TELEMETRI

Use-Case

Cloud Migration & Optimization

Data migration can be difficult, dangerous, and complicated.

Given the President's Report on IT Modernization IT departments across the nation are moving to Infrastructure as a Service (IAAS), resulting in a hybrid enterprise. When IT departments are charged with moving data from controlled, on-premises servers to "the cloud," those cloud environments can offer many genuine operational and cost benefits.

However, these migrations also introduce new sets of fears and risks of control loss and security threats. Such migrations present opportunities to eliminate ballooning costs, improve operations, and enhance security – but in the absence of **Telemetri**, they can also have the opposite impact.

Further, because data centers hold sensitive or proprietary information, such as customer data or intellectual property, sites must be both digitally and physically secured. So, for example, an enterprise migrating from internal onsite infrastructure to the cloud will be highly concerned with ensuring that the places they think they are storing data actually are the places where they are storing data. **Telemetri** provides that degree of transparency.

Telemetri enables users to know exactly where they "live" in the cloud and how they got there.

Telemetri collects data from the entire internet every six days, at every level, country, state, county, city and so forth, creating a comprehensive map of network traffic and destinations. This information enables analysts to precisely determine the location of, and traffic flows associated with, their data.

For example, if regulations restrict data to storage to one cloud hosting environment such as Microsoft Azure or one geographic region, **Telemetri** can identify if the cloud provider is storing or communicating that data elsewhere. In other words, most organizations have a rich security infrastructure but – without a resource like **Telemetri** – lack visibility into what they're interacting with outside the fence: what networks, what chokepoints, what DNFs, and more.

Telemetri doesn't merely monitor and document everything going on in the data center – many different tools can accomplish that function. **Telemetri** was developed to amplify the effectiveness of these investments, not replace them. **Telemetri** is designed to effectively detail how systems are being used, for what, and where.

With a clear understanding of how cloud services are being provisioned and utilized – from data storage through virtualization platforms, data management through networking – cloud systems that are being underutilized can be restructured or disabled, data that's being stored or communicated inappropriately can be identified and locked down, and threats emerging from networks interacting with the cloud host can be promptly identified and acted upon.

Additionally, Telemetri makes its enriched data accessible and understandable to analysts and other human users.

Telemetri provides a comprehensive dataset of enriched network data. Commercial Cloud Provider data is collected as an additional data source. Initially, this data presents in the same format as in which it is captured (log format). **Telemetri** enriches the data to add value, transparency and classify these values into information that can be processed by both machine tools and human users.

For example, cloud telemetry log flow records from AWS come in the following format:

Normal:

version: 2
account-id: 123456789010
interface-id: eni-abc123de
source address: 192.168.21.10
destination address: 13.67.144.7
source port: 20641
destination port: 22
protocol: 6
packets: 20
bytes: 4249
start: 1418530010
end: 1418530017
action: ACCEPT
log_status: OK

Using **Telemetri**:

version: 2
account-id: 123456789010
interface-id: eni-abc123de
source address: 192.168.21.10
destination address: 13.67.144.7
-- Telemetri enrichment
network name: azure : uscentral
network group: Cloud Services
network type: Commercial Cloud Provider
date of expiration: 5/31/2019 23:59
network country: us
network ticpi: 76
asn rank: 23
network asn integer: 8075
network asn: AS8075
-- Telemetri enrichment
source port: 20641
destination port: 22
protocol: 6
packets: 20
bytes: 4249
start: 1418530010
end: 1418530017
action: ACCEPT
log_status: OK

Although this is output from the cloud instance, the first example offers almost no meaning; but when enriched with **Telemetri** in the second example, this problem is resolved and now provides insight into the Microsoft Azure network range.

Similar log data covers almost every aspect of cloud telemetry:

- Infrastructure metrics (CPU, memory, I/O, etc.)
- Application activity (database response times, exceptions, etc.)
- Business activities and KPIs (business transactions per hour, etc.).

Telemetri is used to enrich this data uniquely enabling organizations to remove the often-opaque nature of network telemetry data and visualize Cloud Service Providers which host their data and infrastructure as a service. In other words, **Telemetri** offers users a solution which enables them to see aspects of their cloud deployment that they've never seen before or thought were possible, including exactly where their data is, and where those networks are.