ENTERPRISE MANAGEMENT
ASSOCIATES®

Don’t Wait to Automate: Achieve Immediate Cost, Productivity, and Security Benefits by Automating IT Management

Highlights

Vendor name: KACE

Product name: KBOX

Product function: KBOX provides an appliance-based IT management solution with full and deep hardware and software inventory; distribution and updating of applications; patch management; remote control; reporting; scripting; security vulnerability auditing; security/IT policy creation and enforcement; and help desk ticket management.

Vendor contact information:
Website: www.kace.com
Email: info@kace.com
Phone: 888-522-3638

Pricing information: Starts at $7500 for 100 managed nodes.

Availability: Immediate

Executive Summary

This Enterprise Management Associates (EMA) whitepaper takes a close look at automated IT management, especially for medium-sized businesses. Examining the problems surrounding software and hardware inventory, asset management, software deployment, and patch distribution, EMA has found that manual IT management causes significant problems, including:

- Higher IT operational and resource costs
- Slower incident response times and poor service to end users
- Lower productivity and increased downtime for both IT and end users
- Reduced control and audit capability
- Increased risk of non-compliance to regulations like Sarbanes-Oxley and HIPAA
- Increased risk of unauthorized access, data loss, or system penetration.

> *“If you’re serious about TCO, then it just makes sense.” – Senior Analyst, Manufacturing Company*

Automation systems for IT management significantly reduce, and in many cases, eliminate these problems. EMA research data shows that businesses with automated solutions spend substantially less time and effort on patch management, Operating System (OS) provisioning, application deployment, security and policy management, and virus and spyware detection – reducing time and effort by over 50%. Examples of these reductions are seen in recent case studies from 3 different medium-sized businesses, which have all experienced significant benefits, including:

- Doing more with existing headcount (FTE)
- Lower Total Cost of Ownership (TCO) of managed systems
- Faster response and better service to end users
- Reduced downtime and increased productivity
- Lower labor costs and reduced skill requirements
- Increased security and reduced risk and exposure.

EMA strongly believes that automation of inventory, asset management, software deployment, and patch distribution is in the best interests of all organizations, including small and medium-sized businesses. Automation systems are vitally important to any business, and mid-sized enterprises suffering from IT resourcing, response, or ‘fire-fighting’ issues should especially look at IT automation solutions such as KBOX™ by KACE.

Introduction

Manual IT management – including hardware and software inventory, asset management, software deployment, and patch distribution – is a significant burden on IT, and on the business users it supports. Yet, organizations are often hesitant to consider automation solutions to this problem because of misconceptions around automation.

Compiling an IT inventory – detailing all the hardware and software that exists in the business, on servers, desktops, and laptops – and managing those assets is important for accounting, compliance, security, and timely problem resolution. An accurate hardware and software inventory, for example, enables support personnel to diagnose and correct IT problems much faster. However, collecting this inventory is a difficult and time-consuming process to conduct manually. Administrators waste time on travel, or develop one-off processes which require significant skills, yet are prone to failures. As soon as the inventory is complete, it is out of date, as both administrators and users install new devices, components, software, patches, and updates.

Manually deploying software, distributing updates, and installing patches is even more problematic. Again, administrators must physically go to every server, desktop, and laptop. End users are interrupted from their work while the IT technician travels to the location, and takes over the user's system to administer these updates, or apply software fixes.

Manual administration also has significant security and compliance problems. Security patches are not deployed when they are needed, systems are unprotected from new viruses and attacks, and spyware is installed undetected. Data can be compromised, and license agreements more easily violated, exposing the business to legal risks. Configuration policies are broken, exposing IT to an increased number of incidents and more 'fire-fighting.'

This paper examines the problems caused by manual processes, and how automated management systems provide effective solutions to these problems, by:

- Debunking the five myths that lead medium-sized enterprises to avoid automation solutions
- Examining key drivers including cost, productivity, security, and compliance issues
- Presenting research data that shows the benefits of automation solutions
- Relating in-depth case studies of organizations that have implemented automation solutions

Five Myths of IT Automation

Companies have many misconceptions about the costs and benefits of automated IT management. Debunking the top five misconceptions will allow companies to better evaluate the cost of not automating IT management:

1. **"Automation is too expensive to acquire and implement"** – in reality, it is manual processing that is too expensive to maintain. For example, manually deploying a new version of Microsoft Office in a business with around 1,600 desktops, can cost $56 or more per desktop in labor costs alone (not including productivity loss, travel expenses, courier costs, etc.). By contrast, automating this deployment can reduce this cost to as low as $17 per desktop. SMBs especially cannot afford *not* to implement automation systems.

Do the numbers – You can spend the $30K to automate, or spend the $90K to do it manually" – Senior Analyst, Manufacturing Company

2. **"Automation systems are too complex, difficult to learn, hard to use"** – in reality, automated systems reduce the complexity of IT management, because they have knowledge and best practices built in. For example, an administrator rolling out applications and patches in a Windows environment must manually code, create, package, and distribute the complex command scripts known as ".msi" (Microsoft Installer) files. Automation systems can deploy all types of software, or any type of digital file, without any of this complexity.
3. **"We don't have the time to implement automation"** – implementing automated IT management does require some time for research, learning, and deployment. However, automation recoups this time and effort, improves service, and tightens security in as little as one month of part-time effort. Then the time savings kick in – one SMB with 500 employees estimated time savings of one or possibly even two highly skilled FTEs, up to a quarter of their total IT staff. Instead, this headcount can be redeployed to strategic business initiatives. Businesses who believe they do not have enough time to implement automation are likely to be exactly the businesses that should.
4. **"It is too much effort to automate our IT management"** – again, deploying an automation system does entail some upfront effort. However, this upfront dedication pays back to the business in many ways. Automated IT management makes administrators more productive and more effective, reduces travel time, and provides better service to users. IT administrators can automatically handle routine conditions quickly and easily, and spend more productive effort on prediction, tuning, analysis, and other complex management.
5. **"We have too many fires to fight, to worry about automation"** – this is another reason why a business definitely *should* worry about automation. Automated IT management keeps

the environment more stable, because systems are always up to date with the latest bug fixes and security patches. Administrators have more time to predict, tune, configure, and manage the environment to prevent problems before they occur. Firefighting is less frequent, as IT automation can alert administrators before problems occur (e.g. disks filling up); and it is faster when it is needed, through automated configuration discovery and deployment of fixes. And users can often fix their own 'fires,' through automated self-service for common requests like application provisioning.

Key Drivers for IT Automation

IT Costs and Productivity

There is no doubt that in any organization of significant size, manual IT management creates excessive costs, reduced IT productivity, or both. This is not just a large enterprise issue – any enterprise with more than one fully employed IT administrator will experience these problems.

Manual IT management, especially in Small- and Medium-sized Businesses (SMBs), overwhelms IT administrators. They must physically go to each desktop, and are entirely unproductive during that travel time. Travel to remote offices is also costly, and unfortunately, incidents do not always happen in convenient groups, so administrators are constantly traveling to resolve user problems.

Alternative approaches, such as remote control, or shipping laptop or hard drives, and scripting, are still manual and do not solve the problem. Significant travel is still required, and shipping hard drives or laptops imposes courier expenses, increases risk of data loss or corruption, and leaves the end user unproductive for days at a time while their system is in transit. Administrators, especially in SMBs, have no time for proactive management, such as preventative maintenance, system tuning, and configuration management. Scripting requires complex skills, and each script takes hours or days to write, test, debug, and deploy. End users must also wait while they execute – between several minutes for a simple patch, up to an hour or more for a complex deployment. Lastly, with manual IT management, no reporting trail is available.

"Automated distribution speaks for itself – that's an employee all of its own right there" – Jason Potts, Network Administrator, City of Franklin, Tennessee.

Similarly, manual asset discovery – such as determining the system type, memory, disk space, OS version, applied updates, patch levels, etc. – is difficult, time consuming, and error-prone. Inventories are quickly out of date, so the administrator must repeat the discovery before every update, further reducing their productivity and effectiveness.

"Most people don't have time to build scripts just to run IT" – Jason Potts, Network Administrator, City of Franklin, Tennessee.

The solution is to employ automated IT management for asset discovery, inventory management, patching, and software deployment. The end user goes home in the evening, and overnight, the automation system boots the desktop using Wake-on-LAN, discovers the configuration, installs the appropriate software, reboots the system, and shuts it down again. A single administrator can update hundreds or even thousands of systems automatically. End users come back to work the next day, blissfully unaware that anything has even happened. On-site visits may still be required – notably for hardware problems – but the most common system problems and maintenance are resolved faster and more efficiently, without travel costs or downtime, and users can get back to work much faster.

Security

Manual IT management also adversely affects security, especially around applying security patches, virus updates, and removing dangerous software such as adware, spyware, Trojans, and other so-called malware. An inaccurate inventory will lead to security patches and updates being applied to the wrong systems, and not being applied where they are needed. This exposes the business to significant security risks such as malicious penetration, virus infection, spyware, and more. It can lead to malicious and unauthorized software – such as peer-to-peer (P2P) software like KAZAA or Bit Torrent, unlicensed software, adware, or spyware – being installed without IT's knowledge. Important software such as virus scanners and firewalls may be disabled or removed. This further exposes the business to security risks, and can increase licensing costs as the business over-accounts for licenses just to accommodate rogue installations. It can expose the business to legal action for copyright and license infringement.

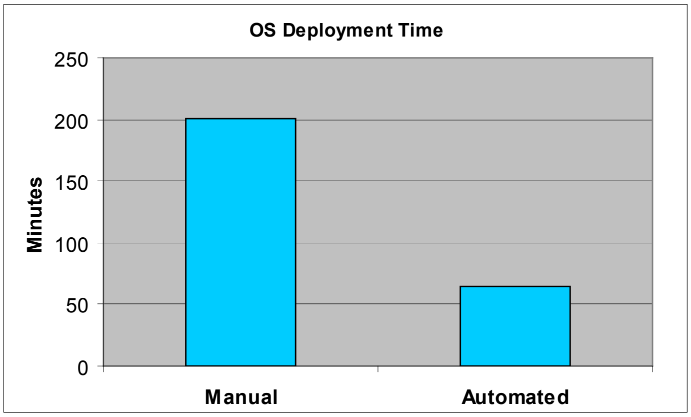
Automated asset discovery and inventory management significantly reduces or even eliminates these problems. Administrators know at a glance what assets are deployed, what updates are required, what patches need to be applied, what security software has been disabled, and what rogue software needs to be removed. This helps to maintain a significantly more secure computing environment, regardless of size, and allows more accurate accounting for deployed software, to meet reporting requirements for financial regulations such as Sarbanes-Oxley. It also eliminates pirate software installations, and enables recovery of unused licenses, to reduce license costs and avoid legal liability.

Automated software deployment maintains a greater level of security. Administrators can easily and rapidly apply security updates and remove rogue installations. They can secure large numbers of systems simultaneously, and automatically. The business stays up-to-date with the latest security updates, firewalls are kept up and running, virus scanners are maintained, and malware is quickly detected and removed – all with rapid response and minimal effort from IT administrators. It establishes process control and audit, to meet compliance requirements for regulations such as Sarbanes-Oxley, and it also helps to protect data, to comply with privacy regulations such as HIPAA.

Automation Outcomes: Empirical Research

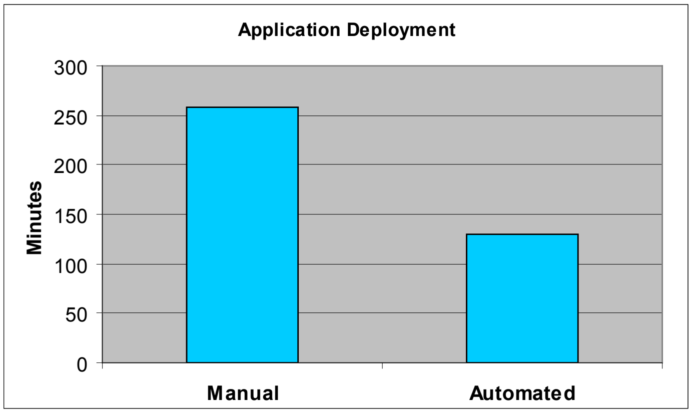
EMA's research data confirms these benefits. EMA recently (2006) surveyed IT administrators from over 200 businesses with mixed operating environments, of which 85% had fewer than 100 servers, on cost of systems management. According to this research, automated IT management will significantly reduce the effort IT administrators spend on routine maintenance.

Operating System Deployment



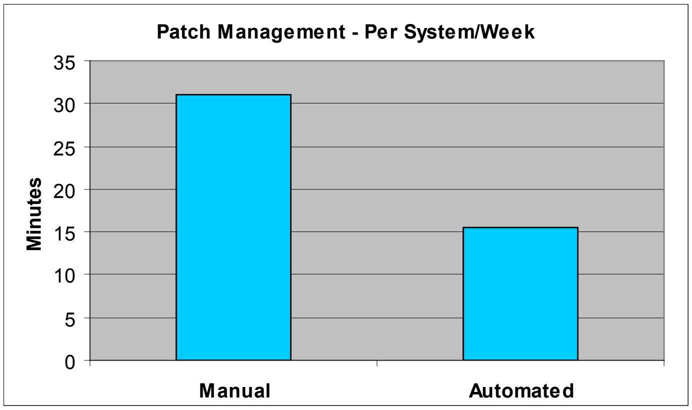
For example, EMA found that on average, administrators using manual provisioning spend as much as 200 minutes on OS provisioning. By contrast, administrators using automation tools on average spend as much as 65 minutes – cutting OS provisioning effort in more than half.

Application Deployment



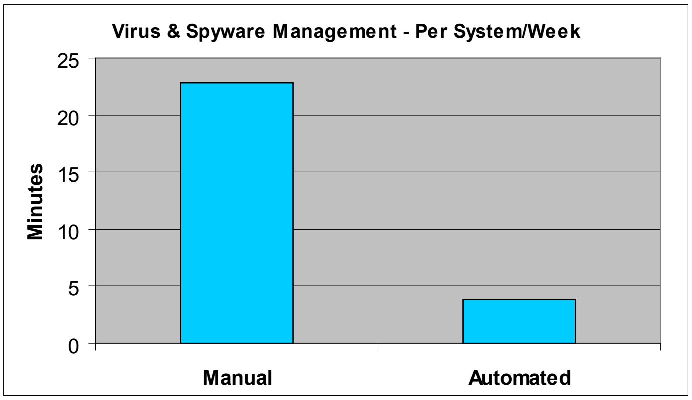
A similar pattern emerged for application deployment. On average, administrators using manual processes spend up to 260 minutes for application deployment while administrators using automated tools on average spend on 130 minutes – exactly 50% of the time of those doing manual application deployment.

Patch Management



The research found that on average, time spent on manual patch management was as much as 31 minutes per system per week. For companies using automated patch management tools, that average drops to just 16 minutes per system per week. The savings add up quickly, on a network of just 100 machines, the saving could amount to as much as 25 hours per week.

Virus and Spyware Management



Virus and spyware management shows an even more dramatic pattern. In the case of manual management of virus and spyware, the average time spent was as much as 23 minutes per system per week. Automated virus and spyware management tools result in the average time dropping to only 4 minutes – an 82% decrease in the time spent per system on this task.

Data Summary

This research shows that IT administrators in SMB environments who use automated IT management tools spend significantly less time on OS deployment, application deployment, and patch management. This allows administrators to work faster *and* smarter. They have more time for complex, and productive tasks, such as capacity planning, system tuning, optimization, predictive analysis, problem solving, and problem prevention.

This research also reinforces the need for automation to reduce the administration effort required for more complex security requirements – i.e. situations that take longer to address (such as virus infections) appear to be either less prevalent, or easier to manage, when IT automation systems are in place.

Customer Case Studies

EMA also conducted a number of interviews with IT administrators using the KBOX by KACE to get a qualitative view of the benefits of IT automation.

Case Study – Local Government

The first interview was with Jason Potts, Network Administrator with the City of Franklin, Tennessee. Franklin is a small town, which is growing rapidly. 10 FTEs support 500 employees across 12 departments and locations, with 50 major applications and over 2200 software titles installed on Windows desktops and servers.

They reached what Potts called "a crunch point," when they did not have enough people to achieve all their critical work. They had skilled people who were knowledgeable about scripting, but who did not have time to write scripts for software deployment, patching, inventory, etc.

They investigated automation solutions including Microsoft SMS and the KBOX looking specifically for:

- Automated inventory to give them better accounting and license control
- Automated distribution to save time and money
- Wake-on-LAN, to help with troubleshooting and faster problem resolution

They selected the KBOX because it met these critical requirements and, among other benefits, they "wanted a solution, not a package of licenses, and additional hardware."

Potts acknowledged that implementation was an additional short-term effort, but said it was a case of "you can pay me now or pay me later," as the solution freed up significant time for IT once it was implemented. This only took one month (elapsed time, while IT was still doing other work) to "get comfortable" with automatically deploying software updates, patches, etc.

The benefits were significant.

- They were able to automate the work that would have otherwise taken 1-2 FTEs to manage. According to Potts, "automated distribution speaks for itself – that's an employee all of its own right there." For example, maintenance of 50 systems for the 911 communications application ("it doesn't get more mission critical"), now takes 10 minutes each, versus the 2-3 days before they implemented automated IT management.

> *"We support about 50 systems for the 911 communications application – it doesn't get more mission critical. With automation, updates now take about 10 minutes each, versus 2-3 days for getting around to all the locations." – Jason Potts, Network Administrator, City of Franklin, Tennessee.*

- Inventory and discovery are now automatic and continuous. When asked to provide details of the environment for this interview, Potts replied "let me just look at the KBOX and tell you exactly," and provided the details in seconds.

- Users benefited from IT's ability to administer end user systems, without any user involvement or downtime. As Potts puts it "they don't know what IT is doing, but they know they can do their job."

Case Study – Law Firm

The second interview was with a law firm in Palo Alto, California (which declined to be named publicly in this paper). The firm has 1000 employees in a central location, and another 600 spread across 7 offices (including one in China). The IT team manages one Microsoft Windows Active Directory (AD) domain, with 130 servers, and 1600 Windows XP desktops.

They were previously performing software distribution and patch management by distributing .msi files using AD, but could not find skilled resources to create these package files. Users were prompted to restart their systems whenever updates were applied, leading either to downtime as users restarted, or delays in applying patches for users who did not restart when prompted. According to the IT administrator, IT "spent a lot more time doing patch and update than more important things, like monitoring, management, and server administration."

They subsequently deployed the KBOX to resolve these problems, and found additional advantages:

- Hooks into AD allow them to leverage AD as much as possible. According to their administrator, "that saves us from grouping things twice – we can link it to the LDAP and we're done."
- The "snooze" option gives users the choice of when to reboot, within a maximum time limit set by the administrator. Critical patches can be applied immediately, but for less important changes, this minimizes user disruption.
- It has simplified their daily administration, reducing the need for additional resources, and for specialized skills, because "you certainly don't have to be an AD expert – you don't need a highly skilled person to run it."

> *"You certainly don't have to be an expert, you don't need a highly skilled person to run it" – Network Administrator, Law Firm*

Case Study – Manufacturing Company

The third interview was with the Senior Analyst for an international equipment manufacturer (which declined to be named publicly in this paper). A team of 10 IT staff provide desktop support for 1,900 employees running Windows 2000 and Windows XP, across multiple offices in the United States and Europe, with a manufacturing plant in Asia.

The Senior Analyst and the IT Manager both came to the company from environments that used automated IT management tools extensively. They were concerned by lost IT productivity and end user downtime caused by manual IT management. Software updates, for example, involved visiting each desktop to install updates and patches manually.

They quickly conducted a review that resulted in several recommendations to improve service and processes. According to the Senior Analyst, "at the top of the list was the need for automated management tools." In addition to automated software distribution, they wanted to automate asset inventory, to improve their hardware and software accounting, and to satisfy Sarbanes-Oxley requirements. They evaluated IBM/Tivoli, Altiris, Novell Zenworks, and Microsoft SMS, and decided on the KBOX. They estimated that the IBM/Tivoli solution would cost $113 per system per year, and SMS around $74 (in software costs alone), compared to a total of $17 per system for the KBOX appliance. The Senior Analyst also found the KBOX to be less complex, and easier to deploy and maintain, saying that it would "do the job at the right price – all the other solutions were overkill."

After extensive evaluation, they had the solution up and running within "a couple of hours," and fully deployed in under two weeks. The Senior Analyst was particularly happy with the appliance-based approach, because there was "no installation, and no server build – you plug it in turn it on." He justified the upfront effort saying, "it's well worth the effort to spend the time to get a tool like this up and running."

He reported the main benefit was in cost savings. The company had previously planned to distribute a new version of Microsoft Office manually, estimated to cost $90,000 in labor costs alone. According to the Senior Analyst, this made for an easy choice, explaining, "You can spend the $30K to automate, or spend the $90K to do it manually," adding "If you're serious about TCO, then it just makes sense." He also estimated that automation saved them more than 2 FTEs. In addition, they can now distribute software much faster, without interrupting users, by configuring software deployment to run overnight.

EMA's Perspective

Enterprise Management Associates strongly believes that manual IT management is a significant and avoidable burden on IT. The travel costs alone can be prohibitive, but the burden also includes downtime and productivity loss for both users and IT. Neither remote control, shipping devices back to IT, nor scripting, address the fundamental problems of manual IT management. Manual IT management creates security problems. Systems are out of date, security patches are not installed, malware remains undetected, and the business is exposed to significant risks. It also introduces problems with compliance – to regulations like Sarbanes Oxley and HIPAA, as well as licensing obligations, and internal policies.

Automation reduces the complexity of IT administration, makes administration faster, and lets administrators manage many more systems than they possibly could manually. Systems are more secure, exposure to financial, legal, and compliance risks is reduced, service to end users is improved, and administrators can focus on preventing fires, not just fighting them. EMA's own research clearly supports these outcomes. Initial deployment of automation systems is at worst an inconvenience, compared to the results it delivers, especially with appliance-based solutions that integrate automated IT management disciplines, and are easy to install and to use.

EMA believes that automated IT management is vitally important to any business. Mid-sized enterprises suffering from overloaded resources, slow response, and excess 'fire fighting' should especially evaluate automated IT management solutions, such as KBOX by KACE. It will allow their IT staff to work faster and more efficiently, reduce the number of unexpected problems, improve service to end users, and reduce security and compliance risks.

About KACE

KACE is a leader in IT automation appliances. The KBOX™ by KACE product line delivers easy-to-use, comprehensive IT automation appliances that are affordable and really work. KACE is a privately held technology company with offices in Mountain View, CA, Charlotte, NC, and Chicago, IL. KACE customers range in size from departments and divisions of Fortune 500 companies to mid-sized businesses across the country.

Enterprise Management Associates
2585 Central Avenue, Suite 100
Boulder, CO 80301
Phone: 303.543.9500, Fax: 303.543.7687
www.enterprisemanagement.com
1131.060506