TENZIR

Slashing SIEM, Cloud, and Data Costs with Tenzir

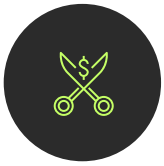
Reduce Costs and Optimize your Cybersecurity Infrastructure with Security Data Pipelines

The growing sophistication of security threats makes increasing demands on security teams ability to manage and analyze large volumes of alerts, events and other data. But many organizations struggle to balance the data requirements for comprehensive protection with financial constraints. As the volume of data and cloud reliance grow, SIEM, cloud, and data costs consume a sizable portion of security budgets, limiting resources for proactive defense measures. To address this, businesses must seek innovative technologies to efficiently manage and analyze data. Tenzir's innovative Security Data Pipelines provide a cost-effective solution to help businesses reduce their expenses and optimize their cybersecurity infrastructure while maintaining comprehensive protection.

Key Takeaways

Complex threats require efficient data management and cost-effective technologies to optimize resources.

Escalating data and cloud costs strain budgets and divert funds from critical security initiatives.



Security Data Operations (SecDataOps) focuses on minimizing data costs and overheads while maximizing data utilization.

Tenzir's security pipelines enable intelligent data filtering, reduction, and deduplication to reduce storage and processing costs.

Tenzir's scalable architecture supports the growth of an organization's security infrastructure without exponential cost increases, ensuring long-term savings and sustainability.

By implementing Tenzir's SecDataOps and leveraging security pipelines, organizations can efficiently manage security data, reduce SIEM, cloud, and data storage costs, and enhance overall operational efficiency.

Dropbox gross margins increased from 33% to 67% after overhauling their infrastructure and repatriating public cloud workloads. [1]

The Cost of Cloud, a Trillion Dollar Paradox, Andreessen Horowitz

[1] https://a16z.com/2021/05/27/cost-of-cloud-paradox-market-cap-cloud-lifecycle-scale-growth-repatriation-optimization/

Problem: Data and cloud costs are consuming security budgets

The rapid growth of data in cybersecurity operations, combined with the expanding reliance on cloud computing, has resulted in SIEM, data, and cloud costs consuming a sizable portion of security budgets. This financial burden not only limits organizations' ability to invest in essential security measures but also impedes their ability to proactively defend against ever-evolving threats.

Complex threats drive complex data needs

Cyber-attacks have become progressively more sophisticated and diverse, and threat actors are constantly adapting and improving their tactics, techniques and procedures (TTPs). Defenders must chase a moving target to keep up and be able to detect and respond to potential eventualities across a porous and expanding attack surface. Many security operations teams today manage a dizzying array of security and general-purpose data solutions to achieve the visibility they require, and especially to manage and make sense of the resulting flood of alerts. As organizations struggle to scale their infrastructure and processes to accommodate the growing data demands, they face additional challenges:

Limited resources

Data engineering teams are often assigned to help security operations with their data needs but are a scarce resource. Without a breach, security projects are often not the most critical business priority, leaving little time to consider efficiency or optimization.

Most security professionals have foundational knowledge of data technology and processes, but they are rarely proficient at data engineering, or even both. More importantly, any time they spend on wrangling data is time in which they are not hunting threats and actively protecting the business.

In addition, there is an ongoing and acute shortage of skilled security and data engineers and analysts, placing constraints on placing additional work on either security or data teams.

Compliance and privacy risks

Compliance and privacy risks are increasingly important concerns for organizations managing large volumes of sensitive data in their cybersecurity operations. Threat detection telemetry and other data that is relevant to security operations is often distributed across different solutions, technologies, cloud services and even physical locations, making it difficult to keep track of everything.

Businesses must navigate diverse regulations, and actively prevent data breaches, which means applying adequate data protection measures, such as pseudonymization,encryption, as well as managing the data lifecycle—from acquisition,through retention, and to disposal.

Increased data storage and management costs

Data computation and storage costs start small but can quickly snowball over time. Users often only recognize the Faustian bargain they made too late, when their data is already locked in, and difficult and expensive to export.
When data costs grow faster than the available security budget, security teams face a stark choice: What data can we afford to collect - and what can't we afford to lose?
Costs also quickly spiral out of control if a need arises to collect and retain data over longer time frames, especially if data needs to be available on-demand for live searching or is frequently replayed into MLOps pipelines.
It is not unusual for security teams to run SIEM for event correlation and alert management, a security data lake for long-term historical investigation and hunting, and various cloud data storage and micro services for cheap data retention and special purpose analytics workloads. To gain a complete picture and respond to threats effectively, data must be moved between all these technologies, resulting in quickly mounting costs, especially without a coherent security data strategy.

Existing approaches fall short

Traditional security solutions are not designed to be data efficient, and generic data engineering tools, while powerful, require extensive customization and entail a steep learning curve to be repurposed for reuse in security operations.
These factors further strain budgets and divert funds from other critical security initiatives like improving incident response or deriving threat intelligence.
Considering these challenges, addressing the escalating costs and overheads associated with SIEM, data, and especially cloud computing has become a top priority for businesses seeking to maintain a robust cybersecurity posture. By finding innovative ways to optimize data management and reduce costs, organizations can not only alleviate financial pressure but also strengthen their security operations and better protect themselves against the ever-present threat landscape.
Security teams need innovative strategies and cost-effective technologies that can efficiently manage, process, and analyze vast amounts of data, while minimizing the associated expenses and overheads.

What about XDR?

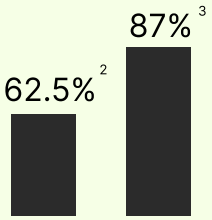
Many organizations are adopting Extended Detection and Response (XDR) solutions to consolidate the number of technologies they need to operate and try to eliminate some of the complexity involved inherent in security operations.
Depending on the specific XDR offering, several security capabilities are usually consolidated. Endpoint detection and response (EDR), network detection and response (NDR), cloud detection and response (CDR), incident management, and threat intelligence are especially common.
XDR streamlines some security data needs, but most security teams will still need to run additional technologies and integrate with other systems. XDR is typically delivered as a cloud-hosted SaaS solution, with similar cost dynamics as cloud SIEM and data lakes.

Solution: SecDataOps and Tenzir Pipelines

Effective threat detection, investigation, and response increasingly means mastering data. Security teams require a new strategic approach that considers cost management and Financial Operations (FinOps) as primary outcomes: Security Data Operations (SecDataOps)

SecDataOps uses the most efficient dataflows

SecDataOps seeks to minimize data costs, whether computational or storage, while maximizing data utility and utilization. Controlling SIEM, cloud, and other data costs means being strategic and aggressive about what data is sent onwards, and in what shape.



Actual SIEM cost savings achieved by organizations applying data reshaping and reduction

[2] https://cribl.io/blog/logstream-power-hour-reducing-splunk-log-data-volume/

[3] https://www.snaresolutions.com/reduce-siem-costs/

Data Reshaping and reduction

A lot of information contained in security events is erroneous, repetitive, or otherwise data-sparse and easily compressed. By filtering, deduplicating, and compacting data at the edge before it reaches expensive consumption-based services and solutions, it is possible to achieve anywhere between 30% and 80% cost reduction. Moving the right data at the right time to the right place can drastically lower SIEM, Cloud and data costs.

Data compaction

Data retention policies are often based on simply aging out older data. Distinct types of data have different business and lifetime values. Instead of just deleting the oldest data, Tenzir's unique compaction algorithm applies aging based on the relative importance of the data.
We can also deploy aggregation pipelines to shrink data by choosing context over fidelity. For example, by converting flow records into an aggregate matrix of who communicated with whom, the data may shrink 10x in size but it's still possible to answer questions like "have we had communication with this entity?". This gracefully degrades the data fidelity and limits the utility, instead of abruptly throwing data away.

Data pre-processing and enrichment

Enriching alert, event, and telemetry data with user, asset, and threat intelligence context is often done on several occasions across different solutions. Similarly, executing detection content, such as Sigma rules, is also often repeated in many instances. Pushing enrichment and detection content execution down to the network edge eliminates duplicate effort, processes data where it's most cost-effective and ensures that the same enriched data is available consistently for any workloads.

Security Data Pipelines are the key to SecDataOps

Tenzir follows a simple philosophy: composable data flow pipelines. Anyone can easily create powerful pipelines by chaining together operators, like Unix pipes or PowerShell commands, with the difference that our operators are specially designed for security data operations use cases.

50% The amount of core business applications that will be built using composable architecture by 2027, according to Gartner, Inc.[4]

[4] https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023

Getting started with Tenzir

Tenzir Community Edition is free to use. You can get started at app.tenzir.com.

The Developer Edition is available at GitHub.
Read the docs. Join the discussion on Discord. Follow us on LinkedIn or Twitter.

For questions or inquiries, visit tenzir.com or contact us at info@tenzir.com.

Tenzir GmbH, Nagelsweg 41, 20097, Hamburg, Germany.

Connect the whole world of Security and Data

You can unify dataflows by combining pipelines to build intricate security stacks that connect to the whole universe of security and data tools. Tenzir's growing operator library makes it easy for security teams to quickly compose data pipelines for any security operations use-case out of plug-and-play building blocks.

Explore all operators, connectors and formats.

Connected
capture data from numerous data sources and connectors, including Kafka and Fluent.

Ergonomic
slice-and-dice, extract, aggregate, and delete rows or columns from event data using simple chained operators.

Security-native
ensure data privacy and protection with security-specific operators for redacting sensitive inputs, pseudonymization and encryption.

Contextual
Enrich event, alert, and telemetry data with operators to add asset, user and threat intelligence context.

Truly Open
Exchange and move data in open formats, including Apache Arrow and Parquet—perfect for your data science workbench or processing engine.

Key Features

Data filtering and reduction
Tenzir allows users to filter out noisy, redundant, and duplicate data, ensuring only relevant information is forwarded and stored, which reduces storage and processing costs..

Data deduplication
Tenzir helps eliminate duplicate data entries, conserving storage space and reducing data processing times, ultimately lowering associated costs.

Selective data forwarding
Tenzir enables users to move only the right data at the right time to various tools and platforms, optimizing SIEM, cloud, and data expenses.

Pipeline development
Tenzir's plug-and-play data pipelines allow security teams to quickly create powerful, streamlined data workflows that save time and resources, reducing overall operational costs.

Open standards and compatibility
Built on open standards like Arrow and Parquet, Tenzir can seamlessly integrate with existing data environments, eliminating vendor lock-in and providing flexibility for cost-effective solutions.

Distributed data processing
Tenzir's data fabric enables distributing data storage and processing across the entire network, optimizing resource utilization and lowering expenses related to data management.

Scalable architecture
Tenzir's architecture supports the growth of an organization's security infrastructure without exponential increases in cost, ensuring long-term savings and sustainability.

Benefits

Reduce storage requirements
Filtering, reducing, and deduplicating data decreases the overall data volume stored, leading to significant savings in storage costs.

Enhance processing efficiency
leaner datasets require fewer computing resources, speeding up data processing and analysis, and reducing cloud compute costs.

Improves data quality
Removing irrelevant, redundant, or duplicate data ensures that only valuable and accurate information is retained for analysis, enhancing the overall quality of the data.

Streamline threat detection
With fewer false positives and enriched datasets, security teams can identify threats faster and more accurately, increasing the effectiveness of SIEM solutions.

Lower data transfer costs
Transferring less data between various security tools and cloud services reduces data transfer fees, further decreasing overall costs.

Enhance compliance
By retaining only necessary data, organizations reduce the risks associated with data privacy regulations and minimize the potential for non-compliance penalties.

Optimize security team resources
Focused datasets allow security teams to spend more time on threat hunting and proactive defense measures, rather than managing large, unwieldy datasets.

By leveraging these features, Tenzir empowers organizations to optimize their security operations while significantly reducing costs associated with SIEM, cloud, and data management.

Conclusion

Tenzir's innovative SecDataOps approach and Security Data Pipelines offer an innovative approach for organizations seeking to balance their cybersecurity needs with financial constraints. By optimizing data management, reducing SIEM, cloud, and data costs, and streamlining operations, businesses can allocate more resources to proactive threat hunting and incident response. Tenzir empowers organizations to maintain and sustain moving-target defense while simultaneously reducing the financial burden associated with traditional security infrastructure management.

About Tenzir

Our mission at Tenzir is to make security data easy. We are fundamentally changing the way that cybersecurity operations infrastructure is built and run. Our vision is to give security teams control over their own data and to free them from vendor lock-in through a fabric of powerful and efficient security data pipelines.

We want to make working with security data easy and affordable, so that security teams can focus on what matters most—hunting threats and safeguarding their digital environments.

For more Information

For questions or inquiries, visit tenzir.com or contact us at info@tenzir.com.