Executive Summary

Internet Security Systems’ Dynamic Threat Protection™ framework combines world-leading security intelligence and best-of-breed technology to deliver simplified, proactive protection against known and unknown attacks.

This multi-layered framework protects with unparalleled speed and accuracy while delivering exceptional value through reduced operational risk and dramatically lower deployment and operating costs. All of this is achieved through fusing three key elements:

1. **World-leading Security Intelligence** for maximum speed and accuracy

2. **Industry-leading Protection Technology** that harnesses the world’s only protection engine and only management platform that spans network, server, desktop and application to detect, prevent and respond

3. **Simplified Protection Process** to ensure proactive protection against known and unknown threats

The cost, time and risk-mitigating benefits of Dynamic Threat Protection are enormous when compared to existing protection options.
Introduction

In an ideal world, security is embraced with maximum speed and accuracy. Organizations are able to swiftly and precisely secure against constantly evolving threats.

Today's reality is a stark contrast to the ideal when faced with securing complex networks, countless servers and thousands of desktops. Today's reality regularly sees organization's multi-million dollar security investments thwarted by a single unforeseen attack. As a result, companies are constantly being forced into reactive mode - scrambling to pick up the pieces and restore order when security breaches occur.

The holy grail of security has always been the proactive detection and protection of systems from both known and unknown attacks in an efficient and cost-effective fashion.

Tall order?

Internet Security Systems' Dynamic Threat Protection™ framework achieves this.

Dynamic Threat Protection combines world-leading security intelligence and best-of-breed technology to deliver simplified, proactive protection against known and unknown attacks.

This multi-layered framework protects with unparalleled speed and accuracy while delivering exceptional value through reduced operational risk and dramatically lower deployment and operating costs. This is achieved through fusing three key elements:

1. World-leading Security Intelligence for maximum speed and accuracy.
2. Best-in-Class Protection Technology that implements the world's only protection engine and management platform that encompasses network, server, desktop and applications to dynamically detect, prevent and respond.
3. Simplified Protection Process to ensure proactive protection against known and unknown threats.

The cost, time and risk-mitigating benefits of Dynamic Threat Protection are enormous when compared to existing protection options. This white paper introduces the concept of Dynamic Threat Protection and illustrates how organizations can simplify security and reduce risk through maximized speed, accuracy and protection on investment.

Reactive vs Proactive Protection

Until now, organizations have had three options to protect themselves:

1. Do nothing
2. Adopt manual protection methodologies
3. Persevere with disparate point solutions

Closer examination shows that all three of these options are expensive, slow and reactive.
Do Nothing
It Won’t Happen To Me

When it comes to online security, many organizations still embrace the ‘ignorance is bliss’ option. ‘There's no reason to spend money on security until there's proof that the organization is truly at risk.’ Unfortunately, that proof usually comes in the form of operational disruption, legal liability and loss resulting from a successful online attack.

An equally precarious situation is when an organization operates with a false sense of security because it has a firewall or other static form of security infrastructure. Firewalls are important, but they are easily circumvented and insufficient for any organization that conducts any aspect of its operations online.

Doing nothing obviously is not a viable, responsible option.

Manual Protection
The Old, Reactive Way

It is theoretically possible to monitor all major public sources for threat information, download all relevant patches and hotfixes and then test and install each one on every potentially affected system. Thus, it is highly unrealistic to expect any organization to have the bandwidth to manually apply every patch to every system. After all:

It takes time to identify, fix and test potentially vulnerable systems. Time is at a premium when an organization is at imminent risk of attack.

It is labor intensive and expensive since each potentially affected system must be individually and manually analyzed and repaired.

The result is predictable. Faced with limited staff resources and impossible time pressures, vulnerabilities slip through, patched systems behave unpredictably, due to poorly understood interactions between the patch and other services, and other IT and security operations are put on hold for remediation.

Manually patching is expensive, time-consuming, labor-intensive, inaccurate and reactive. As with the do-nothing approach, manual protection simply doesn't present a credible, practical protection strategy.

Persevere with Disparate Point Solutions
The Current Slow and Expensive Way

Prior to Dynamic Threat Protection, organizations wishing to practice defense in depth were required to use multiple products for vulnerability assessment, intrusion detection and forensic technologies across networks, servers, desktops and applications. Managing multiple point solutions is time consuming, expensive and complex.

Although effective for one or two specific purposes, they are unable provide an integrated, unified protection posture. Without a centralized means to analyze and correlate the immense volume of data and share in real-time, organizations are forced into a purely reactive mode.
As a result, administrators have no realistic means to separate critical vulnerabilities from minor remediation, and simple intrusion detection systems are powerless to take action until the attack is already in process. Furthermore, data analysis that might indicate more sophisticated or subtle forms of attack must be pulled manually from a variety of point solutions, each with its own logs and data formats.

These solutions are further criticized for their labor and resource-intensive characteristics as each technology requires different deployment, configuration, analysis, updating and management. The manual and semi-automated security strategies that are the standard today do not provide strong protection and are very inefficient. In an era where speed and accuracy counts, they are not advised.

**Dynamic Threat Protection**

The New, Proactive Way

The Dynamic Threat Protection framework provides a clear contrast to other, more limited security methodologies. This new structured approach supersedes the current reactive approach to security, with new innovative, proactive protection products and services.

**So What is Dynamic Threat Protection?**

The Dynamic Threat Protection framework combines world-leading security intelligence and best-of-breed technology to deliver simplified, proactive protection against known and unknown attacks.

This multi-layered framework protects with unparalleled speed and accuracy while delivering exceptional value through reduced operational risk and dramatically lower deployment and operating costs. This is achieved through:

1. World-leading Security Intelligence
2. Industry-leading Protection Technology
3. Simplified Protection Process

**World-leading Security Intelligence**

At the end of the day, security boils down to speed and accuracy. As threats and vulnerabilities continue to escalate, protection must be deployed at maximum speed and with utmost accuracy. Anything less puts the enterprise at heightened risk.

Intruders only need a 1% error margin to be effective. Comprehensive research is key.

Dynamic Threat Protection achieves maximum speed and accuracy through utilizing:

- world-class security knowledge to build and automatically update best-in-class technology
- a first-to-market early warning security advisory service
World-class Security Knowledge
In-depth security research is - and always has been - Internet Security Systems' core competency and foundation. No other organization can match the X-Force’s breadth, depth and rapid response. ISS' X-Force threat research and analysis organization establishes the intellectual capital that underpins ISS’ solutions. This is delivered through X-Press Updates, or automated security intelligence updates. X-Force is unparalleled in its research efforts and is the world number one in security advisories, representing 45% of all vulnerabilities discovered by commercial research entities - 3 times more any other entity.

First-to-market Security Advisory Service For Early Warning
The speed and accuracy by which breaking security research reaches and extends through an enterprise is the crucial difference between proactive protection and reactive security. Working with a trusted research and development organization provides an early warning system for threats as they emerge 'in the wild' and migrate around the world. When coupled with remediation advice, this advanced notice enables rapid, proactive protection. In its absence, security staff are only able to respond once the crisis is upon them and actual intrusions have already taken place. X-Force provides first-to-market advanced warnings of newly emerged threats and vulnerabilities. Through the X-Force™ Threat Analysis Service, X-Force pre-announces all X-Force-discovered vulnerabilities on an average of 30 days prior to public disclosure and within 24 hours for other vulnerabilities.

Best-in-Class Protection Technology
Dynamic Threat Protection uses best-in-class technology to automate the protection cycle. The Dynamic Threat Protection Platform, the core of Internet Security Systems' enterprise protection offerings, significantly improves protection across networks, servers, desktops and applications, while reducing complexity and cost. This platform comprises three key pieces of technology that unite to provide an unparalleled protection solution. They are:

1. **Protection Engine**: the world’s only protection technology that drives ISS Intrusion Protection and Vulnerability Detection agents across network, server, desktop and applications to detect, prevent and respond to known and unknown attacks.

2. **SiteProtector™**: the world's only management platform that provides centralized control, command and event management for network, server and desktop protection products.

3. **Fusion**: the jewel in the ISS technology crown which provides attack pattern recognition and impact analysis with unparalleled speed and accuracy to minimize false alarms, which reduces overall security expenses.

4. **X-Press Updates**: automated updates from the world's #1 security intelligence team.

Following is a closer look at each of these components:

The Protection Engine powers ISS' premier, fully-integrated protection lines:

- **Proventia™ Dynamic Threat Protection Appliances**
- **RealSecure Dynamic Threat Protection Software for network, server and desktop**
- **RealSecure Vulnerability Detection Scanners for network, systems and wireless**
**Detect:** To be the world’s best in prevention and protection, you first must be the best in detection. It is the combined employment of multiple detection techniques that makes ISS the world leader. No single detection technique is effective on its own. Through ISS’ world-leading security intelligence and the optimal combination of these detection techniques, the Protection Engine quickly and accurately identifies threats that other solutions miss. These security algorithms include state-based seven-layer protocol analysis, pattern matching, behavioral analysis, application layer pre-processing, heuristics, TCP reassembly, IP defragmentation and custom signatures, along with proactive vulnerability detection to detect known and unknown threats. The result is unparalleled detection capabilities that extend across 95 network and application protocols that detect over 1700 known vulnerabilities and countless unknown exploits. No other offering on the market even come close to this breadth and depth of protection.

**Prevent:** Once the Protection Engine detects malicious behavior, preventative measures are then initiated. A variety of defense mechanisms are available to safeguard network, server, desktop and application layers. These include inline prevention, active blocking, application control, automatic firewall capabilities and Virtual Patch™ Vulnerability Remediation.

**Respond:** Once an attack is detected and prevented, the Protection Engine can be configured to respond further using an array of built-in and/or user-defined actions. Among these responses are console alerts, event logging, packet and evidence logging, SNMP traps, session kills, account disabling, real-time attack verification, event correlation, aggregation and filtering, email notification, paging, firewall or router reconfiguration and custom responses as desired by the administrator.

**SiteProtector**
Tying together the multi-layered protection agents with the vulnerability detection components under one management console is critical to proactive protection. SiteProtector is the world’s only management platform that provides centralized control, command and event management for network, server and desktop protection products - while simultaneously providing crucial visibility to enterprise-wide system vulnerabilities.
Each agent reports to SiteProtector, with data correlation being applied at every level of the process to minimize excess network traffic and maximize the ability of administrators to quickly and easily focus on the most critical security issues.

**Fusion**

The SiteProtector Fusion module enhances and extends SiteProtector’s correlation capabilities by adding two automated and advanced correlation techniques: Impact Analysis and Attack Pattern Recognition. Fusion immediately estimates the impact of attacks by correlating the target’s known vulnerabilities and operating system to the attack, automatically alerting users to real attacks, while de-emphasizing failed attacks and eliminating false alarms. Fusion also automatically correlates attack activity over time to link seemingly disparate events or incidents - whether occurring now or in the past - into a single, significant incident.

**X-Press Updates**

Finally, each agent within the Dynamic Threat Protection Platform receives regular X-Press Update product enhancements to ensure that the protection system is up-to-date on the latest threats and security developments. A direct deliverable from the X-Force, these enhancements and upgrades are automatically downloaded, self-installed and easily deployed from SiteProtector.

**Simplified Protection Process**

Readiness to combat new threats means responding when a vulnerability is first discovered, not when an exploit is first deployed against its target. That’s why Dynamic Threat Protection solutions employ a unique Virtual Patch capability to automatically protect vulnerable systems. Virtual Patch enables an organization to protect immediately against known and unknown attacks once a vulnerability has been discovered - often long before a patch or hotfix is available.

Through combining the functionality of vulnerability detection, intrusion protection, management and advanced correlation tools, the Virtual Patch process involves automatically updating all network, server and desktop devices, enabling them to detect the exploitation of a newly discovered vulnerability before the required patches are applied.

The result? Proactive protection against unknown threats.

As worms get faster and more sophisticated and exploits more destructive, the only window of opportunity to thwart hackers is during the pre-exploit stage.

Figure 1 - The Proactive Protection Zone
It all starts with a vulnerability being discovered or publicly disclosed. An exploit that takes advantage of this vulnerability then follows. And finally a patch is released and applied. The timing of patch releases varies. However, it is safe to assume that patches are typically applied after an exploit has done its damage. This is so for three reasons:

1. The significant time and effort required to patch all systems.
2. Patches are often made available after the vulnerability has been exploited.
3. The window of time between vulnerability discovery and exploit development is rapidly closing - to the point where zero-day attacks are now a reality. Zero-day attacks take advantage of a known software vulnerability that is exploited in a new way, or an unknown vulnerability that is immediately exploited.

And so, during the post-vulnerability announcement phase prior to an exploit appearing in the wild, a window of opportunity - the proactive zone - is present. It is this point in time that the Virtual Patch process is initiated and proactive security solutions update and begin protecting without knowledge of what exploits may be created.

For example, upon notification of a new threat, vulnerability detection scans launch to distinguish between at-risk systems and not-at-risk systems. From there, organizations are able to pro-actively protect at-risk systems until a patch becomes available.

This pre-exploit time can be years, months or hours and provides a crucial window of opportunity to develop counter measures against possible exploits.

Figure 2 - The Reactive Protection Zone

The post-exploit time zone is known as the reactive zone. All protection efforts initiated in this timeframe are limited to reactive clean-ups and frantic scramblings to pick up the pieces and restore order.

Manual Patching remains in the reactive zone as once the exploit is known, the propagation happens too quickly for patching to be effective. Patching is often not applied until well past the introduction of the exploit.

Disparate Point Solutions also sit in the reactive zone as they don't possess the required agility and precision to deliver proactive protection. Many solutions focus on detecting the exploit. However, before they can do that, they need to spend time analyzing the exploit after it is released.
By employing the Virtual Patch process, Dynamic Threat Protection is the world's only framework that focuses on the post-vulnerability, pre-exploit period with the required speed and accuracy to protect against unknown threats. In fact, Dynamic Threat Protection not only addresses this time period - it is able to extend further back to the pre-vulnerability zone through:

- **X-Force Vulnerability Research** - Akin to pre-emptive strikes in the protection against unknown vulnerabilities and attacks, X-Force's proactive vulnerability research and deep understanding of vulnerabilities as they are discovered, provide the necessary check to accurately detect and stop vulnerability abuse.

- **X-Force Threat Analysis Service** - In this early-warning security advisory service, X-Force pre-announces all X-Force-discovered vulnerabilities on an average of 30 days prior to public disclosure and within 24 hours for vulnerabilities discovered by others.

- **X-Force X-Press Updates** - X-Force X-Press updates continually provide automated security intelligence updates from the world's #1 security research team.

The ultimate result is proactive protection from unknown attacks.

In short, the Virtual Patch process provides a buffer of time, allowing organizations to wait until bulk updates are available, rather than having to apply each individual hotfix and reboot systems. Just like preventive medicine or car maintenance, the Virtual Patch process is based on the long-accepted knowledge that routine, preventive maintenance is far superior to the ‘break/fix’ alternative. It re-defines security maintenance and allows security operations to be handled as part of a normal IT change management process, allowing more effective and more efficient resource planning and more timely response to both known and unanticipated threats.

The cost, time and risk-mitigating benefits of virtual patching are enormous when compared to the current need to disrupt systems on almost a weekly basis.

**Why Is Dynamic Threat Protection So Effective?**

Dynamic Threat Protection evolves disparate point solutions into an integrated protection platform. Best-in-class technology all work as part of the same structure.

Each agent and management application quickly and easily shares critical security data with the other elements of the system. Pattern attacks that are impossible to detect by individual agents quickly become apparent once security is measured across the breadth of the enterprise. Security policy emanates from a centralized resource, which in turn handles data analysis and reporting for both technical and managerial oversight.
A protection solution without correlation capabilities would still send an alert, generating a false alarm. The elimination of these false alarms significantly reduces the overall cost of ownership since administrators only need respond to the most likely and pressing security events.

### Why Adopt Dynamic Threat Protection?

Dynamic threat protection leads to three key advantages over manual protection or disparate point solutions: speed, accuracy and protection on investment. See below the matrix which cross-references these three benefits with each of the Dynamic Threat Protection components – process, intelligence and technology.

<table>
<thead>
<tr>
<th>Dynamic Threat Protection</th>
<th>Speed</th>
<th>Accuracy</th>
<th>Protection on Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROCESS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unparalleled Speed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proactive protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>against known and unknown attacks through the Virtual Patch process, which addresses and protects against newly discovered exposures before scheduled patches and upgrades can be applied.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unparalleled Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Uses advanced data collection, correlation and analysis to minimize false alarms or false positives.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Limits the need for manual intervention in the security process.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Automates the process of discovering and repairing potential security exposures.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection on Investment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Risk:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>through unparalleled speed and accuracy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Cost: The cost benefits are enormous when compared to largely reactive, disparate point solutions and the endless need to disrupt systems to apply patches. Significantly lowers TCO.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SECURITY INTELLIGENCE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unparalleled Speed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Through the X-Force Threat Analysis Service (XFTAS), X-Force pre-announces all X-Force discovered vulnerabilities on an average of 30 days prior to public disclosure and within 24 hours for other vulnerabilities.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unparalleled Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISS X-Force research and development team is the world number one in security advisories, representing 45% of all vulnerabilities discovered by commercial research entities – 3 times more than any other entity.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection on Investment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Risk: Knowing you’re backed by the world’s best in security intelligence.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Cost: X-Force intelligence included in technology maintenance (X-Press Updates). XFTAS available at a very low cost and offers significant value.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TECHNOLOGY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unparalleled Speed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provides proactive protection through the:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Industry’s fastest and most comprehensive impact analysis and attack pattern recognition (Fusion).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unparalleled Accuracy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlike manual or semi-automated systems, dynamic threat protection easily handles massive amounts of constantly changing security.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection on Investment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lowest Cost: Through unified agents and management and automation of security cycle. Lowest risk: through little/no room for human error due to level of automation.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued
Where do I start?

There are two ways to adopt the Dynamic Threat Protection framework:

1. Undertake a four-step transition process internally
2. Minimize your risk completely by partnering with a Managed Protection Service Provider

Four-step Transition

A staggered approach is recommended, rather than overwhelming an organization by trying to protect every asset against every vulnerability and attack up-front.
As outlined in the above diagram, phase 1 focuses on protecting mission-critical assets from the top 20 risks. This initial step quickly produces results and enables staff to become comfortable with the Dynamic Threat Protection process. Phase 2 extends the top 20 protections to critical assets, and expands the protection of the mission critical assets to include the top 50 risks. The process progresses accordingly, providing deeper levels of protection across an enterprise's networks, servers and desktops.

**How does the organization know what the top risks are?**

If an organization is unable to identify its top risks, a vulnerability assessment is recommended. This is undertaken by a security provider with the ability to provide top-tier research, track emerging threats from around the world and provide this information to customers in a timely and easily-understood manner. Combined with a Dynamic Threat Protection platform, this combination significantly increases the organization's ability to protect itself. See Appendix 1 on How to select your Dynamic Protection Platform.

**Managed Protection Service Provider**

The best headstart to adopt Dynamic Threat Protection is to utilize ISS' Managed Protection Services. Utilizing both RealSecure and Proventia protection products, ISS' Managed Protection Services delivers:

- Maximum Protection with unparalleled speed and accuracy through optimal utilization of the multi-layered Virtual Patch process.
- Direct Access to the owners and authors of Dynamic Threat Protection.
- Dual Visibility enabling customers to monitor their own network security activity with local management, while MPS is ever vigilant and responsible for the execution of protection.

**Conclusion**

In summary, Dynamic Threat Protection replaces an expensive, reactive, slow and therefore dangerous protection paradigm with something immeasurably better. Rather than haphazard patching regimes and stand-alone point solutions that companies must figure out how to integrate and operate, Dynamic Threat Protection delivers a simplified, integrated system that reduces the demand on staff and software resources while greatly improving and accelerating the overall protection process.

Many organizations have moved from no protection to disparate point solutions or battle with endless patching cycles - only to seek a superior alternative. With Internet Security Systems' Dynamic Threat Protection, enterprises are able to achieve a dramatically improved level of security. One that delivers speed, accuracy and maximized protection on investment.
Appendix: Dynamic Protection Platform Checklist

Use this checklist when selecting your Dynamic Threat Protection vendor(s) to ensure you have all of the essential elements:

Company Background
☐ Proven history with long-term customers with protection needs similar to yours.
☐ Financially stable and viable.
☐ Public and financial records audited and available.

Components
Examine the entire platform for comprehensive coverage. Does the protection system protect:
☐ across your network, server and desktop infrastructure?
☐ web services on any and all ports?
☐ the top Instant Message networks?
☐ databases?
☐ the wireless network?
☐ application attacks?
☐ against over 100 backdoors and Trojans?
☐ against DoS and DDoS attacks?
☐ against encrypted attacks?
☐ using protocol analysis extensively?

Command and Control
☐ Is there one integrated console that:
  √ sets policies
  √ pushes policies and updates
  √ performs distributed assessments
  √ starts and stops protection agents
  √ incorporates vulnerability assessment data into operations
  √ generates reports
  √ provides enterprise view of security posture?

Correlation
☐ Impact Analysis.
☐ Attack Pattern Recognition.
☐ Correlation occurs across both source and destination IP addresses.
☐ Correlation occurs across multiple protection agents.

Vulnerability Detection
☐ Platform looks for vulnerabilities and misconfigurations across networks, servers, desktops and applications.
☐ Comprehensive vulnerability assessment of Windows, Unix and infrastructure devices.
☐ Accurate OS identification.
☐ Dynamic check assignment for efficient scanning.
☐ Free discovery scans.

Multi-Layered Intrusion Protection Agents
☐ Platform has protection agents for the network, server, desktop and application layers.
☐ Platform has modular security logic at all layers to provide common taxonomy of attack names.
Security Intelligence
- Original vulnerability and threat research and development.
- Responsible disclosure of vulnerability and threat information.
- Platform provider is a security research provider – not a security gatherer.

Security Content
- Platform provider is first to deliver new, comprehensive security information for optimal customer protection.
- Frequent and automated security updates.

Services
Platform provider has added-value services supporting the platform, including:
- Security assessments and penetration tests.
- Policy development and implementation.
- Emergency response.
- Threat analysis services.
- Security education.

Managed Protection Services
- Platform provider can offer managed protection services.

Global Reach
- For multi-national corporations and organizations - platform provider provides localized and regional support in Americas, Europe, Middle East, Africa and Asia.

Technical Support
- 24/7/365 global technical support for the platform.
- Highly-specialized, certified support engineers.
- Multi-tiered, support infrastructure.