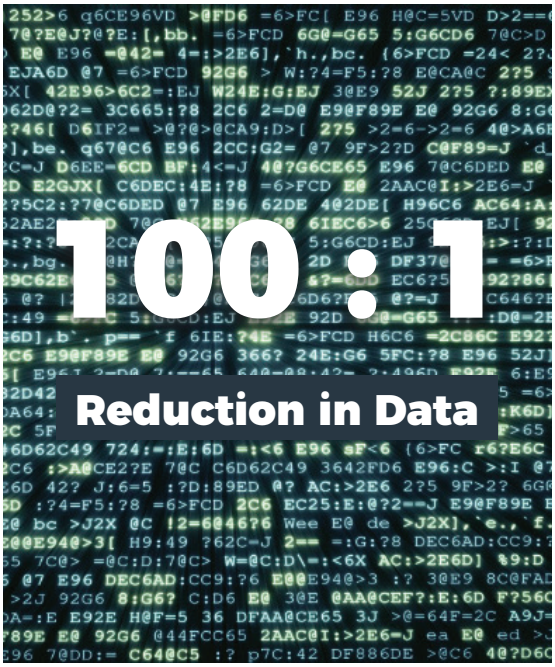
CYFLARE

DATA SIFTER
PERVASIVE DATA COLLECTION

At A Glance

- Captures network traffic,command execution, file events and process information
- Transforms network packets to meta-data and reduces data from 100 to 1
- Detects breach attempts and correlates data
- Lightweight deployment consuming limited CPU and memory
- Deployable either as an agent, container, virtual machine, or physical appliances
- Deployable as an agent in Ubuntu 14.04 + , Centos 7.0 + , Red Hat 7.4 +



Data Sifter Benefits

Data Sifters are lightweight software sensors that consume a minimum of 1 CPU core, 1GB of memory and 2GB of disk space. These sensors can be deployed as VMs inside VMware, HyperV, KVM, AWS or Azure hosts, as a container, as an agent directly on a server or can be deployed as a physical appliance. The purpose of the Data Sifter is to capture network traffic, files, server commands process information, file activity. It performs deep packet inspection, data correlation, security analysis and converts packets into meta-data which result in a 100 to 1 reduction in data. This is all done while preserving all of the important and relevant information inside the packets. The Sifter sends the data off to a Data Refinery that correlates, enriches, stores and performs machine learning.

The benefit of deploying Data Sifters pervasively throughout your infrastructure is to gain better visibility into east to west traffic flows in addition to north to south traffic flows. Other solutions in the market that deliver network visibility such as Firewalls, APM and various network and security tools fail in delivering East to West traffic visibility because they are too heavyweight to deploy pervasively and rely on full packet forwarding in order to do analysis. Data Sifters only forward meta-data, which is a subset of full packet data and therefore allows the system to scale pervasively.

System Requirements

The Data Sifter can be deployed as an **agent, container, virtual or Physical** appliance on standard x86 architecture. The software packaging comes in the form of an RPM, DEB, OVA, QCOW2, VHD, AMI or container that can be deployed onto the server or inside VMware, KVM or as a Docker.

vmware KVM amazon web services Microsoft Azure x86

Minimum Server Requirements

- ☑ Virtual/Physical Machine
- ☑ 1 CPU
- ☑ 1 GB RAM
- ☑ 2 GB DISK
- ☑ 1 NIC

CYFLARE

DATA SIFTER
PERVASIVE DATA COLLECTION

Data Sifter Functionality

The function of the Data Sifter also known as the DS, is to capture RAW Ethernet packets off the physical or virtual wire, perform application identification, capture files, server commands and processes and transform into newly correlated meta-data. The Data Sifters extensible application identification engine can detect greater than 3,000 network applications. After identifying applications it is also able to generate thousands of meta-data records for those applications and derive performance information for those applications as well as detect security events.

By converting packets into meta-data correlated with other information, significant savings can be achieved at a ratio of 100 to 1. For example, if the DS captures 10 gigabits of traffic, the DS will only send 100 MB of data to the Data Processor for storage and analysis. With this benefit, network operators no longer have to build expensive and dedicated monitoring networks because meta-data traffic can be transmitted over the same physical network as the regular traffic.

Data Sifter Deployment

Data Sifters are deployed either as an agent, VM or container within virtual hosts or within the physical network. A Virtual Data Sifter can be connected to the mirror port of a virtual or physical switch. Another useful option of the data sifters deployment is as an agent. When deployed as an agent, additional functionality such as command execution, file activity and process monitoring can be achieved and data can be correlated locally. Data Sifters can be deployed either manually within each virtualized server no differently than you would install a Virtual Machine. They can also be deployed using Puppet, a common Linux orchestration framework, by using VMware's global management tools or by using the management user interface.

Feature Summary

- Quickly identifies applications with the first packet of a flow
- Packet De-duplication & meta-data extraction
- Correlation of meta-data with command execution & process information
- Supports IPFIX, JSON and Syslog output for integration with 3rd party tools
- Multi NIC support on physical appliance for increased throughput and port density
- Multi-Core support up to 64 cores on a single machine
- Centrally manageable & configurable

Data Sifter System Performance

The following table shows the performance characteristics of the Data Sifter when increasing system resources.

Raw Traffic	Meta-Data	Traffic Cores	Memory	Disk Storage
100 Gbps	1 Gbps	32	64 GB	1 TB
40 Gbps	400 Mbps	16	32 GB	512 GB
10 Gbps	100 Mbps	4	8 GB	256 GB
1 Gbps	10 Mbps	1	2 GB	64 GB
256 Mbps	3 Mbps	1	1 GB	2 GB

Flexible Deployment Options

- ☐ Lightweight Virtual Appliance
- ☐ Pre-Configured Hardware Appliance
- ☐ Server Agent

100 Series Appliance supports up to 3 gbps of network throughput