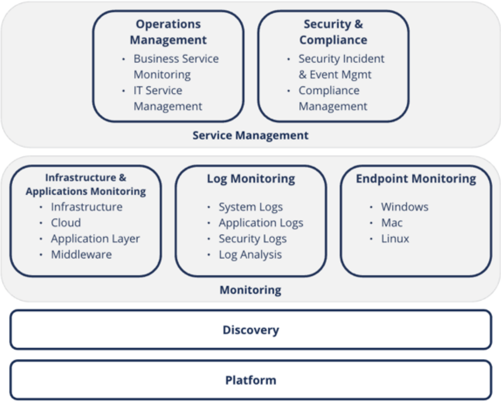
Annex 1:

VirtualMetric Product Description Document

The purpose of this document is to provide a general overview of the capabilities that VirtualMetric's platform provides. The intent is to inform about the structure of the platform, its components and how they relate to each other, as well as operational information.

1. Introduction

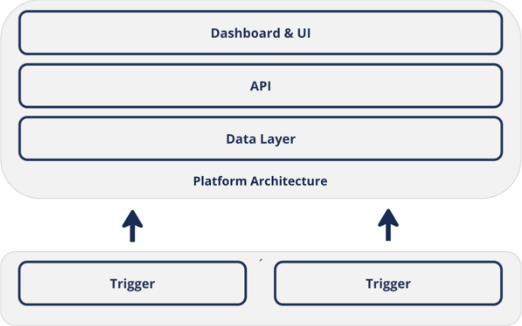


Our all-in-one monitoring platform provides organizations with a way to increase their customers' experience when using their digital services. It helps teams to operate their services more efficiently, focused on security and lowering costs while increasing uptime.

To deal with the extremely high amount of data, that not only needs to be collected and analyzed in a meaningful way but also put in the right business context, our platform comes with several modules.

- The **Platform Layer** provides the right architecture and key components that are used by all our capabilities.
- The Discovery Layer creates an inventory of all IT assets.
- The Observability Layer supports the monitoring of IT assets, whether these are infrastructure components, applications, endpoints, or logs.
- The Service Management layer translates the outcomes of the observability layer to business context, both from an operational perspective but also considering security and compliance-related topics.

2. Platform



The platform is comprised of a management stack and so-called **Triggers** for data collection. It features a multi-tenant setup and can be deployed in high-availability mode. The individual components scale horizontally to optimize performance during data processing.

- The **Dashboard & UI layer** acts as an entry point for users, it fetches the data from the API layer and presents it in the form of dashboards, reports, or analysis overviews.
- The API layer controls the data flow of the platform and takes care of access management, including user and tenant segregation. It processes incoming data as well as data requests from the UI layer. The connectivity capabilities allow for data enrichment from other sources as well as sending information to solutions like IT Service Management tools for incident generation.
- The data layer is optimized for the different use cases the platform supports. It ensures that both telemetry data and information from logs are properly ingested and made available for analysis.
- Triggers are used to collect information from the components in the environment, the extraction process is agentless.

3. Discovery

The **Discovery layer** creates an inventory of the target IT landscape. It automatically detects details such as OS types and related assets. It also detects running applications and their configuration. The discovered configuration will then be used to create a monitoring profile automatically.

4. Monitoring

The monitoring layer provides the means to monitor your IT landscape.

4.1 Infrastructure & Application Monitoring

Metrics can be collected from all layers of the IT infrastructure. From physical devices like hosts or network equipment, virtualized environments, hosts OS information to the application and middleware tier, key metrics are observed. The triggers consolidate the collected data and send it back to the API layer for processing.

4.2 Log Monitoring

Various types of logs can be monitored: System logs, application logs, network logs and security logs. Log information is collected and, through the triggers, sent back to the API layer. After ingestion, log information can be interpreted using the **Log Analyzer**.

4.3 Endpoint Monitoring

IT end user equipment can also be monitored, metrics can be collected from devices running either Windows, Linux or MacOS.

5. Service Management

Leverage the insights gained in the monitoring layer, VirtualMetric improves your customers' experience by supporting your IT management processes. The focus lies on improving IT Operations, as well as Security and Compliance related aspects.

5.1 Operations Management

Monitoring your entire IT landscape allows for a thorough analysis, the impact of changes or deviations can be put into the right context. Through tracking changes, smart alerting and an integration to IT Service Management tools, the right teams can be put to work, driving a shorter mean-time-to-restore (MTTR).

5.2 Security & Compliance

To ensure that the impact of security-related incidents in minimized, VirtualMetric provides Security Incident and Event Management (SIEM) capabilities. Insights gained from log monitoring and analysis are associated with the right context, leading to swifter resolution and even prevention of security-related incidents. Additionally, VirtualMetric tracks your compliance score to ensure that deviations from your configuration can be discovered as early as possible.

Appendix A - Glossary

Application Server

An application server is a physical or virtual server that runs applications like IIS or a MSSQL database. The term is used to describe a server that requires monitoring for both the host OS and the applications running on top of it.

Daily Data Ingest

Daily data ingest describes the amount of raw data that is sent to the monitoring solution for processing on a single day.

Endpoint

An endpoint describes a physical or virtual machine that can be accessed through the network where the number of ports (See “Ports”) describes the number of potential access points to any network. This usually refers to network devices or end-user devices that communicate over SNMP (See “SNMP”)

Hyper-V

Hyper-V is the name of Microsoft’s virtualization solution based on their Windows operation system.

Log Monitoring

Log Monitoring describes the process of extracting and processing event or streaming based information from files that reside on a physical or virtualized machine. The data is extracted from the logs, sent to the VirtualMetric solution, and processed there.

Ports

A port is part of a physical or virtual machine, like a server or network device, that allows a connection to a network to be established.

Server

A server is a physical or virtual machine that runs an operating system. It is used to operate applications, services and/or processes.

Service Monitoring

Service monitoring refers to simple availability checks performed remotely, without the use of an agent. Examples are ping tests (ICMP) or DNS tests.

SNMP

Simple Network Management Protocol is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Socket

A socket describes the part of a physical machine that allows a Compute Processing Unit (CPU) to be mounted.

Subscription

A subscription refers to a service or arrangement in which a customer pays a regular fee to access and use a product, service, or content over a specified period.

Virtual Machine

A virtual machine (VM) is a software emulation of a physical computer, capable of running its own operating system and applications as if it were a separate physical machine.