

{Managed Intrusion Prevention Services (mIPS)}

Not just a detection & prevention tool, but a complete threat management system!

Firewalls only go so far to help in the protection and control of today's application-driven computing environments. As "Set-it-and-forget-it" tools are taking a smaller role, more organizations are looking toward application solutions rather than products.

Today's security demands a focus beyond port control. Application-based threat control and operational expertise are now considered basic elements of any effective security practice.

igxglobal's managed Intrusion Prevention Service (mIPS) delivers more than an application control tool, but a complete threat management system that can work into any organization's budget and process. Moreover, it gives you: *"control over your environment, without the burdens of control!"*

MULTI-METHOD APPLICATION SECURITY

mIPS technology offers a multi-method approach for effective application security. These methods include:

Anomaly-based Detection

Analysis of communication based on defined standards better known as Request for Comment (RFC). Non-standard communication is often used to elicit abnormal behavior from applications for the purposes of compromise or denial-of-service.

Signature-based Detection

Specific signatures are used to look for vulnerability or exploit communications and behavior.

Application Profile Insight

Offers the capability to profile source, destination, service and application into a meaningful matrix highlighting unusual applications destined for and leaving your environment.

Priority & Reference Information

mIPS offers meaningful event priority information as well as valuable reference to assist in the analysis process to identify impact as well as uncover threats in a "Noisy" environment.

PERFORMANCE

igxglobal will assist in the appropriate sizing of the technology to meet specific client requirements. These requirements may include line rate, analysis model as well as susceptibility to attack.

Performance options range from small-capacity units for low line-rate edge implementations to mid and high-capacity units for larger volume and high-performance core system implementations.

FLEXIBLE INTEGRATION

With flexible options, the mIPS system may be integrated in a non-intrusive and transparent sniffer mode or proactive in-line mode. Multiple units may be implemented in any combination of sniffer or in-line mode to satisfy any solution requirement.

Sniffer Mode

Allows transparent connectivity to multiple network segments, acting as a cost-effective single and central overview point for many disparate networks.



SECURITY OPERATIONS



THREAT MITIGATION



SECURITY TECHNOLOGIES



PROFESSIONAL SERVICES



In-line Mode

Integrates in between your critical assets and the bad guys. Especially powerful in VLANed environments, this mode allows you to pass good traffic, alert on questionable traffic and stop malicious traffic!

IGXGLOBAL'S ENGAGEMENT MODEL

Unlike “Set-it-and-Forget-it” technologies, applications security requires engagement between the security experts and the business or risk managers. As such igxglobal’s client engagement includes the following:

Intelligent Implementation

Initial placement, sizing, and configuration are critical to both short and long-term value the overall solution delivers. Ineffective placement or poor configuration can translate into overwhelming volume of useless information or volumes of missed insight.

igxglobal brings expertise and experience to the relationship providing guidance on the most effective implementation techniques.

Accurate Initial Configuration

Generic and default policies may trigger events, however, which are the ones you should be concerned with? In a demanding day-to-day life which are the events you should be most concerned with.

igxglobal’s well defined and systematic approach to initial device configuration is the first step in a well-thought-out and refined threat management and mitigation process.

Security Operations

Many organizations have disengaged from the valuable insight and enforcement that IPS technologies offer due to concerns about lack of resources. This is a valid concern. These tools do require not just administration, but security operations for continued effectiveness.

igxglobal shows value beyond the initial sales and implementation model to deliver security operations for the life of your investment.

igxglobal can provide the following value added support services that offer you control without the burdens of control.

Analysis

An expert security engineer will analyze and review your event data and determine if activities are “Noise” or “Threat” on an ongoing basis.

Noise

Noise events are non-threatening broken (non-RFC compliant) applications or mis-triggered policies. In any event Noise events need to be addressed, either by fixing the problem and if this is not possible, ignoring them.

Threat

Threat events are actual threats that need to be responded to. Threat events may fall under several event categories which may demand different and unique response mechanisms.

The primary objective is to keep a clean environment by eliminating noise and to allow the threat events to be highlighted.

Threat Management

After the analysis and with consideration to events and activities in your environment, igxglobal will categorize threats into defined categories. These categories include:

1. Compromise Attempt
2. Infection Attempt
3. Denial-of-Service Attempt
4. Misuse/Abuse Attempt
5. Reconnaissance

Threat Mitigation & Response

igxglobal clients may choose to pre-define response mechanisms for threats based on category and severity. These response mechanisms include:

Blocking

To block traffic via an access or application control tool.

Electronic Cease & Desist (eC&D)

An igxglobal proprietary approach to stopping attacks at the source.

Eradicate

To stamp out infections and propagation-based threats, spyware and bots.

Ignore

To be aware of and choose to not respond to specific events or types of events.

Forensics

Conduct an investigation to determine point and method of entry, or reference individual behavior to provide evidentiary data.

Human Resources

Cooperate with internal human resources department to conduct burden-of-proof investigations to address mis-use abuse scenarios.

Investigate

At times alerts may require further investigation to determine how they should be categorized.

Device Management

Signature and Pattern Update

igxglobal will actively update all A/V signatures, content categories and patterns to ensure maximum efficiencies and protection.

Monitoring

igxglobal will proactively monitor the solution for availability, health and performance, and take corrective measure to avoid impact to the continuous availability of services.

Management

igxglobal will manage the device and ensure all signatures and policies are up-to-date and up-to-spec. Most importantly, igxglobal can translate your requirements into effective and valid configurations without the significant resources and training on the part of your organization.



SECURITY OPERATIONS



THREAT MITIGATION



SECURITY TECHNOLOGIES



PROFESSIONAL SERVICES