Is Your Intrusion Prevention System Working Alone?
Modern malware does not work alone. It’s designed to share information among infected nodes, which then attack, infect, and mutate in unison. An infected host can easily become a “harvester” looking for new victims, or can become one of the many “zombie” nodes that are responsible for more than 80 percent of the world’s spam.

More than half of today’s Internet attacks come from serial attackers. Just a few malware-hosting sites can infect hundreds of thousands of hosts, and a handful of botnet command-and-control servers can order billions of malicious connections a day. Yet, until now, intrusion prevention systems (IPSs) have worked alone. Even with frequent software and signature updates, an IPS has had to evaluate each attack locally, without knowing whether the source of a connection has been infected.

What Is Cisco IPS with Global Correlation?
Cisco® IPS with Global Correlation is a new approach to threat management that harnesses the power of Cisco Security Intelligence Operations (SIO) (Figure 1) to identify and prevent network attacks more quickly and effectively than standalone security technologies.

With Global Correlation, a Cisco IPS receives global threat updates from Cisco every five minutes, gaining real-time visibility into the reputation of known attackers and networked threats, as well as propagation and mutation trends. Global Correlation combines powerful signature and anomaly inspection technologies with real-time reputation information (Figure 2); this added context enables the Cisco IPS to stop twice as much malicious activity as traditional IPSs that rely on local inspection only.

Context Provides Confidence
Traditional IPSs do not have enough information to block all attacks with confidence. Because they can only block based on their knowledge of behaviors that may be vague or obfuscated, you’re left choosing between risking an interruption to critical applications, and risking a compromise.

Cisco IPS with Global Correlation provides valuable information about the reputation of the counterparty in every transaction, so that the IPS can block suspicious activity from known attackers. Whether it’s a website attack that looks like a faulty browser, or a suspicious DNS request, knowing the traffic source enables the Cisco IPS to block with confidence.

Why Cisco?
Cisco is committed to providing complete security solutions that are integrated, timely, and effective. As infrastructures become more collaborative, increased risk is inevitable. Cisco IPS is the only IPS with Global Correlation, enhancing your business’ ability to identify, analyze, and mitigate today’s threats.

Learn More
Global Correlation is available in Cisco IPS Sensor Software Version 7.0 and later. If you are an existing Cisco IPS customer, you can see the enhanced efficacy of Global Correlation in action today: Simply download the latest version of Cisco IPS Sensor Software from the Cisco Security Software Center, using your existing valid support license.

If you are not a current Cisco IPS customer and you would like to learn more about Cisco IPS and Global Correlation, please contact your local Cisco reseller or representative, or visit http://www.cisco.com/go/ips.