OGREN group

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

Virtual Patching: a Proven Cost Savings Strategy

An Ogren Group Special Report
December 2011

Executive Summary

Security executives, pushing the limits of traditional labor-intensive IT patch processes that cannot close vulnerabilities fast enough, are turning to virtual patching to protect servers and desktops against new cyber threats. Virtual patching offers a proven strategy – delivering timely protection within hours of vulnerability publication – weeks or months ahead of the traditional patch. In addition, security executives leveraging a virtual patching strategy are achieving compelling cost savings by reducing the frequency of patch and software maintenance cycles.

The traditional method of applying permanent software patches and upgrades is much too labor-intensive and invasive to applications to compete with the speed of exploits. 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 server and desktop 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.

Virtual patching inspects and cleans network traffic using host-based filters 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.* The Ogren Group finds that organizations integrating virtual patching into vulnerability management processes are realizing compelling cost savings:

- Helps ward off disclosure incidents by rapidly neutralizing critical vulnerabilities in 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.
- 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.
- Enables cost effective security for virtualized environments. Organizations are embracing virtualized applications for proven cost savings and enhanced security. Virtual patching, residing on the server or within each VM, protects virtualized environments from exploits of vulnerabilities discovered after creation of the VMs.

This special report, commissioned by Trend Micro, reinforces the security and operational cost savings of host-based virtual patching with the Deep Security and OfficeScan products. 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 and endpoints 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 or desktop 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 for continuous compliance of key applications and endpoints. Security and IT teams 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 high engineering costs or risk of extended downtime.

React quickly to new vulnerabilities

One of the most compelling and widely used metrics in security is 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 vulnerability exposure for servers and desktops by automatically delivering a patch within days and most often within hours. The cost savings of virtual patching are being proven by enterprise security teams:

- Reduce the risk of an exploited vulnerability requiring public disclosure of regulated data loss. Since the vulnerability exposure is quickly mitigated, 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 and desktop 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.

Trend Micro virtual patching

Trend Micro's flagship security solutions for servers and end-user endpoints, respectively Deep Security and OfficeScan deliver timely virtual patching within enterprise networks. Trend Micro's virtual patching solution saves IT time and effort throughout the patch process, from notification of available patches, identification of affected applications, and minimization of the points where virtual patches need to be applied:

- **Consolidates notifications of announced vulnerabilities and available virtual patches.** Trend Micro 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.** Trend Micro 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, Trend Micro virtual patching, deployed as a single virtual appliance, 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.

Trend Micro delivers complete virtual patching coverage 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. Enterprise security teams are thus able to deploy virtual patching to servers and desktops across the organization with consistent administration and reporting interfaces.

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 (IDS/IPS, Web Application Protection and Application Control)
- Anti-malware
- Bi-directional stateful firewall
- Integrity monitoring
- Log inspection

OfficeScan users in enterprise environments receive virtual patching benefits with the Intrusion Defense Firewall plug-in, proving an easy to administer solution that includes:

- Virtual patching for operating systems and certain common applications
- Acceptable-use security policies that can block traffic from specific applications, such as those from social media sites
- Firewall protection for remote and mobile enterprise endpoints

- Removal of infected data from network traffic
- Automatic adjustments of security configuration based on an endpoint's location
- Centralized administration and reporting

The Ogren Group research also finds that not only are organizations integrating Trend Micro's virtual patching into security processes, but that those security processes are also evolving to take advantage of virtual patching cost savings benefits. The maturity of virtual patching and the proven cost savings for IT has allowed security teams to address significant enhancements to protecting the business, including:

- **Integration with vulnerability management processes to automate protection.** Automation is the key to driving more costs out of maintaining compliant servers and desktops. Trend Micro has integrated virtual patching with leading vulnerability management vendors to automate the discovery, assessment, and protection of servers and desktops.
- **Integration with virtualization processes to efficiently protect virtualized applications and virtual desktop infrastructures.** Trend Micro's innovative approach of utilizing a single anti-malware virtual appliance on a server that also contains virtual patching software has been deployed by large enterprises. The Trend Micro virtual appliance requires no agents to be bundled into each virtual machine, enhancing performance, preserving VM densities, and automatically protecting VMs that cannot otherwise be easily patched.
- **Integration with cloud-based security systems to cost effectively protect servers and desktops.** Trend Micro utilizes its Smart Protection Network to efficiently feed the latest virtual patches to Deep Security and OfficeScan.

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 and OfficeScan is proving to be a compelling example of a cost savings strategy that carries significant security benefits:

- **React quickly to mitigate the exposure of new vulnerabilities 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 proven 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, delivered through Deep Security and OfficeScan agents, should be on the shortlist of security teams requiring quicker vulnerability shielding and patching 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 and OfficeScan virtual patching has direct cost savings for quickly limiting the exposure to new vulnerabilities and extending the life of legacy applications. This worksheet will help IT analyze the impact of virtual patching for their organization.