

MetaFlows.com / 877.664.7774

715 J ST STE 205 - San Diego - CA 92101

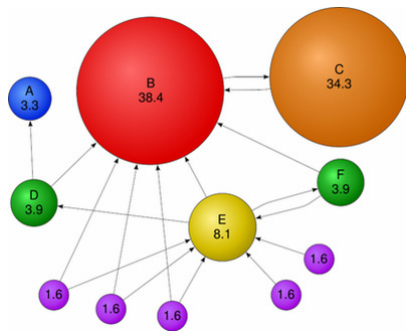
MetaFlows' Security-as-a-Service (SecaaS)

➤ Overview

The Software-as-a-Service (SaaS) model is revolutionizing the software industry because it reduces complexity and cuts costs while increasing productivity and online collaboration. The MetaFlows Security System (MSS) is the first and only product built from the ground-up that uses the SaaS model to simplify and streamline network security monitoring and compliance applications. The MSS's **Security-as-a-Service (SecaaS)** product is a quantum leap in several ways:

- Predictive Global Intelligence. The MSS ranks security events based on global statistics across administrative domains rather than static, local policies.
- Confidentiality. Application data (payload) is never stored outside your network. The security event messages are stored in the MetaFlows Cloud using a highly secure cloud infrastructure (Amazon EC2) that makes these records as secure as your bank account records.
- Reduced IT Costs. The MSS can run on off-the-shelf hardware, VMware virtual appliances or EC2 Amazon instances. All software and intelligence updates are automatically and seamlessly applied without user intervention. All updates are available on the next browser refresh.

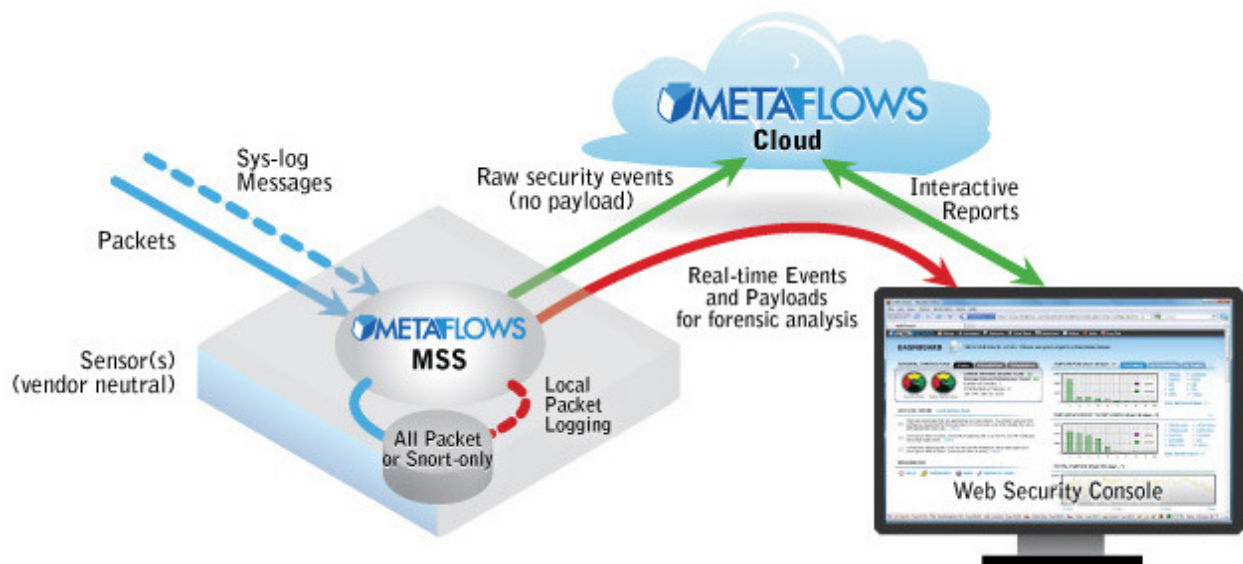
➤ Predictive Global Correlation



The core of the MSS resides in the Metaflows Cloud. Anonymous security event data from Metaflows customers' sensors is automatically sent to the cloud. There it is compared and correlated using a system mathematically similar to Google's page ranking algorithm. The resulting intelligence data can then be pushed out back to the individual sensors to rank security events that have significant global relevance. The outcome of the algorithm is that once a piece of intelligence reaches our system it is not equally distributed to all customers. Instead, it is mathematically weighted and routed to where it is most relevant, just as the first few web pages of a Google search yield the most relevant information for a particular search. This process gives Metaflows' customer actionable intelligence not available anywhere else in the world.

➤ **Confidentiality**

In the default configuration the MetaFlows Security System exports security event messages to the MetaFlows Cloud and stores packet logs on the local sensor's disk. In our system this separation is very strict; the MetaFlows Cloud will **always only** contain security event messages and the local disk will **always only** contain packet logs. This division makes cloud-based security event monitoring much more practical.



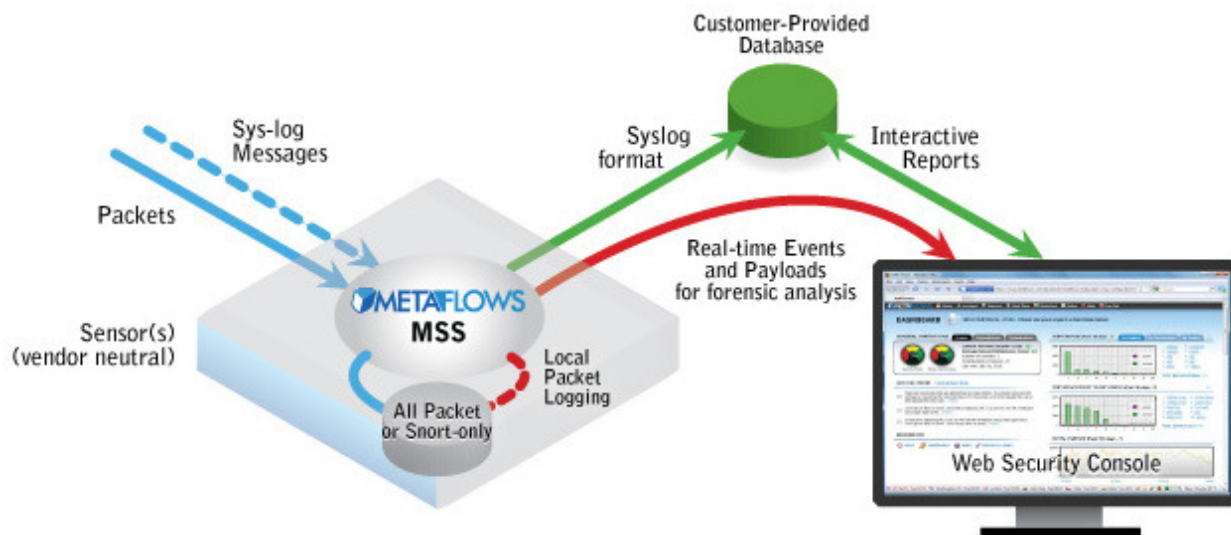
Very sensitive payload data contained in the packet logs is protected by the customer's own network security infrastructure inside the sensor (usually placed behind a firewall). The security event messages are stored in the MetaFlows Cloud using a highly secure cloud infrastructure (Amazon EC2) that makes these records as secure as your bank account records. The advantage of this architecture is that security event data can be globally and anonymously correlated in the MetaFlows Cloud to give you much better security without jeopardizing data confidentiality in any way.

As shown in the figure above, the ranked security events are made available through a web security console either as historical, interactive reports, email alerts or real time event flows. The payloads never leave the sensor's hard disk unless a properly authenticated user queries the sensor for particular payload data to be included in an escalation report. Optionally, the local packet logging can also be restricted to log only the packets that cause security events (Snort logging).

MetaFlows.com / 877.664.7774

715 J ST STE 205 - San Diego - CA 92101

The MSS can also be modified not to export security events to the MetaFlows cloud. In this configuration, depicted in the figure to the left, the security events are instead sent out in standard syslog format and are consumed by a customer-provided database. As in the default configuration, the payloads are still stored locally and available to a properly authenticated user through the Web security console. (See graph below)



➤ **Reduced IT costs using open standards**

The SecaaS model reduces IT expenditures by supporting off-the-shelf hardware, VMWare and/or Amazon EC2 instances.



Off-the-shelf Hardware Appliances			
	Desktop 1Gbps	1u 1Gbps	1u 10Gbps
RAM	4 GB	4 GB	24 GB
Hard Drive	1 TB	1 TB	4 x 1TB
Processor	Intel Core i7	Intel Core i7	Intel Xeon (2)
Ports	2x1G	3x1G	2x1G + 2x10G
IDS/IPS Throughput	500 Mbps	800 Mbps	5 Gbps

➤ **Ultimate flexibility**

Collaboratively monitor your security with a secure Web browser from anywhere in the world.



➤ **Automated software updates**



- i. Metaflows automatically updates all customers' security intelligence data daily. This takes place behind the scenes without any hassle.
- ii. All software updates are implicit (i.e. software updates are applied every time the system is used)
- iii. The MSS appliances are based on open OS standards with built-in update services and easily replaceable components.

