STAT Neutralizer ™
Proactive Intrusion Prevention

Introduction

Current Situation

Information Security decision-makers are responsible for keeping their enterprises secure and online in the face of a growing assault of new polymorphic viruses, self-replicating applets, network-borne attacks, internal saboteurs, and users who do not follow established security policies. Despite their best efforts and the deployment of the most up-to-date software and patches, security engineers know that they are fighting a losing battle. The root of the problem facing network security professionals is that anti-virus suppliers will never overcome sophisticated hackers until the current reliance of IT security upon signature and byte pattern comparison is discarded. Regardless of how often administrators warn users to follow policy and beware of unsolicited e-mail attachments, such warnings continue to be unheeded. Furthermore, as the mobile workforce expands there is the growing threat of malevolent hackers gaining control of users' network access devices. In the end, decision-makers and administrators are left with no way to actively enforce good user behavior and thoroughly protect their network assets from misuse.

Current 'Solutions'

Typical measures to counteract malicious code include Anti-virus software coupled with server-based e-mail scanners. Some packages are focused primarily on mobile code (i.e., Active-X on web pages, e-mail macros) while others focus on macro viruses alone. Other security tools, like Network Intrusion Detection Systems (IDS) and firewalls, by their nature, are concerned only with network traffic and seldom go beyond monitoring network activity for attacks.

Many currently-employed products do not provide centralized policy management or problem logging. Some products rely on the users to download signature file updates, or require administrators to use additional products (e.g., Microsoft's SMS) to roll out updates. Due to the signature-based blocking used by Anti-Virus products, new viruses often spread rapidly before the signature files can be updated. (Both the "Melissa" and "I Love You" viruses were in this category.) To further complicate the problem, the vendors of some applications expect connections to their servers to be left open. What happens when these vendors get hacked? Could some cyber-criminal use these connections to turn off protection for all of these vendors' customers? For this reason, many administrators want to have visibility into, and control over, the update process.

Traditional signature-based and *pattern matching* malicious code prevention (i.e., Anti-Virus software) demonstrated inherent weaknesses with the recent proliferation of the 'Melissa', 'I Love You', and 'Anna Kournikova' viruses. In the case of 'I Love You' and 'Anna', Anti-Virus (AV) software vendors did not have new signature files available in time to prevent hundreds of thousands of initial infections. In fact, the delay in producing the new signature files for 'I Love You' was between 4 to 6 hours and cost the corporate world an estimate $700M in damages. Even if the time required to respond with a signature update were shorter, the extremely high adaptability and rapid promulgation of new viruses is still a limiting factor of traditional approaches. Nowadays, a typical encrypted virus can spread around the globe in a few hours while changing its size and characteristic byte code from computer to computer – thus circumventing pattern matching AV software that must exactly match the attacking code to be effective.

A new breed of products focuses on mobile code by 'wrapping' applications that typically are used to access mobile code (i.e., browsers and e-mail clients). This approach addresses some, but not all of the problem for user workstations. Products of this type are powerless to stop malicious code that has already been installed on the machine or code embedded in services or device drivers (e.g., a keystroke monitor).

In sum, existing solutions are insufficient to offer protection against an ever-changing threat environment. They still leave systems vulnerable to an ever-growing number of threats. A quick look at the headlines will show that defenses need to change. Flexible, real-time protection and policy enforcement is needed…the kind of protection available with STAT Neutralizer™.

The Nature of the Threat

A PricewaterhouseCoopers survey quoted by Security Wire Digest indicated that global corporations suffered more than $1.39 trillion in lost revenue in 2001 due to security breaches. According to the study, a majority of those losses stem from the rapid growth in computer viruses and denial-of-service (DoS) attacks. The combination of these attacks accounted for 60 percent of lost productivity among thousands of survey respondents. The survey indicated that Operating Systems were the top source of security breaches. The magnitude of this problem is indicated by the fact that the survey data were drawn from a global database of approximately 4,500 survey responses from technology professionals in 50 countries, as well as data from surveys released by other companies and media.

In addition to Operating System breaches, other intrusions that an enterprise needs to be prepared for include the following:

1. Trojan horses

Trojan Horses mask their true nature by hiding in an apparently useful/desirable application or piece of data. A majority install themselves in the system directory, and change something so they are run repeatedly (Run key, RunOnce key, or a service). This includes Netbus, Pretty Park (not really a Trojan), and Back Orifice. STAT Neutralizer rules stop exploits typically performed by Trojan Horses.

2. Viruses, worms and other propagation mechanisms

- The current "practice" is replication by e-mail. This includes *Pretty Park*, *Anna Kournikova*, and numerous other attacks generated with the utility that the *Kournikova* author wrote (*I Love You*, etc.).
- Propagation by copying to the Microsoft Word default template (Normal.dot), as done by the Melissa virus.
- Modification of an executable. Older viruses use this method for propagation.

Nimda

Nimda, with over $500M in damage, is being noted as the fastest moving and arguably most complex virus to hit the Web to date. In her Security Wire Digest article, "Nimda Difficult to Recover From," Shawna McAlearney, notes that despite applying patches and updating AV protection, many users infected by the Nimda worm that swept the globe are finding it difficult to successfully clean their systems of the virus. "To the best of my knowledge at this point, there is no way around cleaned files that become reinfected upon reboot," says Sam Curry, director of security architecture at McAfee.com. "This virus is doing so many different things, it wouldn't surprise me if it requires a lot of memory or if, as an incidental piece of damage, it was chewing up resources to the point where the system is unusable--in effect, a denial of service on the user." However, security experts say that tools that are more effective will become available as time passes. "I think…the tools will have improved significantly and will be capable of cleaning an infected system successfully," says Bruce Hughes, content security labs manager at ICSA Labs, a division

of TruSecure. (TruSecure publishes Security Wire Digest) "Right now the tools are still missing some things. I don't think all the tools are removing all the registry stuff yet and there could be other aspects of it that they're overlooking."

3. Unauthorized actions that may lead to host compromise

STAT Neutralizer rules prevent exploits that use unauthorized actions such as addition of disk shares, username / password grabbing (archived SAM, pwl files), and add/modify a user or group.

4. Behavior that may lead to privilege elevation

A common trick is to put malicious code into the path of an Administrator (e.g., create a malicious executable "c:\cmd.exe", and change the PATH environment variable of admin to begin with "c:\"). STAT Neutralizer rules stops this behavior.

5. Stolen laptops

STAT Neutralizer may be used to effectively 'turn off' all capabilities on a lost or stolen laptop computer if it is used to try to connect to the corporate intranet.

6. Non-mobile malicious code

Unlike the traditional signature-based solutions mentioned in the opening paragraphs, STAT Neutralizer is designed to combat the ramifications of any code that produces undesirable behavior in a system, regardless of whether it is mobile malicious – so it protects against malicious actions taken by code which has been implanted prior to installation of the STAT Neutralizer agent or by means other than network access (e.g., copied from floppy, or 'AutoPlay' executions from a CD-ROM).

7. Cyberattacks and cyberterrorism

There are concerns that cyberterrorists will try to disrupt the computer world, resulting in extensive damage to businesses and the economy in the United States.

"If we saw a truly comprehensive and destructive attack on a critical infrastructure – where it was well-planned, well-targeted – it could clearly have a destructive impact," said Michael Vatis, director of the Institute for Security Technology Studies at Dartmouth College.

Consultants like John Pescatore, Vice President and research director for Internet security at Gartner Inc., have been advising clients on how to handle cyberterrorism threats, which he expects will occur as the result of the U.S. military assaults against terrorism.

STAT Neutralizer

STAT Neutralizer draws upon Harris Corporation's rich heritage of providing high-level government and commercial security. For over 25 years, Harris has secured and protected computer networks and systems, and now provides intrusion prevention by stopping network threats before they impact enterprise businesses. STAT Neutralizer works proactively to intercept unwanted behaviors, identify them as undesirable, and prevent damage by taking a predetermined action against the unwanted behavior according to a specific policy. The desired course of action will be executed against the unwanted behavior whether the source is from known or unknown malicious code, human error, or other internal or external attacks.

STAT Neutralizer enforces user policies, using pre-configured rules that work right out of the box.

The STAT Neutralizer agent operation is tailored to the user environment by turning on or off the provided rules that monitor executing code and enforce security policies. STAT Neutralizer's agent-based kernel-level protection ensures complete coverage because all instructions executed in a given computer must utilize the kernel. STAT Neutralizer specifically protects against Operating System

breaches by securing exploitable holes until a new Operating System patch is installed that closes the hole.

Extensive management capabilities in STAT Neutralizer include a centralized console and a web-based administrative interface for remote access and management via a browser. Standard reports, event logs, and an SQL event database allow for immediate diagnosis and recording of intrusion attempts.

STAT Neutralizer's real-time defense provides a robust layer of protection at the kernel level. Because it operates at such a low level in the system, STAT Neutralizer seamlessly integrates with the existing security infrastructure. In this way, STAT Neutralizer invisibly supplements other elements of the total security solution including network-based intrusion detection, anti-virus, hardened Operating System, and network/enterprise management systems.

STAT Neutralizer Components

STAT Neutralizer comprises three components as shown in Figure 1, below:

1. An Administrative server that provides the centralized management and logging capabilities;
2. A browser-based administrative client application, accessible from any machine connected to the network; and
3. STAT Neutralizer Agents that reside on the machines to be protected.

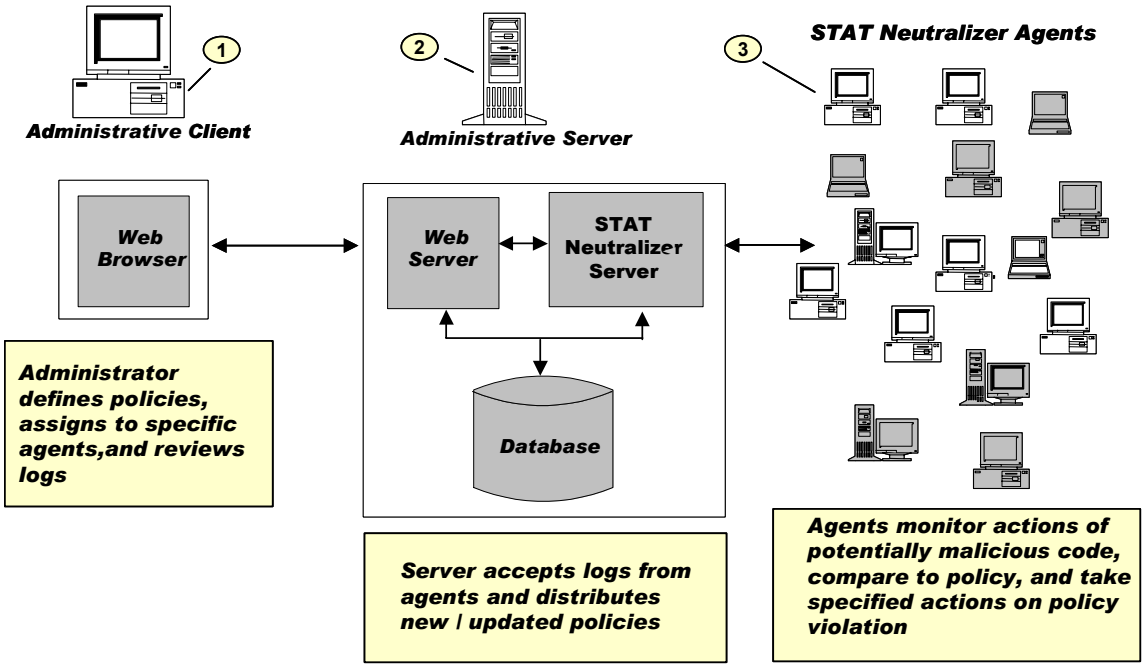

Figure 1 - Typical STAT Neutralizer Installation

Administrative Server

The Administrative Server provides a robust command, control, and monitoring capability. Communication between administrative application users and STAT Neutralizer Agents is protected via SSL encrypted links. The server uses the Apache web server and an ODBC-compliant database engine. Large-scale users may substitute a more powerful ODBC-compliant database engine such as Microsoft® SQL Server for the database engine.

Administrative Client

Administrators may access the STAT Neutralizer system after authenticating on the network by entering a valid user name and password via Internet Explorer. Provided capabilities include the ability to install Agents on machines attached to the network and management of rules, policies, and groups of agents. Additional screens support queries and log reports generation as well as maintenance of the logs.

STAT Neutralizer Agents

Agents monitor all code execution on protected machines by intercepting code at the kernel level, as shown in figure 2, below. The intercepted instructions are compared to the rules that reflect the implemented policy to determine if the instructions should be allowed to execute or be blocked, based on the policies that are implemented. The rules may contain execution limitations based on combinations of the following:

- Execution context: (e.g., it is O.K. for Microsoft Outlook ® to read the address book, but not other applications). Some actions may be denied regardless of context (e.g., modification of the Run key)
- User-specific: Users may be allowed (or denied) access and or capabilities.

If the policy dictates the action, the Agent will log the information about the triggering event (timestamp, event type, user, machine, application, etc.) to the Administrative server. Should network communications be unavailable, the log records are queued and sent when the link becomes available. Similar queuing is employed on the Administrative Server for policy updates.

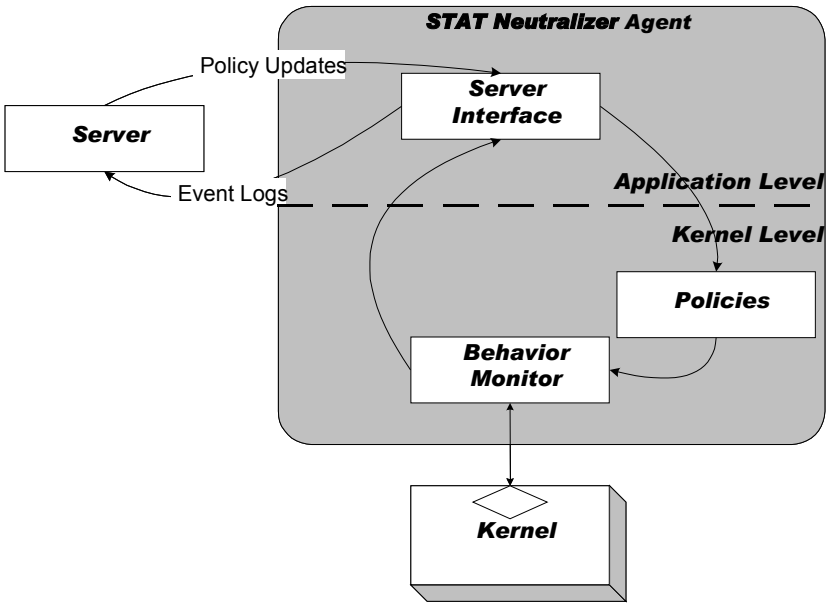

Figure 2 – STAT Neutralizer agent functional block diagram

Currently, available agents protect Windows NT ® 4.0 and Windows ® 2000 and XP systems. Support for Linux and Solaris are scheduled for future releases.

Security Policies

STAT Neutralizer allows policy-based prevention of malicious code execution in real time. A policy is a collection of rules that defines the allowable and unallowable behaviors for an application or group of applications. Policies may vary based on machine type (e.g., a Web server would have different 'allowable behaviors' than a user's workstation). Policies are used in a three-tier hierarchy:

1. **Rules** are the lowest level. They define the specific behavior to look for and the desired response (i.e., Allow execution, Deny execution, Abort Application, and Log the event). Rules may be associated with a specific application, set of applications, or all applications, and may be varied based upon the specific functions of the machines in the system.
2. **Policies** collect a group of rules associated with a common area to be protected (e.g., a Microsoft Outlook policy, or an Apache Web Server policy). These policies are then assigned to groups.
3. **Groups** are made up of assigned machines that have the need for similar rules based upon their function in the enterprise (e.g., User workstation, Web server, etc.). This allows the administrator flexibility to tailor network protection.

Proactive Protection

STAT Neutralizer provides proactive protection from threats as illustrated in the following table of features and benefits:

FEATURE	BENEFIT
1. Behavior based protection	Unlike protection that defends against signature-based malicious code, STAT Neutralizer's behavior-based approach provides powerful, standard protection against polymorphic viruses, self-replicating applets, network-borne attacks, internal saboteurs and uninformed users. STAT Neutralizer's unique capabilities allow protection against a virus like "I Love You" even when .dat updates are not installed and users download infected files. This capability enables STAT Neutralizer to protect against unknown malicious code as well. New exploits that are 'variations of a theme' do not get past the behavior-based scanning, providing powerful protection against polymorphic viruses.
2. Real-time protection	Existing solutions require updates to address the ever-growing number of new and previously unidentified threats. This is insufficient in an ever-changing threat environment. STAT Neutralizer does not require updates, enabling it to always be in protect mode, even against the unknown.
3. 360° protection	Omni-directional protection from threats regardless of origin - internal, external, or if a corrupted disk is introduced into the system.
4. Intrusion prevention	STAT Neutralizer goes well beyond a firewall or Intrusion Detection System (IDS) by preventing intrusions from occurring. Firewalls merely block network traffic; IDS's detect and log events, alerting the operator that a potential intrusion has occurred, but doing nothing to prevent the intrusion. Any encryption schemes used on network traffic (SSL / VPN's) are removed prior to STAT Neutralizer's examination, ensuring that it can identify malicious code.

FEATURE	BENEFIT
5. Prevents malicious code execution regardless of its source	Firewalls and network IDS's by their nature only work with network traffic. In contrast, STAT Neutralizer provides complete protection. STAT Neutralizer works on policies that define allowable behavior, and so may be used to prevent execution of code the administrator deems unallowable on the network. It can prevent your network assets from being used as hosts for denial of service (DoS) attacks.
6. Protection against both the known and the unknown	Traditional anti-virus software relies on known signatures to recognize malicious code. These signatures require constant updates and only work against 'known' exploits. Often they are not adequately updated and kept current by the user. STAT Neutralizer prevents potentially damaging behavior, even from viruses that have never been seen, by monitoring the code as it executes and making its decisions at run time.
7. Strict security policy enforcement	In addition to watching for suspect behavior, STAT Neutralizer can also monitor and enforce policies, such as prohibiting an application or user from accessing certain files or directories, preventing users from downloading and installing their own programs, or even simply informing an administrator when a log file is turned on or off. STAT Neutralizer automatically holds authorized and unauthorized users accountable to security policy and protects network assets from misuse. STAT Neutralizer's policy-based approach to threat prevention literally prevents intentional or unintentional disruptive behavior.
8. Customizable rules	Through the optional Developer's ToolKit, STAT Neutralizer allows administrators to maintain complete control over their rule and policy updates. Administrators can characterize any custom applications and define their actions as 'normal' to allow users access to specific capabilities that other (unknown) applications might not have (e.g., access to a specific database). With STAT Neutralizer, an administrator can have different policies based on machine roles (e.g., Web server, User Workstation, Administrator Station, public kiosk, etc.).
9. Ready out of the box	STAT Neutralizer comes configured with default rules to protect against Trojan Horses, privilege elevation, information gathering, viruses, buffer overflows in selected applications (e.g., IIS), and DoS exploitation right out of the box. Immediately upon installation, systems are safe without needing any signature updates, since new exploits do not get past the behavior-based scanning. Users do not need to be sophisticated, as STAT Neutralizer does not require any customization on their part.
10. Centralized Management	STAT Neutralizer may easily be rolled out using standard administrative features provided by Windows NT/2000. Central console allows for single point of management, while Web access allows for management from any Internet connected PC.

FEATURE	BENEFIT
11. Extensive reporting and log file capabilities	The logging capabilities allow the administrator to track where and when problems have occurred to determine whether additional security measures are indicated (e.g., training a user who seems to have a high number of malicious web accesses). Filtering of logs may be defined in the policies, i.e., the administrator can decide which events to log / not log.
12. Monitoring of logs not required for protection	IDS's and firewalls require constant monitoring of massive log files that they generate in order to appropriately respond to attacks. STAT Neutralizer responds without requiring log monitoring while providing complete logging capability of the actions it has taken to protect against malicious code.
13. Real-time substitute for security patch protection	Many security patches are not deployed due to the extensive testing required prior to changing operational environments. This often leaves systems exposed for many weeks or even months. STAT Neutralizer can trap out many of the behaviors that result from exploiting the vulnerabilities that these patches fix, maintaining the security without requiring patching prior to testing.
14. Significantly reduced false positives	Since STAT Neutralizer looks at executing code, as opposed to network traffic, only attacks or events that would have resulted in harm are logged. Furthermore, STAT Neutralizer's supplied policies protect against many false positives and the administrator can create rules to allow (and not log) behaviors deemed as "false positives."
15. Supports encrypted data	STAT Neutralizer has no problem dealing with encrypted data (unlike Network IDS's), since STAT Neutralizer looks at decrypted, executing code rather than network traffic.

STAT Neutralizer – Part of the STAT Family

Trusted Solutions from a Trusted Source

The STAT family of products is developed and supported by Harris' Government Communications Systems Division (GCSD). GCSD has a long history of providing trusted, secure systems to the Department of Defense and other federal agencies. All of our software has been developed using the SEI CMM Level 3 practices that are standard in the Division.

STAT Product Family

The Harris STAT family of network security software products, backed by decades of Information Security expertise, provides the most trusted solutions in the industry for protecting information and computer systems from hackers, viruses, and other threats. Each product has a role in the defense in depth strategy. The Harris products complement other security products in bringing a total defensive security perimeter to a computer network. STAT products include STAT Scanner, the most comprehensive vulnerability Scanner available today; STAT Analyzer, which automates and streamlines the vulnerability assessment process by correlating outputs from multiple vendors; and STAT Neutralizer, a unique, new intrusion prevention tool that provides proactive protection for the

enterprise. Provided below is a short overview of each product. Additional information is available online at http://www.stat.harris.com.

STAT Scanner

STAT Scanner, the world's leading host-based vulnerability scanner for Windows NT/2000/XP, now also assesses Linux ® (Red Hat ™ and Mandrake™) and Unix® (Sun™ Solaris™ and HP-UX). STAT Scanner's vulnerability database contains 2,500+ vulnerabilities. The product is updated frequently during the month with the newest vulnerabilities, and includes complete, tested solutions for all vulnerabilities found. STAT Scanner is easy to use and is centrally administered. It also allows systems administrators to remotely fix many of the vulnerabilities in their database with a simple point and click interface. The reporting structure can be customized for management or technical personnel with comprehensive reporting of selected machines or an entire domain. Detailed information for use by a systems administrator in addressing the problems is available. STAT Scanner utilizes Crystal Reports®, and can export all reports into a wide variety of formats for customization.

STAT Analyzer

Systems administrators and security engineers typically use a combination of products that report system health from a variety of perspectives. The challenge comes in interpreting many different reports that might, in some cases, be conflicting or inconsistent. STAT Analyzer uses a proprietary artificial intelligence technique[1] to take the outputs of several different scanning tools (STAT Scanner, ISS Internet Scanner™, CyberCop Scanner®, and Nessus Scanner), and integrate them into a single result, evaluated relative to an enterprise's security posture. This saves the systems administrator a great deal of time analyzing these reports individually, and lessens the probability that vulnerabilities or security problems will be overlooked.

In response to requests from network security experts, STAT Analyzer incorporates analysis and reporting capabilities for users of multiple vulnerability scanning tools. STAT Analyzer 2.5 includes a new "Reasoning Chains" report that uses Harris Corporation's *FuzzyFusion* engine to provide unique insight into specific vulnerability exploitation scenarios and how they are derived. This capability reduces the security engineer's analysis time, provides insight into the COTS scanning tools in order to build confidence in the results, and provides insight into how vulnerability combinations can be exploited. Additional new reports include "Fix It", which consolidates correction recommendations from multiple vulnerability scanners into a single report; and "Summary", which provides a summarized rating of the machines by the number of vulnerabilities, as well as the machine's ability to be compromised. STAT Analyzer 3.0 adds support for Nessus, the popular scanning tool developed by Renaud Deraison.

STAT Neutralizer

The newest member of the STAT product family is STAT Neutralizer. It is a unique, new intrusion prevention tool that provides proactive protection for the enterprise, currently targeted to Windows NT/2000/XP environments. STAT Neutralizer allows the systems administrator to enforce "rules of behavior" that are allowed or disallowed. The advantage is that rules can be set up that will not allow mass mailings from an MS Outlook mailbox file, will protect a computer for deletion of system files, and other such obvious malicious behaviors. It intercepts, identifies and prevents damage from malicious code, human error and other attacks -- whether borne internally or externally. STAT Neutralizer can be used to provide heuristic-based prevention that traps virus, worm, and Trojan-based exploits even before they are widely known (and thus not detected by a virus scanner). It accomplishes this by preventing undesirable execution behaviors from occurring. The STAT Neutralizer agent

[1] The only technology currently available that applies data correlation technology to information security. It addresses the differences in the way individual vulnerability scanners and other tools look at security data, and consolidates the disparate data, whether numerical, textual or a combination, into a single, meaningful information repository.

monitors all executing code at the kernel level of the Operating System (Windows NT/Windows 2000/XP) to ensure both high performance and complete coverage.

STAT Neutralizer's extensive management capabilities include a centralized console for a single point of management. With a web-based administrative interface, authorized users can access and manage STAT Neutralizer remotely via a browser. Queries of event logs enable users to stay on top of activity in their network. STAT Neutralizer is also customizable by an organization's security staff – so it can be set up to enforce "specific policies" of an organization.

Conclusion

Information Security decision-makers are responsible for keeping their enterprises online and secure in the face of increasing cyberthreats. To-date, decision-makers and administrators have had no way to actively enforce good user behavior and thoroughly protect their network assets from misuse.

Existing solutions are insufficient to offer protection in this ever-changing environment. Traditional Anti-virus software relies on known signatures to recognize malicious code; Firewalls merely block network traffic; Intrusion Detection Systems only detect and log events. Ultimately, systems are left vulnerable to an ever-increasing number of threats. Flexible, real-time protection and policy enforcement is needed.

STAT Neutralizer offers that protection, providing intrusion prevention -- not just detection. Unlike signature-based solutions, our behavior-based model protects against known and unknown threats, polymorphic viruses, self-replicating applets, network-borne attacks, internal saboteurs and user error. STAT Neutralizer stops network threats *before* they impact enterprise business.