CONFLUENT

Solution Brief

Optimize your SIEM Solutions with Confluent

Combine your security platforms and the most widely adopted real-time data streaming platform to thwart cyber criminals and modernize your cybersecurity posture. Confluent's solution for SIEM optimization augments your cybersecurity platforms to break down silos and deliver contextually rich data to be more situationally aware. With Confluent, you can gain world-class data ingestion and analytics while optimizing for cost and scale. Achieve independence from any given SIEM vendor, and gain the ability to leverage multiple tools and analytic destinations for greater cyber resilience.

Design a next-gen cybersecurity data infrastructure with a real-time SIEM pipeline

Enable threat detection and data engineering at the edge or point of collection for contextually rich insights

Mitigate the impact of increasing data storage and analysis costs that force tradeoffs between cost, flexibility and visibility

Gain unprecedented flexibility to choose your own data destiny, regardless of source or destination, eliminate lock-in and enable best of breed

Why Optimize Your Cybersecurity Solutions?

Security Incident and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools have become ubiquitous in enterprise security operations to detect attacks, investigate security incidents and ensure timely response. Their ability to do so is predicated on the fidelity and speed at which they receive data.

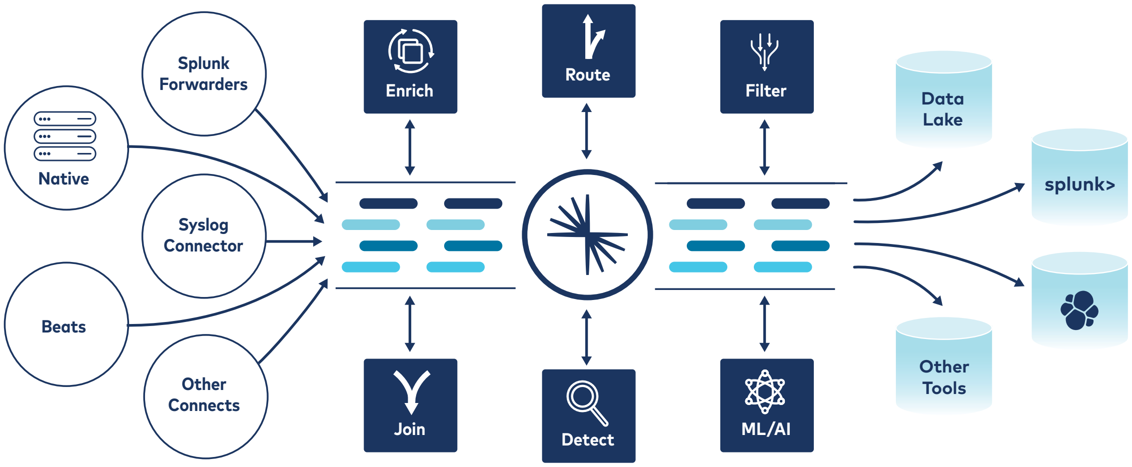
The growing diversity, velocity and exponential volume of security data have rendered legacy SIEM technologies incapable of dealing with the current requirements of Information Security (InfoSec) teams and Security Operations Centers (SOCs).

The need to augment and modernize SIEM solutions is driven by 3 main factors—*scale*, *speed* and *cost:*

- ***Scale*** Capture and curate data at wire speed and petabyte scale across distributed environments that conventional ingest approaches cannot keep up with
- ***Speed*** Detect, filter and enrich data to deliver real-time situational awareness, reduce false positives and respond to incident and threats faster
- ***Cost*** Avoid vendor lock-in from expensive proprietary tools and utilize a tiered data model to minimize software and infrastructure costs

Confluent for SIEM Optimization

Confluent offers an enterprise-ready data in motion platform to capture, analyze and deliver ubiquitous access to any type of data, everywhere. With Confluent, organizations can bridge the gap between old-school SIEM solutions and next-gen offerings by consolidating, categorizing and enriching all data and real-time events from relevant data sources for real-time monitoring, security forensics and an enhanced cybersecurity posture.



Confluent: The global data backbone for next-gen cybersecurity infrastructure

Move from Batch to Real-time at Stream Scale

Ingest, aggregate, and store a diverse and growing set of security event and sensor data into a single distributed, scalable, and persistent platform. Confluent delivers pre-built connectors such as Splunk, Elasticsearch, SNMP, Syslog, AWS Cloudwatch and others to consolidate siloed systems, saving you months of integration effort and empowering your teams to unlock insights even faster. Designed for high performance at massive scale, Confluent can handle trillions of messages per day and petabytes of data effortlessly in real-time, enabling you to move from batch processing to real-time at Intrusion Detection System (IDS) speeds with stream data velocity and volume.

Save Money in License and Infrastructure Costs and Reduce your Overall TCO

Using Confluent as the real-time data pipeline to your SIEM and SOAR solutions, you can aggregate and filter events to reduce ingest and index volume, overall licensing expenses and retention costs that often come with consumption-rate, volume-based pricing. Confluent also reduces the need for proprietary or even intermediary forwarders like the Splunk Heavy Forwarder with Splunk S2S Connector to reduce overall operating expenses and gain centralized visibility. Use Confluent's portfolio of 120+ pre-built connectors to route your data with full fidelity to low-cost storage systems, including Amazon S3, Google Cloud Storage, Azure Blob storage, Snowflake, HBase and others, for long term retention.

Improve Data Quality and Increase Speed to Detection and Resolution

Confluent delivers sophisticated stream processing capabilities to curate, enrich, transform and normalize data in real-time. Filter noisy data by suppressing and masking events that do not contribute to incident detection and investigation. Apply simple business logic such as stateless filtering or stateful aggregations, or design complex business rules with custom code or separate rules engine. Train and bring ML/AI models to your data by embedding analytics models to apply real-time context and aid richer threat and anomaly detection, intrusion prevention, investigation and real-time analysis. Push processing to edge and point of collection to reduce latency and deliver insights faster.

Achieve Unprecedented Flexibility and Freedom of Choice

Whether you're looking to migrate off an old SIEM solution, intelligently route your data to multiple different destinations like Splunk, Elastic, Datadog, Prometheus and New Relic, have low-value data that does not need to go to an expensive SIEM platform or store your data in cheaper storage for compliance and reporting, Confluent delivers the ultimate flexibility. Route your data to any destination of your liking, while maintaining full fidelity of data in a vendor-agnostic format to eliminate vendor lock-in. Democratize access to data to leverage best of breed tools to strengthen cybersecurity and unlock multiple real-time use cases.

As cyber threats continuously grow in sophistication and frequency, companies need to quickly acclimate to effectively detect, respond, and protect their environments. At Intel, we've addressed this need by implementing a modern, scalable Cyber Intelligence Platform (CIP) based on Splunk and Confluent. We believe that CIP positions us for the best defense against cyber threats well into the future.

Our CIP ingests tens of terabytes of data each day and transforms it into actionable insights through streams processing, context-smart applications,and advanced analytics techniques. Kafka serves as a massive data pipeline within the platform. It provides us the ability to operate on data in-stream, enabling us to reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Faster detection and response ultimately leads to better prevention.

— Brent Conran, Chief Information Security Officer