

# Behavior-Based Intrusion Prevention Technology



*Ronda Henning  
Senior Secure Systems Engineer  
Harris Corporation*



## Behavior-Based Intrusion Prevention Technology

### Introduction

Security attacks against computer networks are evolving faster than historical protection solutions. Despite the implementation of a series of protection technologies, including anti-virus, content scanning, firewalls, intrusion detection systems (IDS), and Virtual Private Networks (VPN) (Table 1, below) enterprises are still being penetrated by determined attackers.

The fundamental reason for these penetrations is that the existing tools are all *reactive*. Corrective actions to detect, analyze, develop and test a fix, and then distribute and push it throughout the enterprise, can take days. Meanwhile, the enterprise is suffering significant disruption to business operations. Today's networked enterprise, with thousands of personal computers, laptops, and assorted digital assistants on a network, cannot tolerate a reactive model – one that waits until something happens before it can prevent security problems.

Best commercial practice deploys multiple layers of mechanisms to protect the boundary of an enterprise, specific network segments and servers, and the user desktop. All of these mechanisms require security management services if an enterprise is to maintain control of its security posture. In addition, products such as vulnerability scanners, intrusion detection systems, and anti-virus capabilities all need continuous monitoring and maintenance to ensure that they are kept current. One missed update could leave the entire enterprise vulnerable to the latest penetration attack.

Traditional Security Technologies	
Anti-Virus	Examines attachments and executables for undetected, unwanted consequences by comparing to 'signatures' of known exploit code.
Content Scanning	Examines data/user interactions for potentially malicious or objectionable attachments.
Firewall	Examines protocols/IP addresses. Permits/prevents traffic on a network segment and/or system based on these parameters.
IDS	Detects that something it knows about is happening. If something is going on that is unknown, does nothing.
VPN	Encrypts everything in a session; decrypts at destination. Makes no judgment about what the decrypted data may be.

Table 1. Overview of traditional security technologies

## Behavior-Based Intrusion Prevention Models

Enter the concept of behavior-based intrusion *prevention*. In this model, instead of developing *reactive* security policies, security policy becomes a *proactive* tool to protect the enterprise. Instead of bandaging vulnerable elements of the enterprise, the enterprise becomes self-protecting.

Behavior-based intrusion modeling represents the emerging generation of security technology. These tools, such as STAT Neutralizer™, allow the security officer to determine which behaviors are acceptable and which are not. Just as a parent sets standards for a child’s acceptable behavior and punishes unacceptable behavior, the security officer defines acceptable and unacceptable behaviors in a network.

What makes behavior-based models so desirable is that the model is translated into action at the lowest levels of execution, the kernel. The kernel is the lowest layer an application can access directly. If an application executes on a device, it has to “call” the operating system kernel. “Kernel calls” are the basic language constructs for the execution of instructions. They are documented, defined, well understood and limited in number. While there is any number of combinations, kernel calls are used in standard patterns and universally applied. Figure 1 illustrates the concept of intrusion prevention architecture.

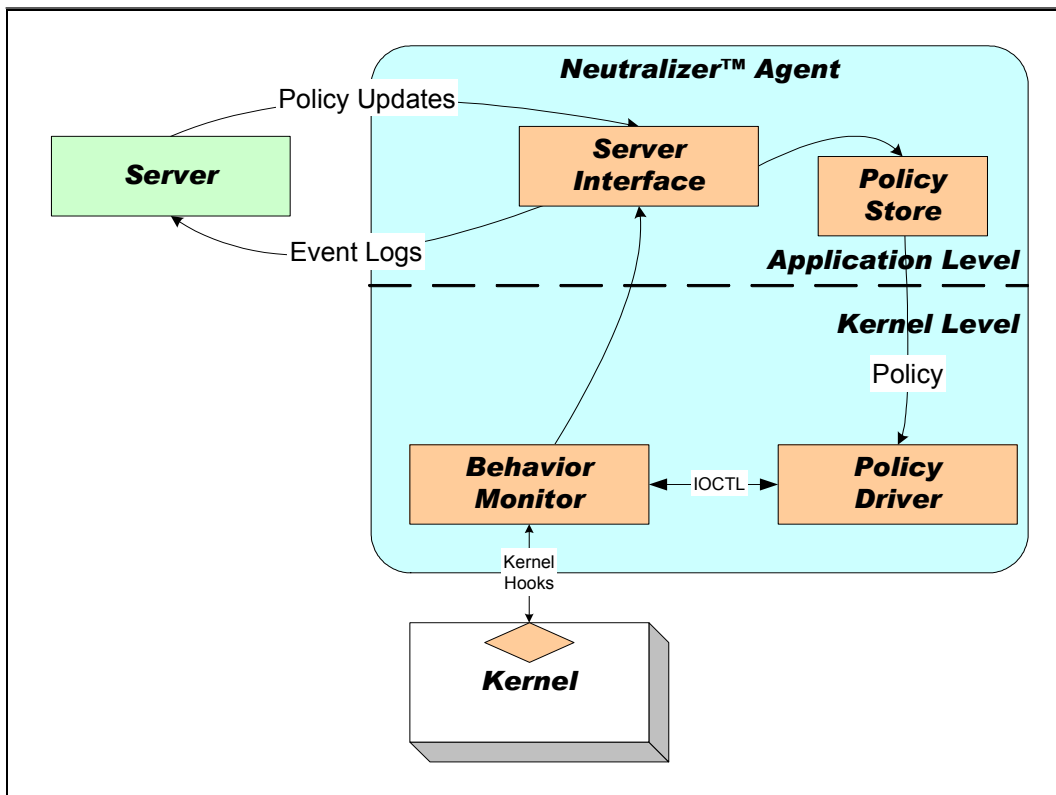


Figure 1. A robust Intrusion Prevention Architecture is policy driven and protects the client and server at the kernel level

By understanding the interaction between the operating system kernel and the application, behavior-based models can determine acceptable and unacceptable activities. For example, acquiring control over a user's address book is an undesirable application level behavior exploited by various types of malicious code. Behavior-based intrusion prevention tools determine that modification of address book contacts is acceptable for Outlook® and unacceptable for all others. Unauthorized address book acquisition is stopped, regardless of the source of the request.

### **Why This Model is Different**

Unlike intrusion detection or virus detection tools, behavior-based models do not respond to established traffic patterns or attachment examination. They examine activity as it occurs. Traditional approaches to the Code Red or Nimda attacks have been to look for patterns of code (i.e. a signature) and then take action. By the time an attack signature has been developed, it has been too late to prevent an attack. With a behavior-based tool, an administrator simply says, "Do not allow," and any attempt to execute that behavior is stopped before anything can happen.

Instead of focusing on reactive correction, behavior-based models proactively examine the normal kernel activity of an application. Once an application's normal behavior has been baselined, a behavior profile can be created. This predefined policy template can be used immediately, or tailored to match the enterprise's requirements. The basic work is done once per application release – not daily or hourly in response to new attacks.

It could be said that behavior-based models just profile a different aspect. By profiling kernel calls instead of individual attack patterns, behavior-based models apply a lowest common denominator approach to the problem.

This approach simplifies maintenance for the end user because vulnerability updates in response to specific threats do not have to be in place to prevent a specific attack from being successful. If an attack occurs – and the behavior model does not allow its behavior – the attack is not successful. The behavior model does not have to understand the attack itself; it just has to know that the behavior the attack exploits is not allowed within the enterprise.

### **Defining Characteristics of Behavior-Based Tools**

Simplicity and centralized management are probably the hallmarks of enterprise-class behavior-based tools. No enterprise wants to deploy a tool that requires in-depth knowledge of every kernel call, every application, and every operating system configuration in use. If a tool requires this level of sophistication, it is not a good choice. It will be too difficult to maintain in operational use.

The best behavior-based tools have graphical user interfaces (GUI) and point-and-click policy definition capabilities. A behavior-based tool has to make policy definition an easy task.

An enterprise security officer can pick and choose among predefined policies, or use them as a starting point and then tailor the policy to the enterprise environment.

Centralized management via a console type interface assists in policy development. Once the behavior-based policy is defined, it has to be communicated to all of the assets to be protected. The best behavior-based tools facilitate this interface with encrypted communications between the management console and the agents to ensure the integrity and confidentiality of the information.

In the event an unacceptable behavior is detected, action options are a desirable feature. When an unacceptable behavior occurs, the administrator needs to know that somebody or something is trying to violate the enterprise security policy. At policy establishment, the administrator can have a set of optional actions to choose from, such as: ‘notify the administrator,’ ‘write the attempt to a log,’ or ‘block the attempt.’

### **When to Deploy Behavior-Based Intrusion Prevention Technology**

Behavior-based intrusion prevention security tools are valuable on all networks. They prevent damaging behavior by monitoring code as it executes – providing powerful protection against viruses, worms, malicious mobile code, and internal or external network-borne attacks. Behavior-based security tools complement traditional anti-virus, intrusion detection, and firewall security products by providing a last layer of defense at the operating system level – stopping threats before they cause harm. Table 2, below, shows how behavior-based security tools complement traditional security products.

<b>Traditional Security Products</b>	<b>Function</b>	<b>How Behavior-Based Tools Complement Traditional Security Products</b>
Anti-Virus	Signature-based anti-virus products protect against known security threats, but have no knowledge of unknown threats.	Behavior-based tools protect against new or unknown threats.
Intrusion Detection	Basic intrusion detection products report that an intrusion has occurred but do not prevent the intrusion from causing damage. Advanced intrusion detection products may stop threats after detection if the attack signature is known.	Behavior-based tools work proactively to prevent the introduction of negative behavior from external and internal sources, from both trusted and unknown sources.
Firewall	Firewalls are concerned only with network traffic, and seldom go beyond monitoring network activity for attacks.	Behavior-based tools watch for ‘bad’ behavior occurring at the host level and are not subject to circumvention by encryption or fragmentation, breaches from inside the firewall, or other common network attacks.

*Table 2. How behavior-based tools complement traditional security products*

## **Why to Deploy Behavior-Based Intrusion Prevention Technology**

Behavior-based security tools represent one of the most maintainable, effective investments in enterprise security available to-date. They do require some care in their initial policy establishment, but a good enterprise security program already has a defined security policy and protection objectives in place. In comparison, administrative logistics associated with traditional security measures are complex and time consuming.

According to Computer Economics, an independent research firm specializing in IT valuations, the 2001 worldwide economic impact of malicious code attacks totaled \$13.2 billion, with Code Red accounting for \$2.62 billion, SirCam for \$1.15 billion and Nimda for \$635 million. Gartner analysts said at their May 2002 Symposium/ITtxpo that by the year 2005, 20 percent of businesses will experience intrusion and that the cost of this intrusion will exceed the cost of prevention by at least 50 percent. A behavior-based intrusion prevention environment can provide a proactive countermeasure that effectively protects the enterprise against these and other security threats.