Enhanced Dynamic Threat Protection™ via Automated Correlation and Analysis
Executive Summary
Correlation is essential to improving the effectiveness of intrusion protection defenses and providing the best possible enterprise-wide network security. Correlation is the process of distilling raw threat data into prioritized, actionable information. The raw data comes from myriad and often disparate events reported by all intrusion detection and prevention systems, as well as other agents deployed throughout the enterprise on desktops and servers. Numerous techniques achieve two related objects: spot all real threats immediately, and minimize or eliminate distracting “false positives” and false alarms. When both objectives are achieved with a comprehensive correlation system, security personnel are able to perform at peak productivity and effectiveness.

The problem is: while correlation is now recognized as an essential element of network security, not all organizations have the full-time, knowledgeable staff necessary to utilize state-of-the-art correlation techniques to full advantage. Automating the various correlation techniques, many of which are quite complex and sophisticated, substantially improves enterprise-wide security, and can dramatically lower overall costs. This technology is available today, as a central part of Internet Security System’s Dynamic Threat Protection™ process.

According to the Computer Security Institute, “Information security requires a whole-hearted organizational commitment of resources to an enterprise-wide program designed to evolve and adapt to new dangers.”

A growing number of organizations have found that pervasive detection with automated correlation holds the most promise in achieving the goal of dynamic protection.

Automated correlation helps close the feedback loop to provide faster, more accurate intrusion detection and prevention. A business context that focuses on the most valuable assets helps prioritize responsive measures to make the security team more proactive and productive. And this increased effectiveness is absolutely essential to driving down the total cost of ownership of network security provisions.

These and many other benefits of dynamic threat protection are indeed quite compelling. For this reason, it is imperative that security administrators and their executive managers make the effort to understand correlation techniques and systems. This white paper outlines both the importance of and considerations for using state-of-the-art correlation systems. The material is organized into two main sections followed by a brief conclusion.

The first section outlines the vital role correlation plays in dynamic threat protection. This section also describes how automating correlation can help enhance security, improve productivity and lower costs. The second section provides an introduction to Internet Security Systems’s RealSecure® SiteProtector™ and the RealSecure® SiteProtector™ Security Fusion Module from Internet Security Systems, which together provide perhaps the most comprehensive and capable set of correlation techniques available today.

Dynamic Threat Protection Defined
No one doubts the need for secure online business operations. The challenge is how to do so efficiently and effectively. Current technologies such as intrusion detection systems (IDS) and vulnerability assessment (VA) do a very good job performing the tasks they were designed to do: uncover potential threats, monitor host or network traffic, detect attacks or suspicious behavior and alert administrators. These applications are widely accepted, well understood and standard practice for organizations of all sizes and markets.

In many business environments, however, rapidly escalating threats and dramatically expanded demands for Internet connectivity mean that IDS and VA need to grow to the next level of

---

Automated Correlation and Analysis

These new intrusion protection systems (IPS) are the natural evolution of the current state-of-the-art. Effective protection requires the best threat identification and response possible. IPS builds on this foundation to provide a significantly improved value on each security dollar invested.

Internet Security Systems’ (ISS) approach is different from any other competitor. ISS extends the IPS vision across IDS, VA and comprehensive security research, analysis and services. This Dynamic Threat Protection process moves enterprise protection from semi-automated intrusion detection and response via semi-compatible point solutions to an automated, intelligent security platform – across networks, servers and desktops, and including fixed, wireless and remote systems.

Dynamic Threat Protection delivers highly integrated operations that in turn create faster response times, focus administrator attention on areas needing the most immediate attention and anticipate security exposures before they become business liabilities. In short, Dynamic Threat Protection provides three distinct extensions of VA and IDS for organizations looking for an additional level of security:

**Accuracy** – Dynamic Threat Protection rapidly and accurately detects attacks and minimizes false positives.

**Performance** – Dynamic Threat Protection operates at increasingly rapid line speeds across the network, and scales from workgroups to multinational organizations with many locations.

**Low Total Cost of Ownership (TCO)** – Dynamic Threat Protection significantly lowers TCO by using advanced data collection, correlation and analysis to minimize the need for manual intervention in the security process and automate the discovery and repair of potential security exposures.

In sum, Dynamic Threat Protection reduces the critical time lag between when a new threat emerges and security staff is able to respond to that threat. This key advantage gives security staff the ability to quickly and easily concentrate their efforts on the most urgent issues first. In addition, it extends protection over time from the most urgent risks on the most important networks and systems to prevention and protection for less critical areas.

**Correlation’s Role within Dynamic Threat Protection**

The expansions of global communications and attempts to protect the enterprise have not gone unnoticed by attackers, whose exploits are now a daily occurrence. The Computer Security Institute (CSI), in cooperation with the Federal Bureau of Investigation, publishes an annual *Computer Security Issues & Trends* report that reveals the extent of the problem. In the 2002 *Computer Crime and Security Survey*, CSI reports that a full 90% of respondents experienced security breaches within the past 12 months, with 80% acknowledging financial losses as a result. Theft of proprietary information and fraud accounted for nearly two-thirds of that financial loss. Even a single, successful attack can cause widespread and significant losses. The Code Red incident, for example, caused an estimated loss of $2.6 billion worldwide, according to Computer Economics.

At the same time, many organizations are finding it necessary to control costs with stagnant or shrinking network security budgets. IT departments also continue to struggle attracting, training and retaining security expertise. The IT staff, nevertheless, remains accountable if inadequate security causes the business to miss out on a market opportunity or, worse yet, face serious financial losses from a security breach. Automated data correlation and analysis within the Dynamic Threat Protection process, is the key that makes security simultaneously more affordable and effective.
Correlation 101
Correlation is the process of distilling raw threat event data into prioritized and actionable information. The raw data is reported as events by all intrusion detection/prevention systems and other agents deployed throughout the enterprise on desktops and servers, and optionally on firewalls, antivirus applications and other security systems. As one can imagine, such a pervasive protection solution can generate an enormous and potentially unwieldy number of events.

Accurate correlation of these security events is vitally important to detecting and preventing attacks, determining the actual business impact of an attack, minimizing false positives and false alarms that diminish productivity, monitoring and reducing overall organizational risk, and measuring the effectiveness of and return on the security investment. Simply put: correlation is the best means available for closing the feedback loop and prioritizing the seemingly endless number of security events into those that pose a real threat and, therefore, warrant immediate attention.

Correlation is not entirely new to the network security arsenal. Prior to the advent of automated correlation systems, many organizations performed some forms of correlation manually. For example, a security administrator might try to match a known attack signature to the known vulnerabilities of the target system to assess the likely success or failure of the attack. Such an attempt requires a detailed understanding of both the particular attack and the particular host operating system’s vulnerabilities. Now imagine extending this deep level of understanding to the many combinations and permutations of circumstances possible, and one begins to understand the frustrating challenge most security administrators face today.

To be even marginally effective, purely manual correlation requires a 24/7/365 staff of security professionals, all of whom must possess substantial security expertise, which helps explain why manual correlation can become prohibitively expensive in diverse, large-scale network environments. Of course, these manual manipulations are prone to human error, which is understandable given the relentless attention to detail correlation requires. Finally, as a tedious, error-prone and time-consuming process, manual correlation can be difficult—if not impossible—to perform accurately in real-time. And when it comes to security, the rapid response enabled by a proactive approach can make all the difference.

For these reasons and more, most organizations are finding it increasingly advantageous to employ proactive management tools that perform some or all correlation tasks automatically and proactively. Faced with more sophisticated and frequent attacks in an environment of budgetary constraints or cuts, these organizations know they need to have their highly paid professionals working smarter—and not just harder. Organizations too small to have a security staff need a way to acquire security expertise without one.

Automated Correlation Systems
Manual correlation efforts are now being replaced with purpose-built correlation or Security Information Management systems (SIMS). Modern correlation systems aggregate and consolidate all input into a homogeneous set of events, normally in a database, then analyze these events using a number of different and effective techniques to uncover potential threat conditions. The result is a proactive, dynamic and coordinated view of security conditions and threats enterprise-wide.

SIMs have numerous advantages over point products and purely manual processes. As a background task performed in software, an automated correlation system operates continuously for around-the-clock protection. When properly configured on a suitable server, an automated correlation system delivers results in real-time – in time to take corrective or preventative action. In addition, an effective correlation solution provides comparative metrics that allow organizations to detect any changes in the security posture, possibly in reference to a benchmark or baseline. In other words, the SIM brings a business context to security events by analyzing the impact on
the most valuable organizational assets. The better systems also provide a high-level knowledge of attack patterns to escalate series of serious threat activity.

Finally, automated correlation systems make it practical to have both deep detection and pervasive protection with agents deployed at all critical network boundaries, and on all desktops and servers across the enterprise. Such dynamic and pervasive protection is now essential to defeating the best and brightest attacks, which have become quite clever at circumventing perimeter defenses via increasingly complex forms of malicious behavior.

Figure 1: Dynamic Protection System – detection, prevention and response at multiple layers throughout the enterprise.
RealSecure® SiteProtector™ and the RealSecure® SiteProtector™
Security Fusion Module
The single most significant on-going expense of any security solution is the cost of accurately
determining which security events warrant a response. Traditionally this process has been labor-
intensive, requiring the skills of many highly paid security professionals to bring meaning to the
relentless stream of events and assess the potential risk posed to the organization. The
RealSecure SiteProtector with the Security Fusion Module automates this labor-intensive task by
correlating the myriad events reported from scanners, intrusion detection/prevention systems,
and other desktop and server agents deployed throughout the enterprise.

RealSecure SiteProtector is part of the RealSecure® Protection System, an integrated threat
management environment designed to make intrusion protection both pervasive and affordable
across networks, servers and desktops. This comprehensive solution includes intrusion detection,
prevention and response, vulnerability assessment, policy compliance, and data collection and
analysis – all coordinated through the RealSecure SiteProtector centralized management
structure.

RealSecure SiteProtector with the Security Fusion Module employs numerous correlation
techniques to achieve the ultimate goal in state-of-the-art correlation: fully automated and
dynamic risk correlation. Risk correlation determines the relationship between the active threats
against the network and systems, and the vulnerabilities of those resources. This "Holy Grail" of
correlation provides any organization with a true risk-oriented view of its enterprise-wide
environment. Risk correlation answers the fundamental question: What are the consequences of
the current vulnerability and attack exposure to the business? And in doing so, it allows available
security personnel to focus exclusively on protecting the most critical business assets.

RealSecure SiteProtector
The RealSecure SiteProtector centralized management console provides unified configuration
and data analysis capabilities for the RealSecure Protection System. SiteProtector simplifies
large-scale intrusion protection deployments through cost-efficient, central command, control and
monitoring capabilities that make the security staff and other personnel more productive.

SiteProtector’s built-in correlation, event analysis and prioritization, and extensive reporting
capabilities are all combined on a single platform to facilitate dynamic, real-time attack and
misuse detection and prevention. Its intuitive graphical user interface helps administrators work
more productively through flexible, customizable views built around asset groupings and event
aggregation. Powerful filters are available to screen for event exceptions (known acceptable
events), false positives and false alarms. By centralizing security analysis and response in a
pervasive intrusion protection environment, SiteProtector is able to detect security threats that
might elude individual systems or agents. The result is an increased awareness of genuine
security threats accompanied by a corresponding reduction of false positives and false alarms.

As an easy-to-use, policy-based command and control console, SiteProtector automates
deployment and management of an enterprise-wide RealSecure Protection System, including
multiple site management via secure remote administration. SiteProtector enables proactive and
pervasive intrusion protection by correlating all events reported by RealSecure vulnerability
assessment scanners and all RealSecure network, server and desktop intrusion
detection/prevention systems. These intuitive views, which eliminate the need for administrators
to learn a special scripting language, help streamline and automate routine security operations.
Automated Correlation and Analysis

Figure 2: Automated correlation dramatically reduces noise, maximizes workflow and focuses attention on critical security events.

SiteProtector employs several different correlation techniques categorized here into four main types: Asset or Target, Custom, Comparative, and Advanced Analysis. These and other correlation techniques all require rudimentary counts of the shear number of events. Essentially, this process of event aggregation tallies then categorizes all “like” events using different criteria, such as name, port, severity, source IP address, and so on.

A significant percentage of competitive security management solutions touting “advanced correlation technologies” are, in fact, merely providing simple event aggregation. So while aggregation is necessary for correlation, it is not—in and of itself—sufficient.

Asset or Target Correlation – This technique assesses events and incidents based on a prioritized view of an organization’s protected assets, which then gives correlation a much-needed business context. The result is that incidents involving the most crucial or valuable business assets take priority over lesser or potentially inconsequential events. For maximum effectiveness, assets can be automatically grouped by criteria that make business sense for the organization. The logical groupings can occur at different levels, from a single department to the entire enterprise, for example, or for specific roles within any group. This context also helps make security status information more relevant to different audiences. Without such a business context at its very foundation, no correlation system can properly protect the enterprise.
Custom Correlation – Building on the foundation afforded by asset correlation, custom correlation gives security administrators the ability to tailor intrusion protection defenses to meet specific needs. The tools available allow an administrator to apply various filters, create or modify different views, define exceptions and incidents, and employ combinations to perform fairly complex correlations. Here are just a few examples made possible by custom correlation:

- **Event Proliferation** – This analysis displays not only the number of events being correlated, but also shows the number of suspected attackers and/or systems being targeted. Viewing security data from an event perspective offers valuable insight into areas for improvement. If certain types of events are more widespread than others, for example, specific actions can be taken to address the situation.

- **Directional Correlation** – Correlating incidents and events based on the direction of the attack is critically important during the initial stages of worm propagation. This analysis determines if the events are *inbound* from sources outside the organization, *outbound* from sources within the organization, or contained *within* the organization (to and from internal systems).

- **Intruder or Source Correlation** – This analysis identifies specific intruders and determines how invasive their activity is across the infrastructure. Intruder correlation also allows for detailed monitoring of a given intruder’s behavior over time.

- **Exception Management** – This analysis helps categorize events as being either meaningful (actionable) or not (acceptable or allowed events between two or more systems that can be ignored). The exception process is tactical and requires internal knowledge about acceptable network activity in your environment, but it is important to managing the flood of events that are generated with a security risk management solution. It is most important to have a system that can remember your decision about an acceptable behavior so that you do not have to see the same set of information (and categorize it) more than one time.

- **Incident Correlation** – Incident correlation reveals patterns in events that occur over time. In this example, aggregated events are analyzed in the broader context of an incident that is being performed in incremental steps. Once a potentially significant event is discovered, an incident is created to track any related activity in the future. Such blended or hybrid attacks may escape detection if not correlated in this broader incident context. Incident correlation may also demonstrate the security team’s pre-emptive capabilities and how the investment in security is benefiting the business.

Comparative Correlation – Comparing correlated or anomalous network threat activity to known baselines and previous vulnerability assessments helps determine changes in the organization’s overall threat situation and risk exposure. This “ounce of prevention” technique can be quite powerful when the input comes from a thorough vulnerability scan of the entire enterprise. Baseline and state comparison views quickly highlight the threats that have appeared since the last time threat activity was analyzed. These views also show the rise and fall of vulnerabilities over time or something as simple as what vulnerabilities appeared or disappeared since the last scan took place. SiteProtector can save these baseline and state comparison views and automatically create periodic reports so that management can easily see security lock-down progress or the need for more resources if progress is not occurring as quickly as expected.

Advanced Analysis Correlation – Advanced analysis correlation goes beyond what is generally possible with custom and comparative correlation techniques. The intuitive user interface allows a security administrator to right-click an event or set of events to conduct an in-depth analysis or just get a quick answer to a specific question about the source, target, agent or asset vulnerability involved in the suspected attack. These questions quickly navigate operators through vast amounts of data to help them quickly decide whether sets of events pose a real threat or if they are a false alarm. After making that single decision, the operator can simply create an incident, if the problem is severe, or an exception, if the activity is normal and acceptable, and continue on to other important activities.
Automated Correlation and Analysis

RealSecure SiteProtector Security Fusion Module
The Security Fusion Module enhances and extends SiteProtector’s correlation capabilities by adding two automated and advanced correlation techniques. The Fusion expert correlation system gives existing personnel access to the collective security expertise of Internet Security Systems’ renowned X-Force™ security knowledge services organization. In effect, Fusion fills in the voids and helps security administrators become more effective at protecting information assets across the enterprise.

The tools available in Fusion give security administrators the ability to apply context, filter unimportant events, quickly navigate through detailed event or incident information, and more. The two additional correlation techniques employed by Fusion are attack impact analysis and attack pattern recognition.

**Attack Impact Analysis** – One of the first tasks that an IDS operator must do after receiving a security alert is determine if the attempted attack was successful. Many operators use vulnerability information about the target to make this determination, or they take on the time consuming task of testing the target host or service to determine its state. Questions that a security professional might ask are:

- Was the target vulnerable to the attack?
- The attacker used an attack that affects Windows only… is the target a Windows desktop or a Solaris server?
- Did the protection agent installed on the target block the attack?

The security fusion module immediately correlates this information, estimates the impact of each attack, and immediately adds this estimation to the IDS alert in a matter of milliseconds before the event is even displayed on the console. So, as soon as the operator sees the IDS alert, the operator also knows whether or not the attack succeeded. Armed with this information, the operator can instantly make an instant decision about whether the alert requires immediate attention without spending minutes or hours researching a targeted host.

**Attack Pattern Recognition** – Attack pattern recognition automates the investigative analysis process. Attack pattern recognition correlates attack activity over time to link seemingly disparate events or incidents—whether occurring now or in the past—into a single, significant incident. For example, multiple failed login attempts on different hosts, or an information gathering attack that...
includes the use of evasion techniques, may well be signs of a “first strike” attack pattern. Very few correlation systems today have been able to achieve this level of sophistication.

With its comprehensive and fully automated capabilities, the Security Fusion Module sets a new standard in the industry. Expert-level, automated correlation allows security professionals to be more effective as they spend less time pursuing minutia and more time responding to real threats. As a result, larger organizations are better able to scale their network defenses for pervasive, enterprise-wide protection, and smaller organizations get the kind of solid security knowledge that previously required a large staff of experts. Fusion handles its expert task by correlating events continuously in real-time to assess the real impact of potential threats. Determining the real impact posed by an attack requires a convergence of the vulnerability and threat spectrums. And Fusion performs this convergence dynamically by assessing any threat condition, or the nature and extent of the attack, in the context of threats to vulnerable—and valuable—business assets. In doing so, Fusion minimizes the so-called false alarms that can distract security personnel from focusing on real risks.

Building upon the correlation capabilities of SiteProtector described above, like asset grouping, and automatically correlating a specific threat condition with the targeted asset’s vulnerability status, the truly important and “actionable” events rise readily and appropriately to the top of the priority list. The result is a much more meaningful and manageable set of attacks for the security team to handle.

Figure 4: Attack Pattern correlation detects patterns in individual attack activity that would normally be missed by less advanced correlation systems. The details of a detected attack pattern are easily accessible through intuitive right-click menus. Additionally, Attack Impact correlation provides impact status for each event involved in the detected pattern.
As a virtual “security expert in a box” Fusion doesn’t sleep at night or get sick or disappear on the weekends or take vacations—and never gets a holiday off. Fusion is there 24x7x365 monitoring, correlating and prioritizing the relentless onslaught of events to make certain the enterprise is protected. And by continuously and automatically putting security decisions into a business context, Fusion permits proactive, pervasive protection—from the agent all the way to the boardroom. For after all, isn’t protecting the business what security is all about?

**The Security Fusion Advantage**
The automated correlation provided by RealSecure SiteProtector with the Security Fusion Module allows large organizations to scale intrusion protection defenses enterprise-wide for more pervasive protection. Advanced correlation allows small organizations to achieve state-of-the-art sophistication without a large staff of security experts. And all organizations—both large and small—get more proactive dynamic protection quite cost-effectively from automation that leads to peak productivity.

SiteProtector with the Security Fusion Module helps make Dynamic Threat Protection a reality, delivering these additional benefits:

- Improves the effectiveness of intrusion protection systems
- Focuses available security personnel on activities that have the most impact
- Gives security a business context for making more informed decisions
- Makes security information pertinent to diverse enterprise audiences: IT management team, security administrators or business managers
- Maximizes productivity by helping to identify false positives and automatically reducing false alarms
- Provides an enterprise-wide view of risk, threats and successful attacks
- Automates manual processes allowing staff to focus on more important tasks
- Optimizes limited resources by providing out-of-the-box security expertise
- Automatically assesses changes—improvements or otherwise—in security status
- Improves the ability to respond effectively and immediately to real threats
- Provides a platform for continual improvements to overall security
- Leverages best-of-breed detection and prevention technologies to deliver pervasive protection

The Bottom Line: SiteProtector with the Security Fusion Module offers better security with less reliance on labor-intensive manual processes, which translates into lower cost for the organization.
Conclusion
Companies often spend more on security systems and solutions without getting better security. But automating the correlation of intrusion protection defenses is virtually guaranteed to provide a solid return on the investment as it enhances network security, improves productivity and dramatically lowers costs. Not only is automated correlation the most cost-effective way to protect network segments, servers and desktops across the enterprise, it may well be the only way for most organizations to obtain such pervasive protection.

The RealSecure SiteProtector with the Security Fusion Module allows any organization—large or small—to have industry-leading security expertise available 24x7x365. Comprehensive risk correlation focuses available resources on real threats, which minimizes the potential for financial loss and drives down the cost of providing security. Better security with a lower total cost of ownership. What more could any organization want—and need—in today’s global economy?

But don’t take our word for it. If you currently use the RealSecure Protection System, try SiteProtector with the Security Fusion Module for yourself to see just how effective an automated correlation system can be for your organization! Internet Security Systems is confident you will find RealSecure SiteProtector and Fusion a must-have tool for your staff, and is offering a free, full-featured version for evaluation. Check it out—risk free—for up to 90 days and see for yourself the power of RealSecure SiteProtector and Fusion.

And if you are currently only evaluating intrusion protection solutions, call us at 888-901-7477 or visit www.iss.net to learn more about how your organization can benefit from the out-of-the-box expertise SiteProtector and Fusion add to the RealSecure Protection System—the industry’s premiere choice in Dynamic Threat Protection.
Appendix A: Correlation Matrix

To be even marginally effective, correlation systems must provide substantial security expertise out-of-the-box. A good solution provides comparative metrics allowing organizations to detect any changes to security posture, possibly in reference to a benchmark or baseline. Better correlation systems bring a business context to security events by analyzing the impact on the most valuable organizational assets. The better systems also provide a high-level knowledge of attack patterns to escalate serious threat activity. Automated correlation systems make it practical to have both deep detection and pervasive protection with agents deployed at all critical network boundaries, and on all desktops and servers across the enterprise.

The Correlation Matrix illustrates how the various correlation technologies available in RealSecure SiteProtector and Security Fusion Module are used in concert to resolve today’s security challenges.

<table>
<thead>
<tr>
<th>Security Challenges</th>
<th>Asset Correlation</th>
<th>Custom Correlation</th>
<th>Comparative Correlation</th>
<th>Advanced Analysis</th>
<th>Automated Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Grouping</td>
<td>Enterprise</td>
<td>User Roles</td>
<td>Filters</td>
<td>Exceptions</td>
</tr>
<tr>
<td>Determine what is really important: Problem Areas; Greatest Risk; Attack Statistics and Demographics; etc.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Demonstrate relevance and context: Correlate security events to business units or groups; track activity through disparate organizational groups; Report impact organizational groups are having on security posture</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reduce time investigating security events: Attackers; Victims; Attacking Victims; Attack Impacts (Vulnerable, Successful, Unsuccessful)</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>NA</td>
<td>✓</td>
</tr>
<tr>
<td>Find the needle-in-the-haystack: 1 significant event out of millions; Attack Patterns over extended periods</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Limited security expertise: Out-of-the-box security expertise; The 'right' security questions to ask: Automated investigation and analysis; Automated security correlation</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Detect changes to normal activity (baseline), and track anomalous activity</td>
<td>✓</td>
<td>✓</td>
<td>NA</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reduce the noise: Known or acceptable events; Unimportant events; False alerts</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Figure 5: NA refers to correlation techniques that can be used to solve problems listed above but are secondary to the other techniques checked.
About Internet Security Systems (ISS)

Internet Security Systems (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical information assets from an ever-changing spectrum of threats and misuse. Software from Internet Security Systems dynamically detects, prevents and responds to sophisticated threats to networks, servers and desktops. Services include 24/7 system monitoring, emergency response and access to the X-Force, Internet Security Systems’ renowned research and development team. Internet Security Systems is the trusted security provider for more than 10,000 corporate customers, including all of the Fortune 50, the top 10 largest U.S. securities firms, 10 of the world’s largest telecommunications companies and major agencies and departments within U.S. local, state and federal governments. Headquartered in Atlanta, GA, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 888-901-7477.

Copyright © 2002 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, SiteProtector, Wireless Scanner, X-Force and X-Press Update are trademarks, and RealSecure a registered trademark, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.