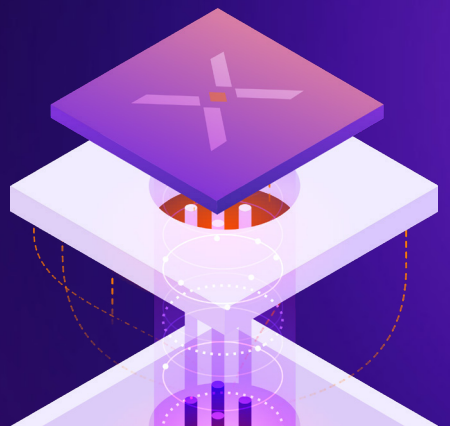
securonix DATASHEET

Data Pipeline Manager

Expand Visibility Without SIEM Cost Bloat

Value-based SIEM data consumption that aligns cost to data value.



OVERVIEW

Align SIEM Cost to Data Security Value

Modern SOCs generate massive volumes of telemetry, but traditional SIEM pricing forces organizations to choose between visibility and cost. Real-time detection telemetry, searchable investigation data, and long-term compliance logs serve different purposes and should not carry the same economic weight. Data Pipeline Manager (DPM) changes that model.

Built natively into Securonix Unified Defense SIEM, DPM routes telemetry dynamically across Analytics, Investigation, and Basic pipelines using one flexible ingest entitlement.

With DPM, security teams can:

- Retain more data
- Deepen investigation context
- Control SIEM cost with predictable economics
- Meet compliance retention requirements
- Expand detection coverage without increasing SIEM spend

The result is broader visibility, predictable economics, and stronger security outcomes.

HOW IT WORKS

Right Data. Right Tier. Right Cost.

Not all security data requires the same level of processing, retention, or cost.

DPM applies premium analytics where it deliers the highest security value, while lower-cost pipelines preserve searchable investigation context and long term retention.

Pipeline	Description	Relative Cost
Analytics	Real-time threat detection and correlation	Highest
Investigation	Searchable forensic and threat hunting data	Medium
Basic	Long-term retention and compliance storage	Lowest

All three pipelines operate under one flexible ingest entitlement, allowing organizations to balance detection, investigation, and retention without separate licenses or storage tiers.

Flexible Entitlement Exchange

1 GB of Analytics capacity equals:

- 2 GB of Investigation data
- 4 GB of Basic retention data

This exchange model expands effective data capacity without increasing the ingest commitment.

KEY TAKEAWAYS

Broader Visibility. Predictable Cost. Better Security Outcomes.

Retain More Data Without Increasing SIEM Spend

Expand detection coverage and retain more telemetry under one predictable consumption model.

Eliminate the Visibility-Budget Tradeoff

Balance analytics coverage, investigations, and compliance retention without premium pricing.

Align Data Cost to Operational Security Value

Apply premium analytics where it delivers the most value and route lower-priority data to lower-cost pipelines.

Manage Everything Through One Entitlement

Manage Analytics, Investigation, and Basic pipelines under one flexible consumption model.

Reduce Effective SIEM TCO

Organizations can lower effective SIEM costs by 30–50% while expanding visibility and retention.

Real-World Operations

Modern SOCs generate massive volumes of telemetry, but traditional SIEM pricing forces organizations to choose between visibility and cost. High-value detection telemetry, investigation data, and long-term compliance logs are often priced the same, even though they deliver very different security value. DPM changes this model.

Traditional SIEM Model

- Organization generates 100 TB/day of telemetry
- Budget supports premium analytics for only 20 TB/day
- Remaining logs are archived offline or discarded
- Threat hunting and investigations lose context

With Data Pipeline Manager

Illustrative 100 TB/day allocation:

- 20 TB/day to Analytics Pipeline
- 30 TB/day to Investigation Pipeline
- 50 TB/day to Basic Retention Pipeline

Outcome

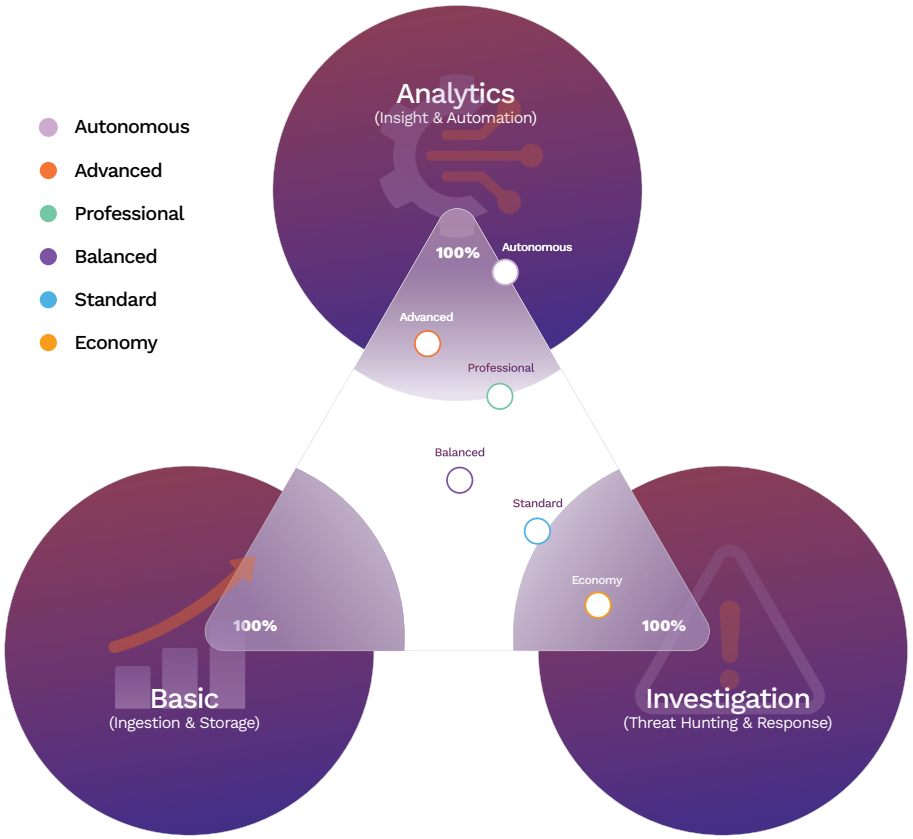
- All 100 TB/day retained across value-aligned pipelines
- Broader searchable context for faster investigations
- Longer, lower-cost compliance retention
- 52.5% lower entitlement consumption than an all-Analytics model

Operational Challenge	How DPM Solves It
SIEM costs growing too quickly	Routes lower-priority logs to lower-cost pipelines while preserving analytics for high-value data
Compliance retention is expensive	Retains long-term logs without premium analytics pricing
Threat hunters need broader telemetry	Keeps broader investigation data searchable at lower cost
SOC teams are dropping logs	Retains more telemetry within predictable budgets
Multiple ingest SKUs create complexity	Unifies all telemetry pipelines under one flexibile entitlement

Data Pipeline Profiles

Distribution across Basic, Investigation and Analytics

Profile	Basic	Investigation	Analytics
Economy	40%	45%	15%
Standard	30%	50%	20%
Balanced	25%	35%	40%
Professional	20%	30%	50%
Advanced	10%	20%	70%
Autonomous	15%	5%	80%



Compared with 100% Analytics Consumption

Progression To Analytics-Driven Value

Profiles evolve from ingestion and investigation toward analytics-led insights and automation.

Investigation At The Core Of Lower Tiers

Economy and Standard prioritize searchable investigation data to expand coverage at a lower effective cost.

Higher Tiers Maximize Analytics Impact

Advanced and Autonomous allocate more capacity to analytics and automation while preserving lower-cost retention and investigation coverage.

Cost Savings

Over 100% Analytics (Free Capacity)

Economy	Standard	Balanced
52.5%	**47.5%**	**36.25%**
Professional	**Advanced**	**Autonomous**
27.5%	**17.5%**	**13.75%**

CUSTOMER BENEFITS

Expand Visibility. Control Cost. Strengthen Posture.

Unified Entitlement Model

Manage Analytics, Investigation, and Basic pipelines through one, flexible ingest entitlement.

Value-Aligned Data Management

Match processing and retention cost to data value and operational purpose.

Elastic Consumption

Rebalance telemetry across pipelines as detection, investigation, and compliance priorities change.

Operational Transparency

Track entitlement use and remaining capacity in a unified dashboard.

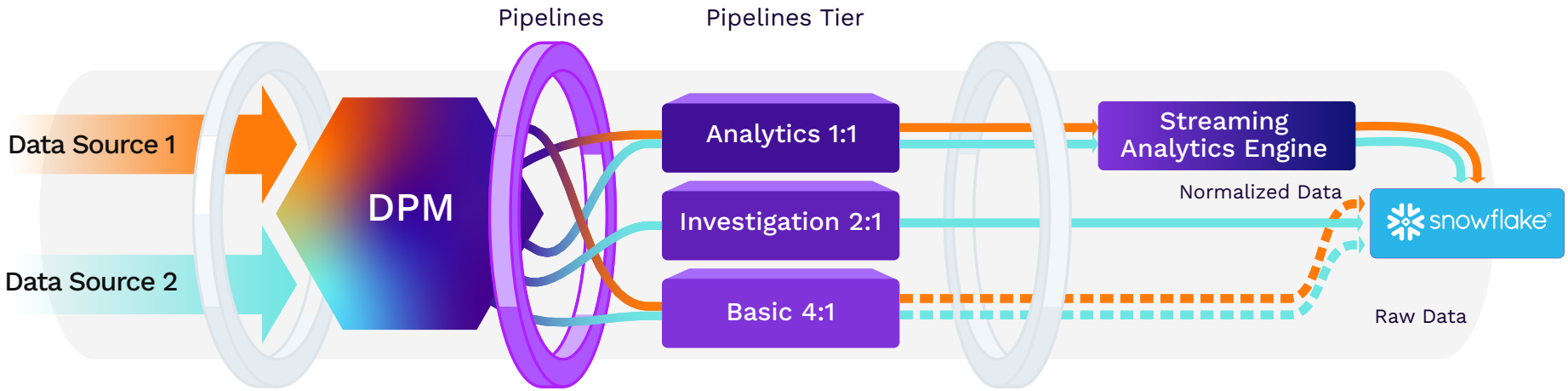
Future-Ready Architecture

Extend the model to additional data tiers and storage destinations as the data strategy evolves.

APPLICATIONS

Built for Adaptive Data Strategies

Elastic Log Ingestion	Route telemetry dynamically as detection priorities change
Cost-Optimized Retention	Retain compliance and forensic data longer without premium analytics pricing
Threat Hunting at Scale	Keep more searchable investigation data available to threat hunters and responders
Unified Data Governance	Centralize visibility, entitlement tracking, and auditing across all telemetry pipelines
MSSP Multi-Tenant Operations	Apply value-based data management across customers with simpler, more predictable billing



Why Securonix

Modern SIEM economics should reflect the value each data set provides, not treat every byte the same. Data Pipeline Manager is native to Securonix Unified Defense SIEM and is designed to align telemetry cost with detection, investigation, retention, and AI-driven workflows.

By aligning SIEM cost to data security value, organizations can:

- Lower effective SIEM TCO
- Retain more telemetry
- Expand detection and threat hunting visibility
- Improve investigation depth
- Support trusted AI-driven workflows with the right data
- Simplify governance through one entitlement

The result is a scalable, predictable, and outcome-driven approach to security operations.

How Securonix Compares

Traditional SIEM Pricing	Data Pipeline Manager
Charges all telemetry equally	Aligns cost to data value
Separate hot/cold storage licensing	One unified entitlement
Premium pricing for retention	Lower-cost retention pipelines
Visibility constrained by budget	Retain more telemetry safely
Multiple pricing meters and SKUs	Simplified operational model

Specifications

Specification	Description
Pipeline Tiers	Analytics, Investigation, Basic
Consumption Model	Single unified ingest entitlement
Relative Capacity Model	1 GB Analytics = 2 GB Investigation = 4 GB Basic
Measurement Period	30-day rolling average GB/day
Platform Integration	Native to Securonix Unified Defense SIEM

Take the Next Step.

Keep More Data. Reduce SIEM Cost. Improve Security Outcomes.

Learn more about Data Pipeline Manager:
www.securonix.com/data-pipeline-manager

For product documentation and pricing details:
documentation.securonix.com