VirtualMetric

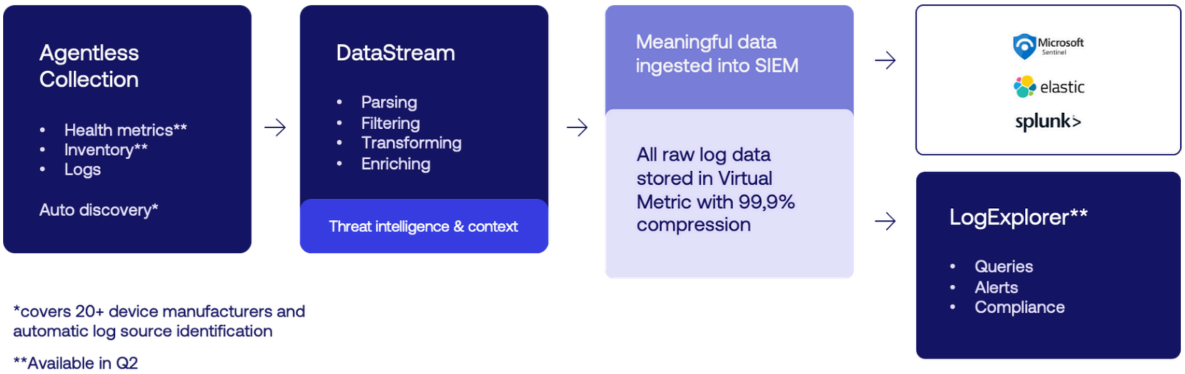
virtualmetric.com

Introducing DataStream

The Ultimate Pipeline Engine for Speed, Efficiency, and Security

Vectorized Pipeline Engine

VirtualMetric's vectorized pipeline engine is designed for unparalleled speed and efficiency. By utilizing all available cores, it processes maximum log volumes in record time and ensures parallel data ingestion to target SIEMs. With over 10x ingest performance compared to traditional solutions and up to 99% disk and network compression, VirtualMetric minimizes bandwidth usage and reduces disk space for queuing—delivering unmatched performance and cost savings.



Agentless Collection

- Health metrics**
- Inventory**
- Logs

Auto discovery*

→

DataStream

- Parsing
- Filtering
- Transforming
- Enriching

Threat intelligence & context

→

Meaningful data ingested into SIEM

→ Microsoft Sentinel, elastic, splunk>

All raw log data stored in Virtual Metric with 99,9% compression

→

LogExplorer**

- Queries
- Alerts
- Compliance

*covers 20+ device manufacturers and automatic log source identification

**Available in Q2

Redefining Telemetry Sources

Unlike classic solutions that focus solely on data collection via protocols or third-party agents, our **Dataset** approach categorizes data at the source—such as Windows Event Logs, Linux Audit Logs, or Windows User Activity—streamlining pipeline processing and enabling advanced RBAC. With datasets, you can

- Define role-based access controls
- Ensuring teams working on the same source are fully isolated and unable to view each other's data.

Agentless OS Data Collection

Without requiring third-party tools or pre-configurations, you can collect data seamless from operating systems like Windows, Linux, Unix, MacOS, Solaris, AIX, and more. . Our system leverages **read-only user rights** for secure remote access, ensuring data integrity and compliance.

By integrating with Credential Stores or Active Directory Service Accounts, VirtualMetric eliminates the need for user credentials, streamlining secure connections. Collected data is automatically translated into Datasets, optimizing it for maximum efficiency in the pipeline engine, and ensuring unparalleled performance for audit and forensic data processing.

Crafted for Seamless Microsoft Sentinel Integration

VirtualMetric's pipeline engine is specially crafted to integrate seamlessly with Microsoft Sentinel. By extracting context from log messages, our solution automatically ingests data into the appropriate ASIM tables, drastically reducing manual effort and accelerating integration. With contextual filters, users can easily optimize data ingestion, ensuring only relevant information is sent to Sentinel—saving time, reducing costs, and enhancing efficiency.

Reliable Pipeline Engine with Zero Data Loss

VirtualMetric's Write-Ahead Log (WAL) architecture provides a robust foundation for data reliability by securely storing all routing and pipeline states on disk. This ensures zero data loss, even in the event of a crash. Unlike solutions that require additional components like Kafka, VirtualMetric caps log duplication at just one message while maintaining simplicity in deployment. The WAL approach also minimizes the risk of system downtime, ensuring that your telemetry pipeline is always reliable and consistent, even under heavy loads.

Familiar Pipeline Language with Extensive Processor Support

VirtualMetric's pipeline engine adopts the widely recognized Elastic Ingest Pipeline format, allowing IT and Security Engineers to create and manage pipelines effortlessly. With over 50+ processors, VirtualMetric provides the most comprehensive processor support in the industry, enabling low- or no-code management for tasks like parsing, enrichment, filtering, routing, and more. Engineers with Elastic experience can seamlessly leverage this robust and flexible pipeline engine, reducing onboarding time while enhancing operational efficiency.

Advanced Data Routing Options with Seamless Flexibility

VirtualMetric simplifies data routing with its advanced reroute processor, eliminating the need for manual filtering conditions required in other solutions. This processor allows users to route data effortlessly to destinations at the pipeline or content pack level without relying on a source-based approach.

With VirtualMetric, advanced filter conditions can be applied for precise data routing, and the Dataset concept further streamlines routing by enabling multiple data sources to converge into a single SIEM endpoint. This flexibility empowers IT and Security Engineers to design efficient and scalable routing strategies with ease.

Introducing VMF 3.0: The Next-Gen File Format for Pipeline Engines

VirtualMetric File Format (VMF) 3.0 is a state-of-the-art file format engineered specifically for high-performance pipeline engines. Evolving from Apache Avro, VMF combines the efficiency of a row-based format with the ability to handle massive volumes of small data chunks. Its advanced design enables disk-level merging without consuming system resources, overcoming the limitations of Avro OCF, which requires resources for merging compressed files. VMF achieves up to 99% compression, making it ideal for both storage and network transport. Out of the box, it supports features like Bloom Filters, Zero Trust Storage, Log Chaining, and TSA, making it the ultimate file format for forensic integrity, fast searches, and secure data handling.

More information?

For more information please contact us at:

michiel@virtualmetric.com
www.virtualmetric.com