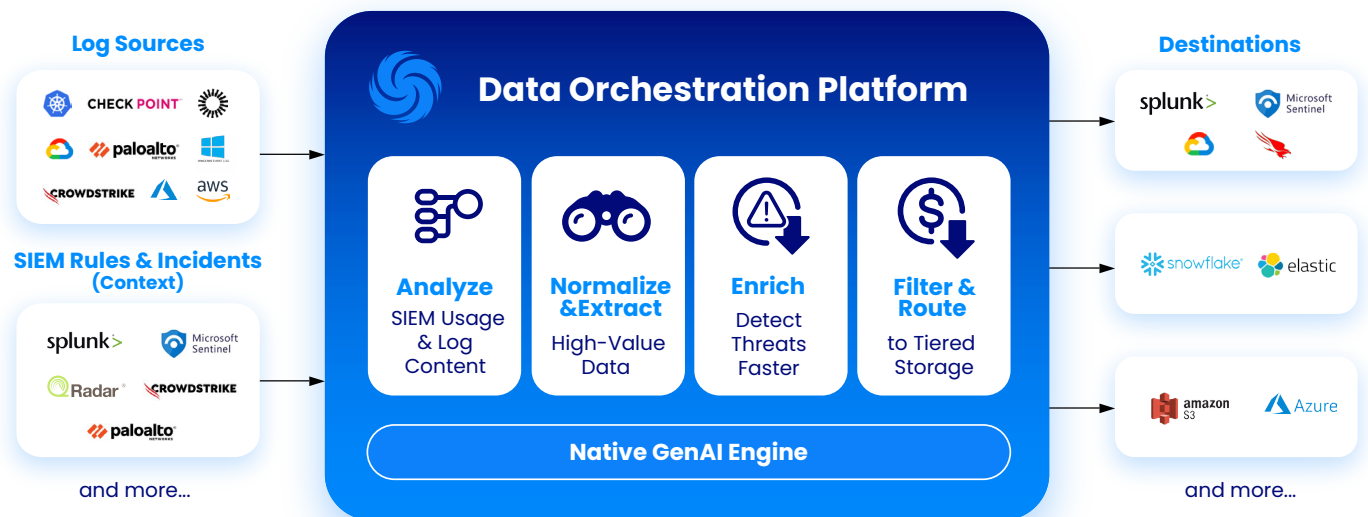


# Modernize Your Security Data Stack

CeTu is the data orchestration platform for the modern SOC, designed to handle the growing scalability demands of security telemetry. Built upon a no-code, security-aware AI model, CeTu's agentless platform optimizes data costs (ingestion, compute, storage) while seamlessly integrating with your SIEM to continuously strengthen security and compliance. Unlike first-generation pipeline tools, it delivers rapid time-to-value – in days or weeks vs. months or years – without manual log analysis and custom scripts.



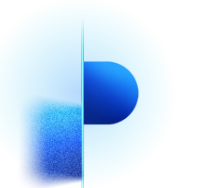
## Boost security

- Quickly visualize structure of logs to understand what you're collecting
- Leverage AI-powered analysis of logs to create new aggregations and enrichments that reduce risk
- Extract more security value from your existing sources
- Ensure you don't miss critical security events



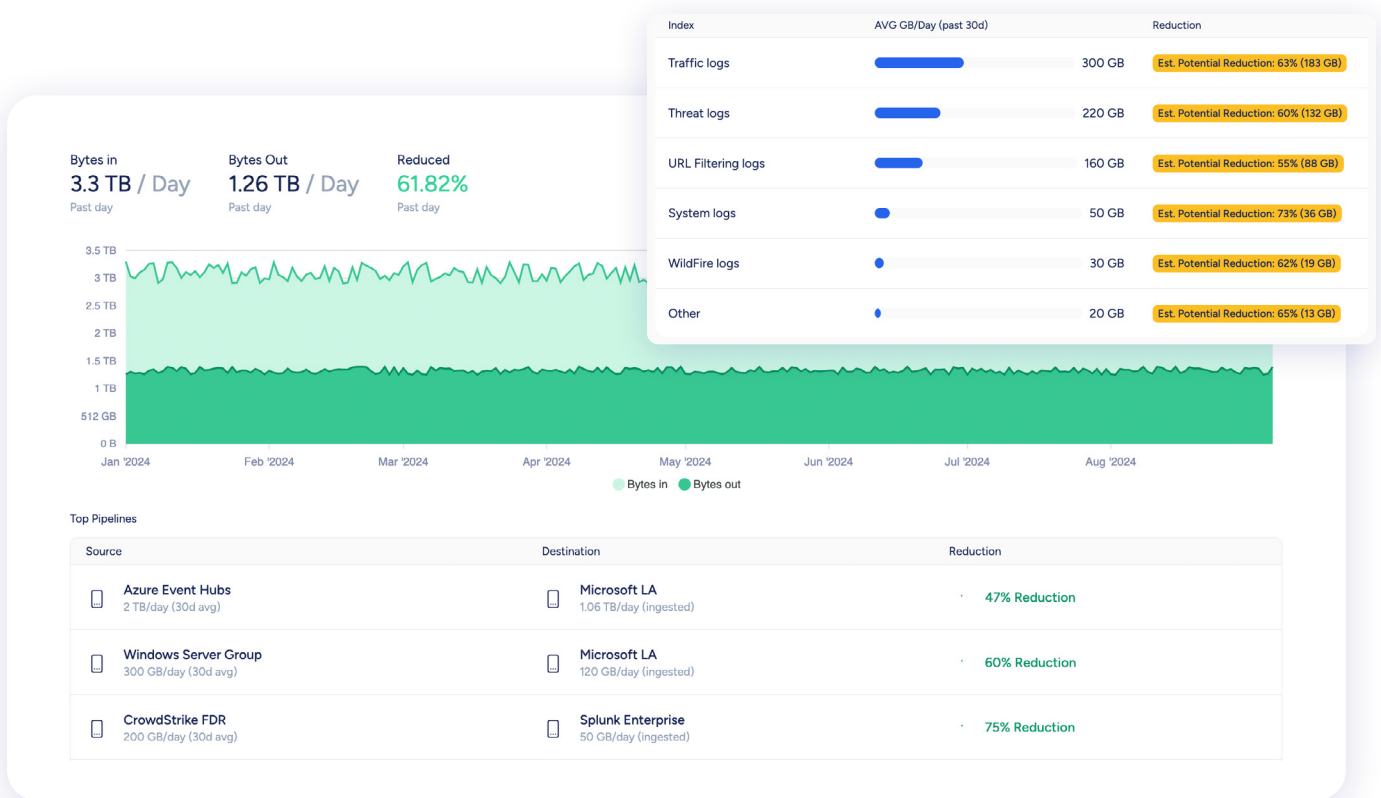
## Scale easily

- Simply point at new log sources and ingest data in the right format
- Automatically filter high-value data for your SIEM while routing non-critical data to low-cost cloud storage
- No prior schema knowledge required
- Easily review & customize via visual no-code approach (drag-and-drop)

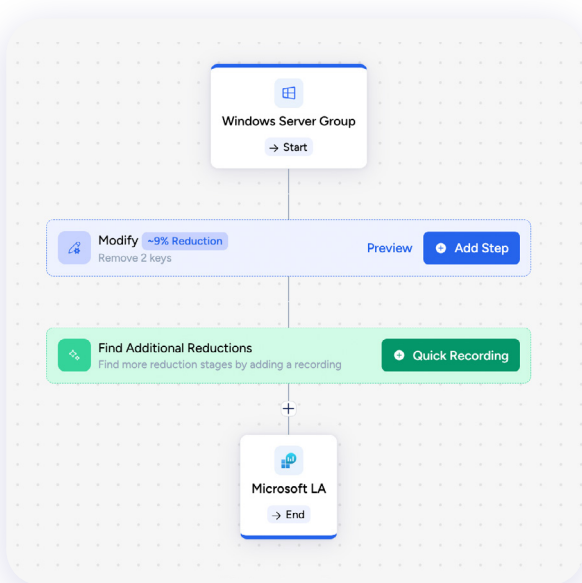


## Accelerate migrations

- Gain granular visibility into data required by your SIEM – without missing data to spot breaches before it's too late
- Easily connect & format new data sources
- Vendor-agnostic approach – easily reconfigure sources & destinations at any time
- Lower data costs (ingest, compute, storage)



Gain immediate visibility into the structure and content of your logs.



SecOps-specific GenAI model automatically identifies new metrics to identify unusual or suspicious activity, as well as opportunities for data reduction.

**Suggesting Aggregations**

- The log file you have provided appears to originate from a Palo Alto firewall, with each record reflecting an individual network session. Consider adding the following metrics to enhance your monitoring capabilities:
  - DDoS Detection**  
In a DDoS attack, allowed traffic mimics normal behavior to overwhelm a network. Since much of your traffic is marked as "allowed" but isn't tracked for DDoS detection, it's crucial to monitor it. Tracking source IPs, destination IPs, and bytes sent helps detect traffic spikes from multiple IPs—key indicators of DDoS attacks.
  - Threat Detection Based on Signature Matches**  
This metric involves monitoring the number of threat events that match known malicious signatures. By analyzing these events, you can identify attempts to exploit vulnerabilities or deliver malware. This is crucial for understanding the types and frequencies of threats targeting your network.
  - File Analysis Results from WildFire**  
Tracks the results of files analyzed by the WildFire cloud-based threat analysis service. This metric provides insight into potentially malicious files that may have been transmitted through your network. It's essential for detecting zero-day exploits and advanced persistent threats (APTs).
  - Anomalous Traffic Patterns**  
Monitors traffic patterns that deviate from the norm, such as unusual spikes in traffic volume, unexpected traffic sources, or unusual port activity. This metric is vital for detecting potential breaches or compromised systems within your network.

**DDoS Detection**

Here you go! I've set up a metric to monitor potential DDoS attacks by tracking unusual traffic patterns

```

if log_type is TRAFFIC
  Group by NAT_Source_IP Source_IP_address
  Group by NAT_Destination_IP Destination_IP_address
  Group by Bytes_Sent Volume_of_data
  
```

Save metric

### About CeTu

CeTu is the data orchestration platform for the modern SOC. Based on its deep contextual understanding of your security infrastructure, our agentless platform enables SecOps teams to effortlessly scale data pipelines, strengthen security and compliance, and optimize costs.

Founded by security experts from industry leaders such as Microsoft and Zerto, with backing from early-stage investors in Palo Alto, Zscaler, and Armis, CeTu is currently deployed in some of the world's largest and most complex SOC environments. C'est tout!

For more information, visit [cetuo.io](https://cetuo.io)

