



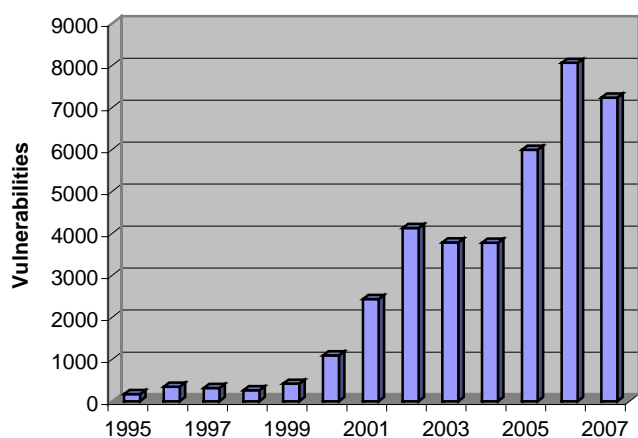
Proactive Patch Management

Even the Best Software Sometimes Needs Patching	2
The Reality Behind Most Virus Outbreaks	2
The Patch Management Cycle	3
Essential Elements of a Good Patch Management Solution	3
Conditions for a Patch Management Solution To Be Effective	4
The Consequences of No Patch Management	4
The ROI for Automated Patch Management	5
Benefits of LANrev Automated Patch Management	6
Conclusion	7



Even the Best Software Sometimes Needs Patching

Software flaws that compromise the security of the system are often referred to as vulnerabilities. As the complexity and source code for modern operating systems has grown dramatically so has the number of vulnerabilities in the OS. The CERT Coordination Center estimates that software vulnerabilities have grown in number from 171 in 1995 to 8,064 in 2006¹. If past history is any indicator this number will only get bigger in the future.



Year	Vulnerabilities	Year	Vulnerabilities
1995	171	2002	4129
1996	345	2003	3784
1997	311	2004	3780
1998	262	2005	5990
1999	417	2006	8064
2000	1090	2007	7236
2001	2437		

When a vulnerability is discovered OS vendors typically release an OS patch referred to as a security update to repair the problem and prevent future security breaches due to exploitation of the vulnerability. According to the CERT Coordination Center, deploying these patches in a timely fashion soon after they become available helps secure the OS and prevent 95% of security breaches. However, many computer systems are often not patched for months or not at all. With virtually all modern workstations being attached to a local area network with Internet access, leaving them inadequately patched is not an option.

The Reality Behind Most Virus Outbreaks

Unpatched computers are a major security problem because viruses often take advantage of these vulnerabilities to infect them. The 2006 Computer Security Institute/FBI Computer Crime and Security Survey reports that virus contamination continues to be the number one source of financial losses for enterprises and accounts for 30% of financial losses due to security breaches². Even more alarming is the advent of "zero-day" exploits where an exploit is written to take advantage of the vulnerability before or within 24 hours of its discovery. Luckily zero-day exploits are the exception rather than the norm. In reality, most viruses take advantage of known vulnerabilities that have already been patched by the OS vendor but whose associated security update has yet to be deployed. For example, the Slammer virus, which reportedly took down a 911 call center, airline booking systems, and ATM machines exploited a known vulnerability that Microsoft had provided a patch for six months prior. The same was true for the now infamous Nimda worm. It took advantage of an already known and patched vulnerability that Microsoft had provided a security update for a month before. Code Red, Blaster, and MyDoom – all these viruses exploited known vulnerabilities for which there was a patch or some other known fix.

As the complexity of modern operating systems has advanced so has the technology hackers use to create viruses and worms. Often exploitation tools are posted on the Internet that allows even novice programmers such as "script kiddies", who have little or no knowledge, to create a computer virus with just a few clicks. Because of the interconnectivity of modern networks, viruses can quickly infect a significant number of computers within minutes or hours. All it takes is single person to open an email containing the virus to potentially infect all unpatched computers on an entire network.

This underscores the importance of keeping your enterprise's workstations up to date with the latest OS patches. Patches, as a preventative measure, are only useful if you deploy them before your workstations become infected. Thanks to incidents like those mentioned above, patch management is now at the forefront of many organizations' security focus since they want to avoid the downtime and expense of an infestation. The premise of patch management is to be proactive in deploying available patches before you have a virus or hacker attack to prevent these from happening in the first



place. It's far less expensive in terms of cost and user downtime to prevent these than to fix them afterwards. But being proactive implies you are patching systems that are currently functioning normally. Doing this could potentially create problems so why take the risk? It's been shown that proactive patch management reduces unplanned downtime and allows you to test and plan ahead. It's much easier to manage the known risk of a bad patch than the unknown risk of a virus outbreak or hacker attack. Being reactive is simply not an option because by that point it's too late. Even if you repair a machine after it's been infected or hacked it can simply be infected or hacked again unless you apply the security update for vulnerability to all your client machines.

So this begs the question, why don't enterprises apply patches when OS and software vendors make them available? One reason is that it's hard to keep up with new patch releases. With today's shrinking IT budgets, overwhelmed IT staff just don't have the resources or time to continually check OS vendor sites for new patches. Many corporations don't want to deploy a patch until they've had a chance to test the patch themselves in their own environment. It's important to make sure that a patch does not break any of your other mission critical applications. However, this must be done within a reasonably short time frame. Waiting too long can result in even more dire consequences. Keep in mind that these patches have already been tested to some degree by the OS or software vendors themselves. An unintended conflict with an application might make just that application unavailable while a virus infection, on the other hand, could make the entire workstation unusable.

The Patch Management Cycle

Effective patch management is a complicated cycle that involves several stages. The solution you choose must be able help you with each of these.

1. Inventory and assessment - Identify missing patches and the computers that need them. You also need to determine which computers already have them installed, as well as get a count of computers missing each patch.
2. Patch testing - For the most part, a lot of testing has already been done for you by the OS vendor but they cannot account for every application since everyone's computing application environment is different. They may

not always catch every conflict. So it still makes sense to do a test deployment on a subset of machines to discover any conflicts with applications specifically used by your company.

3. Deployment - Distribute the patches to your live environment after confirming there are no conflicts with any of your existing applications.
4. Verification - Verify that the patch installed correctly, is present, and is no longer needed by the target computers.

Essential Elements of a Good Patch Management Solution

Due of increased awareness of the importance of keeping clients up to date with patches, the patch management space is crowded with both dedicated patch management products and client management suite with a patch management component. Before selecting a patch management solution you must take into account several factors to determine which one best fits your needs.

1. Patch management tools can be either agentless/scanner-based or agent-based. By definition agentless or scanner-based tools have no deployment costs and do not require you to install any kind of client. The drawback is that they often do not catch laptops or other systems that are either off the network or asleep at the time of the scan. Active agent-based products do not have this problem and can generate significantly less network traffic.
2. Does your computing environment include more than just one platform? Chances are the answer is yes since there are very few homogeneous sites with just only Windows or only Mac workstations. A Yankee Group survey of 700 IT professionals and executives found that 8 out of 10 companies use Macs in their enterprise³. If this is the case, your patch management solution will need to support patching both Windows and Mac OS X.
3. The proposed solution must not only be able to deploy the required patches but also report which ones and how many are missing on client machines so you can accurately gauge the severity of the problem. In addition it must also be able to report on the deployment status of assigned patches.
4. Trying to keep up with patch releases is practically a full time job and most IT departments simply do not have the time and resources to constantly monitor the OS



vendors' web sites for new patches. Your patch management system should be able to automatically generate new OS patches for you in a reasonable amount of time without any intervention so that you only have to decide which ones to deploy and which ones to reject.

5. Your chosen solution must also be more efficient at deploying the selected patches and use less bandwidth than the built-in OS update mechanisms. Otherwise why wouldn't you use what's built into the OS. The system should not generate patch packages that no client is missing since that would just be a waste of bandwidth and hard disk resources. In a distributed environment the system must also be able to deploy patches from multiple locations so that clients get their patches from a site that's closest to them, reducing the network load on your WAN connections.
6. Your patch management solution must be flexible enough to let you target patches to a test group first before deploying it to your entire network. Otherwise how will you test the patch first before deploying it to your live environment? It must also allow you to select which patches to deploy and which ones to reject. It's important that you test each patch against all known system configurations in a test group before deploying to your production environment. This lets you ferret out potential application incompatibilities and conflicts that the OS or software vendor was unable to or did not have the time to test for. What you want to avoid is deploying a patch that does more harm than good to end users' machines. Pressure on a software vendor to release a security update for a known vulnerability in a timely fashion can sometimes lead to hastily released patches that can degrade system performance.
7. The patch management system must also be able to exempt particular client machines from a patch if it's determined that there's an application conflict with a patch.

Conditions for a Patch Management Solution To Be Effective

For a patch management solution to be successful and have a meaningful impact at your organization some business conditions must be met.

The complexity of patch management can sometimes make it an overwhelming and daunting subject but it's one that every organization must

deal with. To make it more manageable you need to add structure to the patch management policy that accompanies your patch management solution. It should outline the details of who is responsible for what, when you need to apply a patch, and how you're going to do it. Having a well laid out patch management process can often compensate for a shortage of resources or time.

The executive team must acknowledge the risk of unpatched systems and recognize the corresponding benefits of having a patch management system in place. Without leadership from the top, any patch management solution is doomed to fail, either due to a lack of funding or enforcement. With buyoff from upper management you can standardize on patch management policies and procedures that everyone must follow. This makes it much easier to implement a patch management solution successfully throughout your organization.

You must also have a current inventory of all your workstations. If you don't know what computers you own then how will you know whether they are patched adequately or not? Having an automated asset inventory system in place is essential for this, as well as knowing which machines are missing what OS patches. Your inventory solution must also know what OS and third party applications are installed on client systems if you are to patch them. It should be able to automatically target just the affected target systems while also being able to exempt others that may have a known conflict. For OS patches, the patch management system must be able to determine whether a target needs a patch or not before installing it. For third party applications, it should be able to target only systems that actually have the application installed.

Your IT staff should have clearly defined responsibilities so that the task of investigating, testing, and approving patches is assigned to a specific person or team. These individuals must possess the skills and knowledge to be able to identify new vulnerabilities and their associated security updates as they become known.

The Consequences of No Patch Management

In today's complex networks an unpatched system is not just a danger to itself but a problem for your entire network. You could manually patch workstations but this is unworkable due to its labor



intensive nature. Consider the following potential consequences of not having a patch management system in place and your computer network is compromised.

1. A significant drop in employee productivity as a result of computer downtime - If mission critical systems are affected it may lead to a loss in business due to an inability to complete business transactions. End users whose workstations become unusable are essentially unable to work during the time it takes to recover their machines. Limited IT department time and resources are used up fixing compromised machines.
2. Loss of proprietary intellectual data or confidential customer data - Could your company withstand the negative publicity and potential lawsuits? Loss of intellectual data can lead to a decline in competitiveness while potential lawsuits from customer data loss directly impact on your bottom line.
3. Loss of business from partners or customers due to a decline in credibility or a drop in confidence in your company's security - Few people want to do business with an organization if they believe their personal or corporate data is at risk.
4. Remediation time to fix compromised computer systems - In the case of virus attacks this can often mean having to rebuild the workstation from scratch by reinstalling the entire OS. During this period they are obviously unusable. Unless you have loaner systems available these end users are essentially unproductive while their computers are being fixed.
5. Potential loss or corruption of user data - This can either be the result of a virus outbreak or hacker attack itself or from the associated attempts to repair the system after the attack.

The ROI for Automated Patch Management

The National Institute of Standards and Technology (NIST) recommends all organizations consider implementing an automated enterprise patch management solution. NIST worked out the costs for recovering from outbreaks, manually patching client machines to prevent an outbreak, and automatically patching machines to prevent an outbreak. Below are estimates for each of these options for a company with 1,000 computers. Educated guesses have been made that a) 1/2 of unpatched computers will become infected and that

b) 10 out of 20 patches released will be for vulnerabilities exploitable by a virus. The formulas and calculations used below are derived from those used by the NIST but have been modified⁴.

Costs for recovering from outbreaks

$$\text{Annual Cost} = W \times T \times I \times R$$

$$\$1,600,000/\text{yr} = 500 \times 8 \text{ hrs/inf} \times 10 \text{ infs/yr} \times \$40/\text{hr}$$

W = 500 = number of workstations

T = 8 = time fixing systems or lost in productivity

I = 10 = number of times machine is infected

R = 40 = hourly rate of IT technician/employee

The following assumptions have been made.

- Each infected computer costs 8 hours of downtime, 4 for IT to rebuild it and 4 in lost end user productivity.
- Hourly rate of \$40/hour for IT staff and employee salary.
- Computers will be infected 1/2 of the time there is a vulnerability, so 10 times a year.

Costs for manually patching computers

$$\text{Annual Cost} = W \times R (C + P)$$

$$\$932,000/\text{yr} = 500 \times \$40/\text{hr} \times (43.3 \text{ hrs/yr} + 3.3 \text{ hrs/yr})$$

W = 500 = number of workstations

C = 43.3 = time to check for patches per year

P = 3.3 = time to apply patches for one year

R = 40 = hourly rate of IT technician

The following assumptions have been made.

- Checking for new OS patches takes 10 minutes per day.
 $10 \text{ mins/business day} \times 5 \text{ business days/wk} \times 52 \text{ wks/yr} \times 1\text{hr}/60 \text{ mins} = 43.3 \text{ hrs/yr}$
- Applying a patch takes 10 minutes. 20 OS patches are released in a year.
 $10 \text{ mins/patch} \times 20 \text{ patches/yr} \times 1\text{hr}/60\text{mins} = 3.3 \text{ hrs/yr}$

Costs for automated patch management solution

$$\text{Annual Cost} = S + A$$

$$\$119,200/\text{yr} = \$36,000/\text{year} + \$83,200/\text{year}$$

S = cost of software [purchase price + maintenance]

$$500 \text{ wkstn} \times (\$60/\text{yr} + \$12/\text{yr}) = \$36,000/\text{yr}$$

A = salary of administrator to manage solution

$$40 \text{ hrs/wk} \times 52 \text{ wks/yr} \times \$40/\text{hr} = \$83,200/\text{yr}$$

The following assumptions have been made.

- The price for the patch management software is \$60/seat.
- Maintenance for the patch management software is 20% of the purchase price.

Cost comparison summary

No patch management	\$1,600,000/yr
Manually patching computers	\$932,000/yr
Automated patch management solution	\$119,200/yr



As you can see, the most cost effective solution is, as the NIST recommends, to implement a patch management system. Keep in mind that there is a point at which it can actually become more expensive to manually patch client machines than to actually deal with the results of a mass infection. This can occur if the number of vulnerabilities that lead to an outbreak become significant lower than the number of patches to be deployed. Under all circumstances an automated patch management system is the always least expensive route.

Benefits of LANrev Automated Patch Management

LANrev's automated patch management features unparalleled simplicity and ease of use. Once you enroll clients in patch management they will automatically download and generate software patch packages and upload them to LANrev without user intervention as long as at least one client needs them. Regardless of how many clients need a particular patch, it's only downloaded once directly from either Microsoft or Apple. For example, if 1,000 of your client machines needed the same patch, it's only downloaded one time by LANrev. Unneeded patches are simply ignored. Clients not enrolled in patch management are exempt and will not attempt to install a patch even if you assign one to them. This provides a way for you to exclude particular client machines from LANrev patch management as needed.

Once patches appear in the Unconfirmed Patches section you simply assign them to a particular distribution group to deploy them. It's that easy. LANrev is intelligent about which patches it installs so you can assign a patch to either All Macs or all PCs and they will only install on agent machines that actually need them. Assigning patches to these default distribution groups essentially sets a baseline patch level for all your client machines. Clients simply ignore assigned patches they don't need. You don't have to worry about assigning patches to the wrong clients or redundantly installing a patch when end-users manually update their system.

LANrev patch management is flexible enough to let you assign patches to an arbitrary group of machines or a group that fits a particular set of selection criteria. To test patches simply assign them to a small distribution group of test machines to check for application conflicts before deploying them to your entire production environment.

LANrev's smart distribution group architecture also lets you exclude specific machines in case they have a software conflict with a particular patch.

For enterprises with large networks and multiple sites, LANrev's distributed staging server architecture ensures that assigned patches are only sent once to each site regardless of how many clients at the site have been assigned those patches. For example, if you have 3 sites, an assigned patch is only replicated twice, once from the master site to each of the two secondary sites. The assigned patches are then distributed to clients from a local staging server on the same network segment as them. LANrev also allows you to throttle the bandwidth for this replication process between sites, as well as for the actual software distribution itself, to minimize its impact on your network. Additionally you can set a time window for the replication of patch packages so that it occurs outside of business hours.

LANrev also provides Missing OS Patches reports on how many clients, as well as which clients, are missing what patches. Installed Software reports can tell you how many and which clients have a particular OS patch installed. After a patch is deployed with LANrev, Installation Status reports provide an audit trail on whether the patch installation is in progress, installed successfully, or failed (along with an error message).

To further minimize the disturbance to users during the patch deployment process LANrev also has options for setting a time window for installation and for forcing installations to occur at startup/login or only when the local user is not logged in. For optional non-critical patches you can even let your end users defer them (with an optional time limit) if needed.

For third party patches LANrev lets you define your own custom software packages for deployment. Installation conditions can be used to add intelligence to the custom packages for third party patches, ensuring that they only install on client machines where the application to be patched is actually installed and still unpatched. This prevents patches from installing on machines that either don't have the application installed or are already sufficiently patched.

In the event that your network has already been breached and you know the nature of the attack LANrev's custom information items provide a quick and easy way to discover which computers on your



network have been compromised. You can then protect the remainder of your network by quarantining these infected machines to a particular network segment.

While OS patches have been tested by the OS vendor they cannot catch all conflicts since everyone's computing application environment is different. Some patch management vendors charge a subscription fee to access patches that have been tested and vetted by them. The added value that you're paying for this though is minimal because there's little chance that their test computing environment is identical to yours. In some client management suites, patch management is an extra add-on module that you must pay for separately. With LANrev there is no add-on or recurring subscription fee for its automated patch management because it's already included.

LANrev is one of the few cross-platform patch management solutions that supports both Windows and Mac OS X. Unlike some of its competitors LANrev is an all inclusive client management suite. So while you may purchase LANrev for its cross-platform patch management you'll also benefit from its many other cross-platform features including asset inventory, software distribution, disk imaging

(Mac only), power management, remote configuration, and computer theft tracking and recovery.

Conclusion

Having a proactive patch management system in place, along with a comprehensive patch management policy, can provide immediate and tangible benefits for both your enterprise and its end users. Greatly reduced downtime, lower rates of virus infection or hacker attacks, and less resources spent on fixing client machines are all benefits that any CIO can get behind. Patch management can understandably be a cumbersome and daunting task that can leave many IT staff dazed. With the right patch management system, it doesn't have to be this way. A product like LANrev can automate virtually all of this for you including missing OS patch reporting, patch generation, patch deployment, and patch deployment status reporting. Proactive patch management leads to considerably lower unexpected downtime, happier end users, and significant cost savings, all of which can put a smile on your CIOs face.



-
- ¹ http://www.cert.org/stats/vulnerability_remediation.html
 - ² http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
 - ³ <http://www.yankeegroup.com/pressReleaseDetail.do?actionType=getDetailPressRelease&ID=2394>
 - ⁴ <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

About LANrev

LANrev was founded by industry veterans with a vision for comprehensive, yet simple systems management tools. Our mission is to develop software that supports modern, heterogeneous systems and networks, using platform-neutral functionality and adaptive architecture. LANrev empowers administrators without burdening them, by providing comprehensive management solutions that are both affordable and easy to deploy, configure, and maintain. This allows corporate, educational, and government enterprises to leverage their current infrastructure while offering higher levels of helpdesk service.

United States

LANrev LP
4287 Beltline Road, #308
Addison, TX 75001
Telephone: (214) 459-0136
Fax: (214) 276-1350
info@lanrev.com

Europe

Pole Position Software GmbH
Weingasse 26
91077 Neunkirchen am Brand
Germany
Telephone: +49-9134-99420
Fax: +49-9134-997911
info@lanrev.com

Copyright ©2008 LANrev

Provided for informational purposes only. LANrev is a trademark of LANrev. All other trademarks, company names, and product names mentioned herein are used for identification only and are the property of their respective owners.