The Business Case For

Desktop Intrusion Prevention

PIVX Solutions, Inc.

Overview

PreEmpt from PivX Solutions, Inc. defines a whole new approach to Windows host security. Using *Desktop Intrusion Prevention*—proprietary risk-mitigation technology in conjunction with world-class security research, PreEmpt (formerly known as *Qwik-Fix Pro*) protects all versions of Microsoft Windows from known and *unknown* remote security threats, including worms, Trojans, spyware and other malware. This unique capability is provided through automated repair of critical security-related software flaws and automated security configuration management. This serves to protect PreEmpt users in advance of malicious exploits - in some cases months before they are released by hackers.

In this paper, we describe the business value of Desktop Intrusion Prevention in preventing costly attacks to your organization, and explain why existing, reactive security solutions are inadequate against today's rapidly changing threats, and how PreEmpt effectively closes the gaps left open by even the current best of breed of security products.

> *"Security flaws and errors found in software are responsible for the exploits that lead to identity theft, unauthorized funds transfer and fraud, costing the U.S. economy $59.5 billion per year."*
> -National Institute of Standards and Technology.

Microsoft Windows operating systems and related applications such as Internet Explorer contain thousands of security-related software flaws that have been, or could be, exploited by malicious programs written by hackers. A fraction of those errors have been discovered, fewer have been repaired by Microsoft (in the form of "patches"). Experts agree that many more exploitable errors are still there waiting to be discovered.

PreEmpt was developed to shift the balance of power away from the malicious code-writers who seek to cause informational and financial damage to your organization. Simply put, PivX's world-class vulnerability research team discovers, analyzes and develops mitigation procedures, either a series of steps to lock your systems down through configuration changes or by actually re-writing vulnerable software to make it secure, in memory at runtime, without the need to recompile proprietary code. Through PivX's enterprise-class desktop client and server architecture, we then distribute these mitigation packages called "Fixes" to our desktop software clients, providing the immediate benefit of our ongoing security research.

It's like having a world-class team of security researchers protecting each and every one of your organization's Windows-based computers.

Introduction: The Business Need for a Proactive Approach

2004 was the worst year ever for malware: worms, viruses, trojans, spyware and adware. This trend, now clearly driven more and more by financial gain, continues to rise at alarming levels. In 2005, we have already seen exploits targeting vulnerabilities even *after* Microsoft has released patches to fix them – taking advantage of the fact that in most companies, fewer than 50% of desktops have the vendor patch installed by the six-month mark.

2004 provided these alarming statistics:

Malware caused $100 billion in damage worldwide in 2003.
Source: Computer Economics

- New viruses were up 50%
- The average time between discovery and exploit dropped to 5.8 days.
- Spyware was running on 25% of corporate desktops
- Phishing attacks grew at 30% per month
- Up to 30,000 computers were added to remote-control "bot" networks *per day*
- Spam accounts for more than 70% of all email

This deluge continues unabated, despite the widespread deployment of traditional security solutions, including:

- Perimeter defense (hardware firewalls)
- Server and desktop anti-virus products
- Software firewalls
- Anti-spyware products

Attacks on Microsoft platforms are the most common—
Windows is used by over 94% of Internet users

Why do the problems continue to grow? Simply put, the defenses are not getting to the *root* of the problem. The most effective way to deal with any problem is at the *source*.

An excellent starting point is the paper published by the National Security Agency entitled "The Case for Using Layered Defenses to Stop Worms." The paper can be downloaded at http://www.nsa.gov/snac/support/WORMPAPER.pdf. This paper analyzed the attack vectors used by malware and looked at what types of defenses would stop these attacks. It found that host-based intrusion-prevention systems and strong configuration could defeat or block 12 of the 14 different classes of attack vectors. Anti-virus could stop just *two*. Software firewalls, 6 more. The paper concluded that *no* single technology could protect against all types of malware, but that a layered defense including host intrusion-prevention provided the best defense.

Because it is unique, PreEmpt does not fit cleanly into the Host Intrusion-Prevention System (HIPS) category, but it *is* the category with which PreEmpt is most closely identified. The difference between PreEmpt and the other products in the HIPS category is that PreEmpt *is not* behavioral-based and does *not* maintain rule sets that require regular maintenance or need to be trained to recognize new and potential threats.

The Best Defense is a Good Offense: PreEmpt

> ***Average loss to Fortune 500 companies is $2M per worm***
> Source: Aberdeen Group 2004 Survey

PivX Solutions has taken a proactive approach to fending off increasingly sophisticated attacks, incorporating radically new approaches in its groundbreaking risk-mitigation framework.
PivX's "*Desktop Intrusion Prevention*" technology – the core technology of its flagship product, PreEmpt, has proactively blocked *thousands* of worms, viruses, trojans, and malicious spyware—*by blocking the root cause of Windows vulnerabilities*—since the technology was first released in August 2003, including *all* the fast-spreading worms that caused the most damage, such as Blaster, Sasser and MyDoom.

PreEmpt has stopped 100% of Internet Explorer command execution exploits since the software was released. Anti-virus vendors stopped less than 10%.

The Advantages of Desktop Intrusion Prevention

- Puts the benefit of a world-class security expert on every desktop
- Addresses the underlying software vulnerabilities—not each specific threat
- Protects from future threat variants without signature updates
- Minimizes the downtime and costs associated with viruses and worms
- Provides increased protection before deploying vendor patches
- Provides the ability to re-write vulnerable code as it executes in memory without making permanent changes to your systems and without adversely affecting performance.

Desktop Intrusion Prevention is a Critical Part of a Robust Security Architecture

Desktop Intrusion Prevention	Desktop Intrusion Prevention prevents attacks that reactive (signature-based) solutions can't by blocking the root cause of Windows vulnerabilities
Anti-virus	Signature-based, reactive solution. Can't block fast spreading worms like Sasser
Software Firewall	Can't block IE "Port 80" exploits, the fastest growing class of threat
Host IPS	Relies on complex rule sets. Intrusive desktop solution that still allows malware to run before blocking behaviors.

Leveling the Playing Field: Whitehats vs. Blackhats

PivX Labs monitors dozens of sources of novel security research and employs some of the best-known and most talented white-hat security researchers in the world today. They continuously research and catalog a large range of vulnerable functions across all versions of the Windows operating system and many commercial applications. More important than just finding the vulnerabilities, our research team identifies the root cause of the vulnerability and then develops the specific steps necessary to mitigate the risk associated with the vulnerability, the proof-of-concept attack code to validate the mitigation, and then deploys these steps as an automated "Fix" via our desktop and server products.

Through the combination of vulnerability-specific configuration changes, best-practice security-hardening and run-time changes to "harden" vulnerable system functions, PreEmpt effectively blocks against an extremely wide range of known and unknown remote Windows exploits.

In the short period since PreEmpt was released, it has received industry-wide accolades for its novel innovations in proactive Windows security. It has been the subject of numerous articles in the industry press and has garnered glowing praise from many of the industry's leading journalists. It was also a finalist in two categories at this year's RSA conference ("SC Magazine Global Awards") for Best Intrusion Solution and Best Network Security Solution and was named a finalist for the 2005 Datamation Product of the Year.

I have Antivirus and Firewalls. Isn't that enough?

> *The most common methods used to defend against worms today are reactive, e.g., virus- scanning, or software-patching. These mechanisms have no hope of preventing fast spreading worms, or worms that use zero-day exploits to carry out their attacks.*
> -The Case for Using Layered Defenses to Stop Worms (NSA)

Unfortunately, although many users feel they are adequately protected with current solutions, history proves they are not. The primary product categories currently used to protect Windows computers are anti-virus, software firewalls, anti-spyware and Host Intrusion-Prevention Systems (HIPS). While each of these categories contains a wide array of popular and competent solutions, there is a common weakness in all of them:

Signature-based solutions require that each new exploit must first be discovered after it is already circulating and infecting computers around the Internet, then it must be reverse-engineered and a signature developed and distributed before the application can detect and isolate it as a threat – this is a losing battle!

With the rapid mutation and self-propagation of threats such as Blaster, it is impossible to stay ahead of the flood with a *reactive* solution. In the specific case of software firewalls,

they simply cannot block attacks which look like legitimate functions on ports that are used for common network traffic, such as port 80 for web browsing.

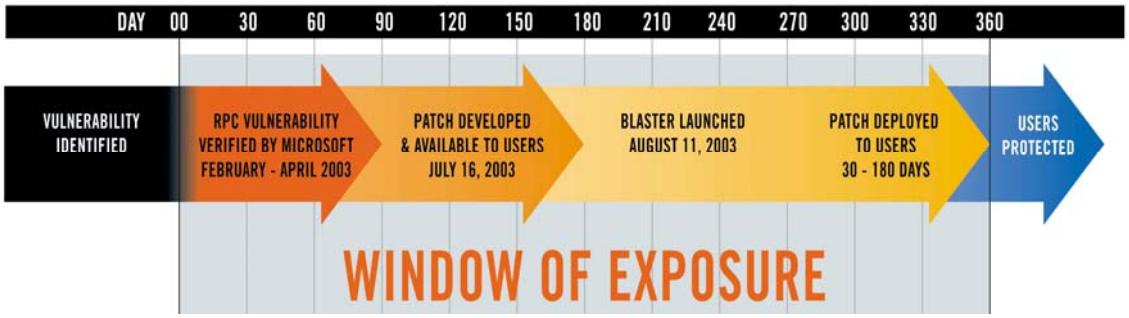
Without a powerful proactive threat mitigation solution as part of your Information Security architecture, your Windows computers are vulnerable to every new threat until a new signature is developed and deployed, or until a new patch is installed.

Blaster: A classic example of the Window of Exposure

The Blaster worm changed the security landscape forever. It was the first worm to wildly and rapidly propagate *without* user interaction, spreading across millions of unprotected hosts within *minutes* of its release into the wild. Many instances of Blaster's effect on companies were documented in the wake of its destructive path.

In an ICSA Labs survey of over 8,800 businesses released in August 2003, the Blaster worm cost medium-sized firms an average of $475,000, while larger firms reported losses of over $4 million.

If any of the firms hit by Blaster had been using PreEmpt, they would not have suffered an instant of down time, no out-of-pocket costs and no hit to their credibility. PreEmpt had a preemptive "Fix" for the vulnerability that Blaster exploited in June 2003 and was on the street defending Windows users in its first Beta release in August 2003.



Windows users were exposed to the vulnerability exploited by Blaster for 180 to 360 days.

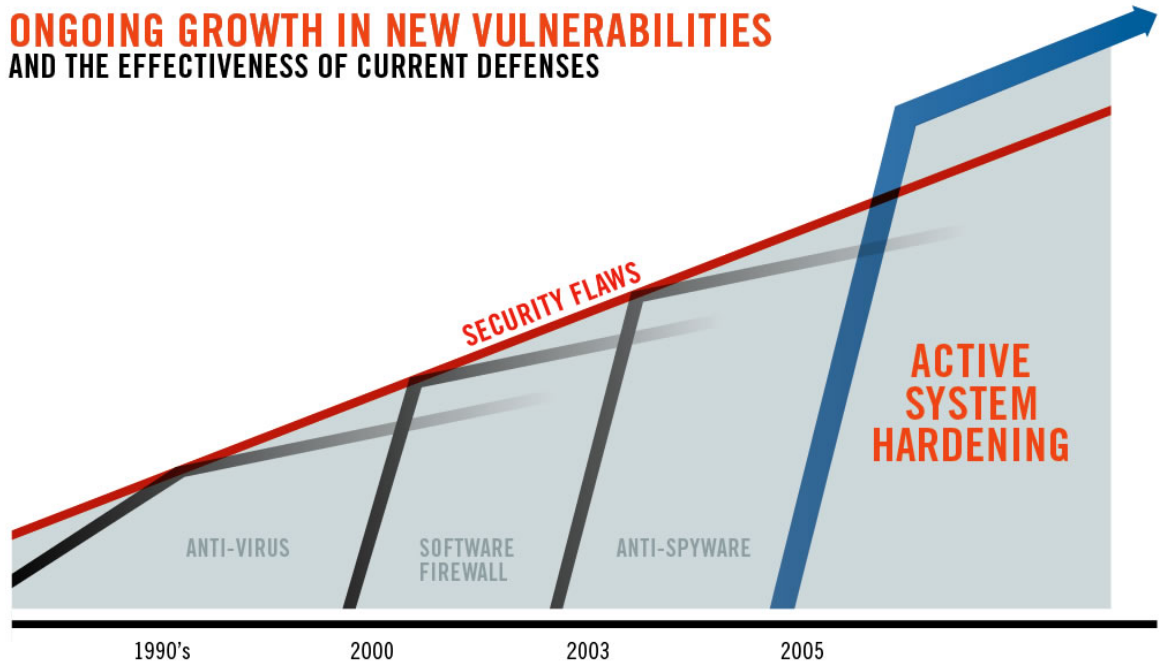
Shifting the Balance of Power

> **#1 Immutable Law of Security:**
> *If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.*

As mentioned above, malware writers are prolific, smart and motivated. They adapt and tend to follow the path of least resistance. Since many of the easiest attack pathways have been closed to them by anti-virus software and software firewalls, they are forced to find new ways to attack systems. But with the financial incentives available, new attack methods are constantly being discovered and then widely distributed.

Even the most widely-known, traditional HIPS solutions like Cisco CSA and McAfee Entercept have a fatal flaw. They rely on building a recognition model and then defeating malicious program actions *after* malware is already running on your machine. Microsoft's #1 Immutable Law of Security states that *if a bad guy can persuade you to run his program on your computer, it's not your computer anymore*. The general problem with any rules-based solution is that the bad guys know the rules too. Malware authors have become experts at modifying their actions to avoid detection. The *best* possible automated defense is to block the vulnerabilities the malware exploits to get onto your machines in the first place.

This chart provides a vulnerability timeline, illustrating that as each milestone threat event occurred, a category of response solution was developed to attempt to catch up with the threat. Many were able to briefly catch up to the existing threats. PreEmpt actually puts you ahead of the threats.



How Desktop Intrusion Prevention Works

PreEmpt is deployed as a client or agent that resides on each system being protected. The client communicates to PivX's Update Servers using standard HTTP and HTTPS protocols on regular intervals to request updates. Fixes are developed by our world-class team of security researchers and then are automatically deployed to user machines.

System protection can occur in a number of ways —

1. System Configuration Changes

The first method of Desktop Intrusion Prevention is implemented through system configuration changes in the Windows Registry. These changes are either vulnerability-specific mitigations or best-practice hardening steps. The best example of this is over *200* registry changes necessary to prevent malware from exploiting weaknesses in the Internet Explorer "My Computer" Security Zone. This one fix blocks entire classes of malware including well known recent examples such as Bizex, Bofra, Scob and ADODB.

2. Best Practice Security Measures

Experienced IT administrators implement a series of security "best practices" before exposing a computer to the Internet. This includes turning off unnecessary services and disabling functions that are known to have remotely exploitable vulnerabilities. Examples of fixes in this class include, restricting LSA anonymous sessions and disabling the "HTML Application" MIME type. By blocking access to vulnerable and rarely used Windows functionality, PreEmpt users were protected from thousands of specific threats including Sasser, download.ject plus all their many variants *without signature updates.*

3. Runtime Process Injection Framework™

The third method of system protection in production utilizes the extremely powerful PivX proprietary **Runtime Process Injection Framework**™. This technology framework allows PreEmpt to insert "hooks" into specific system or application functions to enforce input validation. In other words, if a particular function expects input to conform to a certain format, PreEmpt has the ability to block all other types of input – effectively hardening that particular function, in memory, at runtime.

This latter class of Fix is extremely effective at blocking buffer overflow exploits. Buffer overflows, by definition, rely on unexpected inputs. By ensuring that only valid inputs are passed to vulnerable functions, PreEmpt eliminates the potential for exploiting known or unknown buffer overflows with very low use of system resources.

4. Virtual Registries

The fourth method of hardening utilizes a proprietary PivX technology to provide each and every application or process on the system with its own, unique and protected virtual Windows registry. Virtual Registries allows for highly restrictive security policies to be applied to those applications that represent the greatest risk to your systems (e.g. Internet Explore) without causing the prohibitive compatibility issues that would otherwise arise

when system-wide security policies are enforced. Virtual Registries also prevent applications or malware from making unauthorized system-wide registry changes. This is a technique often employed by spyware applications to reinstall or restart themselves after

To summarize, the PreEmpt Desktop Intrusion Prevention methodology:

- "Fixes" based on advanced security research
- Repairs software flaws in memory at runtime
- Creates discrete mitigation objects
- Does not make permanent code changes
- Fixes are easily reversed
- Provides increased security for all versions of Windows
- Extensively tests for regressions against over 180 permutations of Windows and Windows applications
- Implements a scalable, secure, networked deployment and management system
- Uses standard network protocols
- Automatically deploys Fixes to the client

Enterprise Deployments & Management

PreEmpt Enterprise Edition is designed to be deployed and managed within the organization's Microsoft Active Directory infrastructure. System administrators can perform remote installations and control all aspects of the client's function across the organization. The product automatically utilizes existing enterprise web-caching servers to control the amount of traffic generated during updates from the PivX data centers. In addition, the Active Directory template allows new updates to be released first to a testing environment before system-wide deployment.

The Benefit of a Patch Without the Downtime

It's worth noting that unlike OEM software patches, the PivX approach does not make permanent code changes and hence greatly simplifies application compatibility testing and system downtime. For example, if a new Fix is found to adversely affect an enterprise application, it can be turned off, instantly restoring the application's function.

Conclusion: Business Need and Business Value

The threats are real, the loss and exposure to businesses is real and not getting any better. Hossein Eslambolchi, CTO of AT&T Labs recently warned of security problems of "biblical proportions" unless more is done to improve the quality of software code. As shown in this paper, the historical cost of dealing with compromised systems is high and the financial and regulatory motivations for mitigating these IT security risks are growing each day.

At PivX, we are dedicated to improving the security of the software your organization has come to rely upon. Our number one goal is to seek out and stop the vulnerabilities that exist today – to stop the threats of tomorrow before they cause damage. We have a proven track record of success and a technology framework that puts the benefits of a world-class security researcher in each and every one of your Windows-based systems.