Lower Security Risks and Costs with Virtual Patching

A Trend Micro White Paper

Trend Micro Deep Security

August 2010

VIRTUAL PATCHING:
LOWER SECURITY RISKS AND COSTS

I. INTRODUCTION

Patch management for vulnerability remediation can be a painful exercise for IT departments. If it were easy, patch release and deployment would be predictable events and vulnerabilities would be addressed within acceptable timeframes. Instead, emergency patches persist, IT staffs scramble to deploy them and security officers brace themselves for the worst case—a data breach or unplanned system downtime. Beyond emergency patches and uncertainties caused by vendor acquisition, predictable events such as planning to maintain security for out-of-support (OOS) enterprise software pose an added challenge. For such systems, ongoing security patches cease, forcing IT operations to choose between expensive support contracts or accept the risk of exploits targeted at OOS systems with unpatchable vulnerabilities.

This white paper reviews enterprise challenges with security patch management including risks to various areas of IT—security, compliance, operations, and budgets. It discusses how traditional approaches to remediating vulnerable systems can create new problems and provides a new model is needed to keep pace with the ever-increasing number of attack vectors.

Trend Micro Deep Security offers 'virtual patching', which shields vulnerabilities in critical systems until an actual patch is available and deployed—or as permanent protection in the case of OOS systems. Complementing traditional patch management, Deep Security's virtual patching mitigates risk across network topologies, platforms, and applications—including commonly targeted Web applications—and enables enterprises to maintain regulatory compliance, including necessary logging and reporting capabilities. For OOS systems such as those running Microsoft Windows 2000, Deep Security also helps organizations avoid expensive support contracts by eliminating the need for customized patches.

II. PATCH MANAGEMENT TODAY

The primary goal of software patching is to keep operating systems and applications working smoothly and securely. For widely used systems such as Microsoft Office or Windows Vista, the process is relatively predictable, but life gets significantly more complex when older applications, custom development, and out-of-support operating systems enter the picture. Add budget constraints that that constrain migrating away from OOS platforms or remediating supported platforms and a hacker community eager to exploit unpatched system vulnerabilities, and you have a situation ripe for disaster, or at least a nasty note from auditors. .

COMPLEXITIES OF THE TYPICAL PATCH DEPLOYMENT PROCESS

The mere availability of a patch doesn't give IT a green light to deploy it across all business systems. Even the very predictable "Microsoft Patch Tuesday" releases are scrutinized every month by IT organizations to ensure that the risks are actually addressed without breaking existing applications. Typically, patch management follows a structured process that includes[1]:

- Obtain the patch from a trusted party and check the integrity of both the patch and the patch source
- Test the patch to ensure the vulnerability is remediated and the patch will not break other applications
- Notify affected parties of any necessary scheduled downtime to apply the patch
- Deploy the patch to all affected systems
- Recheck operational efficiency of patched systems and remediate as required

The complexity and frequent time-critical nature of even predictable patching before a vulnerability is actually exploited is a significant burden on IT operations and consigns them to a state of reactivity and continuous catch-up. Consequently corners may be cut, risks may persist, and proactive IT projects may languish.

Against this background, it is hardly surprising that IT departments spend 33% of their time on patch management but only 27% rate their patch management process as being effective.[2]

ADDITIONAL CONSIDERATIONS

Beyond the predictable nature of "Patch Tuesday"—and its constant companion "Exploit Wednesday"—multiple additional factors must be borne in mind when implementing patch management programs.

- Emergency patches that must be applied immediately, with consequent downtime, overhead, and cost
- The operational challenge of patching virtualized systems and the rapid growth in the use of such systems
- Mandatory requirements for timely patching to ensure compliance with internal IT governance and external data protection legislation
- Increasing frequency of zero-day attacks and attacks targeted at specific industries and platforms
- Ongoing consolidation of vendors and consequent disruption of patch development and distribution
- Growing use of "unpatchable" POS systems, ATMs, and embedded systems as a vector for malware delivery

REGULATORY COMPLIANCE

In addition to the specific timeliness requirements of the PCI regulations[3], periodic audits to ensure up-to-date patches on critical systems—ones that store or process regulated data—must be undertaken to comply with many industry regulations.

The most conclusive way to prove the timely application of patches to external auditors is through tamperproof logs showing patch download and deployment. Internal auditors often use patch management administrator software with sophisticated reporting to monitor and update status of patch management tasks.

RISK WINDOW:
TIME FROM VULNERABILITY DISCOVERY TO PATCH RELEASE TO PATCH DEPLOYMENT

Security concerns over unpatched systems are well founded. More than 86% of enterprises reveal that they have experienced security breaches due to malware, over a third have experienced attacks on web applications, and almost one third have had OS vulnerabilities attacked. Patch management processes exacerbate the problem by occupying the same IT resources as are required to remediate compromised systems.[4]

As a result, the gap between discovering the vulnerability (or being notified of a critical security patch) can extend for weeks or even months before appropriate patches are deployed to all production systems. The challenge is not getting easier over time, with the National Vulnerability Database reporting an annual average of close to 6,000 software vulnerabilities between 2006 and 2009.

Buying time to manage the window between when a vulnerability is discovered and a patch can be deployed is a critical element in maintaining an adequate security posture.

III. THE LATEST SECURITY CHALLENGE: OOS SYSTEMS

Clearly no software application will be supported in perpetuity; every IT manager has at some time received an End of Life (EOL) announcement, which specifies a date after which a particular program will be out-of-support (OOS) and no further patches will be issued except by special (and costly) individual agreements. The most recent recruit to this growing club is Microsoft Windows 2000, which was designated OOS on July 13, 2010.

Yet even with an organized end-of-life process, many organizations appear to be caught off guard or unprepared for the inevitability of OOS software. And those who do research the options find that those options often bring their own share of challenges.

Undesirable Options for Addressing Out of Support (OOS) Systems

- *Ignoring the associated risks*
- *Eliminating these systems*
- *Purchasing custom support contracts*
- *Isolating them on the network*
- *Hardening systems*

WHERE IGNORANCE IS NOT BLISS: THE RISK OF IGNORING VULNERABILITIES ON UNSUPPORTED SYSTEMS

Ignoring the risks associated with the continued use of unpatched OOS systems is not wise for many reasons, not the least of which is that newer, supported platforms often share code with earlier releases. A new exploit on a supported platform can also affect an older OOS system that shares its code. This is the case with Windows 2000 and Windows XP, for example; even a few Windows 2000 installations left “live” on a network can be exploited by savvy hackers who see Windows 2000 as an easy entry point long after Windows XP patches have been deployed. If operating system migration has not yet been completed, enterprises with these systems are already at risk. As soon as the next Windows XP vulnerability is announced and a patch is released, the clock will start ticking until an exploit targets this same vulnerability on Windows 2000. And once the attacks start, they unlikely to stop because there will be nothing there to stop them.

While enterprises should plan for the eventual elimination of OOS systems, such plans are frequently dogged by budgetary constraints or technical limitations. The most common reason for retaining older platforms is to support existing business-critical applications that have not been ported to newer operating systems. This situation occurs all-too-frequently when an application vendor seeks to build its customer base by acquiring the developer of an older system with a large installed base.

CUSTOM SUPPORT AGREEMENTS FOR OOS SYSTEMS

In the name of “customer service”, vendors may offer custom and extended support agreements for OOS software which entitle customers to emergency security patches. However, such agreements are frequently cost-prohibitive for all but the largest organizations; Windows 2000 agreements start at $50,000 per quarter[5], and some OOS contracts for Windows NT v4 have exceeded $1 million.[6] Not unsurprisingly, many enterprises find such costs to be unpalatable, driving them to find alternative methods to mitigate the risk or, in some cases, accept the risk of a potential compromise.

Acquisitions bring their own complexity to the extended support contract. For example, when Oracle acquired Sun, Sun's customers were required to renew their support contracts with Oracle in order to receive patches; a similar situation occurred when Oracle acquired middleware vendor BEA Systems.

ISOLATION

One approach to managing risks associated with OOS software might be to make such systems hard for hackers to reach. Isolating these systems on separate networks or VLANs adds a layer of difficulty that hackers may decide is simply too much trouble. However, network isolation may not be practical for essential business systems, and therein lies the conundrum. Making OOS systems hard to reach adds a layer of security but may also prevent them from being used effectively, obviating the reason for retaining them in the first place.

The Perfect Storm - Windows 2000 After July 13, 2010

- *Vulnerability announced for Windows XP*
- *Hackers start writing exploits based on this XP vulnerability*
- *Some exploits are successful before XP patch release*
- *Patched XP systems are protected, 2000 systems continue to be attacked indefinitely*

SYSTEM HARDENING

Hardening OOS systems (removing unnecessary services, user accounts) may appear to be an acceptable way to minimize risk. However, authorized users will still need access to these systems, so restricting user accounts alone may not be practical for business reasons. Hardening through removal of unnecessary services and ports is not trivial when business applications are designed to run on general-purpose operating systems with a variety of application services and ports (e.g. RPC ports, web services), and may break the application. Restricting application ports may also render stateful packet-filtering firewalls ineffective, since many applications dynamically allocate ports as needed.

APPLICATION WHITELISTING

Whitelisting OOS applications could potentially enable IT to be alerted if malware has affected and made changes to such an application, but does not remove the problem of dealing with such an event when identified. Using whitelisting to instead permit only the use of explicitly-authorized software on an OOS system is conceptually sound, but in practice would likely prove unmanageable; IT would need to update signatures for authorized executables and upload them into the white listing system every time one of those executables was patched.

Given the challenges of all these scenarios, why does patching remain such a keystone of enterprise IT policy?

IV. SYSTEM VULNERABILITIES ARE EVERYWHERE

Patch management is both a solution and a source of frustration, so why do IT security policies continue to mandate timely and accurate patching of vulnerable systems? The answer is that, short of rewriting the original source code, patches are the most targeted way in which to remediate software vulnerabilities in specific operating systems and applications.

In addition to OOS software, a number of other critical IT areas are vulnerable to the "ignorance is bliss" school of security management.

ENTERPRISE APPLICATIONS

In 2009, over 5,700 critical software flaw vulnerabilities were reported in operating systems, databases, servers, and other applications, according to the US National Institute of Standards and Technology (NIST).[7] Patching these vulnerabilities can be disruptive and time consuming, requiring systems to be rebooted and potentially impacting service level agreements. Even when a patch is available, it can take weeks or even months before the patch can be fully deployed because of internal testing requirements.

LEGACY WEB APPLICATIONS

As we've seen with OOS systems, not all flaws can be patched. Some vulnerabilities are caused by mis-configured systems, while others may be due to coding flaws in custom-built and legacy web applications. In the former case, manual intervention may be required; in the latter case, developers with the necessary subject matter expertise may not be available to fix the application, as was the case with Y2K and COBOL.

Four out of five records breached in 2009 were the result of SQL Injection attacks on web applications[8] web applications are particularly vulnerable because they're inherently open and accessible to attackers. In addition, content and functionality are increasingly complex and programmers untrained in secure software development practices. Perimeter security won't shield these systems and it can be difficult to locate and assign the custom development resources necessary to fix the code.

NON-TYPICAL SYSTEMS

Unattended or embedded systems such as point-of-sale systems, kiosks and medical devices are often considered un-patchable despite significant levels of vulnerability; many such systems run on a variant of Windows XP and connect directly or indirectly to both the Internet and corporate networks. Often, low-bandwidth connections with remote locations make deploying large patches prohibitively time-consuming and/or expensive. At other times, regulations or service level agreement uptime requirements may preclude such systems from being patched.

THE HUMAN FACTOR

The broad interconnectedness of today's systems has expanded the perimeter of the corporate network well beyond the physical boundaries of the enterprise. Users' personal smart phones and USB drives are frequently plugged into corporate endpoints, social networking applications are downloaded without the knowledge of the IT department, remote users may only occasionally connect to the corporate network and receive patches—and all have the potential to create a direct connection between the network or data center and whatever might be lurking on the Internet. Human behavior remains a top cause of security breaches in business today.

V. A NEW APPROACH: VIRTUAL PATCHING

The dual challenge of vulnerability risks and patch management is clearly not being adequately met by traditional solutions. Multiple gaps exist that need to be filled by a solution that does not:

- Require the isolation of critical systems
- Entail whitelisting applications on critical systems
- Call for the removal of unused user accounts and unnecessary services
- Further reduce security and operability by blocking ports
- Involve IT in attempting to block social networking and smart phones

> *"Lots of tools produce reams and reams of data. Deep Security is different—it actually helps us focus in on the right issues."*
>
> — *Ralph Michaelis, CIO, Carleton University*

Trend Micro's answer to the unwinnable challenge of patching unpatchable systems is Deep Security Virtual Patching, a non-disruptive "vulnerability shield" that protects systems during the risk window—and beyond, for those systems on which the risk window never ends, as a patch will never be released.

DEEP SECURITY: A COST-EFFECTIVE COMPLEMENT TO PATCH MANAGEMENT

Trend Micro Deep Security shields vulnerabilities in critical systems until a patch is available and deployed or in place of a future patch that may never materialize. Either way, enterprises get a timely, cost-effective complement to traditional patching processes that can significantly lower costs, reduce disruptions, and provide greater control over the scheduling of patches. Designed to provide comprehensive protection for all servers—physical, virtual, and cloud—as well as Windows endpoints, Deep Security can be deployed as an agent on a physical or virtual machine, or as a virtual appliance on a VMware ESX server to protect guest virtual machines.

SECURE AGAINST ATTACK

If a hacker locates a vulnerability, he may try to exploit it. Deep Security Intrusion Detection and Prevention (IDS/IPS) rules shield against known vulnerabilities—for example those disclosed on Microsoft Patch Tuesday—from being exploited. Deep Security includes out-of-the-box vulnerability protection for over 100 applications, including database, web, email and FTP servers. In addition, IDS/IPS rules also provide zero-day protection for known vulnerabilities that have not been issued a patch, and unknown vulnerabilities.

ELIMINATE THE GUESSWORK

Vulnerability shielding leverages the Deep Security IDS/IPS rules described above and requires updating when new vulnerabilities are announced. However, rather than relying on a new software patch for protection, the existing Deep Security engine is already at work, checking for updates to IDS/IPS rules. Recommendation scanning streamlines security update management by automatically recommending which rules need to be deployed to protect a given system. Deep Security scans the system to identify which IDS/IPS rules need to be deployed to optimize protection—based on the OS version, service pack, patch level, and installed applications. In addition, as the server environment changes and patches are deployed, Deep Security automatically recommends which rules can be removed to minimize resource utilization.

TIMELY UPDATES

Security updates from a dedicated team of security experts ensure the latest protection by continuously monitoring multiple sources of vulnerability disclosure information to identify and correlate new relevant threats and vulnerabilities. Trend Micro also receives vulnerability information from Microsoft in advance of their monthly security bulletins, making it possible to anticipate emerging threats and provide more timely protection.

WEB APPLICATION SECURITY

Web application protection rules defend against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities, shielding these vulnerabilities until code fixes are completed. Security rules enforce protocol conformance and use heuristic analysis to identify malicious activity.

SECURING NETWORK CONNECTIONS

Enterprise-grade, bi-directional, and stateful firewall allows communications over ports and protocols necessary for correct server operation, and blocks all other ports and protocols. This reduces the risk of unauthorized access to the server.

EXTEND COVERAGE TO END USER SYSTEMS

Trend Micro Intrusion Defense Firewall shields vulnerabilities in Windows desktops and laptops, and seamlessly plugs into the Trend Micro OfficeScan console for unified management.

VI. HOW DEEP SECURITY WORKS

Deep Security combines server and application protection software with vulnerability response services to enable systems to become self defending. The solution consists of the Deep Security Virtual Appliance, Deep Security Agent, Deep Security Manager, and the Security Center.

DEEP SECURITY VIRTUAL APPLIANCE

Transparently enforces security policies on VMware vSphere virtual machines for IDS/IPS, web application protection, application control, and firewall protection—coordinating with Deep Security Agent, if desired, for integrity monitoring and log inspection.

DEEP SECURITY AGENT

The Deep Security Agent is a small software component that is deployed on the server or virtual machine being protected and which enforces the security policy.

DEEP SECURITY MANAGER

The Deep Security Manager enables administrators to create security profiles and apply them to servers. It has a centralized console for monitoring alerts and preventive actions taken in response to threats, and can be configured to automate or distribute security updates to servers on demand. The Manager can be used to generate reports to gain visibility into activity and meet compliance requirements. New Event Tagging functionality streamlines the management of high-volume events and enables workflow of incident response.

SECURITY CENTER

The Security Center is a dedicated team of security experts who help customers stay ahead of the latest threats by rapidly developing and delivering security updates that address newly discovered vulnerabilities. The Security Center manages the customer portal used for accessing these security updates and information. Security updates can be delivered to Deep Security Manager automatically or on-demand for deployment to thousands of servers within minutes.

VII. WHY TREND MICRO

Focused on threat management since its founding 20 years ago, Trend Micro provides virtual patching capabilities to protect against threats targeting the vast diversity of systems in today's enterprises. Trend Micro continues to provide innovation with the Smart Protection Network, correlating real-time data on new and unknown threats and delivering continuously updated protection.

With over one billion U.S. dollars in annual revenue, over 1,000 threat researchers—and over 4,000 employees—around the world, Trend Micro has the size, the speed, and the unique in-the-cloud core technology infrastructure required to handle today's enterprise security. No other security vendor can match the strengths Trend Micro offers enterprises. That is why thousands of enterprises around the globe continue to put their trust in Trend Micro.

VIII. CONCLUSION

Trend Micro Deep Security provides advanced protection for servers in the dynamic datacenter, whether physical, virtual or in the cloud. Deep Security combines intrusion detection and prevention, firewall, integrity monitoring and log inspection capabilities in a single, centrally managed software agent.

Deep Security enables IT operations to better manage systems and improve compliance by protecting vulnerable and Out of Support systems by extending the timeframe available to IT operations to deploy patches. Deep Security protects confidential data and critical applications to help prevent data breaches and ensure business continuity, while enabling compliance with important standards and regulations such as PCI, FISMA and HIPAA. Whether implemented as software, virtual appliance, or in a hybrid approach, this solution equips enterprises to identify suspicious activity and behavior, and take proactive or preventive measures to ensure the security of the datacenter.

Used in conjunction with traditional security and patch management solutions, Trend Micro Deep Security adds an essential extra layer of protection for the enterprise's most vulnerable systems.

For more information please call us at **+1-877-21-TREND** or visit **www.trendmicro.com/virtualpartching**

REFERENCES

[1] NIST publishes the federal government's guidelines for patch management at http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

[2] "Analytics Report: Global Threat, Local Pain: 2010 Strategy Security Survey", Information Week

[3] The Payment Card Industry Data Security Standard (PCI DSS) requires up-to-date security patches within one month of release (Req. 6.1).

[4] See also 'ISO/IEC 13335-4 Information technology' framework, "ISPE25, CISWG Information Security Program Elements" (US Federal security requirement), and IT UCF, "Establish and maintain a software change management (including patching) metrics management program." http://www.unifiedcompliance.com//matrices/live/02081.html

[5] Securely Using Windows 2000 After Support Ends, Neil MacDonald, Gartner Research Note G00205521 dated July 10, 2010

[6] "Plan for the End of Support of Windows 2000", Gartner; Michael A. Silver, Neil MacDonald; Publication Date: 14 September 2009 ID Number: G00170059

[7] "Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0", US National Institute of Standards and Technology; http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf

[8] "2009 Data Breach Investigations Supplemental Report - A study conducted by the Verizon Business RISK team", page 4