BEST PRACTICES

Systems Management

KASPERSKY lab

THE BUILDING BLOCKS OF ENDPOINT SECURITY

“Do more with less” has become a business mantra over the past few years, but it’s nothing new to IT professionals. Business has always looked to squeeze the maximum possible benefits out of IT resources at the lowest possible cost – the real challenge for IT pros today is keeping pace with complexity in the face of limited resources.

PriceWaterhouseCoopers’ Global State of Information Security report for 2012 found organizations of all sizes struggling to keep pace with a constantly evolving threat landscape while keeping a firm grip on an ever-expanding array of devices, software, applications, hardware and user profiles.

Kaspersky Lab’s 2012 Global IT Risks Survey reveals an increasingly chaotic security landscape, where over 40 per cent of businesses feel unprepared for the threats around them. It’s not surprising: Kaspersky Labs is tracking an average of 125,000 unique threats every day. Fifty-eight per cent of users surveyed said their IT security was under-resourced in at least one area of staff, systems or knowledge.

TOO MANY MULTIPLES

It's no longer just about outside threats, either. Increased platform, device, software and application diversity is making life difficult for IT managers, causing complexity and resource drain:

- Multiple devices
- Multiple vendor solutions
- Multiple management consoles
- Multiple operating system images
- Multiple network devices
- Multiple policies.

Complexity undermines security, efficiency and growth. It creates room for error and limits your ability to manage change. IT professionals are all too aware of the challenges. But what can you do to mitigate them without restricting end user needs or over-burdening already strained resources?

Effective **systems management** can go a long way towards supporting best practices that optimize IT resources while enforcing a blended security posture capable of dealing with a constantly evolving threat landscape. Time-consuming manual processes and lack of visibility into your network are just two of the greatest challenges faced by today's IT manager.

From **license management to software installation, automated vulnerability scanning and advanced patch management, OS image creation/deployment** and **network access control**, every hour you don't spend on day-to-day maintenance and monitoring is one you can spend developing new ideas or supporting new business initiatives. Here's how.

CENTRALIZE, AUTOMATE, CONTROL

There are some fundamental steps that any business can take to ensure optimal performance of IT, reduce costs, improve service levels and increase agility:

- Standardize your desktop/laptop strategy and keep images to a minimum.
- Manage PC, laptop and smart device settings and configurations from a central location.
- Implement and maintain comprehensive security tools.
- Automate software distribution, patch management, vulnerability scanning and other routine tasks.
- Optimize software and hardware budgeting and usage.
- Implement effective, easy-to-manage Network Admission Control (NAC).

Automation of key, routine tasks — from security to troubleshooting — allows IT administrators to switch from a 'firefighting' approach to a strategic one in which business needs are aligned with and supported by IT policies. Automation can help reduce the errors often associated with performing manual processes in complex systems.

EFFECTIVE IMAGE/PROVISIONING CONTROL AND IMPLEMENTATION

Every year, you deploy new hardware and applications while constantly upgrading software, operating systems, applying patches and updates. That's time-consuming, expensive and, as inventories grow, complex.

Preparation and management of a 'Golden Image' — a fully optimized master image (or clone) of a complete desktop — saves significant time and resources. This perfect system set-up is stored in a special inventory on your network, ready to be rolled out when and where you need it. For businesses intending to migrate to a new operating system, image/provisioning control, inventory and deployment can be automated. The real benefit of this is that administrators can roll out a new operating system after hours, using BootOnLAN technology — more time saved and less disruption.

Effective image/provisioning deployment ensures operating systems are implemented with optimal security settings, but don't forget to ensure the security of the images themselves — best practice calls for securing and controlling access to all images.

This should include:

- Strong passwords
- Protecting client authentication certificates
- Access controls to protect the 'reference' computer used to capture the operating system you're using for the golden image. This prevents any malicious software from being inadvertently included in the image.
- Ensure the image is stored in a secure destination, so that it cannot be compromised
- Maintain security patches and updates on the reference system, ensuring that all newly rolled-out systems are optimally secured.

If your business is considering a migration to Windows 8, effective image/provisioning management will allow you to standardize the operating system used across all devices on your network. Choose a solution that allows you to automate and centrally manage images. Add an extra layer of convenience by opting for a solution that will automatically save end user data.

SOFTWARE INSTALLATION AND DEPLOYMENT

Software upgrades. New software. New versions of currently used software. You can't manually upgrade every machine at your business; you'd never have time to do anything. Software deployment can be automated and optimized to ensure it has the minimum impact on your network, making it completely transparent to end users via 'silent deployment' technology.

Some tips:

- **Keep your deployment options open:** In addition to standard MSI packages, choose a solution that supports other types of executable files, such as exe, bat or cmd.

- **Be flexible with deployment:** Options that allow both on-demand and scheduled deployments will give you greater flexibility. Scheduled deployments are particularly useful in large package scenarios — simply deploy after hours when network disruption will be minimal.

- **Installation Package modification:** This functionality gives further flexibility by allowing you to set installation parameters to ensure compatibility with your policies.

- **Remote installation and traffic management:** If you're supporting remote office locations, choose a solution that allows further traffic management by assigning update agent status to a selected workstation. Installation packages will be downloaded by this machine first, before being distributed to other local workstations, minimizing network load and significantly reducing Internet connection usage.

- Further load reduction can be achieved using Multicast broadcasting technology, which allows for one-to-many or many-to-many broadcasts.

- **Remote troubleshooting:** No more frustrating phone calls with end users — remote troubleshooting saves time and effort, allowing you to resolve issues quickly and directly.

Software deployment and upgrading is a mundane fact of life for IT administrators. By automating and optimizing it, you can ensure that best practice guidelines are the default setting. In multi-site or multi-system scenarios, software deployment controls can help reduce complexity and the errors associated with repeated manual processes.

EFFECTIVE LICENSE MANAGEMENT AND CONTROL

The ability to manage and control software licenses across the business gives IT professionals one of the easiest cost-cutting wins available.

Apart from enabling cost-reduction by eliminating over-spending on unnecessary software, effective licensing control supports a more effective security strategy — when you know exactly who is running what software on your network, it's easier to apply your policies.

Best practice in software/hardware licensing management requires that you have complete visibility into every piece of software and hardware running on your network. Automatic device discovery technology supports this, helping you to ensure that all licensing obligations are observed.

Here are some further steps you can take:

- **Software inventory:** Automate the compilation of an inventory of all software used on your network and gain complete visibility and control. This list allows administrators to control usage, inform end-users if they're running any prohibited/unlicensed software and, if necessary, block the use of undesirable applications.

- **License planning:** Once you've got an inventory in place, it's easier to control license usage according to departmental requirements — for example, you may find users in the accounts department have unnecessary licenses for office productivity software. These licenses can be redeployed or you can cut costs by phasing them out.

- A clear picture of the licenses in use in your business will also allow you to ensure that they are kept up to date. You can also automatically track any breaches.

- **Hardware inventory and device tracking:** Like its' software counterpart, a hardware inventory gives you a complete view of every device in use on your network. Automate new hardware discovery and notification to keep up to date while monitoring any changes and transferring unused devices to archive.

- **Reporting:** Centralized reports give comprehensive information on every piece of software and hardware in use on your network, along with usage history. Insight gleaned from reports will allow you to control usage among groups at any level.

License control can be a time consuming, often complex task. Automating it not only frees your time but ensures your business meets some key best practices, among them: Compliance, Cost-effective software and hardware management and comprehensive visibility into what's happening on your network. Small effort, big rewards. What are you waiting for?

ADVANCED VULNERABILITY SCANNING AND PATCH MANAGEMENT

Managing and administering software updates while constantly monitoring for potential vulnerabilities is one of the most important, challenging and resource-intensive tasks faced by any IT department.

Faced with a constantly evolving threat environment in which criminals repeatedly scan systems for any sign of weakness, it's vital that IT administrators can find and fix gaps in security before they're exploited.

Vulnerability scanning performs this task for you: It scans the devices and software on your network in much the same way a criminal would, looking for weak points that could be exploited. Once located, patch management can fix those gaps, installing the necessary updates or repair software to all the machines on your network.

Vulnerability scanning, implemented in tandem with an effective patch management strategy, can help you to keep one step ahead of criminal hackers.

Here's how:

- **Keep up to date:** Out of date software creates weak spots across your business, whether it's on your servers or at the endpoint. Automated regular, scheduled vulnerability scans will keep you abreast of weak points, allowing you to automate the implementation of patches and fixes.

- **Automate:** Effective patch management improves reliability and IT efficiency. By automating the deployment of software updates, and the administrative tasks that go with it, you can minimize downtime associated with patch deployment, auditing and roll-back.

- **Roll back the clock:** Updates/installations don't always run smoothly. Sometimes, patches can cause instability or are incompatible with other software or drivers on your machines. Choose a solution with integrated image/provisioning and rolling back to a properly functioning, optimized system will always be easy.

- **Gain complete visibility:** By automating scanning, you'll have complete visibility into the current state of patching and updates on all machines.

- **Prioritize:** Comparing the results of your scans against multiple vulnerability databases will help you to gain an understanding of the risks associated with any vulnerability. Based on this insight, you can prioritize patching, rolling out less urgent fixes after hours and spreading the load on your network.

- **Report:** Accurate, up-to-date and detailed information is a vital part of any security and risk management strategy. By running reports on your scans, you add another layer of insight — allowing you to examine and report on potential weak spots, spotting and tracking changes and also giving detailed insight into the patch status of every device and system on your network.

Targeted attacks, advanced persistent threats, automated attacks and zero-day vulnerabilities all shrink the time between vulnerability discovery and the creation of an exploit. By automating and scheduling regular scans and patch implementation, IT administrators can streamline their patching and vulnerability scanning processes without compromising on their effectiveness.

NETWORK ADMISSION CONTROL (NAC)

You've got control over images/provisioning, you have effective licensing controls in place, you've automated software installation and have advanced scanning and patch management controls in place. Now it's time to apply similar levels of insight and control to your network and the devices and machines that connect to it.

Network admission control (NAC) enables IT administrators to enforce security policies — by refusing or limiting network access based on any device's compliance with those policies. Essentially, NAC allows IT administrators to set the terms under which anyone can use their network, including guest devices. For organizations supporting BYOD initiatives or an increasingly mobile workforce, NAC ensures that all devices — from laptops to PCs and smart phones – are running up-to-date, secure versions of your specified applications and software.

NAC supports existing security strategies and polices, while enforcing best practices, including:

- Prevent unauthorized devices from accessing the network
- Detection and identification of new devices connecting to the network
- Forcing all devices, including guest systems, to meet your specified security requirements
- Detection and repair of endpoint vulnerabilities
- Insight and reporting into compliance with your security policies.

Before implementing NAC, it's important to have a clear vision of what you want to achieve — for example, you may wish to allow guest internet usage in a communal area of your premises, but block access to internal networks. You probably want to ensure that all guest laptops are malware free and have a certain level of security in place.

Here are some questions you should be asking yourself:

- Who is allowed to connect to the network?
- What services and resources are people allowed to access?
- When is that access to be granted?
- What locations are people allowed to connect from?
- Should certain kinds of user groups be restricted to certain kinds of resources or have access limited to particular times?

Automatic device discovery is a vital component of effective NAC. This can differentiate between company-owned and guest devices, and apply policies and access accordingly. Save time and effort by automating access – this allows you to create an access policy once, but apply it to all devices.

An extra layer of security can be applied to guest devices via a 'Captive Portal'. This automatically ensures that all guest devices are directed to a special portal. Guests are given a password and login; once authenticated, they can access the internet and, if allowed, some pre-specified company resources.

EFFICIENCY THROUGH CENTRALIZED CONFIGURATION AND PATCH MANAGEMENT

As IT professionals struggle to do more with dwindling resources and budgets, there's a danger that complete visibility and control over business networks will be lost as administrators are forced to focus on urgent issues, often to the detriment of essential-yet-mundane tasks.

By centralizing and automating many essential configuration and management tasks, IT administrators can not only save themselves time, but money too. Effective systems management, driven by centralized configuration and patch management tools, supports many of the best practices that optimize IT resources while enforcing your company-specific policies.

ABOUT KASPERSKY LAB

Organizations need intelligent security technologies to protect their data — and they also need intuitive and uncomplicated IT efficiency tools. Kaspersky Lab's 2,500 employees are driven to meet those needs for the 300 million plus systems they protect — and the 50,000 new systems a day that are added to their number.

Kaspersky Systems Management is a component of Kaspersky Endpoint Security for Business. Combining award-winning anti malware, IT policy enforcement tools, centralized management and cloud-assisted protection, Kaspersky's business security products are the right choice for your organization.

Talk to your security reseller about how Kaspersky can bring secure configuration to your networks, the devices that run on them — and more!

Kaspersky Lab ZAO, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab