OGREN group

Eric Ogren
92 Robert Road
Stow, MA 01775
m: 978•618•9240
eric@ogrengroup.com

Virtual Patching: a Compelling Cost Savings Strategy

An Ogren Group Special Report
November 2010

Executive Summary

IT patch processes are at a critical crossroads. Exploits appear in the wild only a day after announcement of a vulnerability; most damage from automated attacks occurs within the first 15 days of the news and 80% of exploits appear within 60 days. Even with a concentrated effort in maintaining compliant configurations, the average organization still takes over 30 days to patch standard operating systems and applications, and months or years to patch complex business applications. This *window of vulnerability,* the time between recognizing the vulnerability and applying a vulnerability-closing patch, is when the business infrastructure lies open to attacks and is most vulnerable.

The traditional method of applying permanent software patches and upgrading software is much too labor-intensive and invasive to applications to compete with the speed of exploits and to adequately protect the business. Virtual Patching offers an alternative strategy – delivering timely protection within hours of vulnerability publication – weeks or months ahead of the traditional patch. Virtual patching, also known as vulnerability shielding, uses host-based IPS rules or filters to inspect and clean network traffic to efficiently correct or block application input streams that might otherwise exploit vulnerabilities, *before the malware even reaches the vulnerable target and without disruption to applications and business operations.* Virtual patching closes the window of vulnerability and allows IT to save resources by reducing the frequency of patch and software maintenance cycles.

While patching vulnerabilities or permanently correcting application code remains important, virtual patching significantly reduces the risk of a successful attack and helps reduce the costs of security. The Ogren Group finds that a security strategy incorporating virtual patching offers a compelling cost savings to organizations:

- Shrinks the window of vulnerability for critical servers and desktops. Virtual patching acts to prevent exploits of known vulnerabilities within hours of announcement.
- Allows orderly patch maintenance based on IT schedules. Security teams research, test, and deploy traditional patches in a controlled manner with fewer panic patch incidents. IT can save resources by lengthening the interval between standard patching cycles.
- Secures applications while engineering corrects vulnerabilities in applications. Virtual patching buys time for application vulnerabilities to be permanently corrected in custom application code following secure software development lifecycle procedures.
- Postpones upgrade costs by extending the life of legacy systems. Many organizations have legacy applications or operating systems that are no longer supported with patches or upgrades. Virtual patching allows IT to extend the life of legacy applications, postponing the costs of re-engineering or upgrade.

This special report, commissioned by Trend Micro, reinforces the security and operational cost savings benefits of virtual patching with the Deep Security product. Information in this report derives from Ogren Group research and interviews with enterprise security officers of global organizations.

Virtual Patching

Virtual patching is a host-based security capability that shields applications from vulnerabilities until permanent corrections from procedures such as patch management and software maintenance can be applied. Instead of modifying executable programs, with resultant complexities in quality assurance and software asset management, *virtual patching operates on network streams, inspecting inbound traffic and shielding applications from exploits, even though the vulnerability has not been permanently patched.* The enhancements to an organization's patch process that virtual patching delivers significantly lessen the workload throughout the entire patch process:

- Applies easily in the network data path without change to the application environment. Virtual patching does not require modification of the application or operating system, reducing the overhead burden of testing and deploying patches, and sometimes recovering from bad patches.
- Reduces the incentive to use network firewall and router rules to avoid patches. Many security teams look to adjust firewall or router rules in order to avoid applying software patches, which may unnecessarily block legitimate traffic to other applications and can lead to undesirable maintenance side-effects in the network.
- Sustains production applications for better uptime and SLA performance. Critical applications can be shielded from vulnerabilities with virtual patching without scheduling off-hours downtime.

Virtual patching accelerates the time to patch, closing the window of vulnerability for continuous compliance of key applications. This vulnerability shielding strategy of shrinking the window of vulnerability allows security and IT teams to reduce operating costs by requiring fewer software patch cycles and software maintenance fixes. In addition, virtual patching is the only pragmatic method of shielding legacy applications where patching becomes unappealing due to costs or risk of extended downtime.

Shrink the window of vulnerability

One of the most compelling and widely used metrics in security is the window of vulnerability, or the elapsed time from the vendor's announcement of a vulnerability until IT has deployed the patch in affected systems. While security teams cannot control when exploits arrive through the network, IT can control how long an attacker has to exploit an un-patched vulnerability within the corporate infrastructure. In many cases, it can take 30 days or more to research, test, and deploy a patch to operating systems and often longer for applications. Virtual patching shrinks that window of vulnerability by automatically delivering a patch within days and most often within hours.

- Reduce the risk of an exploited vulnerability requiring public disclosure of regulated data loss. Since the window of vulnerability is quickly closed, the risk of losing regulated data and incurring costly public disclosure expenses is significantly reduced.

- Reduce the need for ad-hoc emergency patching or software corrections. Virtual patching buys time for IT to schedule permanent patches and software corrections in an orderly fashion. Less resource is expended on emergency application of high priority patches or quick engineering corrections to the source code.
- Service level agreements and application uptime are enhanced. Virtual patching automatically secures application environments by patching vulnerabilities without application downtime.

Extend the life of legacy applications and platforms

Many organizations have mission critical applications that execute on operating system platforms that are no longer supported by the OS vendor or are considered to be too fragile to patch. Legacy applications may not be easily upgraded to newer OS versions due to lack of engineering priority on newer revenue generating applications, risk of extended downtime of the application, or prohibitive costs of rebuilding an application that has been previously expensed. Virtual patching gives IT an alternative to extend the life of applications on legacy OS platforms by reducing compliance, security, and operational costs issues for the business.

- Virtual patching may obviate the need for expensive support contracts for legacy operating systems. For instance, support contracts for Windows 2000 start at $50,000 per quarter and Oracle has instituted a pay-per-patch plan for Solaris 8.
- Postpone application replacement expenses. Virtual patches can prolong the life of applications based on unsupported operating systems – postponing new investments in servers, operating system licenses, and application software upgrades.
- IT can protect in house-developed applications with custom virtual patches It is easier to deploy a virtual patch in the network data stream than it is to re-engineer application software. Virtual patching allows organizations to save engineering expenses by applying custom developed virtual patches for legacy applications.
- Virtual patching may be the only pragmatic way to shield legacy application vulnerabilities. Legacy applications or production systems, such as those based on Oracle databases, may be too sensitive for invasive software patches, but can be further protected from exploits with virtual patching.

Deep Security

Trend Micro delivers virtual patching to organizations for servers and endpoints as a module within the Deep Security product (as well as an Intrusion Defense Firewall plug-in for the OfficeScan endpoint protection product). Deep Security provides software-based integrated security for systems operating in standalone, virtual, and cloud-based environments with a single, centrally managed solution that includes:

- Deep packet inspection (IPS, Virtual Patching, Web Application Protection)
- Anti-malware for VMware environments.
- Bi-directional stateful firewall protection.
- Integrity monitoring.
- Log inspection.

Deep Security has features that save IT time and effort throughout the patch process, from notification of available patches, identifying affected applications, and minimizing the points where virtual patches need to be applied:

- Consolidates notifications of announced vulnerabilities and available virtual patches. Deep Security virtual patching leverages relationships with critical infrastructure software vendors and industry organizations such as CERT, SANS, Bugtraq, VulnWatch, PacketStorm, and Securiteam to keep security teams continually informed of vulnerability shield and patch availability.
- Automatically discovers applications and vulnerabilities. Deep Security virtual patching detects the presence of applications and evaluates the applications for vulnerabilities to make prioritized recommendations for IT.
- A single virtual patching instance shields multiple virtual machines. For virtualized data center applications, a single Deep Security virtual patching agent saves IT time and effort by automatically shielding application vulnerabilities all across the virtual machines on the server. Alternatively, virtual patching can be executed and managed on a per VM basis.

Conclusions and recommendations

IT organizations are evolving their infrastructure to reduce operating costs, efficiently meet compliance mandates, and flexibly deliver new services to the business. The Ogren Group believes that virtual patching with Trend Micro's Deep Security is a compelling example of a cost savings strategy that carries significant security benefits:

- Shrink the window of vulnerability for critical servers and desktops. Virtual patching delivers timely vulnerability protection without application modification, reducing the time required to test and deploy critical patches.
- Allows orderly patch maintenance based on less frequent IT schedules. Security teams research, test, and deploy traditional patches in a controlled manner with fewer patch deployment cycles.
- Extend the life of legacy applications. Virtual patching can remove vulnerabilities from expensed applications on older operating systems such as Windows 2000 and Solaris 8, avoiding expensive support contracts.
- Reduce business disruptions and costs associated with emergency patch and software fix operations. Virtual patches, delivered automatically from Trend Micro allow IT to patch and correct software for high priority vulnerabilities on planned work schedules.

The Ogren Group recommends that enterprises take advantage of the compelling cost savings of virtual patching. In particular, virtual patching services can save IT time and money while enhancing the security of data center applications. The Ogren Group believes Trend Micro's virtual patching should be on the shortlist of security teams requiring quicker vulnerability shielding and patch coverage to ensure a secure and compliant business.

Virtual patching cost savings worksheet

Utilizing virtual patching reduces your security risks while reducing operating costs. Individual expected cost savings will vary by organization based on the strategies chosen. Use this worksheet to help itemize the cost savings of virtual patching in your organization.

Optimize the operational efficiency of the patch process

The number one job of virtual patching security is to protect the business from malicious code and theft of regulated data and intellectual property. Virtual patching filters are deployed in hours, protecting applications until permanent patches or software fixes can be applied.

$_____	Reduce the annual cost of emergency out-of-band patches	Factor in time required to test and apply patches given a weighted cost of IT labor.
$_____	Reduce the annual cost of emergency software fixes	For certain applications this includes outsourcing fees or in-house charge-backs.
$_____	Reduce the frequency of standard patching cycles	With the protection of virtual patching you may be able to extend the interval between standard patching cycles, freeing IT to focus on other activities and reducing downtime
$_____	Enhanced application uptime savings	Applications remain operational with virtual patching, resulting in extra hours of uptime that can be reflected in revenue or improved SLAs.
$_____	Reduce the risk of disclosure incidents	Shrinking the window of vulnerability translates into a lower probability of regulated data loss and withholdings for disclosure incidents.
$_____	Reduce the costs of patch roll-backs	Patches are invasive to applications and operating systems. It is not uncommon for a patch to break a system in production use and have to be removed.
$_____	Reduce the costs of discovering available patches	Deep Security virtual patching automates monitoring of vendor advisories and vulnerability sources including CERT, SANS, Bugtraq, and VulnWatch to provide IT with comprehensive notifications of patches.
$_____	Reduce the patch applicability research effort	Deep Security virtual patching automatically recognizes applications and their patch levels. Also, virtual patching lessens the incentive to deploy patch work-arounds in firewall and router rules.
$_____	Protect “untouchable” applications	Applications may be considered un-patchable because of cost or the risk of down-time – e.g. Oracle database servers.

Extend the life of legacy platforms and applications

Legacy applications, especially those running on Windows 2000, Oracle 10.1, Red Hat 3, and Solaris 8 operating systems, are expensive to keep compliant. Virtual patching allows the ROI of legacy applications to improve as the lifetime is extended.

$_____	Reduce the annual cost of legacy platform support contracts	Vendors may charge per patch, or require expense relief for supporting retired software.
$_____	Reduce the costs of migrating legacy applications	Extending the life of an application postpones investments in servers, platform software, and application engineering.
$_____	Reduce sustaining engineering expenses for legacy applications	Applications remain operational with virtual patching, allowing IT to postpone permanent software corrections

IT initiatives such as virtual data centers, virtual desktop infrastructures and protection of cloud-oriented application systems are strategic decisions, with longer term cost savings benefits. Trend Micro's Deep Security's virtual patching has direct cost savings for shrinking the windows of vulnerability and extending the life of legacy applications. This worksheet will help IT analyze the impact of virtual patching for their organization.