September 25, 2005

PivX Solutions, Inc.
Reducing the Windows of Exposure Through Defense in Depth

WHITE PAPER

>pivx_

Overview

Reactive security solutions, which include anti-virus software, are no longer sufficient to protect networked computers from today's fast-spreading worms and viruses. PreEmpt 2.0™ offers next generation Desktop Intrusion Prevention that blocks most worms, viruses, and other malware from infecting Microsoft® Windows® based desktops and servers. PreEmpt 2.0 works by blocking the root causes of Windows vulnerabilities before they can be exploited by malicious code writers. For instance, PreEmpt 2.0 users were automatically protected ahead of time from all the worms that made headlines in the last few years , including MSBlaster, Bizex, and more recently, Sasser, and all its' variants.

To achieve this new level of protection, PreEmpt 2.0 relies on the extensive security research performed by PivX Solutions and its global network of world-renowned security researchers. Companies around the world, including Microsoft, Boeing, Sony and GMAC, rely on PivX Solutions to ensure that their networks and desktops are secure. World-renowned for its unique and detailed security research, PivX Solutions continually analyzes vulnerabilities in Microsoft Windows, as well as the spread and infection vectors of specific threats such as viruses and worms.

A New Approach Is Needed

Businesses rely on the Internet. Yet the same Internet that provides instant communication with customers, vendors, and employees also exposes your private network and computers to a continuous and ever-growing stream of threats to your privacy and business-critical information.

Anti-Virus software and other reactive, signature-based security solutions can only protect you once a particular instance of a threat has been identified on the Internet and analyzed, typically hours after the worm or virus began attacking and propagating. That model worked great when malicious code spread relatively slowly. A few systems would get infected, but the vast majority would be protected when their Anti-Virus software downloaded the "signature" of that new threat.

Today's fast-spreading worms and viruses can infect every vulnerable machine on the Internet within *minutes*. Some worms shut themselves down long before the Anti-Virus vendors have even had a chance to analyze how they spread. Many of those leave thousands of Trojans in their wake. PreEmpt 2.0 protects against a wide range of threats by blocking entire classes of vulnerabilities. This solution guards you against threats to your systems long before Anti-Virus or other reactive solution providers have even named the latest threat, let alone determined how to protect against it or released updated signature files to trap it.

To illustrate this point, we need to look no further than the recent outbreaks of viruses and worms such as **MS Blaster, Bagle, soBigF, My Doom, Netsky, and Sasser**. In February 2004, the **W32.Bizex** worm infected 50,000 machines in less than three hours. Yet, before Anti-Virus vendors could update Anti-Virus signatures, the worm had already stopped its spread. At this point, the damage had already been done. While Anti-Virus products now protect against Bizex, PreEmpt 2.0, by blocking the underlying vulnerability exploited by Bizex, offered superior protection more than four months before this specific worm had even been released.

PreEmpt 2.0 offers superior preemptive protection over existing solutions because it does not rely on virus signatures or exploit traffic fingerprints to detect and mitigate threats. Instead, PreEmpt 2.0 uniquely targets the underlying weaknesses responsible for the vulnerabilities that attackers rely upon. PreEmpt 2.0 does not have to be updated every time a new virus or worm is discovered, so it avoids the current ‘beat the clock’ scenario where the vendors of security products rush to develop and distribute updates to protect their customers after the fact. Instead, PivX Solutions focuses its efforts on proactively analyzing the root cause of classes of vulnerabilities and attack vectors while vendors of reactive solutions scramble to keep up.

PreEmpt 2.0 doesn’t change existing files or introduce new functionality, nor does it require the complex policy definitions or extensive profiling of traditional Desktop Intrusion Prevention (HIP) systems. System modifications introduced by PreEmpt 2.0 are always performed at run-time and each fix is completely reversible. PreEmpt 2.0 is updated regularly as new attack vectors are analyzed and fixes are developed. In most cases, PreEmpt 2.0 is configured to automatically deploy fixes. However, the PreEmpt 2.0 management console allows you to define update and deployment policies to suit your organization’s security policies.

PreEmpt 2.0 does not replace traditional *patch* management. Instead, PreEmpt 2.0 strengthens your security by reducing your “Window of Exposure” to known and unknown threats. With PreEmpt 2.0 in place, IT organizations have the time to properly test and deploy vendor patches knowing that they’re still protected from the underlying vulnerabilities. Further, if regression testing shows that a vendor patch introduces new problems or causes conflicts with business critical applications, they can decide to delay loading the patch, confident that their systems are already protected.

This added measure is crucial to overall security, as the current approach to patch management has well-understood problems. As reported in CNET,

> “Top security officers have warned that patching software flaws is still far too difficult, with many companies left vulnerable because they are lagging behind on applying critical updates. Vulnerability assessment firm Qualys supported the statements with data culled from monitoring its clients’ networks. The data, collected over two years, shows that it takes a month to cut by half the number of vulnerable computers connected to the Internet.”

“What the data is telling us today is that we have a cycle of fixing vulnerabilities . . .that leaves us open to significant exposure,” said Gerhard Eschelbeck, CTO of Qualys. “The large number of systems vulnerable to last winter’s Slammer worm, which took advantage of a six-month-old flaw, underscores the issue, as does the MSBlaster epidemic last August,” reports CNET.

In summary, PreEmpt 2.0 provides a critical additional layer of defense to existing security measures such as Anti-Virus Software, Firewalls, Intrusion Detection Systems, and Patch Management Solutions. Qwik Fix Pro offers next generation Desktop Intrusion Prevention by blocking the root causes of worms, viruses, and malware, not just their symptoms, in all versions of Microsoft Windows. By blocking the underlying vulnerabilities, PreEmpt 2.0 protects against so-called “Zero Day” vulnerabilities, providing revolutionary new protection to your desktop PCs, servers, and network.

Qualifications

PivX Solutions and its security researchers are experts in the security of multiple operating systems and Internet browsers. Our researchers have located numerous critical vulnerabilities in the most widely used applications and are thought leaders in the Cyber Security industry.

PivX Accomplishments

Industry-Leading Security Research

- Located *hundreds* of Critical Vulnerabilities in Microsoft Windows and Internet Explorer as well as in Outlook, AIM, ISS, Apache, SQL, and ISA Server and numerous other desktop and server applications

Public Information Sharing

- Frequent contributors to BugTraq, Dshield, NTBugtraq, VulnWatch, and Full-Disclosure Mailing Lists
- Creator of the now infamous, 'Unpatched Vulnerability' page that has been transitioned to the 'Unpatched Mailing List'

Recognized Experts in Vulnerability Assessment and Mitigation

- Expert source for security and vulnerability related reports in the 300+ publications in the IDG Network, the CMP network as well as the CNET and ZDNet media networks
- Frequent contributor to Security Industry Panels
- Partner with Institute for the Critical Information Infrastructure Protection
- Participated in the Software Development Task Force at the prestigious invitation-only 1st National Cyber Security Summit sponsored by DHS, BSA, TechNet, the US Chamber of Commerce, and ITAA
- Co-Chaired two sub groups of the Department of Homeland Security's Software Development Lifecycle Security Task Force

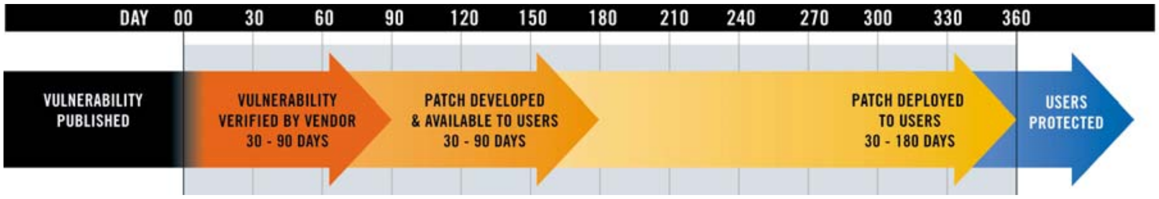
Vendor Patch Management – Window of Exposure

What is the **‘Window of Exposure’**?

The Window of Exposure is the period of time during which you are vulnerable to a threat and have not yet implemented countermeasures to mitigate that threat.

Traditional Timeline Without PreEmpt 2.0

In the ideal scenario, a security researcher discovers a vulnerability and works responsibly and discreetly with the vendor, informing them through a back channel, providing time for the vendor to develop a patch. The public is only made aware of the vulnerability once the patch has been made available. In this scenario the Window of Exposure is decreased to a 30-90 day timeframe. However, more often the public is made aware of a new vulnerability long before anyone has had a chance to develop and test a permanent patch. This not only puts extra pressure on the vendor to rapidly create and test a patch, but as we’ve illustrated below, it also impacts users through an expanded Window of Exposure.


DAY
00
30
60
90
120
150
180
210
240
270
300
330
360
VULNERABILITY PUBLISHED
VULNERABILITY VERIFIED BY VENDOR 30 - 90 DAYS
PATCH DEVELOPED & AVAILABLE TO USERS 30 - 90 DAYS
PATCH DEPLOYED TO USERS 30 - 180 DAYS
USERS PROTECTED

A typical threat scenario in today’s world consists of a series of steps, each of which takes up some period of time. These include:

Vulnerability Published, **Day 1**

- A vulnerability is published on a mailing list or IRC (Internet Relay Chat), or recognized by an independent security researcher. On an average day, as many as a dozen potential vulnerabilities can be released.

Vendor Acknowledgment, **Day 14-60**

- The vendor researches and acknowledges the vulnerability. At this point, they start creating a patch. This typically happens no less than 14 to 60 days after the vulnerability has been published publicly.

Vendor Testing, **Day 30-90**

- The vendor performs regression testing on the patch. This important step has become much more critical over the last few years as many vendor-supplied patches have been rushed out before sufficient regression testing was completed. The net result is that although many patches have successfully eliminated a particular vulnerability, they have often caused stability problems, and some have even introduced *new* vulnerabilities in the process. Many system administrators have become reluctant to install patches because of their experience with regression defects. As a result of these defects, testing can contribute significantly to the length of the Window of Exposure.

Patch Availability, **Day 60-180**

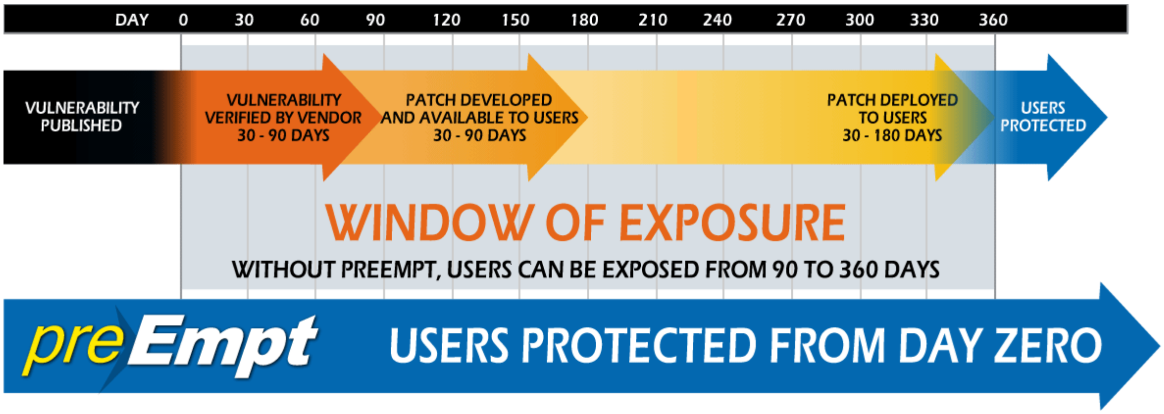
- The vendor has finished testing the patch and publishes it. This typically happens 30 to 120 days after the vendor has acknowledged the threat. In the case of the recently deployed ASN.1 patch, the period between discovery of the vulnerability and the availability of a patch was *200* days.

Patch Deployment, **Day 90-270**

- The patch becomes widely deployed. This typically happens 30 to 90 days after the vendor has made the patch available.

Timeline with PreEmpt 2.0 Installed

With PreEmpt 2.0, the Window of Exposure is significantly reduced or even eliminated. Some of the same steps exist as before, but the timeframes have changed and the focus on the Window of Exposure is removed. The new Window of Exposure consists of the following:


DAY
0
30
60
90
120
150
180
210
240
270
300
330
360
VULNERABILITY PUBLISHED
VULNERABILITY VERIFIED BY VENDOR 30 - 90 DAYS
PATCH DEVELOPED AND AVAILABLE TO USERS 30 - 90 DAYS
PATCH DEPLOYED TO USERS 30 - 180 DAYS
USERS PROTECTED
WINDOW OF EXPOSURE
WITHOUT PREEMPT, USERS CAN BE EXPOSED FROM 90 TO 360 DAYS
preEmpt
USERS PROTECTED FROM DAY ZERO

Fix Published, **Months before Day Zero**

- PivX Solutions analyzes a new attack vector and creates a fix that mitigates the root cause of the threat posed by a class of vulnerabilities. It automatically distributes this fix to PreEmpt 2.0 users.

Vulnerability Published, **Day 1**

- A specific vulnerability is identified and published.

Vendor Acknowledgment, **Day 14-60**

- The vendor acknowledges the vulnerability and starts to create a patch. This typically happens 14 to 60 days after the threat has been published.

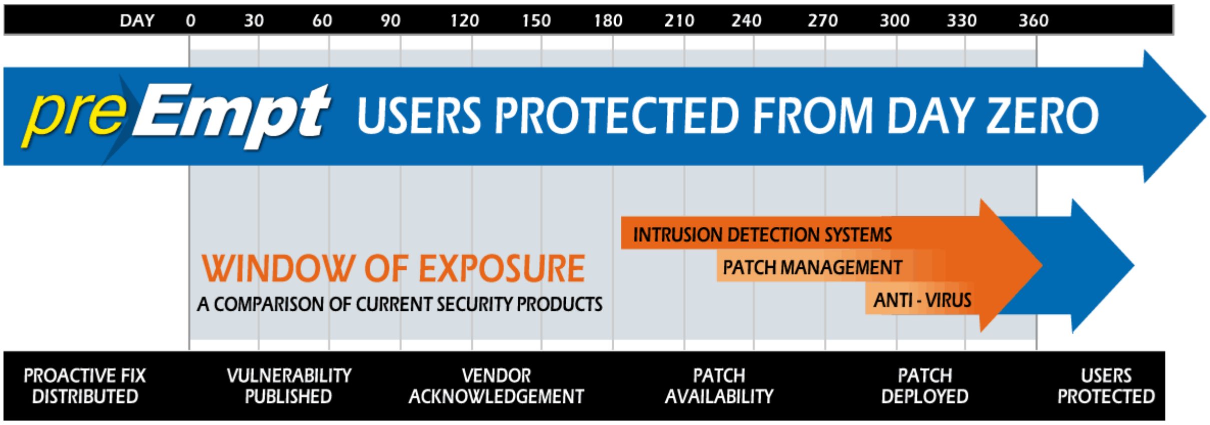
Patch Availability and Deployment, **Day 60-270**

- The vendor publishes a patch. With PreEmpt 2.0 you're already protected. You have time to perform proper testing of the patch to ensure that it doesn't cause additional problems or conflict with business critical applications and then deploy the patch at a convenient time.

In this scenario, PreEmpt 2.0 has taken some of the pressure off of the vendor's shoulders as they can now thoroughly test and refine the patch for regression defects, knowing that their customers have a threat mitigation solution in place. When users decide to install the patch they have increased confidence that it will be trustworthy, even before they test it themselves. Everybody wins … except the bad guys.

Timeline Comparisons

To further demonstrate how PreEmpt 2.0 reduces your Window of Exposure, compare at what point during the Window of Exposure current security products start to secure your Windows systems:



- **Anti-Virus** applications require an active threat to be released before new signatures can be created. You aren't protected at all against fast-spreading worms. Slightly modified version of existing viruses require new signature files reopening the Window of Exposure

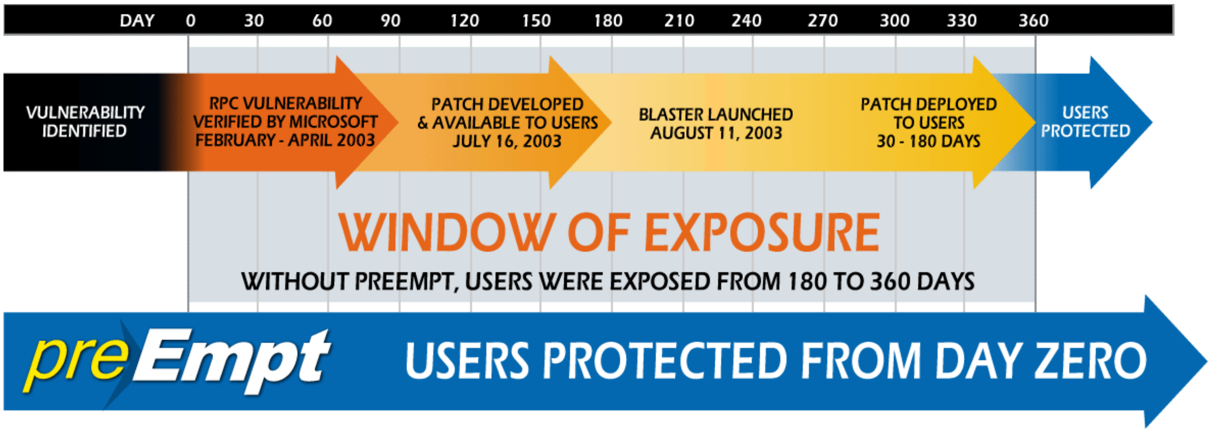
- **Patch Management** applications require the vendor to develop, test, and release a patch before it can be used to secure your network. Even then, you are left with the burden of testing the patch on your network since it introduces a permanent functionality change that could have 'unadvertised' and unexpected effects.

- **Intrusion Detection Systems** require that an exploit for a vulnerability be identified before network traffic can be logged, analyzed, and used to generate signatures for the exploit. Behavioral systems may or may not identify and block the exploit until your systems have already been infected.

These solutions do a good job of protecting you from vulnerabilities once specific threats have been discovered. However, none of these solutions works to protect you from the threat posed by those vulnerabilities *in advance*. In contrast, PreEmpt 2.0 secures your Microsoft Windows systems from entire classes of threats, not just specific vulnerabilities. That is how PreEmpt 2.0 reduces your Window of Exposure**.**

A Real-World Example Of The Window Of Exposure: MSBlaster

This example of the Window of Exposure is validated by real-world experience, as illustrated by reviewing the actual steps that led to the release of the MSBlaster Worm in August of 2003:


DAY 0 30 60 90 120 150 180 210 240 270 300 330 360
VULNERABILITY IDENTIFIED
RPC VULNERABILITY VERIFIED BY MICROSOFT FEBRUARY - APRIL 2003
PATCH DEVELOPED & AVAILABLE TO USERS JULY 16, 2003
BLASTER LAUNCHED AUGUST 11, 2003
PATCH DEPLOYED TO USERS 30 - 180 DAYS
USERS PROTECTED
WINDOW OF EXPOSURE
WITHOUT PREEMPT, USERS WERE EXPOSED FROM 180 TO 360 DAYS
preEmpt
USERS PROTECTED FROM DAY ZERO

December 2002, Day -210

- PivX researchers identify a vulnerability in RPC DCOM as a security hole that future malware writers could exploit to compromise a machine. PreEmpt 2.0 is updated to block the vulnerability. PreEmpt 2.0 users are protected.

February 2003, Day -150

- Microsoft begins work on the RPC DCOM vulnerability.

July 16, 2003, Day 0

- Microsoft acknowledges the vulnerability and releases a patch.

August 1, 2003, Day 16

- PivX warns of an exploit to the RPC DCOM vulnerability in an eWeek article entitled, “Crackers Tuning Up For Massive Net Attack.”
- Thor Larholm, Senior Security Researcher at PivX warned in a post to BugTraq that machines that had loaded Microsoft’s official patch were still vulnerable to Denial of Service (DoS) attacks against the same flaw.

August 11, 2003, Day 26

- MS Blaster is launched and it hits the Internet with a vengeance, exploiting a flaw within Microsoft Windows’ Remote Procedure Call (RPC) process, enabling the attacker to gain full access to the system.
- Windows NT, Windows 2000 and Windows XP machines were all affected.

September 20, 2003, Day 66

- Microsoft issues a revised patch that corrects the flaw in the original patch that allowed the DoS attack to happen.

- Even with the revised Microsoft patch, deployment of the patch has been slow, with 30% of attacks in the last half of 2003 having been caused by the MSBlaster worm (Internet Security Threat Report, March 2004).

PreEmpt 2.0 users were protected before Microsoft even publicly acknowledged the RPC DCOM vulnerability. PivX security researchers identified the root cause of what would subsequently be publicized as a specific vulnerability. By blocking the root cause rather than the symptoms, PreEmpt 2.0 users were unaffected by the MSBlaster worm that appeared 8 months *after* PivX issued the fix in PreEmpt 2.0.

Fixes

The fixes that are distributed through PreEmpt 2.0 are the essence of the solution. These are the targeted counteractions that PivX Solutions has produced as a result of its extensive security research and its renowned domain knowledge. Each fix is designed to mitigate the impact of a vulnerability or class of vulnerabilities by targeting its attack, spread, and infection vectors.

Below are descriptions of several Fixes. The complete list of security fixes applied by PreEmpt 2.0 will change over time as new vulnerabilities are discovered and new Fixes are distributed to block those vulnerabilities. The complete list of current Fixes can be viewed within the PreEmpt 2.0 control panel. All Fixes are enabled by default in order to provide maximum protection, however each individual PreEmpt 2.0 can be disabled if desired.

Example Fixes:

Secure the IE My Computer Zone

- Many viruses and worms are able to trick Internet Explorer into running code within the My Computer zone. A malicious program running within the My Computer zone has full system privileges. Securing the IE My Computer zone protects against many common types of attacks.

Disable Dangerous URL Protocols

- Internet Explorer has the capability to run many types of potentially dangerous files. This PreEmpt 2.0 disables this common attack vector.

Restrict LSA Anonymous Sessions

- This PreEmpt 2.0 restricts Local System Account anonymous (or null) sessions. LSA anonymous sessions are inherently insecure and utilized by many worms and viruses to gain elevated privileges.

Disable the Messenger Service

- The Windows Messenger service (not the same as Instant Messaging) is rarely used but is a frequent target of worms, viruses, and other malware. PreEmpt 2.0 disables this service.

How is a PivX Qwik-Fix different from a permanent or ‘virtual’ patch, an IDS rule or an Anti-Virus signature? There are a number of important differences:

1. Each Qwik-Fix is reversible. Any action that the fix performs on your Windows system can be reversed with a simple click of a checkbox.
2. Each fix is self-contained. Included within the fix package are all the files needed to install and remove each Qwik-Fix.
3. No fix ever changes any existing files or introduces any new functionality. Any modifications to applications that are needed to protect your systems are always performed at runtime without introducing permanent changes.

Distribution of Fixes

PreEmpt 2.0™ is an agent-based application. This means that each of the workstations or servers you want to protect needs to have the PreEmpt 2.0 Client™ installed, not unlike your Anti-Virus solutions. On a pre-scheduled basis, the PreEmpt 2.0 Client queries an update server to determine whether there are any available fixes, modified fixes or updates to the PreEmpt 2.0 Client components.

The request from the PreEmpt 2.0 client to the PreEmpt 2.0 Update Server™ contains details about a number of items related to the Windows installation, including:

- Licensing information
- Software version of PreEmpt 2.0
- Details about the Windows operating system configuration
- Details about related third-party applications

These details are required to secure your Microsoft Windows systems by accommodating custom responses according to the software installed on that specific machine. Some of the fixes that PivX Solutions develops are targeted at different Windows versions (Windows 95 – XP) or different third party applications. By delivering just the fixes that your specific Windows system needs, we ensure the least possible impact on your working environment with the highest possible degree of protection.

All communication between the PreEmpt 2.0 Client and the PreEmpt 2.0 Update Server is based on open and interoperable standards. The data is encoded as XML and encrypted, then transmitted using the HTTP protocol over port 443 to accommodate corporate firewalls and ease of administration. If your Windows system can surf the web, it can retrieve fixes from the PreEmpt 2.0 Update Server.

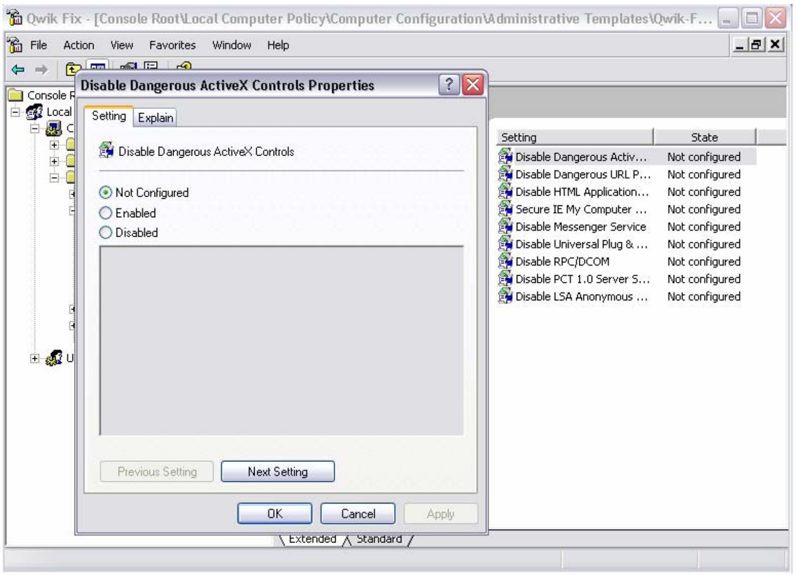
All communication between the PreEmpt 2.0 client and the PreEmpt 2.0 Update Server is encrypted to protect your privacy and avoid any possible man-in-the-middle attacks. Further, a secure checksum is distributed for each available fix or component.

Once the PreEmpt 2.0 Client has received a list of available fixes and components, it retrieves these from a PreEmpt 2.0 Download™ server. This download server is more often than not the same as the update server, but can be kept logically and physically distinct, as desired.

All fixes downloaded from the PreEmpt 2.0 Update server are cryptographically signed by PivX Solutions to ensure your safety. Only fixes and components that are verified to originate from PivX Solutions will be applied.

Enterprise Management

PreEmpt 2.0 used Microsoft Active Directory for deploying and managing the PreEmpt 2.0 client across a corporate network. The PreEmpt 2.0 Management Console enables an IT administrator to define group policies, manage installation of new Fixes, view reports of client usage and availability, and diagnose communication or other problems.



Qwik Fix - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Qwik-F...

Disable Dangerous ActiveX Controls Properties

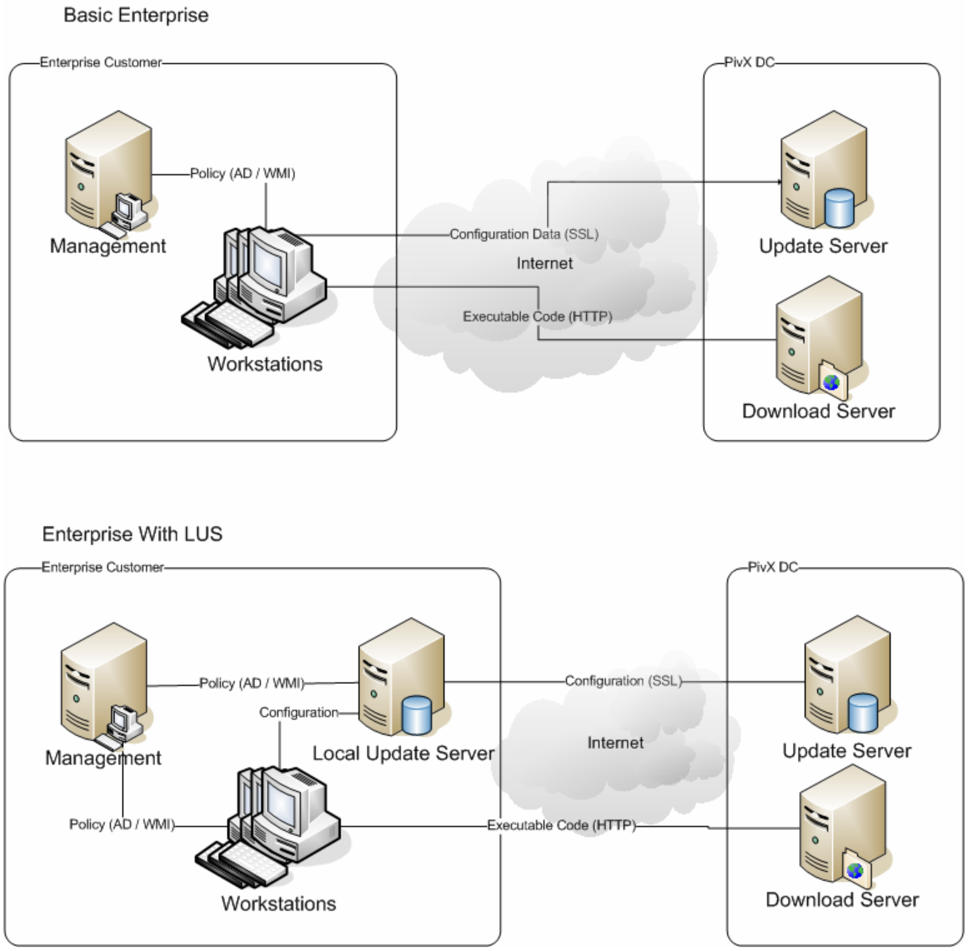
Disable Dangerous ActiveX Controls

● Not Configured
○ Enabled
○ Disabled

Setting	State
Disable Dangerous Activ...	Not configured
Disable Dangerous URL P...	Not configured
Disable HTML Application...	Not configured
Secure IE My Computer ...	Not configured
Disable Messenger Service	Not configured
Disable Universal Plug & ...	Not configured
Disable RPC/DCOM	Not configured
Disable PCT 1.0 Server S...	Not configured
Disable LSA Anonymous ...	Not configured

When using Windows 2000 and later versions, preEmpt options are displayed directly in the MMC explorer and list windows. The configuration displayed demonstrates how specific Fixes can be enabled or disabled on a user computer. Group policies controlled from the Management Console allow IT administrators to determine how much control local users have over PreEmpt 2.0 on their computer. For instance, developers can be granted the rights to disable certain Fixes or even to disable PreEmpt 2.0 entirely. Specific personnel can be restricted from disabling some or all Fixes or even be aware that PreEmpt 2.0 is running on their PC. Every feature of PreEmpt 2.0 can be managed and controlled from a central location using the Management Console.

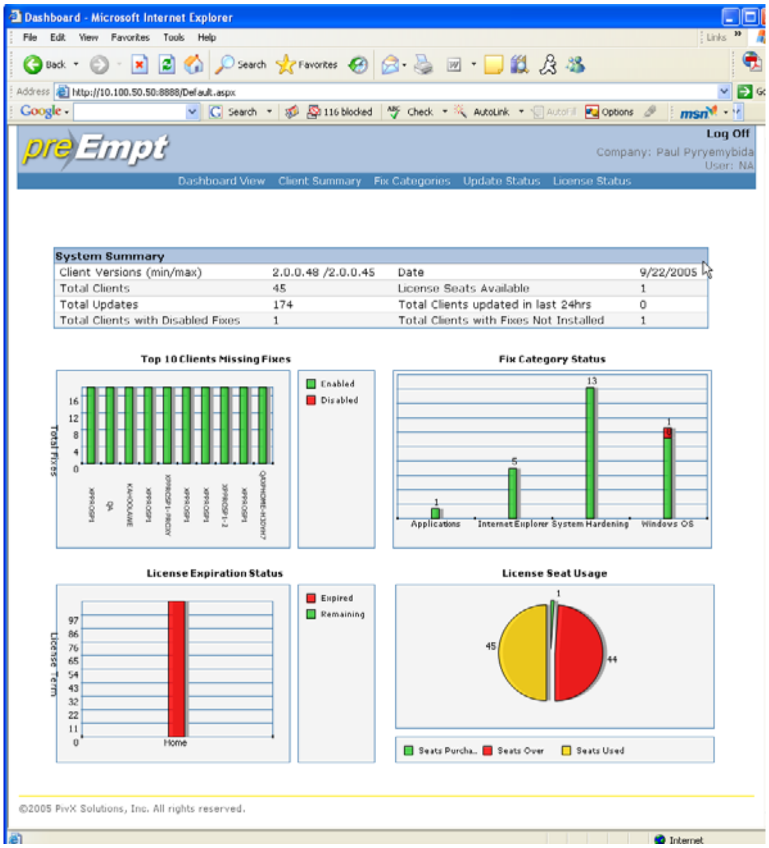
Securing the Enterprise Desktop



These diagrams demonstrate the two primary Fix updating mechanisms used by preEmpt 2.0. Enterprises can either update their desktops from the PivX update servers, or from a locally deployed update server (LUS). Either option provides the same military grade encryption and assurance that all Fixes and program updates are direct from PivX.

Enterprises have the option of deploying a Local Update Server to support updating of desktops from within their own networks and not using public internet secure broadcasts to perform fix and application updates.

Reporting



System Summary			
Client Versions (min/max)	2.0.0.48 /2.0.0.45	Date	9/22/2005
Total Clients	45	License Seats Available	1
Total Updates	174	Total Clients updated in last 24hrs	0
Total Clients with Disabled Fixes	1	Total Clients with Fixes Not Installed	1

©2005 PivX Solutions, Inc. All rights reserved.

The reporting options allow the Enterprise user to view summarized and detailed views of each deployed desktop and the associated Fixes. When new threats are released in the wild, administrators can review the fix associated with the threat and verify that each desktop is protected. Reports also can be used for compliance reporting to validate the protection status and historical updates for each desktop.

Summary

Worms, viruses, and malevolent code are increasing in their introduction, speed, sophistication, and success. 2003 was a record year for worms and viruses, according to Computer Economics, with total reported damage exceeding $100 billion. In 2003, we saw Slammer, MS Blaster, and Sobig.f, which according to John Chambers, CEO of Cisco, propagated so fast that it touched 150 million computers in less than three minutes. So far in 2004 we have already seen MyDoom A, B and C, DoomJuice, Bagle and Its 20 variants, and the May 1, 2004 release of the Sasser worm and it variants, ***all* of which were blocked by PreEmpt 2.0 in advance.** The bottom line is that current *reactive* security solutions are not sufficient to protect desktops by themselves. Clearly a *Proactive* Threat Mitigation solution is needed as well.

Proactive Philosophy in Practice

In this White Paper, we have highlighted the benefits that a truly proactive solution such as PreEmpt 2.0 provides. However theory is one thing, practice is another – and PivX Solutions has successfully proved our theory and philosophy about Proactive Threat Mitigation in the real world.

In Q3 2003, we released a public BETA version of PreEmpt 2.0 that was designed to validate the philosophies and proprietary methodologies of Proactive Threat Mitigation. This public BETA version included just a few of the myriad proactive fixes that we are developing. Even with a limited number of Fixes included as part of the BETA test, PreEmpt 2.0 was able to proactively protect our 200,000+ BETA users from several dozen unknown vulnerabilities, worms, and exploits.

Some of the more noticeable threats that the BETA version of PreEmpt 2.0tected against include, but are not limited to:

Mydoom (IFRAME Variant)
Bofra
Bobax
Korgo
Sasser
MSBlaster
Bizex
MiMail
SoBig
Scob
Download.ject
Welchia
Nachi
Scane
Multex
SDBot variants
Gaobot variants
Trunlow
Psyme
AIM buffer overflow
Downloader.Botten
VBS.Cuerpo.A@mm
Exploit-ByteVerify
VBS.Laske@mm

W32.Dinfor.Worm
VBS.Seeker.F
Blaster.K / LoveSan
ADODB.Stream
MS JVM class loader
ICQ SCM local file planting
Shell: Folders
MhtmlRedirLaunchExe
MhtmlRedirParsesLocalFileLocal
ZoneInCache
1stCleanRc
MHT attacks
execdror6HTML Application
exploits
Ibiza CHM execution
BackToFramedJPU
XP Self-Executing Folders
Shell.Application
showHelp CHM
DoubleSlash zone bypass
LinKillerSaveRef
NAFfileJPU
NAFjpuInHistory
PoisonousSTYLEforDialog

RefBack
SaveRef
SaveRef_DocumentWrite
visSWFurl
WsBASEjpu
WsFakeSrc
WsOpenFileJPU
execdror5
DblSlashForCache
XMLObject zone bypass
AutoScanJPU
BackMyParent
BadParent
BodyRefreshLoadsCPU
Findeath
HijackClick
Linkiller
LinkillerJPU
IredirNrefresh
VBS.Redlof
I-Worm.Lentin
Yaha
I-Worm.Fintas
I-Worm.GOPWorm

Goner
Scalper
Swen
I-Worm.Sysnom
I-Worm.Updater
I-Worm.Valcard
I-Worm.Welyah
I-Worm.Zoher
MSN-Jitux
Worm.P2P.Surnova
Worm.Sadmind
WinHLP.Pluma
HTML.NoWarn
VBS.Redl

For more information regarding PreEmpt 2.0 you can visit:
http://www.pivx.com

For enterprise licensing information, please email PivX at:
sales@pivx.com