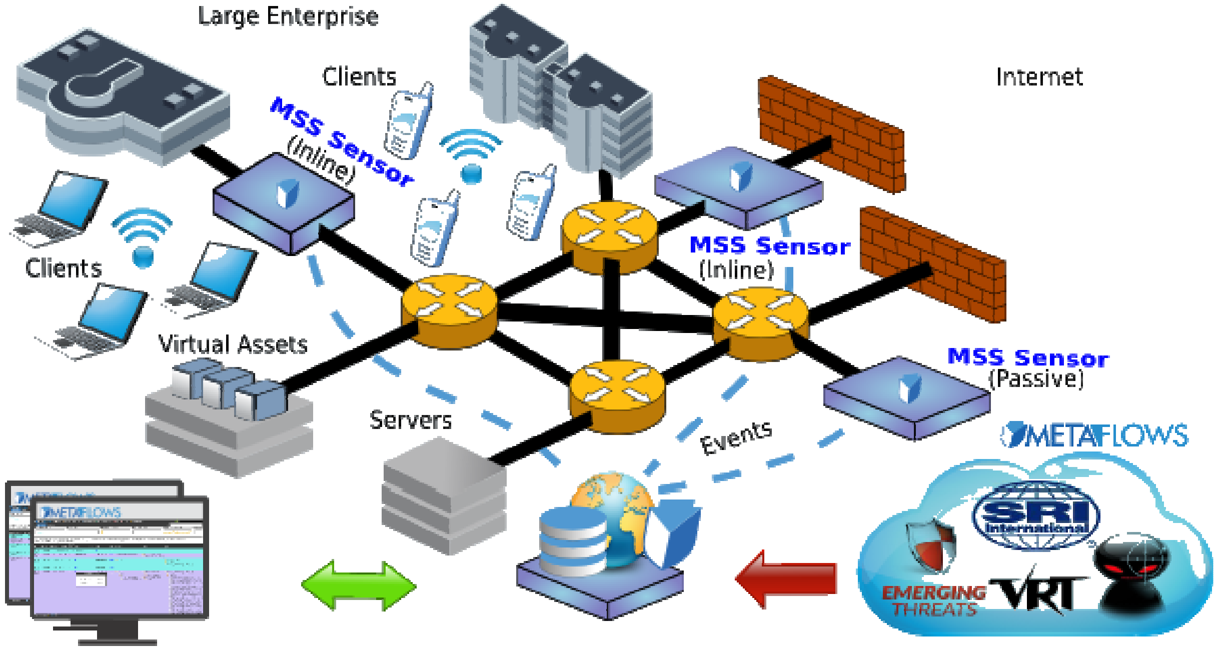
METAFLOWS®
A NEW APPROACH TO NETWORK SECURITY

MetaFlows.com / 877.664.7774

715 J ST STE 205 - San Diego - CA 92101

The MSS Global Enterprise

Our software monitors network traffic to detect and prevent security problems. Security event messages are exported to the MSS Global Enterprise cloud infrastructure where they become available for secure browsing. The advantage of this architecture is that security event data can be globally and anonymously correlated in the MSS cloud to give you much better security awareness. Once malicious activity is detected, it can be easily shut down using our powerful web-based forensic interface.



Advanced Malware Detection

The MSS provides high-speed malware detection/prevention using BotHunter, daily signature updates and Geo-location intelligence.

SIEM & Log management

Merge real time security information with 3rd-party network-based and host-based monitoring systems.

Intrusion Prevention

Efficient and cost-effective network protection. Easily shut down exploits, Bots, C&C communications, Phishing attempts or sites with bad reputation.

Security Software as a Service

Rich analysis and advanced reporting tools from a secure web browser. Access actionable alerts anytime from anywhere.

Flow Analysis & Monitoring

The MSS adds flow analysis to catch covert data exfiltration and/or anomalous communication patterns. You need to know where your data is going.

Cloud Security

Seamlessly monitor cloud-based assets. The MSS efficiently secures your cloud without the dangers of traffic replication.

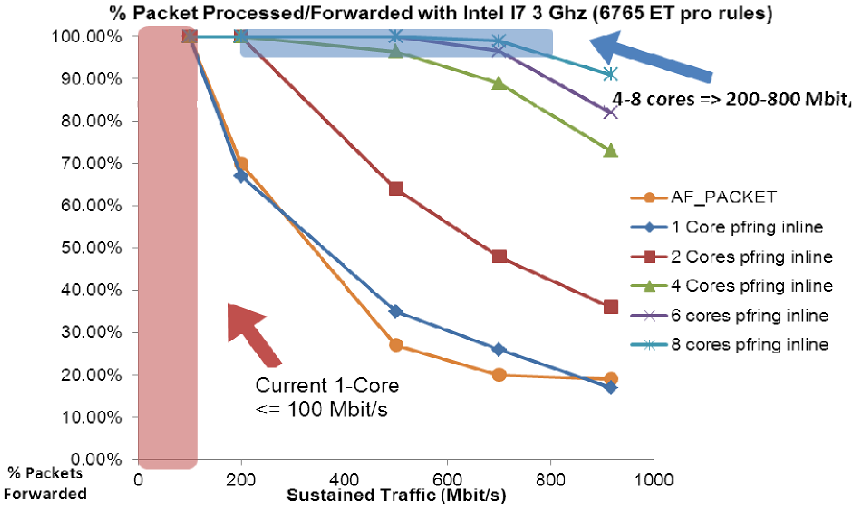
The portion of the MSS software running on the sensors is a highly configurable coordination program that allows running a mix of best-of-breed, open source and proprietary monitoring plugins (Snort, BotHunter, Ntop, OSSEC, p0f, syslogd, etc). The MSS software provisioning and configuration is managed through a web browser allowing multiple users to share system management functions. The MSS sensor software can run on:

Throughput (Mbps)	Operating System	Hardware	Application
100-200	Linux CentOS VMware Windows server 2008	Single CPU, Amazon AWS	Small Enterprise Cloud Security
<800	Linux CentOS	Single CPU 8-12 cores	Small/Medium Enterprise
800 -5000	Linux CentOS	Dual CPU 24 cores	Medium Enterprise
5000-10000	Linux CentOS	Quad CPU 64 cores	Medium/Large Enterprise

Advanced IDS for Malware Protection

The MSS reliably finds Malware using a 3-layered approach. Each layer is highly scalable and works independently to progressively increase the detection accuracy.

Layer 1: Session Level

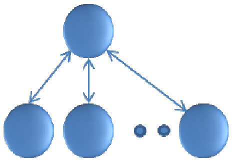


Traditionally, security events are generated by reconstructing a single session between two endpoints and finding known patterns that indicate a security violation within that session. This is the most basic level of intrusion detection and it is the extent of what most network security products offer today. It usually results in a very high false positive rate where important events are obfuscated by the huge volume of uninteresting security events. The MSS runs Snort as our session-level tool. Using a powerful open-source open source kernel module called PFRing, we have been able to parallelize Snort for both inline and passive applications. This allows performing session-level analysis on inexpensive off-the-shelf hardware. The MSS can process up to 800 Mbits of traffic with almost no packet drop using a standard, off-the-shelf machine costing approximately $1000.

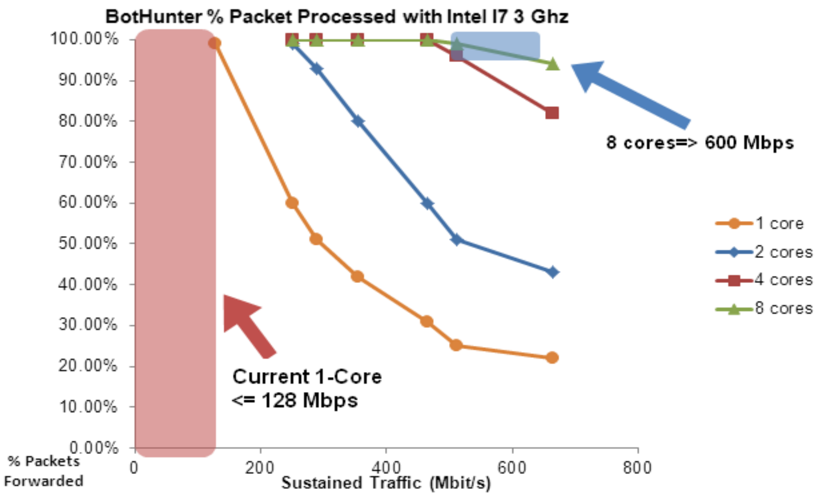
Layer 2: Inter-Session

With inter-session correlation, we identify typical infection behavior by looking at alerts from multiple sessions belonging to a single home machine. The MSS positively scores alerts based on observing at least two events corresponding to the typical phases of a Bot Infection.

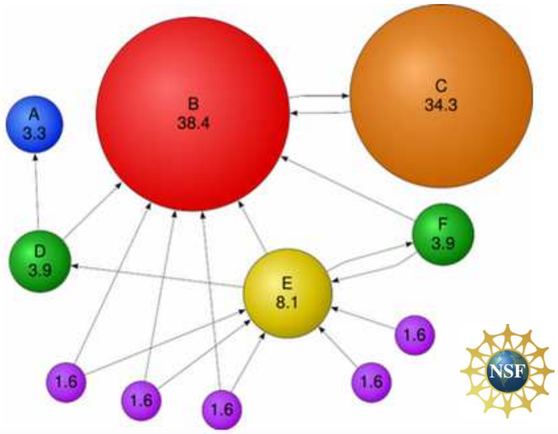
1. Inbound scanning
2. Exploit
3. Egg download
4. C&C communication
5. Outbound scanning/propagation



Inter-session analysis tends to eliminate false positives almost entirely and brings true positives to the forefront. This proprietary analysis is performed by Cyber-TA's BotHunter (licensed to Metaflows by SRI International). BotHunter intelligence feeds and rules are updated weekly from the SRI Malware Threat Center. BotHunter also benefits from our multi-processing framework. The MSS can run BotHunter on as many cores as are available. As the number of cores increases, BotHunter's ability to process more network traffic increases dramatically.



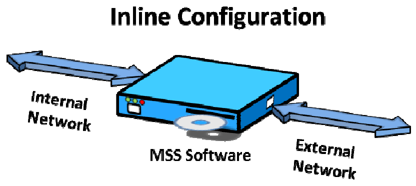
Layer 3: Inter-Domain (Predictive Global correlation)



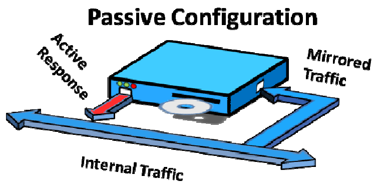
Security events are compared between domains

Research funded by the National Science Foundation has led to the developed of a proprietary inter-domain correlation algorithm that is mathematically similar to Google's Page ranking. Event scores are autonomously obtained from a global network of honeypot sensors monitored by the MSS. The honeypots are virtual machines that masquerade as victims. As the honeypots are repeatedly attacked, the MSS records both successful and unsuccessful hacker techniques and corresponding security event information. The security events that trigger false positives are ranked negatively, thus providing insight into events that should be routinely ignored or turned off. Security events that trigger true positives are ranked positively thus improving their visibility. This information is then propagated in real time to each of our subscribers' sensors in the system to augment the session level and inter-session-level ranking described above. This additional inter-domain correlation is important because it adds operational awareness based on real-time intelligence.

Soft Intrusion Prevention

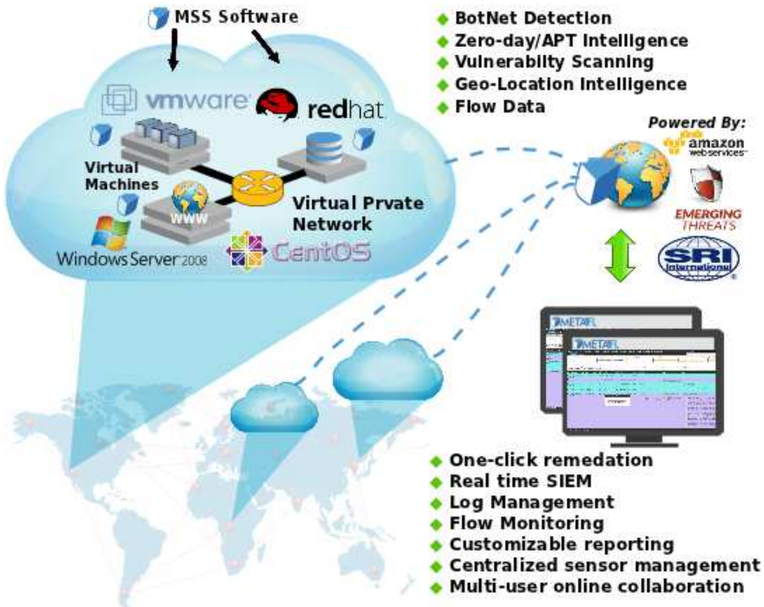


A traditional IPS costs tens-of-thousands of dollars. The MSS can be deployed as an intrusion prevention system in either inline or passive mode on a standard, $1000 machine. The MSS delivers high-performance intrusion prevention inline using multi-threaded IDS. Inline deployment requires at least 2 hardware interfaces and a third virtual or hardware management interface. Blocking traffic is as easy as clicking on any of the snort rules on the rule management interface, saving and reloading the rules.



In passive mode, the MSS uses an active response system that disrupts TCP (and sometimes UDP) sessions to block unwanted traffic like Torrents or other potentially disruptive applications. The active response mechanism works by injecting spoofed TCP reset packets as well as other session hijacking packets into the network. This gives IDS operators the ability to block unwanted traffic without having to modify firewall rules.

Cloud Security



As an Amazon EC2 certified solution provider, MetaFlows offers turn-key cloud instances (MS Windows Server or CentOS 6) instrumented with the MSS software. The MSS can also be installed on a variety of other platforms including VMware ESX and other virtualized environments. The advantage of using the MSS in cloud security monitoring applications is that it does not require the installation and maintenance of additional instances dedicated to storing and analyzing the security events. The MSS, therefore, enables meeting and exceeding Enterprise reporting and logging compliance standards in a cost-effective and scalable way. All security event data (weather originating from traditional hardware devices or from the virtualized instances) is securely stored in the MetaFlows cloud and is accessible using a secure web browser.

Management Console Requirements

The MSS console requires Mozilla Firefox or Google Chrome. We recommend a minimum of 4 GB of memory and a fast CPU because a portion of the data analysis and correlation is actually performed in the browser