus what can be discarded. All SLDM tools have some capability to filter data and reduce event size to make querying faster, but there is an opportunity for startups to deliver more intelligent data routing capabilities.

Hybrid organizations with diverse data sources seek SLDM vendors that comprehensively manage this task with predefined schema or standard data mapping.

For example, startups like Databahn or Abstract Security have solutions which require high security intelligence expertise and offer predefined schema alongside greater guidance on rule-setting during pipeline creation.

However, whether a tool should provide this schema or allow the customer's analysts to decide what data should be routed and where is highly dependent on the target customer. If an enterprise primarily uses Microsoft technologies and maintains consistent data sources, they may prefer a tool that allows them to define custom rules, such as Cribl or Aerospike.

How data is routed and the schema used to send logs to either an S3 type of solution or Splunk is critical and top-of-mind for CISOs. Security leaders are concerned about missing important information that may be sent to a cold storage facility instead of undergoing human analysis. This underscores that whether predefined by the SLDM tool or customized and coded by an expert security team, routing schema must be intelligent and keep humans in the loop.

> *You must have data in a form where you eventually have a human investigation because you do not know the process and the method of an attacker. It is not as simple as ignoring logs by dropping them in cold storage to reduce log growth. If you don't have a system that allows flexibility or agility, none of that important information is being processed or collected for analysis."*

George Webster

CEO, Ziggiz

At the moment, data analysis at the edge or in the pipeline is limited by a lack of context. Next-generation SLDM will utilize pattern recognition, automated responses, and flexible human interfaces in a sustainable manner. This will empower pipelines that are more efficient and better optimize SIEM storage.

3) Using AI to Reduce Latency in Detection and Analysis

> *"The difficulty we face is to control the data quality; the performance indicators related to that are the most relevant [to selecting a SLDM solution]. The analyst who has to interpret the data system often does so in near-real time, not real-time. Thousands of alerts may not be reviewed, and for low-urgency alerts there can be minutes or hours between detection and analysis."*

Joaquin Sanchez Iglesias

Security Monitoring & Analytics, Santander

We believe that a new era of security log data management is being ushered in by artificial intelligence (AI). Databahn has already been implementing retrieval augmented generation (RAG) to prepare data for utilization in large language models (LLMs) and enable better analytics. Other examples include Ziggiz's work using AI to unify data formats and enable faster processing and routing, and Auguria's security knowledge layer (Auguria SKL) which applies AI models to identify important data and map it to a priority level without the need for manual data rules engineering.

In addition to working with log data, AI can power log analysis. Machine learning (ML) and AI-based tools can create algorithms based on ingested data to identify system log patterns and anomalies- functions traditionally in the domain of security data analysts. Many companies are developing AI and ML capabilities in-house to perform analytics on top of the SIEM; however, the strength of the model or algorithm is dependent on the volume and quality of the log data. Training models at the pipeline stage- before volume reduction takes place- can build more effective model capabilities.

AI can be applied to log analysis to streamline data retrieval by grouping logs while reducing latency during issue identification and anomaly detection. For example, Edge Delta's ML-powered automated observability enables security teams to better analyze data at the source and correlate logs to alerts.

The variety of use cases for AI in the data management process reflects the opportunity for next-generation SLDM solutions to equip security teams with better and faster security detection and response capabilities, maximizing human ingenuity and operational workflows.

Final Thoughts on the Future of Security Log Data Management

The exponential growth of data volumes in large enterprises demands a sustainable solution. Going forward, the persistent enterprise desire to gather as much data as possible warrants pipelines which are more robust and SLDM solutions which meet a variety of data management and detection needs.

Our take on the market: Bullish

SLDM startups can solve extremely important pain points for organizations collecting security logs, including unmanageable log volume, high SIEM costs, and vendor lock-in. These problems are expected to persist as companies continue to gather more data and more types of data. Cribl's recent $319M Series E round and broad brand awareness is a good indicator that SLDM is top-of-mind for investors, CISOs, and other executives who are likely to begin evaluating related tools if they have not already done so.[13]

Here's what might change our minds:

1) If SIEM vendors moving into the log routing space (like Splunk) can refine their capabilities, vendor lock-in becomes less of an issue. Subsequently, there may not be much opportunity for SLDM startups to grab market share and circumvent the reliance on SIEMs for log data management and analytics.

2) If log volume continues to grow at the current rate, filtering (a capability many SLDM startups are focused on) may only be a short-term fix. Large scale enterprises might need to shift their focus to core infrastructure issues which impact log data management.

Fundamentally, SLDM startups can help address problems that CISOs and security analysts face around logging costs, data management, and threat detection. We are excited to see how this market continues to grow and evolve.

Acknowledgements

Special thanks to the following individuals for their insights and contributions.

Chris Bisnett
CTO & Co-Founder, Huntress

David Emerson
CTO, SolCyber

Jerry Kowalski
CISO, Jefferies

Ramin Safai
CISO, Point72 Ventures

Joaquin Sanchez Iglesias and Guillermo Fuente Diaz
Digital Services, Santander

Ricardo Villadiego
CEO & Founder, Lumu Technologies

George Webster
CEO, Ziggiz

Preisha Agarwal
Research Analyst

Rey Kirton
Principal

Ernie Bio
Managing Director

Leo Casusol
Managing Director

With Conor Higgins and Tanya Loh

About Forgepoint

Forgepoint is an early-stage venture capital firm that invests in transformative cybersecurity, artificial intelligence, and infrastructure software companies protecting the digital future. With the largest sector-focused investment team, over $1 billion in AUM, and an active portfolio of more than 30 companies, the firm brings over 100 years of collective company-building expertise and its Advisory Council of more than 100 industry leaders to support entrepreneurs advancing innovation globally. Founded in 2015 and headquartered in the San Francisco Bay Area and London, Forgepoint is proud to help category-defining companies reach their market potential.

Learn more at https://www.forgepointcap.com and https://www.linkedin.com/company/forgepoint-capital.

Company Highlights: Security Log Data Management

HUNTRESS

Managed detection and response for SMBs

huntress.com

LUMU

Real-time visibility and compromise detection over network threats

lumu.io

Portfolio

Forgepoint is proud to partner with these companies securing the way people live and work. For more information, see https://forgepointcap.com/companies/.

1KOSMOS · aka identity · ANITIAN · AppMap · BISHOPFOX
cinchy · Constella INTELLIGENCE · Converge · CyberCube · FORESCOUT
GetReal · HUNTRESS · hyperproof · Instabug · interos
loginradius · LUMU · Lynx · NowSecure · nudge
Qevlar AI · RAD SECURITY · RAFAY · RAPIDFORT · REVERSINGLABS
SECURE CODE WARRIOR · SolCyber · SPHERE · STRATA · SUREFIRE CYBER
SYMMETRY · Synadia · uptycs · VERITUITY · whistic

Exits

CLOUDFLARE AREA 1 SECURITY · Attivo NETWORKS A SentinelOne Company · BehavioSec A LexisNexis Risk Solutions Company · SECUREAUTH | CLOUDENTITY · concourse LABS A FORTINET COMPANY
CYSIV A FORESCOUT COMPANY · ermetic a Tenable company · IDX A ZEROFOX COMPANY · Akamai | noname · Remediant NOW PART OF netwrix

snowflake | truera

Notes

[1] Haleliuk, Ross. "Security is about data: how different approaches are fighting for security data and what the cybersecurity data stack of the future is shaping up to look like," Venture in Security, Sept 25, 2023. ventureinsecurity.net/p/security-is-about-data-how-different

[2] "Understanding Managed SIEM Pricing and Costs," LK Technologies, https://lktechnologies.com/understanding-managed-siem-pricing-and-costs/

[3] Shook, Shane. "TIPS #15, How can companies strike a balanced approach to log management?" Forgepoint Capital, Apr 18 2024. forgepointcap.com/perspectives/tips-15-how-can-companies-strike-a-balanced-approach-to-log-management/

[4] Singer, Omer. "Survivor's Guide to SIEM in 2024," Omeron Security, May 23, 2024. www.omeronsecurity.com/p/survivors-guide-to-siem-in-2024?r=gcu4i&triedRedirect=true

[5] "Fair Use Wins: Court Sides with Cribl in Splunk's Lawsuit," Cribl, Apr 23, 2024. cribl.io/news/fair-use-wins-court-sides-with-cribl-in-splunks-lawsuit/

[6] "Data infrastructure startup Cribl raises $319M at a $3.5B valuation | TechCrunch," Gartner, Aug 27, 2024. https://techcrunch.com/2024/08/27/data-infrastructure-startup-cribl-raises-319m-at-a-3-5b-valuation/?guccounter=1&guce_referrer=aHRocHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEEflaY2koZo6cFlEQcPn-OIKuhKsnMoY6vg4MHLhn_9W4pLVaOR4c3ag_hetxpkkynksDhWpV4ELZH-3HyDQSxu57hzBJc-z2I25raphCbnZyZXCRtP3PzhE6u7o6gm-mEv_H2kRWNutAR1ZDnTehEpZrkd9yvz2fT5pQwoG9_T

[7] "Use Central Log Management for Security Operations Use Cases," Gartner, Mar 20, 2020.

[8] "Breaking up with Datadog," Edge Delta, 2024. edgedelta.com/company/blog/how-to-reduce-datadog-costs-with-edge-delta

[9] Open Cybersecurity Schema Framework (ocsf.io)

[10] "From Data Chaos to Cohesion: How OCSF is Optimizing Cyber Threat Detection," AWS, Aug 5, 2024. aws.amazon.com/blogs/opensource/from-data-chaos-to-cohesion-how-ocsf-is-optimizing-cyber-threat-detection/

[11] "What is Open Telemetry?" Open Telemetry, 2024. opentelemetry.io/docs/what-is-opentelemetry/

[12] Berkowsky, Jake. "Security Data Lakes, Normalization and OCSF," Medium, Jan 4, 2024. medium.com/snowflake/security-data-lakes-normalization-and-ocsf-ec94b70fcdc9

[13] Wiggers, Kyle. "Data infrastructure startup Cribl raises $319M at a $3.5B valuation," TechCrunch, Aug 27, 2024. techcrunch.com/2024/08/27/data-infrastructure-startup-cribl-raises-319m-at-a-3-5b-valuation/

Forgepoint

/ Forgepoint Forward /

What's Ahead in Security Log Data Management

Backing builders of the /digital future/

forgepointcap.com
650.289.4455
400 S. El Camino Real / Suite 1050
San Mateo, CA 94402

Website LinkedIn