

*Reference Guide
White Paper Series*

Systems Management for Small
and Medium-Size Businesses,
Agencies, and Institutions

By Joel Shore
December 2004

EXECUTIVE SUMMARY

Businesses, government agencies, and educational institutions of every size must maintain key aspects of their data networks. Timely download and installation of patches to guard against outside attacks is critical. Internal protection against unauthorized employee-installed applications is essential. Compliance is vital in protecting the company against legal exposure from using unlicensed copies of commercial software. And deploying new software or major upgrades demands efficient best practices.

Corporations and enterprises, with their large IT staffs and budgets, can choose from several high-end tools to automate patch management, inventory and license compliance, and software deployment. Small and medium-size businesses and government agencies with 2,000 or fewer employees have similar needs but limited resources, requiring a systems management solution that is affordable and easily installed, requiring minimal administrative resources. This paper examines a systems management solution for small and medium businesses from Executive Software.

INTRODUCTION

In network safety, size doesn't matter. Whether your company has 10 computers, a hundred, or a thousand, it's vital to apply

security updates as they are issued, prohibit the use of unauthorized software, ensure that the instances of installed applications do not exceed the number of purchased licenses, and install application upgrades efficiently.

Fail for a moment to perform these systems management tasks and you jeopardize the business itself: mission-critical data stolen through security breaches, network crashes caused by incompatible software, ruinous legal exposure from using pirated software, and wasteful software deployment practices.

Large corporations and public-sector agencies deal with these very same issues, but on a larger scale. The key difference is that their well-staffed IT departments use high-end, complex systems management tools best suited for enterprises with thousands of computers installed worldwide. These tools often require dedicated servers and administrative staff. They are too expensive and too complicated for small and medium-size businesses (SMBs), local and state government agencies, and most educational institutions.

It doesn't have to be that way. Even if yours is among the four million American businesses that have fewer than 1,000 employees, your systems management needs are no less crucial; it's only the scope of the challenge—and budget—that differ. After all, fewer than 7,000 companies in the United States have more than 1,000 employees, according to the U.S. Census Bureau. That leads to an inescapable fact: The business of America is small business. And your small-business network deserves equal protection.

To maintain systems health, SMBs require tools that are affordable, require no dedicated server, and no dedicated staff. Systems management for SMBs should be easily installed and, once configured, run in a set-it-and-forget-it mode that requires only the slightest administrator intervention.

U.S. Business Size by Employee Base

Employees	Companies
1 to 99	4,121,841
100 to 499	65,482
500 to 999	6,279
1,000 to 4,999	5,367
5,000 to 9,999	684
10,000 and up	668

Source: U.S. Census Bureau
www.census.gov/epcd/www/smallbus.html

This report was sponsored by Executive Software, however, the sponsor had no input into the content of this report, conclusions reached, or opinions expressed by Reference Guide Testing Laboratories.

And one other, but significant differentiator exists: enterprise-grade systems management platforms often require the deployment of an “agent” on each user’s computer. A small program that usually is present in memory, an agent performs specific tasks and reports its results, in this case, to the enterprise systems management application, most likely resident on one or more dedicated servers. Once results are reported, the server-based program swings into action, performing whatever actions are needed. Though such an arrangement makes sense when many thousands of computers are involved, it’s neither necessary nor desirable for smaller networks. Agents complicate setup, requiring a time-consuming software deployment to every computer, certainly not the best use of an SMB’s valuable technology resources.

This paper examines the three key components that together form a comprehensive systems management environment: patch management, rogue software detection and license compliance, and software deployment.

The 1,090 security vulnerabilities cited by the federally funded CERT Coordination Center in 2000 exploded to nearly 3,000 in 2004

THE PATCHWORK QUILT

It doesn’t take an expert to know that security is the top concern of IT professionals in multinational enterprises. Small businesses, and even home offices, are no different. There’s good reason to be concerned: The 1,090 security vulnerabilities cited by the federally funded CERT Coordination Center in 2000 exploded to nearly 3,000 in 2004.

But there’s more. Not only is the number of vulnerabilities rising, the speed at which they replicate is growing ever faster. In 2001, the “Code Red” worm doubled its infection rate every 37 minutes. Bad enough. But in 2003, the “Slammer” worm doubled the number of systems it infected every 8.5 *seconds*. The result was millions of computers, and the data they contained, compromised. With the Blaster, MyDoom, and Melissa exploits only recently past, and others sure to come, the task of keeping your organization’s computers updated with the latest security patches demands unprecedented—and seemingly superhuman—diligence.

SMBs aren't keeping up. Security auditing firms, essentially companies paid to break into corporate networks, are nearly unanimous in identifying the single most common cause of security breaches: failure to keep systems current with security updates and patches.

Omit one critical security patch, and your entire network—and the business itself—are at risk.

The solution seems simple enough: Download and apply patches to each server, desktop, and mobile PC. But in practice, it's anything but simple. In fact, it's more like the impossible dream.

Since the debut of the Windows XP operating system in October 2001, Microsoft has released hundreds of patches and updates. Deciding which to install on each system and keeping track of them is no easy task. While many patches address security issues, others are simply feature add-ins or bug fixes for various applications. If the patch is security related, it is assigned a severity level of critical, important, moderate, or low, depending on the vulnerability being addressed. Some patches are issued more than once. Others are modified and then re-issued. Finally, patches released individually over time are sometimes collected and rolled into so-called cumulative patches.

Even for an individual who has a single PC to manage, determining which patches are necessary and which are not requires a significant investment in time. In an environment with even just a few dozen systems to manage, the complexity quickly becomes overwhelming.

In enterprises with thousands of computers, patch management is handled with high-end software tools. Available from a variety of vendors, including Microsoft, these tools generally require a dedicated server, specialized training, and often a full-time administrator. Though the expense of such a solution is more easily absorbed within the scope of a large IT department, the cost and administrative overhead is prohibitive for most SMBs, government agencies, and educational institutions.

In 2001, the “Code Red” worm doubled its infection rate every 37 minutes. By 2003, “Slammer” doubled every 8.5 seconds.

What's needed is an affordable, automated patch-management solution conceived with the needs and constraints of small and mid-size organizations in mind. Such a solution would not require an expensive dedicated server, costly training certification process, or full-time administrator. An ideal solution would install quickly, automatically survey each system on the network, and keep track of patches with minimal administrative intervention.

The Patchkeeper module of Executive Software's Sitekeeper systems management suite meets these requirements.

Patchkeeper manages the collection and deployment of security patches. It finds, downloads, and deploys software updates to each system on the network, whether it's one or more than one thousand. Perhaps most importantly, Patchkeeper scans the network, determining for each computer which patches have been installed, which are missing, and which are not necessary. Missing patches can be installed automatically, with no administrator action required, or patches can be installed on test systems only until the administrator approves them for site-wide rollout.

With the critical task of patch management under control, the second phase of overall systems management comes into play: software inventory control and license compliance.

KEEPING TRACK

Maintaining tight control of your network requires two separate, but equally vital, management initiatives: prohibiting the use of unapproved software and ensuring that every installed application is legitimate. Sitekeeper's Inventory and License Compliance module is a powerful tool that provides these capabilities.

It's common for users to install their favorite applications and utilities. These might include peer-to-peer clients for downloading music files and other software, instant-messaging applications, or on-screen "ticker tapes" for displaying news headlines. The problem with these applica-

During March 2002, fewer than 9,000 spyware incidents were reported to one tracking Web site. In March 2004, the number soared to 532,000.

tions is not in their primary function, but what lies “under the hood,” unseen by the user.

Seemingly innocent on the surface, these applications are notorious for the performance troubles and security woes they cause. A music-swapping program might contain spyware that logs every keystroke on that system, capturing user passwords, credit-card numbers, and other proprietary data which it sends periodically to a cyber-thief. Another program may pop up advertisements every few minutes. Not only do these programs create a security risk, they consume valuable network bandwidth, consuming resources and slowing access for every other system.

Programs that contain spyware are seemingly everywhere. According to an April 2004 report in *Computerworld*, an industry newsweekly, fewer than 9,000 spyware incidents were reported by users to one Web site in March 2002. Just two years later, in March 2004, the number of spyware incidents reported soared to nearly 532,000.

Despite admonishments to users against installing unauthorized software, the warnings are often ignored. Users had little to fear: until the advent of powerful systems management software, it was impossible to restrict these programs from use. With Sitekeeper’s software inventory capability, this is no longer the case.

Sitekeeper does not look for spyware, but its inventory scans provide a means whereby system administrators can monitor what’s installed on specific systems. For example, systems used by individuals known to be careless about what they install, or users whose privileges allow them to install software, can be organized into logical groups that are scanned and monitored more aggressively than the rest of the network.

Perhaps even more dangerous is software that is being used illegally. It’s simple: if you can’t prove that each installed copy of a word-processing, spreadsheet, CAD, e-mail, or any other application has been bought and paid for, you are considered to be running pirated software.

In a 2003 study, the Business Software Alliance reported that 22 percent of the software used in the United States is unlicensed, a loss of \$6.5 billion to the software industry

The use of unlicensed software is a serious problem with dire legal consequences. In a 2003 study, the Business Software Alliance, a software industry trade group, reported that 22 percent of the software used in the United States is unlicensed, representing a loss of \$6.5 billion to the software industry.

But it's not just the software companies that suffer. Businesses caught using unlicensed software, whether deliberate or due to poor record keeping, are subject to severe legal and financial consequences.

Consider Oct. 12, 2004. On that one day, the Business Software Alliance collected \$2.2 million in settlements from several companies found to be using unlicensed software. One well-known New York hotel coughed up \$147,500 after an audit revealed it had unlicensed copies of applications and utilities on its computers. A small designer of trade show exhibits agreed to pay a penalty of \$45,000 after an audit revealed it had unlicensed CAD and other applications software on its systems.

To protect against legal and financial exposure brought on by software piracy, it's essential to know precisely what software is installed on every computer

To protect against legal and financial exposure brought on by software piracy, it's essential to examine each computer in the network and know precisely what software is installed.

The Inventory and License Compliance module of Executive Software's Sitekeeper systems management suite provides this capability. From the system on which it installed, the compliance module scans and reports what is installed on each computer, providing the information necessary to zero in on unauthorized software. The module is self-contained and requires no reporting-agent software to be present on each user PC.

© 2004 Reference Guide. All rights reserved. Reproduction without express written permission is prohibited. Reference Guide is an independent entity that makes no endorsement of the companies, products, or technologies discussed in its reports. For additional information regarding product evaluations, white papers, permission to quote, analyst commentary, or reprint inquiries, contact Reference Guide Testing Laboratories via e-mail at info@rgtl.net. Reference Guide, Reference Guide Testing Laboratories, Reference Guide Product Review Series, Reference Guide White Paper Series, Reference Guide Acquisition Index, the Reference Guide logo, and RGTI are trademarks or registered trademarks of Reference Guide. Sitekeeper is a trademark of Executive Software. All other company and product names and logos are trademarks or registered trademarks of their respective owners. Information in this report is believed to be accurate as of its date of publication, however Reference Guide shall not be held responsible for typographical or factual errors.

Scans can be run on demand or on a predetermined schedule, and logical groups can be defined, ensuring that the systems of known troublemakers are scanned more often. Systems can be managed by domain, IP address range, or Active Directory.

With the ability to clamp down on the use of unauthorized software and maintain license compliance in place, it's now possible to examine the last component of a comprehensive systems management environment: Company-wide operating system or application upgrades.

SNEAKERNET GETS THE BOOT

It's one thing to remotely gather and centrally maintain an inventory of the software installed on each computer, but what happens when the time comes to roll out a new version of Microsoft Office, Corel WordPerfect Office, Adobe Photoshop, or Autodesk AutoCAD?

Years ago, the only method available for updating applications software was to physically visit each machine with disks in hand, performing an actual hands-on upgrade. It was a slow, unwieldy process that was hardly cost-effective. The travels of a technician from one PC to another gave rise to the term "sneakernet."

For large corporations, sneakernet disappeared years ago, replaced by complex utilities that perform a "push" installation according to a predetermined schedule. Individual machines no longer required an in-person upgrade, conserving valuable IT resources. But in small organizations, sneakernet is alive, if not exactly well.

In organizations with limited IT resources, push installations are equally valuable. Why install the same program five or five hundred times when once is all that's required? The math speaks for itself: If an IT technician earns \$30 an hour, a single 30-minute software installation to a 200-seat network costs your organization \$3,000, not including employee benefits. To upgrade complex desktop applications, such as the Adobe Creative Suite Premium, which ships on six CDs, 30 minutes just won't do.

PushInstaller, the final component of the Executive Software Sitekeeper suite, was built with networks of fewer than 1,000 computers in mind. Easily installed and not needing a dedicated server, PushInstaller is a model of simplicity. An IT technician selects the computers on which the application is to be installed then directs Sitekeeper to the location of the application's installation files. Last, the technician tells Sitekeeper to install immediately or to begin at a scheduled time.

In addition to providing an efficient means for upgrading existing systems, PushInstaller is well-suited to the deployment of new computers. Once connected to the network, a new computer can have all of its software installed in a single, non-stop operation. The shuttling of CDs into a drive is eliminated. And unlike using disk images, which have to be completely recreated each time your software specification changes, Sitekeeper makes it easy to include new versions or additional software on your new-system installation.

CONCLUSION

Large corporations already make use of large-scale systems management tools to maintain patch integrity, prohibit rogue software, maintain license compliance, and install new software remotely. Small and medium businesses, agencies, and institutions with 1,000 or fewer employees, are equally in need of similar tools but must work within the constraints of a limited budget and a small or non-existent IT staff.

Recognizing the enormity of the market clamoring for similar tools, Executive Software developed Sitekeeper. Implemented as an affordable solution that requires no special equipment, Sitekeeper is easily installed, nearly self-configuring, and frees the IT staff to pursue other projects. For businesses, governmental agencies, and schools with fewer than 1,000 networked computers, Sitekeeper provides an effective means for maintaining network health, ensuring compliance, and deploying applications.

Reference Guide

P.O. Box 725 • Southborough, MA 01772
info@rgtl.net • (508) 397-5550