



**Qwik-Fix Pro™
Technical Whitepaper
March 2, 2004**

Author: Thor Larholm, Senior Security Researcher

Table of Contents

Preface	3
Qualifications.....	5
Window of Exposure	5
Traditional timeline without Qwik-Fix Pro	5
Timeline with Qwik-Fix Pro installed.....	7
Timeline comparisons	9
Distribution of fixes	10
Enterprise management	11
Fixes	13
Cost Savings and Advantages.....	13
Summary Conclusion.....	14
Proactive Philosophy in Practice	14

Preface

Qwik-Fix Pro™ is a new desktop security application in a category that we have labeled Proactive Threat Mitigation. Realizing that the threats of today and tomorrow have a continually growing impact and are propagating and spreading at an ever increasing rate, Qwik-Fix Pro works to proactively protect against threats to the Microsoft Windows platform before they are discovered and well before malicious code writers have a chance to develop exploits to compromise hosts that are vulnerable.

To accomplish this goal, Qwik-Fix Pro relies on the extensive security research performed by PivX Solutions and its global network of security research experts. World renowned for its unique and detailed security research, PivX Solutions continually analyzes myriad vulnerabilities, as well as the spread and infection vectors of threats such as viruses and worms. The result of this extensive research is a number of targeted counteractions that are distributed as fixes to our users through Qwik-Fix Pro. PivX Solutions continuously revises and hardens these fixes to ensure maximum protection for Qwik-Fix Pro users.

How does Qwik-Fix Pro complement patch management, Anti-Virus or “virtual patches”?

To put it simply, Qwik-Fix Pro works proactively before an incident occurs, while other desktop security solutions work reactively once a particular instance of a threat has been identified in the wild and analyzed, typically hours after the exploit is attacking and propagating. By mitigating the possible impact of a wide range of threats, Qwik-Fix Pro works to guard you against threats to your systems long before other solution providers have even named the threat, let alone determined how to protect against it.

For evidence that the current reactive security methodologies are not adequate in protecting customers one need look no further than the recent outbreaks of viruses and worms such as MS Blaster, Bagle, soBigF, My Doom, and DoomJuice. As recently as February 24th, the W32.Bizex worm infected 50,000 machines in less than 3 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, Qwik-Fix offered superior protection four months before the worm had even been released.

Qwik-Fix Pro offers superior protection over existing solutions because it does not rely on virus signatures or exploit traffic fingerprints to detect a threat. Instead, Qwik-Fix Pro uniquely targets the underlying weaknesses that are responsible for the vulnerabilities that attackers rely on. Since Qwik-Fix Pro does not have to be constantly updated as new vulnerabilities are discovered, it avoids the current ‘beat the clock’ scenario where the vendors of security products rush out updates to protect their customers after the fact. Instead, PivX Solutions focuses its efforts on proactively analyzing entire new categories of vulnerabilities and attack vectors while vendors of reactive solutions scramble to keep up.

No fix that Qwik-Fix Pro delivers to your Windows systems will change existing files or introduce new functionality. System modifications that are needed to protect you are always performed at run-time and do not introduce permanent changes because every fix that is deployed through Qwik-Fix Pro is reversible. So you can stop conducting regression tests and worrying whether your business applications will stop working, and instead deploy fixes immediately with no risk so your Windows systems are secured as soon as possible and your 'Window of Exposure' is reduced. In fact, we recommend most of our users configure Qwik-Fix Pro to automatically deploy fixes, however, with our management console you are able to define update and deployment policies to meet your organization's needs.

Traditional patch management is not made obsolete by introducing Qwik-Fix Pro into the equation. Instead, Qwik-Fix Pro strengthens your security by helping to reduce your Window of Exposure, offering proactive solutions that protect against threats in advance as well as rapid deployment of updated fixes as new attack vectors are identified.

This added measure is crucial to overall security, as the current patch management approach is fatally flawed. As reported in CNET on 02/25/04, "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 MSBlast epidemic last August" reports CNET.

Qwik-Fix Pro provides the perfect complement to existing security measures that one should have in place such as Anti-Virus Software, Intrusion Detection Systems, Firewalls and Patch Management Solutions. A proactive solution such as Qwik-Fix Pro can reduce the impact of attacks against your Windows systems regardless of the route they take to get there, in contrast to existing Anti-Virus and IDS solutions that react to a particular vulnerability only after an exploit targeted against it has been identified in the wild. Since Qwik-Fix Pro protects against many threats before they are discovered, you can safely deploy patches once they have been tested to your satisfaction, as opposed to the current "rush to patch" scenario. Meanwhile PivX and Qwik-Fix Pro security researchers will be researching new attack vectors and exploit pathways, to help you stay several steps ahead of the bad guys, and continue to reduce your "Window of Exposure".

Qualifications

PivX Solutions and its security researchers are experts in the security of a breadth of operating systems and browsers. Our researchers have located numerous critical vulnerabilities in the most widely-used applications and are thought leaders in the Cyber Security industry. Our accomplishments include:

- Located 100's of Critical Vulnerabilities in Internet Explorer and Windows as well as in Outlook, AIM, ISS, Apache, SQL and ISA Server
- 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'
- 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 Prevention
- 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-Chairing two sub groups of the Department of Homeland Security's Software Development Lifecycle Security Task Force
- Taught Cyber Security and Threat Prevention Classes at the University of California
- Located root vulnerabilities in Apache Server
- Located DSL router's administrative privileges vulnerability
- Located critical vulnerabilities in Turbo Tax and Tax Cut Pro

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 that mitigate it.

Traditional timeline without Qwik-Fix Pro

To clarify how Qwik-Fix Pro complements current security solutions, we would like to highlight how it changes the **Window of Exposure**.

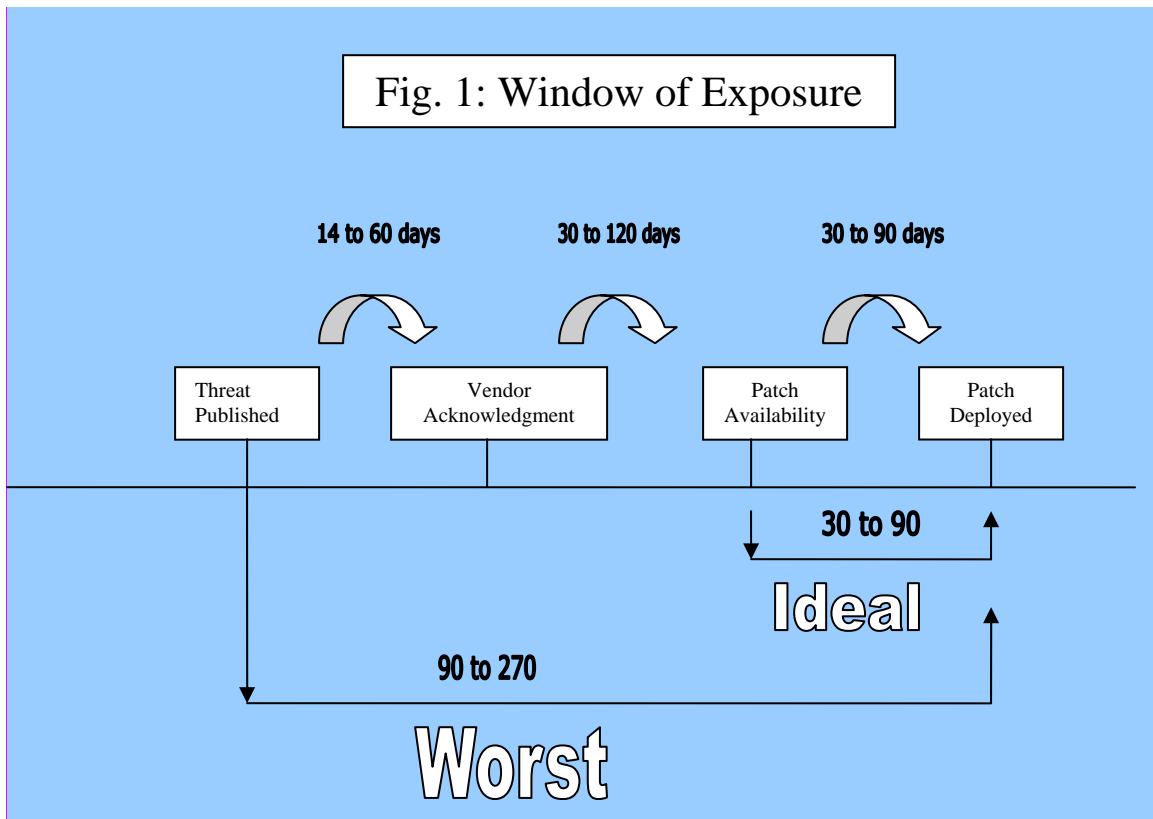
A typical threat scenario in today's world consists of a series of steps, each of which takes up some period of time. These include:

- **Vulnerability Published, Day 1**
 - A vulnerability is published on a mailing list or IRC, 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 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.

In the ideal scenario, a security researcher who discovers a vulnerability works responsibly and discreetly with the vendor, informing them through a back channel, and the public is only made aware of the vulnerability once a patch has been made available. In this scenario the **Window of Exposure** is decreased to a 30-90 day time frame. 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 above, it also impacts users through an expanded **Window of Exposure**.

We have established two separate scenarios with different timeframes for **Window of Exposure**. One is an ideal scenario with a timeframe of anywhere between 30 and 90 days, and the second, more common scenario, has a worst-case timeframe of anywhere between 90 and 270 days.

These scenarios are illustrated in Figure 1 below.



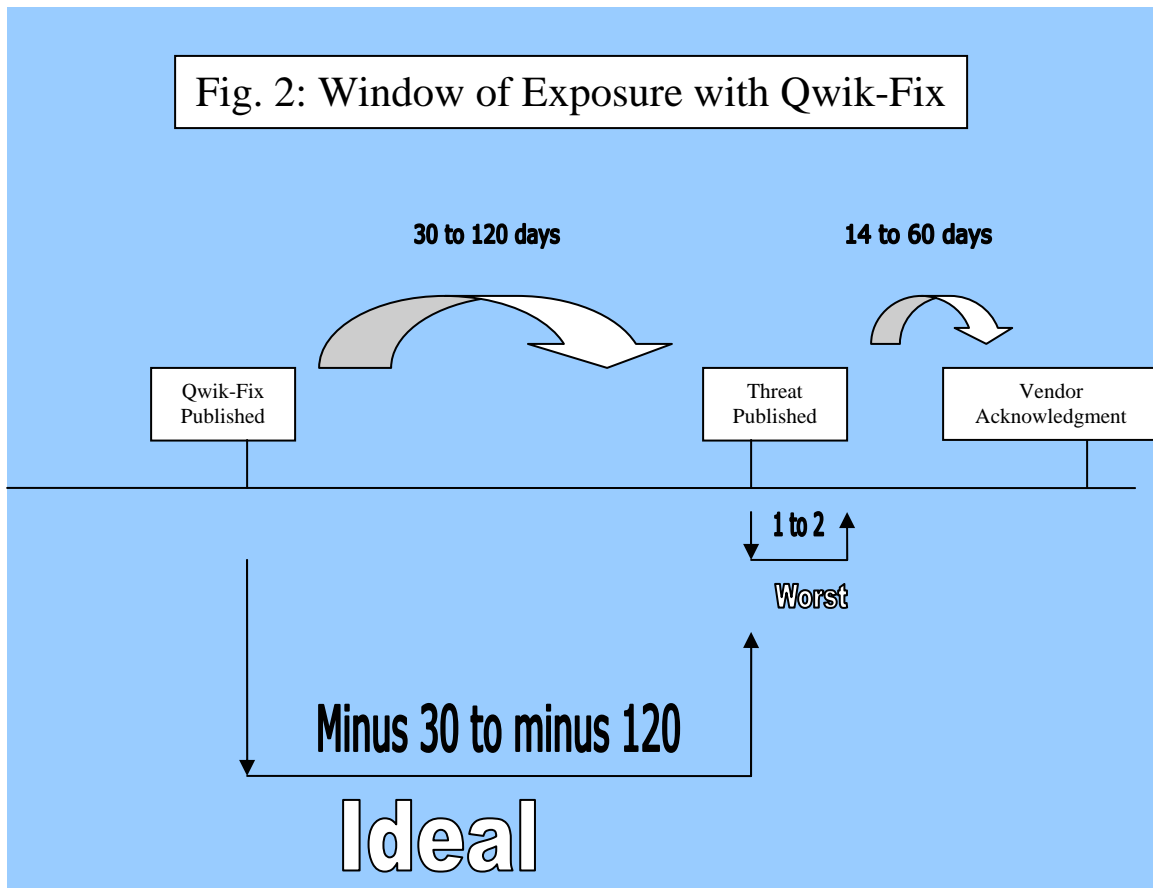
Timeline with Qwik-Fix Pro installed

By introducing Qwik-Fix Pro, the **Window of Exposure** is significantly reduced. 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:

- **Fix Published, Day 1**
 - PivX Solutions has analyzed a new attack vector and has created a fix that proactively mitigates the threat posed by a category of vulnerabilities. It is automatically pushed out to Qwik-Fix Pro users.
- **Vulnerability Published, Day 30-120**
 - A vulnerability is published or recognized. This typically happens 30 to 120 days after a fix has been made available through Qwik-Fix Pro.
- **Vendor Acknowledgment, Day 44-180**
 - The vendor acknowledges the vulnerability and starts to create a patch. This typically happens 14 to 60 days after the threat has been published.

In this scenario, Qwik-Fix Pro 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 can have increased confidence that it will be trustworthy, even before they test it themselves. Everybody wins ... except the bad guys.

This scenario is illustrated in figure 2:

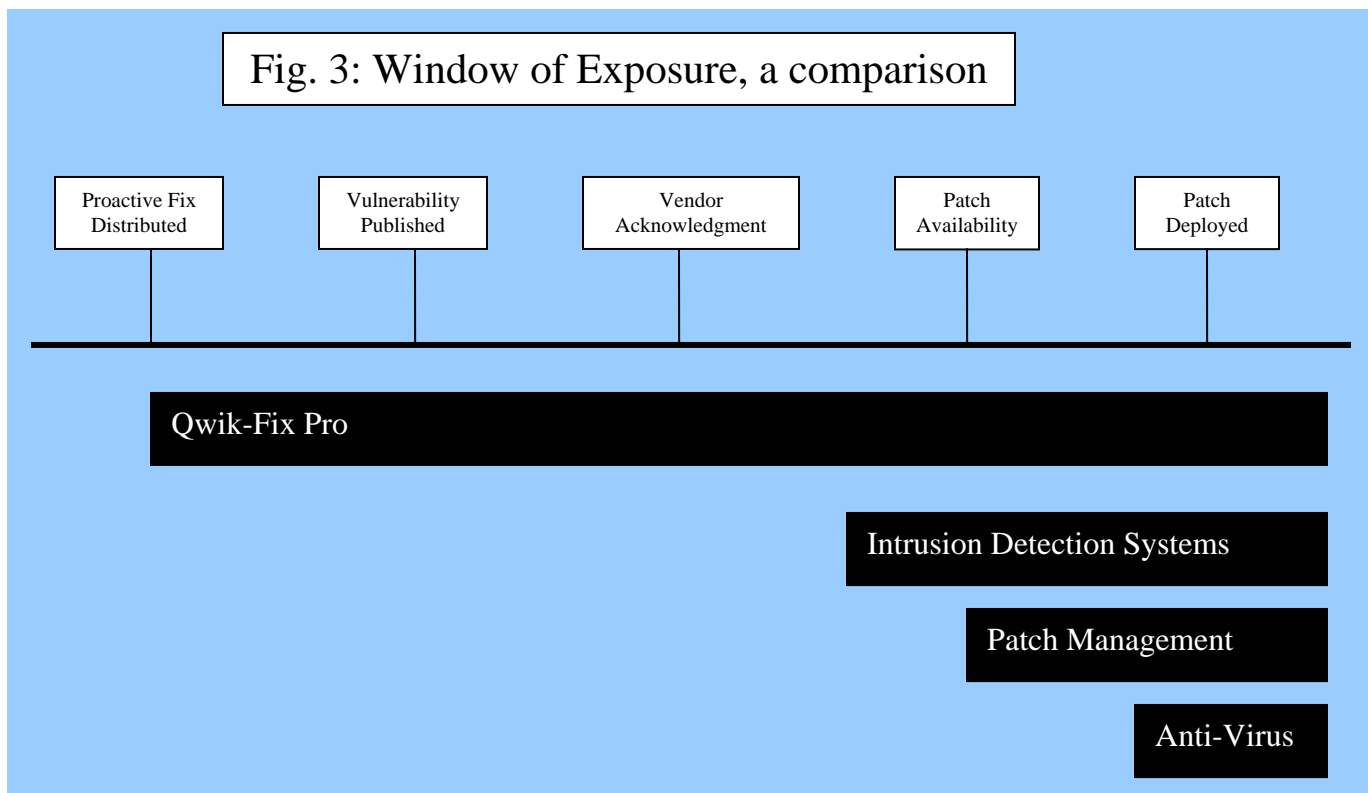


Timeline comparisons

To further demonstrate how Qwik-Fix Pro changes the **Window of Exposure**, let's compare at what point during the **Window of Exposure** current security products start to secure your Windows systems:

- Patch Management applications require a patch that eliminates a vulnerability be developed and available before it can be used to secure your network. Even then you are left with the burden of testing the patch since it introduces a permanent functionality change that could have 'unadvertised' effects.
- Intrusion detection systems require that an exploit for a vulnerability is created and in widespread use before network traffic can be logged and used to generate signatures for the exploit.
- Anti-Virus applications require that a virus is released before new signatures can be created.

These solutions do a good job of protecting you from vulnerabilities once it has been discovered. However, none of these solutions works to protect you from the threat posed by those vulnerabilities *in advance*. In contrast, Qwik-Fix Pro is proactive; it secures your Microsoft Windows systems from general threats, not specific vulnerabilities. That is how Qwik-Fix Pro reduces your **Window of Exposure**.



Distribution of fixes

Qwik-Fix Pro™ is an agent-based application. This means that each of the workstations or servers you want to protect needs to have the Qwik-Fix Pro Client™ installed, not unlike your Anti-Virus solutions. On a pre-scheduled basis, the Qwik-Fix Pro Client queries an update server to determine whether there are any available fixes, modified fixes or updates to the Qwik-Fix Pro Client components (see Figure 4).

The request from the Qwik-Fix Pro client to the Qwik-Fix Pro Update Server™ contains details about a number of items related to the Windows installation, including

- Licensing information
- Software version of Qwik-Fix Pro
- Details about the Windows operating system
- Details about related third-party applications

These details are required to secure your 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 or different third party applications. By delivering just the fixes that your specific Windows system needs, we are ensuring the least possible impact on your working environment with the highest possible degree of protection.

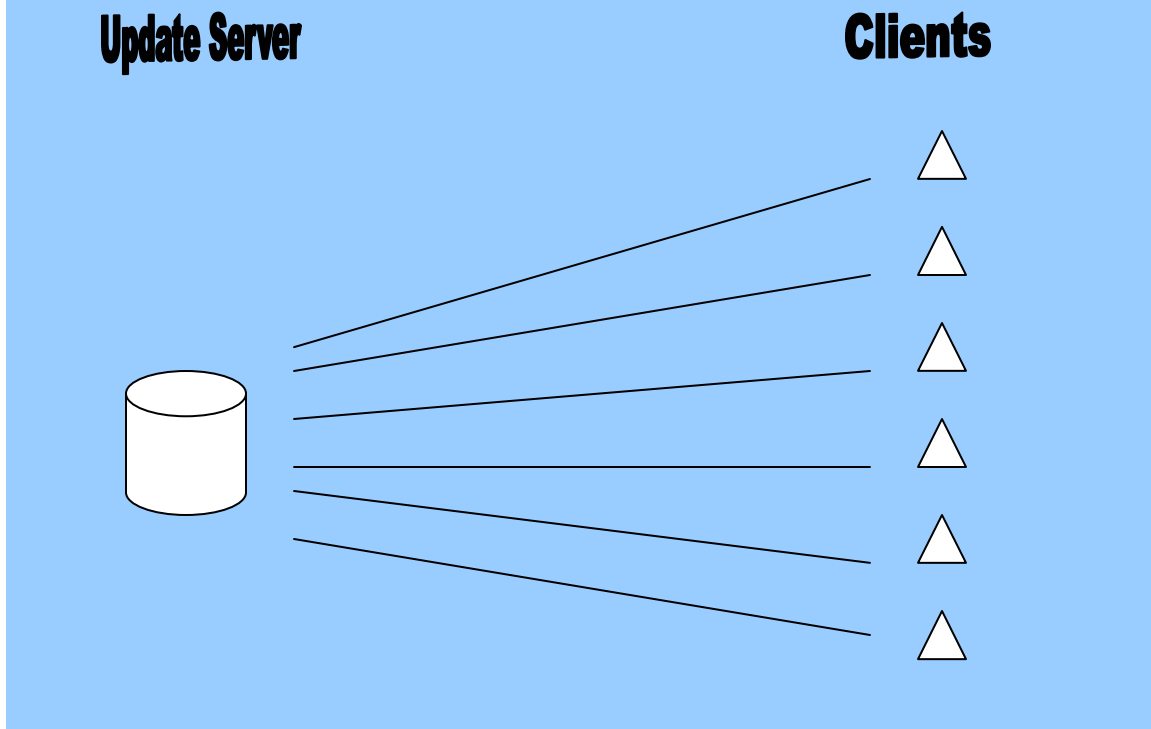
All communication between the Qwik-Fix Pro Client and the Qwik-Fix Pro Update Server is based on open and interoperable standards. The data is encoded as XML and transmitted using the HTTP protocol over port 80 to accommodate corporate firewalls and ease of administration. If your Windows system can surf the web it can retrieve fixes from PivX Solutions.

All communication between the Qwik-Fix Pro client and the Qwik-Fix Pro 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 Qwik-Fix Pro Client has received a list of available fixes and components, it retrieves these from a Qwik-Fix Pro 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 that are downloaded from the Qwik-Fix Pro Update server are cryptographically signed by PivX Solutions to ensure your safety and avoid any possible man-in-the-middle attacks. Only fixes and components that are verified to originate from PivX Solutions are applied after being verified.

Fig. 4: Distribution of fixes



Enterprise management

Qwik-Fix Pro also offers an enterprise management module for corporations. As with our distribution methods, the management of Qwik-Fix Pro is created on open standards and anyone with a web browser can use it to configure and manage Qwik-Fix Pro.

PivX Solutions is very flexible on management solutions and has a set of pre-configured solutions that we can use as a starting point to tailor for your particular Qwik-Fix Pro installation:

- Complete outsourcing
 - You install the Qwik-Fix Pro client on your Windows systems and they communicate directly with our update and download servers located outside your network. We manage the servers and your configuration centrally and automatically distribute fixes to your Windows systems when they are available.

- For private individuals and many small businesses, this solution makes perfect sense as it requires no management on your part.
- Self-managed outsourcing
 - The Qwik-Fix Pro clients still communicate with our external update and download servers, but you manage your own configuration through our web application and make your own choices on how often your clients query for updates and under what circumstances they automatically download and apply fixes. Among others, you can divide your Qwik-Fix Pro Clients into groups and select which kind of fixes apply to any group. For example, your developers might need fewer restrictions than your office personnel. This solution offers an increased amount of configuration options and reporting features.
 - For many small to medium sized businesses, this solution offers the perfect mix between implementation costs and manageability.
- Onsite solution
 - The Qwik-Fix Pro update and download servers are located on your internal network to optimize response time and minimize information exchange between your network and the outside world. Further, the web application interface runs off an application server on your internal network and acts as a failsafe proxy between your Qwik-Fix Pro Clients and PivX Solutions, enabling you to create test networks and intricately tailor the configuration of all aspects of the Qwik-Fix Pro solution.
 - This solution is tailored to the specific needs of larger businesses that require an extended level of control, isolation, privacy and management features. Implementation costs are higher but management features are abundant and long-term costs are significantly lowered.

Each of these solutions incorporates:

- Fix management
 - Detailing new fixes and their configuration possibilities, what software products they protect against and any updates to new fixes.
- Group policies
 - Enables you to distribute different sets of fixes to different groups of people in your organization.
- Client activity logging and reporting
 - Reports about client usage and availability.
- Diagnostic problems
 - Details about specific clients that experienced errors applying fixes or communicating with the server.

Fixes

The fixes that are distributed through Qwik-Fix Pro 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 caused by a threat by proactively targeting its attack, spread and infection vectors.

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 distinct differences:

1. Each fix that PivX Solutions distributes is reversible. Any action that the fix performs on your Windows system is not permanent and can always be reversed.
2. Each fix is also self-contained. Any files that the fix needs are contained in itself. Therefore, both installation and removal of a fix is included in the same package.
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.

Cost Savings and Advantages

The advantages of deploying Qwik-Fix Pro are numerous. First and foremost is peace of mind for a system administrator in knowing that their PC's are safe from known and unknown attacks. This has been proven dozens of times during our Beta test period. Moreover, as system administrators have become busier due to having more to do with fewer resources, they have also become nervous about the integrity of vendor-supplied patches that have sometimes caused more regressions than what they fixed in the first place. Qwik-Fix Pro actually buys both the vendor and the system administrator more time to thoroughly test for regressions and affords them the luxury of less pressure to deploy until sufficient testing is able to be fully completed.

In terms of savings, it largely depends on the customer and specific issues such as: tolerance for risk, the cost of downtime per hour and sub-issues: the cost of lost business, the cost to repair the damages, the cost in terms of lost productivity and competitiveness, and the soft dollar cost of lost trust with an end consumer. Together with a group of graduate students at the USC Marshall School of Business, PivX has created an ROSI Calculator for Qwik-Fix Pro that helps to quantify the advantages that a specific company can enjoy with Qwik-Fix Pro installed.

Summary Conclusion

Worms, viruses and malevolent code are increasing in their introduction, their speed, sophistication and their success. 2003 was a record year for worms and viruses, according to Computer Economics, with a reported damage total of over \$100 billion. In 2003 we saw Slammer, MS Blaster and Sobig.f, which according to John Chambers, propagated so fast that it touched 150 million machines in less than 3 minutes. So far in 2004 we have already seen MyDoom A, B and C as well as DoomJuice to name only a few. MyDoom already eclipsed SoBig in terms of the number of compromised machines. The bottom line is the current reactive security solutions are not sufficient in protecting desktops all by themselves. Clearly a proactive threat mitigation solution is needed as well.

Who are the most likely candidates for adoption of a Proactive Threat Mitigation solution?

Companies that lack expertise in both Windows and Internet Explorer browser operation and security functionality and testing, those that lack specific internal IT resources to research, test and deploy system-wide fixes and companies whose access to the internet is critical to their business are best candidates for a Proactive Threat Mitigation tool like Qwik-Fix Pro. Outsourcing this function allows them to maximize their internal IT resources and focus those resources on projects that are more aligned with a company's objectives. This is highly preferable to the current method of employing only reactive solutions and the resulting rush to deploy insufficiently tested patches to critical vulnerabilities. The vulnerability research identification and mitigation that Qwik-Fix Pro provides also provides a more predictable, relaxed and cost effective method of staying one step ahead of the bad guys.

Proactive Philosophy in Practice

In this whitepaper we have highlighted the benefits that a truly proactive solution such as Qwik-Fix Pro 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 Qwik-Fix 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 Qwik-Fixes included as part of the BETA test, Qwik-Fix was able to proactively protect our BETA users from several dozen unknown vulnerabilities, worms and exploits.

Some of the more noticeable threats that the BETA version of Qwik-Fix protected against includes, but is not limited to:

Bagle
Bizex
MiMail
SoBig
Blaster
Welchia
Nachi
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
LocalZoneInCache
1stCleanRc
MHT attacks
execdror6
HTML Application exploits
Ibiza CHM execution
BackToFramedJPU
XP Self-Executing Folders
Shell.Application
showHelp CHM
DoubleSlash zone bypass
LinKillerSaveRef
NAFfileJPU
NAFjpulnHistory
RefBack
WsBASEjpu
WsFakeSrc
WsOpenFileJPU
execdror5
XMLObject zone bypass
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.Redlof

**For more information regarding Qwik-Fix you can visit:
<http://www.pivx.com/qwik-fix/>**

**For Enterprise license information, please email PivX at:
corporate@qwik-fix.net**

**Qwik-Fix is a trademark of PivX Solutions, LLC.
Microsoft Windows, Windows and Internet Explorer are registered
trademarks of Microsoft. All other trademarks are property of their owners.**