

## **Host Threat Prevention: a New Weapon in the War against Desktop Threats**

### **Introduction: How safe are your desktops?**

Given the recent spate of destructive viruses like SoBig, the desktop PC has emerged as one of enterprise security's major points of exposure. Traditional approaches to PC security—anti-virus and personal firewalls—only partially address security threats in the form of malicious executables that are becoming more frequent and more sophisticated. This paper examines desktop security issues and explores how one vendor in particular, SecureWave, addresses this area with their software products.

Host Threat Prevention (Host Threat Prevention), a new class of security product, allows only previously approved processes to execute while preventing any other processes from running. Unlike the conventional sandbox approach that isolates sources of vulnerability, Host Threat Prevention doesn't attempt to quarantine running processes, which can become tremendously complicated with today's Windows applications. Instead, Host Threat Prevention works by enabling known, trusted code processes to run while preventing all others from executing. This stops malicious code, such as viruses and worms, from running underneath the processes. As such, Host Threat Prevention is efficient and readily dovetails with existing security components including enterprise access control, identity management, intrusion detection, and anti-virus.

This paper examines the tools and strategies organizations have been employing in the war against Windows viruses and attacks. It reviews the existing defensive arsenal, identifies the drawbacks of the current types of tools, and describes a new class of tools, Host Threat Prevention, based on the concept of default-deny. Finally, introduces SecureWave, as an example of a Host Threat Prevention solution for the Windows environment.

## **Crumbling defenses: Counting on the wrong weapons**

It is no secret. Windows is riddled with code that can leave a business vulnerable to attack, which is why the PC desktop has emerged as a primary source of enterprise security worries. The extensible nature of Windows vastly increases the difficulty of defending the desktop, which leaves the enterprise highly vulnerable. For example, current PC practices undermine desktop and perimeter defensive measures. Users readily download unknown code and open unsolicited attachments and email messages. In doing so, they become unwitting accomplices in security breaches.

In addition, new classes of threats are emerging that the current defenses was never intended to combat. Personal USB storage devices, for example, allow for the easy attachment of new storage, but also pose a threat by allowing malicious code to bypass perimeter defense thereby introducing another point of vulnerability. Similar to USB storage, almost any I/O device attached to the PC bypasses whatever perimeter defense is in place and introduces additional threats. Not only can malicious code enter into the system but confidential and private information can leave via personal memory devices ranging from USB memory sticks to removable memory used in cameras and handheld organizers. Finally, the very flexibility of Windows itself, which is designed to support nearly unlimited numbers of ports and services, renders the system vulnerable to attack.

To date, the predominant defensive strategy has been a combination of perimeter defense and desktop anti-virus software based on black lists of offending code. Perimeter defense calls for security systems to identify malicious code at the boundary of the system and reject it before it can enter and do damage. Anti-virus software does the same with virus attacks. But here's the catch: unless the code has previously been identified, perimeter defenses can't recognize and repel it. Similarly, intrusion detection systems are only effective against previously identified threats. Patch management, which closes security holes in the operating system, is too slow and cumbersome to serve as a first line of defense.

At best current defense strategies attempt to contain damage and then fix it after the fact. The organization, however, will still suffer some amount of disruption and incur significant costs resulting from an attack. These strategies also are very costly to maintain. Black lists and

patch management require extensive ongoing labor. Administrators must continually update black lists and download and deploy the latest patches. They must do it fast, and they must enlist the active participation of all users. Any delay in updating the latest virus signature or patch of a system vulnerability leaves the organization susceptible to attack. Such security administration takes time and attention and diverts valuable people from other, more productive tasks. It also puts the hackers and crackers in control, not administrators. At a time when organizations everywhere are feeling financially constrained and IT organizations already are stretching overburdened resources to the breaking point, security administration becomes a painful burden that seemingly gets larger every day.

Given these challenges, Hurwitz & Associates recommends that a new class of security product, call Host Threat Prevention, be added to bolster defense efforts at the perimeter and especially on the desktop. Managers have painfully learned how fruitless it is to try to anticipate new threats or try to keep the outside world from getting in. With Host Threat Prevention, however, it doesn't matter what happens outside or what new threats enter since Host Threat Prevention only allows known, trusted code to execute.

### **New strategy required—default-deny**

Host Threat Prevention is based on the principle of default-deny, in which everything is automatically prevented except that which has been explicitly approved. In short, the default position is always no. Host Threat Prevention uses default-deny to reinforce conventional security products with an effective defense at the desktop against any unknown threats—those that readily evade perimeter defense—as well as attacks from other channels, such as USB and I/O devices. As such, it delivers defense from the perimeter to the desktop against any potential threats.

Through default-deny, Host Threat Prevention fills the critical gap in today's conventional defenses, which address only known, recognizable attacks. To guard against unknown threats—those initial attacks that strike before black lists and patches can be updated to defend against the new attack, organizations can implement Host Threat Prevention, which stops unknown attacks as well as attacks from non-conventional directions, such as through USB devices and other I/O devices attached to the desktop. Host Threat Prevention simply

stops all code that isn't pre-approved from executing at all. As a result, it will stop known any malicious software without even having to know what it is, whether the latest unrecognized virus or the most innocuous game.

Through default-deny Host Threat Prevention is particularly effective on the Windows desktop, which has emerged as major point of vulnerability. Default-deny is based on a simple premise: allow only what the business needs and has approved; deny everything else. In practice, default-deny is simple to implement. It follows a three-step process:

1. Identify the portfolio of executables—the organization typically runs a finite number of Windows applications with a known number of executable files. These can be readily identified. Changes to this set of applications and executables are usually known well in advance and don't occur that frequently.
2. Specify the use of particular I/O devices—the organization specifies the approved I/O devices and USB storage devices and defines policies that restrict usage to only what is absolutely necessary.
3. Block everything not previously identified or specified—malicious code may still enter the system but it cannot cause damage because it is not on the tightly controlled list of approved applications, executables, and I/O devices. Thus, it will automatically be prevented from executing.

In short, everything unknown that might do damage—executables—fails. The advantages of Host Threat Prevention are numerous. In addition to being straightforward to implement and execute, it is easily maintained, which makes it less costly to operate. No longer must administrators continuously update virus definitions and install patches. Most importantly, it stops unknown threats as well as known threats. Therefore, with Host Threat Prevention there is no need to predict where the next threat will come from or what shape it will take.

Could Microsoft create a Host Threat Prevention as part of Windows? Certainly, but it would go against everything Microsoft is trying to achieve with Windows. Microsoft designed Windows to be a universal operating system able to run on any Intel-based device from the smallest handheld to large servers. It architected Windows to support almost any application or service a developer cares to create for the Windows platform. While this is one of Windows' great strengths, it also is the source of its security vulnerabilities. It would be unrealistic to expect Microsoft to thoroughly re-architect Windows to incorporate Host

Threat Prevention capabilities based on default-deny. At Hurwitz & Associates, we don't foresee Microsoft doing this anytime soon. Host Threat Prevention is one capability that Microsoft is probably happy to leave to outside product developers.

### **SecureWave delivers default-deny—the primary layer of defense**

SecureWave is a security software company that has emerged as a leading proponent of default-deny defense for the Windows environment. Unlike the conventional perimeter defense solution providers, SecureWave addresses the problem through host intrusion prevention, which takes place at the application execution and I/O device management level where it blocks everything but the approved applications, executables, and I/O devices.

With its default-deny approach and focus on the Windows desktop, SecureWave represents an example of Hurwitz & Associates' concept of a Host Threat Prevention-based defense. As such it complements whatever components of conventional defense are already employed, such as anti-virus, IDS, and patch management. Since the Host Threat Prevention product doesn't remove any of the offending code but rather renders it harmless by preventing it from executing, anti-virus and intrusion detection products still are needed to remove the undesirable code. By using SecureWave in conjunction with these other products, enterprises can protect themselves against any threats on the desktop regardless of how they enter the environment and remove them at their leisure.

The SecureWave default-deny approach allows the organization to manage and control Windows workstations in a way that is non-disruptive, non-intrusive, and transparent to workers. SecureWave allows workers to run the applications they need while enabling the organization to focus its resources on its portfolio of Windows applications without the distraction and disruption of viruses and other code-based attacks.

The SecureWave approach is delivered through two products:

- SecureEXE blocks all unauthorized software (including viruses, games, personal software, etc.). If a virus enters the Windows environment, it simply cannot execute, which renders it harmless.

- SecureNT enables the administrator to remotely control and audit activity on all I/O devices of each workstation, from memory sticks and floppy drives to PDAs, DVD/CD-ROM, tape drives, scanners, parallel and serial peripherals, or any other plug-n-play device.

In all cases, any malicious code or unapproved code simply sits there unable to execute. Using conventional anti-virus and intrusion detection tools, the organization can, if it so desires, clear out any malicious code at its convenience.

Unlike conventional perimeter defense tools, which rely on a black list, SecureWave uses a white list—a list of approved applications, executables, and devices. Where black lists are difficult to maintain and keep current, requiring nearly constant vigilance and even then will fail in the face of unknown code, white lists are simple to build and easy to maintain. Only the approved applications, executables, and devices on the white list are able to run; everything else, whether malicious or not, is blocked. Authorized administrators and managers can add new applications to the list of approved executables after they have been assured of its safety.

SecureWave solutions are designed and developed for medium- to large-scale system environments. Through the default-deny approach SecureWave enables organizations to achieve greater security with less effort and at a lower cost.

### **Hurwitz Security Vision: Round out your desktop security strategy with Host Threat Prevention**

Security technologies such as perimeter defense, anti-virus protection and intrusion detection do part of the job, but they still leave the enterprise vulnerable through its Windows desktops. They cannot prevent unknown attacks and threats from unconventional directions, such as USB attached devices.

Hurwitz & Associates recommends companies augment their conventional perimeter and desktop defenses with a Host Threat Prevention solution based on the default-deny principle. Host Threat Prevention fills a critical security gap, ensuring that enterprises can run their trusted business processes without disruption by malicious code from any source.