



# Leverage IPS to Make Patch Tuesday Just Another Day

# Contents

Introduction .....	3
Evolution of a Practice .....	3
Weaknesses of the Model .....	4
Lack of timeliness .....	4
Inherent predictability .....	4
Painful disruptions .....	5
A Better Approach .....	5

## Introduction

Ask a network administrator to list the things that cause him or her the most stress, and the answer will likely include security patching and Patch Tuesday.

Thanks in part to Microsoft, which uses the second Tuesday of every month to distribute patches for a variety of software programs, the day has become known among technologists as 'Patch Tuesday.' While this patching schedule has many benefits for beleaguered administrators, it creates a situation in which they must struggle to address multiple vulnerabilities in a very short period of time, or risk their network's security.

Responsible administrators struggle to patch in a timely fashion without disrupting their networks, but patching all of an organization's assets takes time. Server patches must be tested before deploying. Endpoint patching is further slowed by logistics, since administrators don't have direct possession or control of end-point devices and there may be a diversity of software versions. Administrators want to limit this vulnerable period between the availability and the complete deployment of the patch.

This white paper discusses the inherent challenges of Patch Tuesdays, and the need for the complimentary, pre-emptive protections offered by intrusion prevention systems (IPS). While patching is still necessary, an IPS can help make the process less disruptive and solve many of the security problems associated with patching delays.

## Evolution of a Practice

Tuesdays didn't become Patch Tuesdays overnight. Starting with the Windows 98 operating system, Microsoft included a 'Windows Update' process that automatically checked for patches to Windows and all of its components.

In general, this updating strategy suffered from two problems that affected users at opposite ends of the scale. Less experienced users were not aware of the update function and did not run it. More experienced users at large companies found the function difficult to manage, since it became increasingly difficult to make sure various systems across a particular network were all up-to-date.

Under the new Patch Tuesday process, Microsoft accumulates new security patches over the course of each month, and then dispatches all of them at once on the second Tuesday of the month. This allows system administrators to prepare for the testing and deployment of the patches. Patch Tuesday was a major step forward for security, allowing a more controlled patching process for which administrators could plan and prepare.

Not surprisingly, other vendors have jumped on the bandwagon. At last check, more than two dozen major vendors were distributing patches of some sort on the second Tuesday of every month. While the Patch Tuesday strategy helps to keep networks up to date in a manageable fashion, it also has its own set of shortcomings which need to be addressed.

### Check Point provides the protection advantages detailed in this document:

- **IPS Software Blade**—Complete, integrated IPS protection and industry-leading performance
- **IPS-1**—Standalone, dedicated IPS
- **SmartDefense**—IPS capabilities integrated into core Check Point security gateways
- **SmartDefense Services**—Protection updates for SmartDefense and other Check Point products

### Weaknesses of the Model

While patching and Patch Tuesday is an important part of any responsible organization's security practices, it is not infallible. Despite all the effort by administrators to patch systems, networks are still vulnerable.

According to a recent report by Verizon Business, most breaches are not detected until months after the fact, and are often not promptly remedied<sup>1</sup>. This translates into months, if not years, of exposure.

The answers lie in the inherent shortcomings of scheduled patching. Patch Tuesday presents three major challenges: it isn't timely, it gives hackers a roadmap to attack, and it's disruptive to everyday network operations. Overall, the main problem with Patch Tuesday is that while patching is a necessary part of good security practices, it is not a complete solution to the problems that vulnerabilities present.

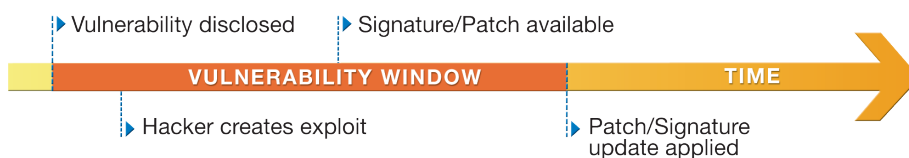
#### Lack of timeliness

The first major challenge with Patch Tuesday is the issue of timeliness. Since patches are released according to a set schedule, Microsoft and other vendors struggle to have patches ready for the next Patch Tuesday. If a vulnerability is discovered late enough, the patch might not be ready in time and may be withheld until the next Patch Tuesday. This can mean a delay of a month or more. Really thorny vulnerabilities may go unpatched for years.

Microsoft and others have tried to overcome this issue by releasing out-of-cycle patches — unscheduled patches that they release to address critical issues. However, these unscheduled updates send administrators into a tizzy, and once customers return to out-of-cycle patches, everyone is back to scrambling again.

#### Inherent predictability

Another challenge with Patch Tuesday is its inherent predictability. Hackers know organizations receive patches on the second Tuesday of every month, so they use this information to time their attacks for the 'vulnerability window'. This is the period of time between when a vulnerability is found and the time that patches are completely applied across an organization. This is distinct from the time before the patch is available since organizations may not immediately apply them, or may fail to apply them completely across the entire organization<sup>2</sup>.



According to a recent report by Verizon Business, in 71 percent of surveyed security breaches involving known vulnerabilities, the patch that would have prevented exploited vulnerabilities was available for more than one year.

<sup>1</sup> 2008 Data Breach Investigation Report, Verizon Business.

<sup>2</sup> Ibid.

A recent example of how the vulnerability window can be exploited is the Downadup worm. Although protections against this worm had been readily available for months, millions of computers, mainly in enterprise environments, became infected several months after the patch became available.

From a hacker's perspective, preying upon the vulnerability window makes perfect sense.

Some Hackers go to work on the exploits immediately after Patch Tuesday, knowing that most organizations will not manage to apply all of the patches right away. This phenomenon is known as 'Exploit Wednesday'.

What's more, some hackers even wait until just after Patch Tuesday to start exploiting an unknown, undisclosed vulnerability so Microsoft has to wait until the next update to fix it. This further expands the vulnerability window surrounding Patch Tuesday, and could potentially give a hacker over a month to attack vulnerable systems.

### **Painful disruptions**

The third major challenge with Patch Tuesday is that it can be painfully disruptive to network operations. Until a patch is applied across an entire organization, protection is incomplete. Miss one patch on one machine and the entire organization is possibly at risk. With dozens of servers and potentially thousands of endpoint computers at a large organization, it is easy for administrators to overlook patching some critical machines or to simply take time to actually reach every machine. Endpoint computers are not under an administrator's direct control or possession.

What's more, some patches can be incompatible with existing programs — a huge headache for large companies that may have strict software policies and require a rigorous test of patches before deploying them. Other patches require reboots, which can be disruptive to organizations.

In 2007, for instance, Skype experienced a two-day outage following Patch Tuesday. According to company officials, the hiccup was caused by a previously unidentified software bug exposed by an abnormally high number of restarts.

The bottom line: patching is a necessary but painful exercise that still leaves an organization open for attack.

### **A Better Approach**

There are drawbacks to both scheduled and unscheduled patches with advocates on both sides, but the true solution to maximizing network security doesn't lie exclusively in patching. While a sensible, well-managed patching strategy is still a must, the weaknesses in the patching strategy can be minimized by implementing a robust Intrusion Prevention System. Such a system detects and blocks threats as they enter a network, before they reach servers and endpoint computers. IPS can detect vulnerabilities in real time, without disruption to the computing environment, and provides a perfect compliment to a well-executed patching program.

Rather than waiting for patches and then frantically trying to apply them across a complex system, an IPS can help in taking a more proactive approach. An IPS quickly provides protection across an organization, giving administrators breathing room to apply patches to servers and endpoint computers across an organization.

In the example of the Downadup worm, mentioned previously, IPS protection against the worm can be configured in minutes, protecting an entire network while administrators work at patching vulnerable computers. Check Point IPS customers were able to apply a protection against this worm the same day the related vulnerability was discovered, months before the worm began to spread.

The better IPSs don't rely solely upon signatures, but rather provide broad-based protection. By protecting against classes of attack, by enforcing the correct and expected use of protocols — rather than blocking signatures for individual attacks — an IPS helps an organization stay a step ahead of hackers.

This kind of protection often means that the system is protected against vulnerability not only before the patch is released, but sometimes even before a vulnerability is discovered or disclosed. While patching is still necessary, having preemptive IPS protections in place means that not only is the vulnerability window slammed shut, but that patch testing and distribution can proceed with less disruption.

In the last year, several very serious DNS vulnerabilities have been disclosed, most notably the Kaminsky and related cache poisoning vulnerabilities. Check Point's IPS products have provided effective defenses against the related exploits since 2004, and continue to add new protections, giving Check Point customers multiple layers of protection.

Also, with centralized management, a good IPS can ensure that all the vulnerable parts of a system are protected. With a few clicks in the management console, a whole organization can be up-to-date with the latest protections.

### Conclusion

By taking this comprehensive approach, which combines robust IPS functionality with a concerted patching strategy, network administrators can better equip themselves to handle Patch Tuesdays and secure the network between updates. Check Point provides a variety of solutions to protect network infrastructures and data, including IPS capabilities on dedicated appliances and full IPS capabilities integrated into comprehensive security gateways. Check Point's integrated solutions include SmartDefense Services and the Check Point IPS Software Blade. Customers interested in a dedicated IPS can use IPS-1. These solutions can compliment your existing patching strategy, resulting in better security and less administrative overhead. Visit the Check Point website for more information on how to get pre-emptive, easy-to-deploy IPS protection that defends your network before the patch.



## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

### CHECK POINT OFFICES

#### Worldwide Headquarters

5 Ha'Solelim Street  
Tel Aviv 67897, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-624-1100  
email: [info@checkpoint.com](mailto:info@checkpoint.com)

#### U.S. Headquarters

800 Bridge Parkway  
Redwood City, CA 94065  
Tel: 800-429-4391 ; 650-628-2000  
Fax: 650-654-4233  
URL: <http://www.checkpoint.com>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMSecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.