Route, reduce, redact:

Manage your security data pipeline

Google Cloud Next 25



Proprietary



Ketan Nayak

Group Product Manager

Google Cloud



John Schieferle Uhlenbrock

Executive Director, CyberSecurity Operations & Engineering

Fortrea



Travis Lanham

Software Engineer

Google Cloud

Proprietary

Data overload in security operations



Complex architecture

Diverse tools and sources make unified security visibility difficult

Data that’s valuable for security outcomes is also valuable for other operations



High costs

Exploding security data telemetry drives up

Inefficient data handling further inflates these costs and not all data is created equal



Increased data needs

Make most of data while being compliant

Need for redaction, compliance, and data transforms

Proprietary

Pressure Points: Challenges in Our Logging Architecture

Rapidly Growing Telemetry

Security telemetry has surpassed our original ~1TB/day projections.

Limited Log Visibility

Standard EDR solutions (e.g., CrowdStrike, Defender) provide alerts but lack detailed raw Windows logs required for deeper security investigations.

Limited Architectural Flexibility

Existing Chronicle forwarders limit flexibility, restricting our ability to rapidly adapt or expand logging strategies.

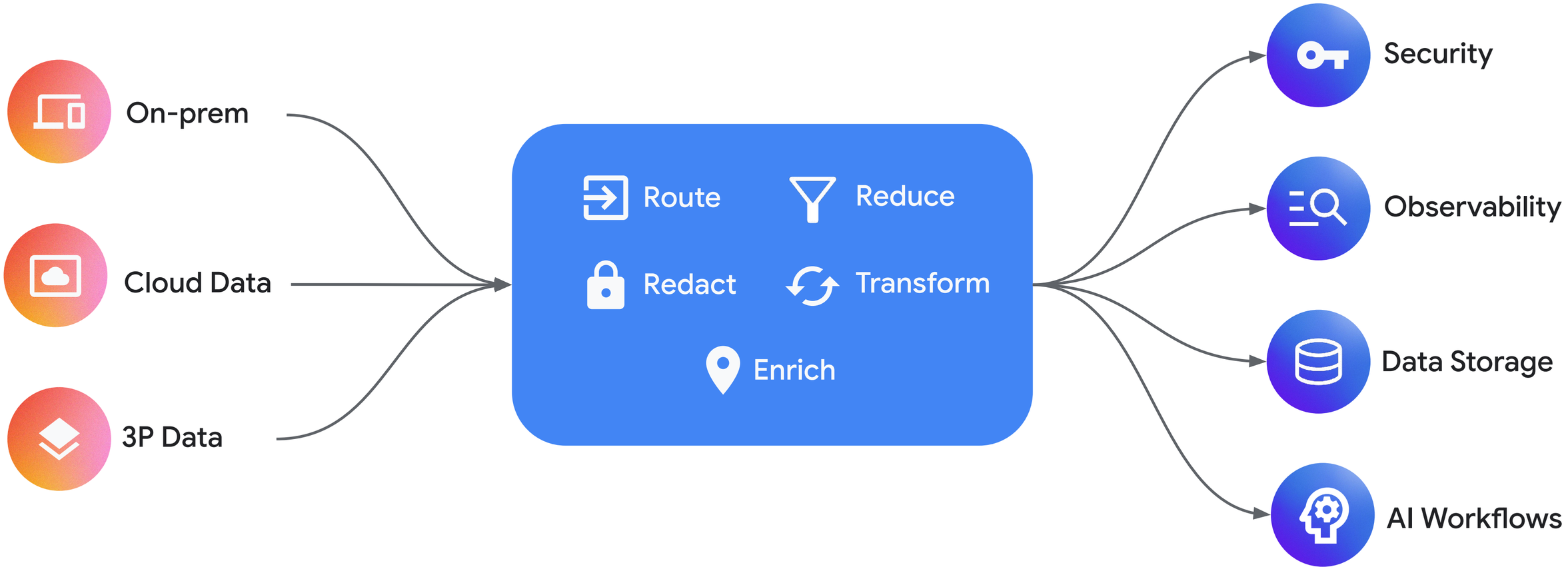
Operational Cost Pressures

Increasing data volumes risk exceeding our Chronicle licensing budget, challenging our ability to maintain cost-effective operations.

Fortrea

Proprietary

Data Pipeline Management



Proprietary

Data pipelines with Google Security Operations

In partnership with bindplane

Routing

Route any data to SecOps

Route to Google and non-Google destinations

OpenTelemetry based collection

Reducing

Ingest what you need and save costs

Filter out the data you don’t want

Transforming

Redact sensitive data with PII data masking

Transform data with advanced processors

Proprietary

Data pipelines with Google Security Operations

In partnership with bindplane

Routing

Route any data to SecOps

Route to Google and non-Google destinations

OpenTelemetry based collection

Reducing

Ingest what you need and save costs

Filter out the data you don’t want

Transforming

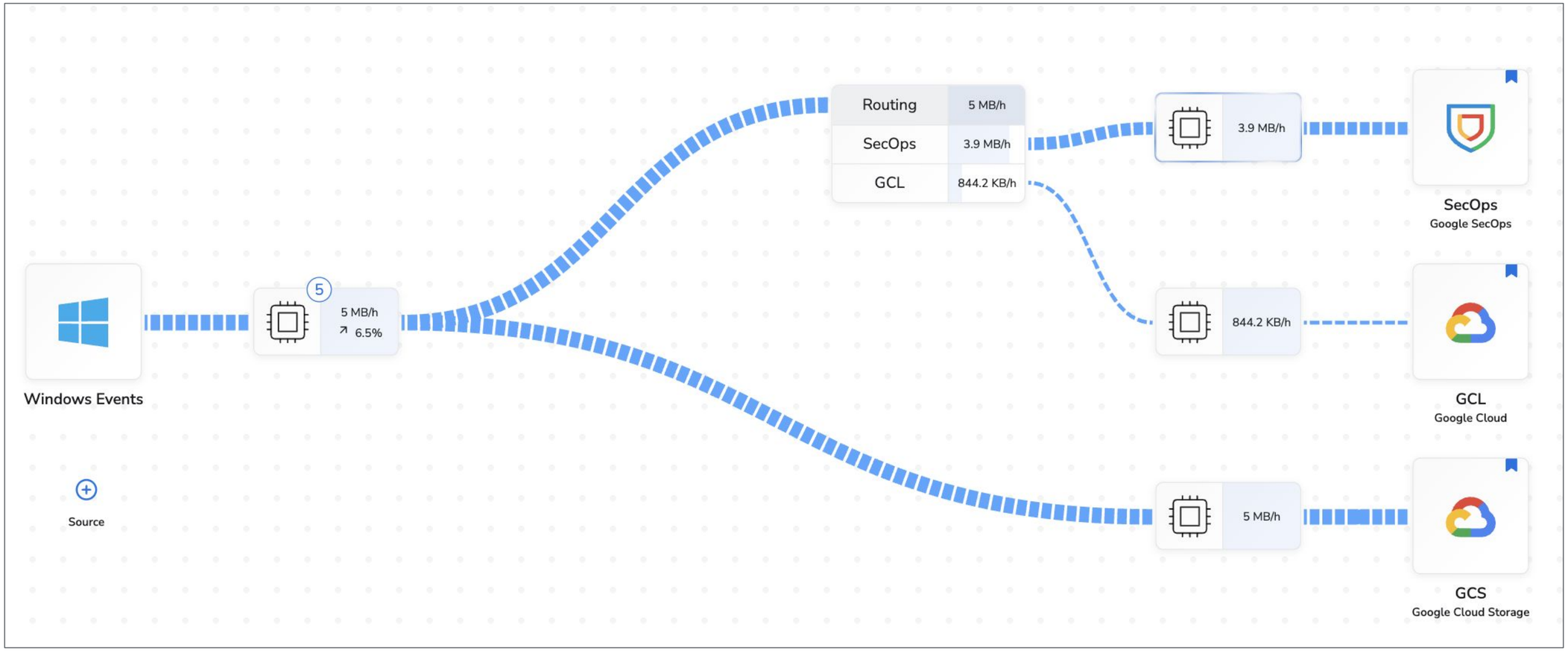
Redact sensitive data with PII data masking

Transform data with advanced processors

Proprietary

Route

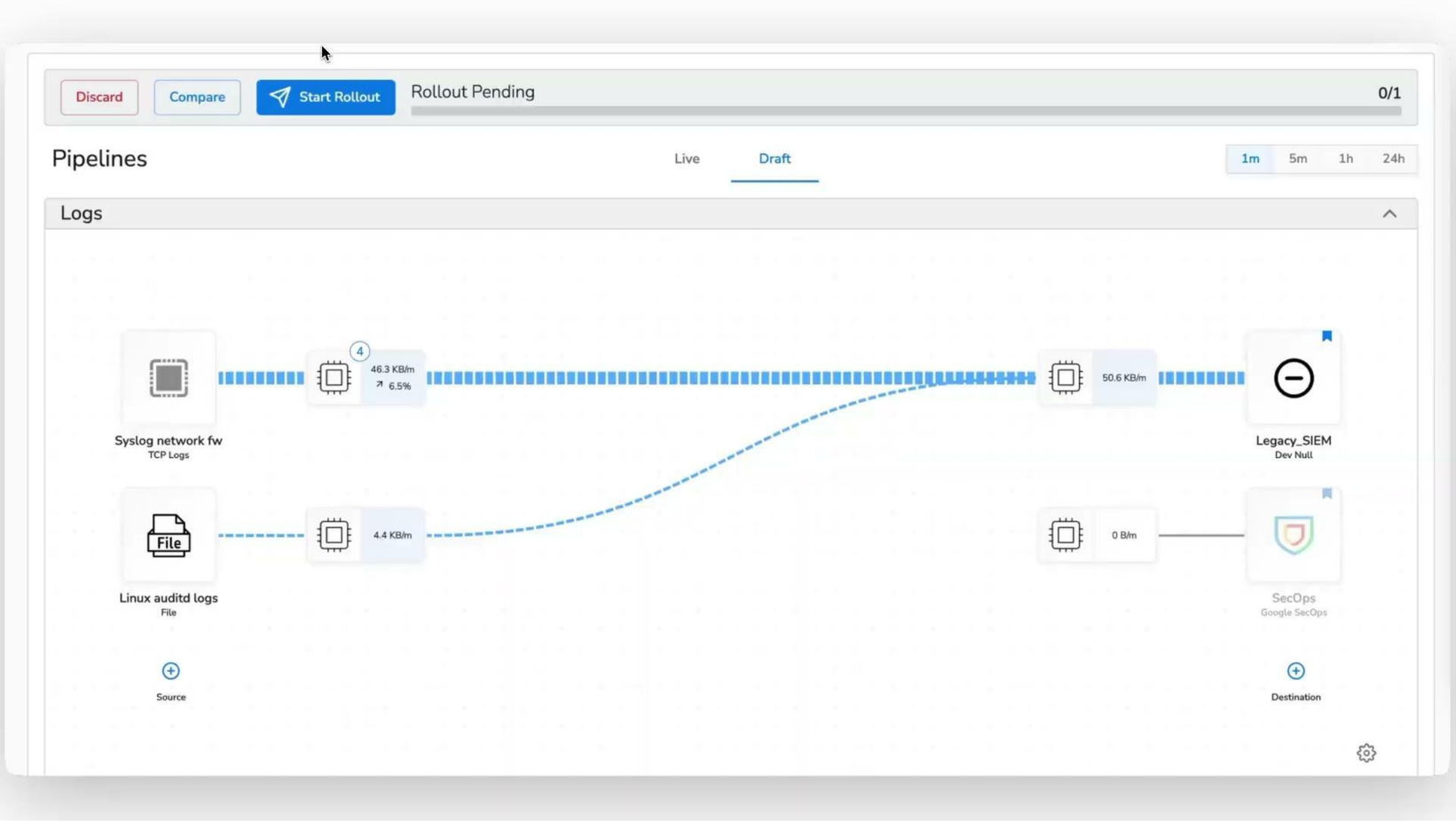
Route security data, ITOps, and all categories of data to Google destinations



Proprietary

Route

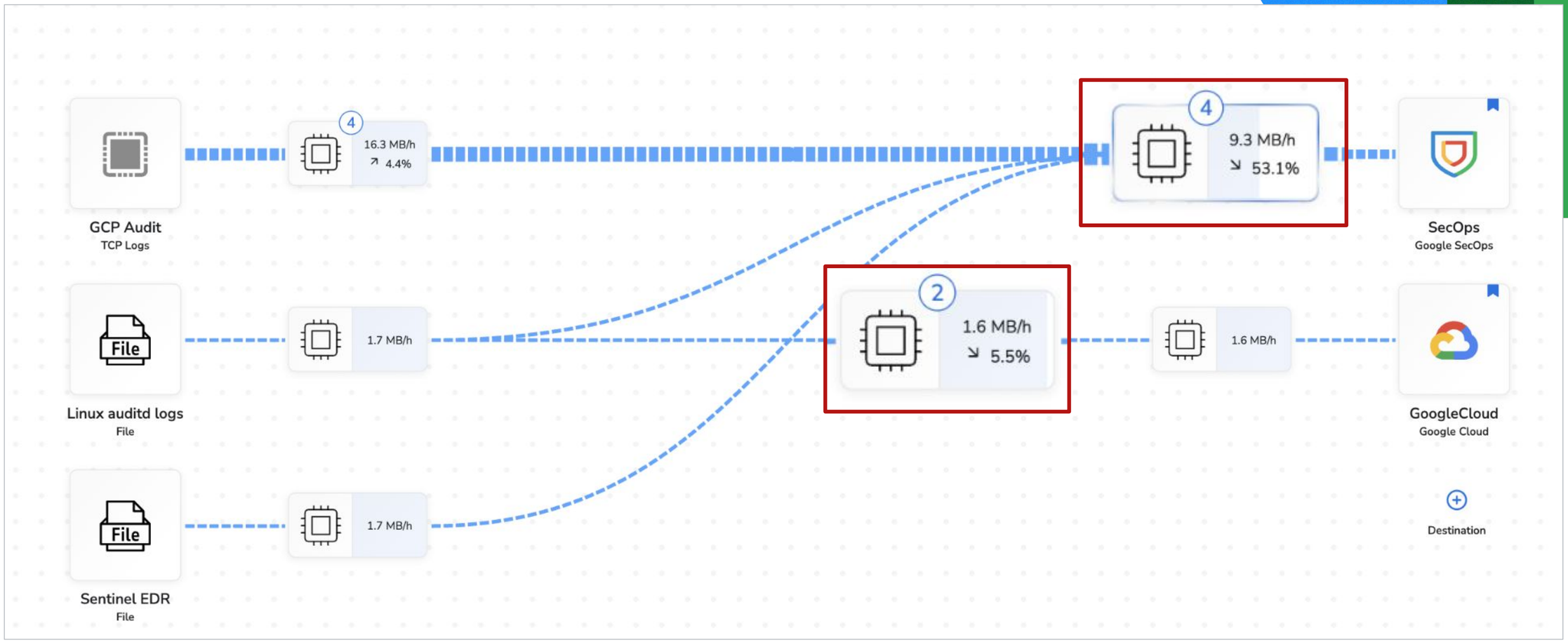
Migrate SIEMs by routing to a non-Google destination



Proprietary

Reduce

Filter and save costs



Proprietary

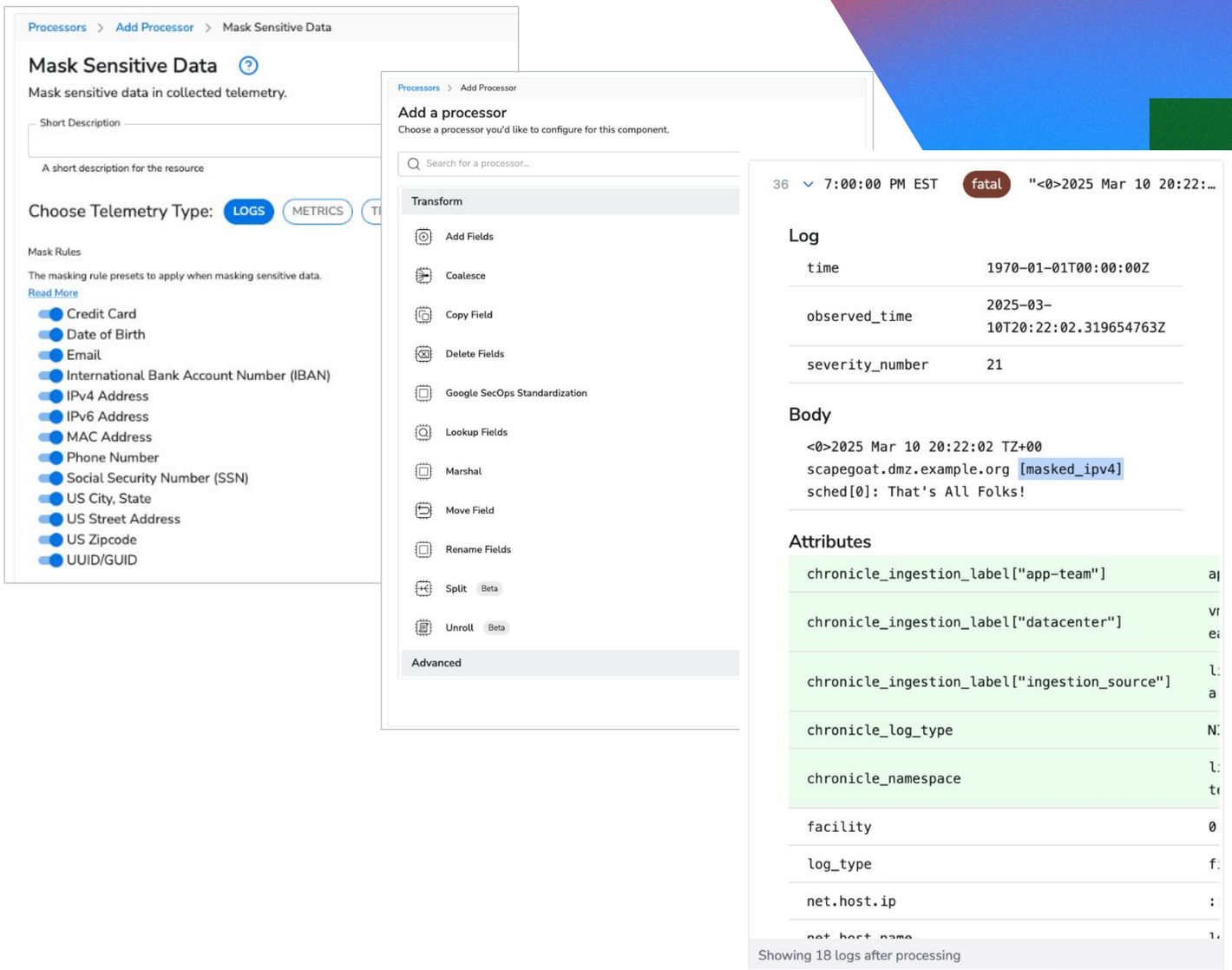
Redact and more

Compliant redaction

PII redaction and
Masking

Beyond redaction

Data transformation
suite that works for you



Proprietary

DPM with Google Security Operations

Accelerated time to value

Collect data from a wide range of sources

Enterprise-grade, compliant

Adheres to regulations with data masking & scales for largest customers

Consolidate tooling

Routing, redaction, and filtering in one tool

Included out of the box

First party solution for Google Security Operations customers

Centralized management

Manage agents, deploy configurations, and monitor data flow

Proprietary

Precision pipeline: Route, reduce, redact in action

Route: Dynamic Data Routing

Route security logs simultaneously to SecOps and an independent data store, enabling continuous monitoring of log source operational health

Reduce: Targeted Data Extraction

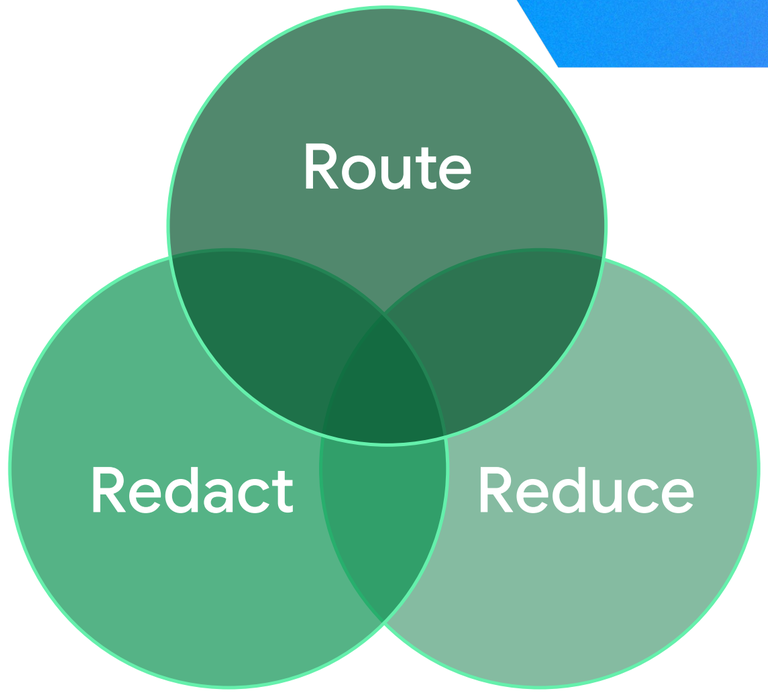
Selectively extracted only critical Windows Event IDs from Domain Controllers' security logs → 33% reduction in data storage requirements.

Redact: Future-proof Compliance

Currently preparing to ingest logs containing PHI and PII, laying groundwork for automated redaction of sensitive information

Broader Application Log Ingestion (Future)

Planning capabilities to ingest diverse, non-standard log sources more easily—streamlining our future operational visibility and adaptability.



Fortrea
Proprietary

“With Bindplane we’ve been able to unify our telemetry into a single pipeline while standardizing on OpenTelemetry at the same time. This has allowed us to move significantly faster, managing growing data volumes with fewer resources.”

Product Manager, Cybersecurity Security Operations at a Multinational Retailer

Proprietary

Product demo

Proprietary

Data pipeline feature entitlement

	Standard / Enterprise	Enterprise+
BINDPLANE EDITION	Google	Enterprise Google
ROUTE	Google	Google and Non-Google*
REDUCE	Regex	Advanced
REDACT	-	PII masking
TRANSFORM	Basic	Advanced
PLATFORM	Gateway, Silent host monitoring, Fleet Mgmt	

*Limited to first 12 months

Proprietary

Q&A

Proprietary

Continue your learning journey!



Interested in other security sessions?

BRK3-041: Accelerate security incident response with Gemini, Thurs, 12pm

BRK2-153: Ready, threat, go! Unlock the power of threat-driven security operations, Thurs, 1:30pm



Check out the Security Hub!

SOC Experience

Mandiant Cafe

Google Cloud Security product demos

And more!



Get a Date Pipeline Management demo

Visit us at the Google Security Operations demo pod located in the Security Hub in the Expo

Proprietary

Your feedback is greatly appreciated!



Complete the session survey in the mobile app

Proprietary

Thank you

Proprietary