KASPERSKY lab

BEST PRACTICES

Systems Management

www.kaspersky.com

YOUR GUIDE TO SYSTEMS MANAGEMENT BEST PRACTICES.

Enhance security and manage complexity using centralized IT management tools.

Unpatched vulnerabilities in popular applications are one of the biggest threats to business IT security. This risk is compounded by increasing IT complexity. If you don't know what you've got, how can you secure it? This Best Practice Guide shows you how...

Increased platform, device, software and application diversity is making life difficult for IT managers, causing complexity and resource drain. Devices and software aren't the only things multiplying; Kaspersky Lab detects 350,000 new threats every day, many of them designed specifically to exploit vulnerabilities in popular business applications to gain access to sensitive data, steal money or block systems until a ransom is paid.

Complexity undermines security, efficiency and growth. It creates room for error and limits your ability to manage change. Effective systems management can go a long way towards supporting best practices that optimize IT resources while supporting a multi-layer security strategy capable of dealing with a constantly evolving threat landscape. Here's how.

1. CENTRALIZE, AUTOMATE, CONTROL

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

- Standardize desktop/laptop strategy and keep images to a minimum.
- Manage PC, laptop and mobile device settings and configurations from a central location.
- Implement and maintain comprehensive security tools.
- Automate hardware and software inventories, software distribution, vulnerability scanning, patch management and other routine tasks.
- Enable remote troubleshooting and software installation, including remote office coverage.
- Implement Role-Based Access Control – customize centralized console views according to roles and rights.
- For enterprises, integration with SIEM systems helps minimize administrator workload and tools while simplifying reporting.

Automation of key, routine tasks – from security to troubleshooting – facilitates a 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.

2. EFFECTIVE IMAGE CONTROL AND IMPLEMENTATION

Every year, new hardware and applications are deployed, along with regular upgrades to software, operating systems, patching and application 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 the network, ready to be rolled out as needed. For businesses migrating to a new operating system, image control, inventory and deployment can be automated. The real benefit of this is that it enables after-hours rollouts, using Wake-on-LAN technology – more time saved and less disruption to end users.

Effective image deployment ensures operating systems are implemented with optimal security settings, but don't forget the security of the images themselves – best practice includes securing and controlling access to all images, including via:

- Strong passwords
- Protecting client authentication certificates
- Access controls to protect the 'reference' computer used to capture the operating system being used 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 where it cannot be compromised.
- Maintain security patches and updates on the reference system, ensuring that all newly implemented systems are optimally secured.

Effective image management allows you to standardize your chosen operating system across all devices on your network. Choose a solution that enables the automation and centralized management of images. Add an extra layer of convenience by opting for a solution that will automatically save end user data.

For added control and flexibility, look for a solution that enables OS images to be edited after creation. UEFI support, the ability to create a boot flash drive with Windows PE and the option to import an OS image from a distribution package are all features that will further enhance usability and efficiency.

3. OPTIMIZE SOFTWARE INSTALLATION AND DEPLOYMENT

Software upgrades. New software. New versions of current software. Manually upgrading every machine in the business would leave no time for other tasks. Software deployment can be automated and optimized to ensure minimal network impact, making it completely transparent to end users. Some best practice tips:

- Keep deployment options open by choosing a solution that, in addition to standard MSI packages, supports other executable file types, such as exe, bat or cmd.
- Be flexible with deployment: options that support both on-demand and scheduled deployments enable greater flexibility. Scheduled deployments are particularly useful in large package scenarios – deploy after hours when network disruption will be minimal. Kaspersky Systems Management enables the automatic installation of over 100 popular applications, identified via Kaspersky Security Network. These can be installed after hours, if required.
- Choose a solution that enables remote deployments from a single console. Save on traffic to remote offices with Multicast technology for local software distribution.
- Installation Package modification functionality gives further flexibility by allowing the setting of installation parameters to ensure compatibility with policies.
- Choose a solution that enables remote troubleshooting: no more frustrating phone calls with end users – remote troubleshooting saves time and effort, allowing problems to be solved quickly and directly. User permissions and session logs/audits add an extra layer of security to remote sessions.

By automating and optimizing software deployment and upgrades, it's possible to ensure that best practice guidelines become a default setting for your business. In multi-site or multi-system settings, software deployment controls help reduce complexity and the errors associated with repeated manual processes.

4. TAKE CONTROL OF ASSETS

Knowing exactly what devices and applications are being used on your network is a key component of effective IT security. So is having insight into which areas need attention.

Best practice involves having complete visibility into every piece of software and hardware running on your network. Automatic device discovery supports this, helping ensure that all obligations are observed. Some further steps include:

- **Software inventory**: Automate inventory compilation and gain complete visibility and control. This list enables administrators to control usage, inform users if they're running any unauthorized/unlicensed software and, if necessary, block use of undesirable applications. Management and control of software licenses across the business is one of the easiest cost-cutting wins available, helping to eliminate spending on unnecessary software.

- **Hardware inventory and device tracking**: Enables a complete view of every device in use on the network. Automate new hardware discovery and notification to keep up to date while monitoring any changes and transferring unused devices to archive. Network Access Control (NAC) means guest devices can be safely added to the network, blocked if they don't meet security requirements or have different policies applied to them.
- **License planning**: With an inventory in place, it's easier to control license usages according to departmental requirements – for example, you may find users in the accounts department have unnecessary licenses for graphic design software that could be redeployed or phased out. In addition, a clear picture of licenses enables up-to-date management.
- **Reporting**: Centralized reports give comprehensive information on every item of software and hardware on the network, along with usage history. Insight from these reports enables usage control among groups at any level.

License control can be time-consuming and complex. Automating it not only frees time but ensures the 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.

5. ENABLE ADVANCED VULNERABILITY ASSESSMENT 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 the IT department.

Faced with constantly evolving, targeted threats used by criminals repeatedly scanning systems for any sign of weakness, it's vital that IT administrators find and fix gaps in security before they're exploited.

Vulnerability assessment performs this task for you: scanning the devices and software on the network, looking for weak points that could be exploited. Once located, patch management can fix those gaps, installing the necessary updates or repairs to all machines on the network.

Implemented alongside an effective patch management strategy, vulnerability assessment can help you keep one step ahead of cyber criminals. Here's how:

- **Stay up to date**: Out of date software, whether it's on servers or workstations, exposes the business to attack. Automated software scanning enables rapid vulnerability detection and prioritization.

Kaspersky Systems Management enables the automatic delivery of patches and updates in the shortest timeframes for both Microsoft and non-Microsoft software. For greater control, administrators are notified about patch installation status. Non-critical fixes can be postponed until after-hours, even if computers are switched off, using Wake-on-LAN. Multicast broadcasting enables local distribution of patches and updates to remote offices, reducing bandwidth requirements.

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.

- **Report**: Run reports on scans and gain another layer of insight into organizational IT security. Examine and report on potential weak spots, track changes and gain detailed insight into the patch status of every device and system on the network.

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

6. CENTRALIZED MANAGEMENT AND ROLE-BASED ACCESS CONTROL

By centralizing and automating essential security, configuration and management tasks, such as vulnerability assessment, patch and update distribution, inventory management and application rollouts, IT administrators not only save time, but optimize security.

A single, integrated administration console, Kaspersky Security Center, supports the administration of system security for desktop, mobile and virtual endpoints across the network, through a single interface. In complex enterprise networks, Role-Based Access Control (RBAC) enables the customization of console views and functionality according to administrator role, rights and privileges. For example, a particular administrator may be able to view all IT security management areas on the console, but only able to edit Vulnerability and Patch Management functions.

7. SIEM INTEGRATION FOR ENTERPRISE ENVIRONMENTS

Many organizations, particularly enterprises, are using Security Information and Event Management (SIEM) systems to collect logs and other security-related data for analysis. Security systems capable of reporting to leading SIEM systems help reduce administrator workload and tool requirements while simplifying the enterprise reporting process.

Kaspersky Systems Management integrates with IBM QRadar and HP ArcSight for event transfer capabilities.

FINALLY

Software vulnerabilities have become the focus of well-planned, targeted attacks on businesses of all sizes. Effective application and patch management, coupled with vulnerability assessment and other systems management capabilities can deliver an integrated approach to business IT security.

Kaspersky Systems Management is a managed component of the Kaspersky Security Center. Each feature is accessed and managed through this central console, using consistent, intuitive commands and interfaces to automate routine IT tasks and enhance business security.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

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

KASPERSKY lab