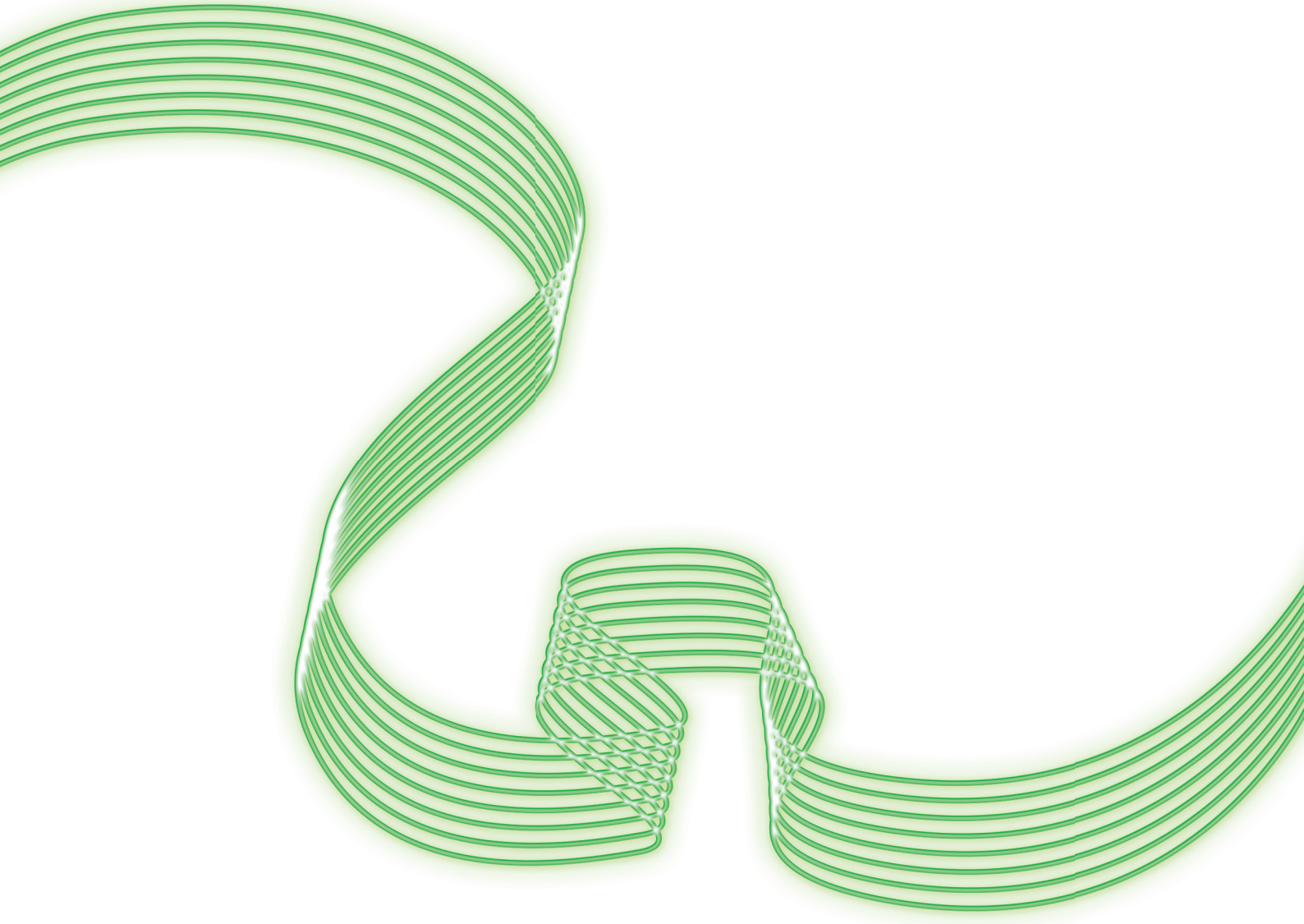

# CUTTING COMPLEXITY– SIMPLIFYING SECURITY

With corporate IT becoming increasingly complex, how can you boost efficiency… while improving corporate security?

With Kaspersky, now you can.
kaspersky.com/business

Be Ready for What's Next

KASPERSKY lab

# Contents

# Executive Summary

1.0

## 1.1 COMPLEX IT IS COSTING BUSINESSES… DEARLY

Because corporate IT environments are becoming increasingly complex, the task of managing them is also much more involved and time consuming than ever before. This growing complexity brings many disadvantages for businesses:

- **Increased costs** – More time and effort is being devoted to everyday systems management tasks.

- **Overloaded resources** – The list of regular IT management tasks expands whenever a new device or new software application is introduced onto the corporate network.

- **Impaired agility** – With so many routine IT management tasks filling the working day, there's less time for IT personnel to help the business to introduce new services that could generate a competitive advantage.

- **Security vulnerabilities** – Manual processes, plus the need to use separate control consoles for different tasks, can create the ideal conditions for operational errors… and those errors can result in serious gaps in security.

- **Lack of visibility** – The sheer complexity of most corporate IT environments is making it difficult for IT personnel to gain a clear understanding of all of the hardware and software that's operating on their network. This is of fundamental importance. Without an accurate view of their entire IT infrastructure, businesses are unable to:
  - Control how their IT estate is being used – both to boost efficiency and meet compliance or legal obligations
  - Manage their IT environment – in order to maintain service levels and productivity
  - Secure all of their systems and sensitive data against malware and attacks

## 1.2 CUTTING THROUGH COMPLEXITY – TO BOOST EFFICIENCY AND IMPROVE SECURITY

The latest IT Systems Management solutions can simplify and automate a vast range of routine IT management tasks, in order to:

- **Reduce the burden on IT personnel** – so that they can devote more time to strategic IT projects that can improve business efficiency and competitiveness
- **Manage and reduce operating costs**
- **Eliminate many common sources of IT management errors**
- **Ensure more rigorous security for systems and data**

Among the best of these solutions are products that include a unified management interface that enables IT personnel to monitor and manage a wide range of systems management tasks… from a single console.

# The case for efficient systems management solutions

2.0

## 2.1 THE GROWING IMPORTANCE OF IT

With IT supporting more and more essential processes – for virtually all sizes of business – it's vital that all elements of the corporate network are efficiently managed, in order to:

- Deliver all of the mission-critical business processes that modern organisations demand
- Maintain high levels of service for the business's employees and customers
- Free up existing IT resources – to work on new, strategic IT projects
- Manage and minimise costs

As IT continues to play an ever greater role in enabling the introduction of new services and in enhancing existing processes, IT departments are also faced with having to manage greater numbers of devices and a wider range of different types of endpoints.

## 2.2 THE GROWING THREATS TO BUSINESS

At the same time, the number of threats to corporate systems – and the security of precious data – is growing exponentially. Unfortunately, those threats are also becoming increasingly sophisticated in their efforts to undermine companies' security provisions – so both the volume and the effectiveness of security threats are increasing.

Today's malware and cybercrime attacks can be relentless in their attempts to exploit security vulnerabilities, in order to:

- Steal money from the targeted business
- Destroy the targeted organisation's business reputation or competitive position – for example, by:
  - Implementing a Denial of Service (DoS) attack that effectively takes the business's web-based services offline for a period of time
  - Stealing commercially sensitive information – including valuable intellectual property (IP)
- Harvest personal data about a company's customers or employees – for identity theft and to steal money from individuals

## 2.3 WHY COMPLEXITY HAS TO BE COMBATTED

Complexity – in all its forms – can be very damaging for a business. Consider some specific points about how complexity affects IT:

- Complex IT systems management processes:
  - Absorb valuable support resources
  - Waste money
  - Leave a business with less time to devote to strategic IT projects

- Complex IT security management processes greatly increase the risk of costly errors that could leave the business vulnerable to malware or targeted attacks.

Because IT environments are becoming more complex – with a wider range of devices and access points – businesses must proactively seek ways to combat the effects of this complexity. There is a need to identify methods that:

- Simplify and automate many of the everyday IT management tasks
- Minimise the need for specialist training to perform common IT management activities
- Ensure the corporate network remains secure – despite the evolving nature of IT security threats

## 2.4 OVERLOADED BY EVERYDAY SYSTEMS MANAGEMENT TASKS

For most IT administrators, the average working day is likely to include many or all of the following tasks:

- Setting up new workstations, laptops and servers
- Distributing new software applications across various elements of the corporate network
- Ensuring software licence obligations are met – and unlicensed software is prevented from running
- Applying policies on how devices are able to access the corporate network
- Controlling how applications are allowed to run on the network
- Detecting security vulnerabilities within operating systems and applications
- Assessing the severity of each vulnerability and setting priorities for remedial action
- Implementing the latest patches and updates that eliminate security vulnerabilities
- Supporting mobile and remote users in how they can access corporate systems
- Controlling restrictions on how 'guest devices' can access the corporate network

## 2.5 ADDITIONAL ISSUES FOR THE IT TEAM

It's clear that such a long list of IT management challenges is placing an enormous burden on IT departments. However, several other factors are also adding to the issues that have to be tackled:

- Portable devices – such as removable storage devices – are creating more opportunities for data to 'leak' from the business
- Users are downloading unlicensed software and applications that may contain malware
- Bring Your Own Device (BYOD) initiatives are generating new operational challenges and security problems

… all at a time when malware is becoming more sophisticated and cybercriminals are developing new – and highly lucrative – ways to attack companies' systems and data.

## 2.6 THE POTENTIAL BENEFITS OF IMPROVED SYSTEMS MANAGEMENT SOLUTIONS

Despite all of these issues, IT departments are being tasked with meeting the business's need for resilient IT services that serve the needs of employees, mobile personnel, customers and suppliers – while maintaining the highest levels of security for all systems and data. In addition, for most businesses, all of this has to be achieved while complying with tight budget restrictions.

To help IT teams with this balancing act of service delivery and budget control, vendors have been trying to develop more comprehensive systems management solutions that can:

- Simplify and automate the:
  - Deployment of operating systems
  - Distribution of application software
- Enable remote troubleshooting
- Generate automatic inventories of all hardware and software, in order to:
  - Give the business total visibility of all elements of its IT environment
  - Simplify the monitoring and control of software licences
- Automatically detect software vulnerabilities – and prioritise patch distribution tasks
- Run regular, scheduled security scans
- Prevent the use of illegal or unwanted software
- Set and manage policies on access to corporate resources

# Systems management – the key challenges

3.0

## 3.1 VISIBILITY

### Why visibility is vital

Whenever a new business process is introduced or a new IT project is rolled out, it's likely that new hardware and software will be introduced into the corporate network. With each passing year, the constant addition of new devices and applications can mean that many companies eventually find that they have relatively poor visibility of exactly what hardware and software is running on their network.

However, without granular-level visibility of every server, laptop, router, switch, removable storage device – and every operating system and application – how can the business effectively manage and secure its network?

- Visibility of hardware helps IT teams to:
  - Implement controls that prevent sensitive data being downloaded onto unauthorised, removable storage devices
  - Monitor attempts to introduce new, unauthorised devices onto the corporate network
  - Identify and retire any old, unsupported devices

- Visibility of software helps IT teams to:
  - Manage how operating systems and applications are patched and updated – in order to ensure systems and software run smoothly and to eliminate security vulnerabilities
  - Prevent the use of unauthorised applications that may contain malware
  - Support compliance objectives – by detecting and eliminating any illegal, 'pirated' software that employees may have downloaded
  - Manage the company's inventory of software licences – so that money is not wasted on unused or unnecessary licences
  - Identify old applications that are no longer supported by the manufacturer

### Mobility adds to visibility issues

With increased use of mobile devices – including Bring Your Own Device (BYOD) initiatives that let employees access the corporate network via their own smartphones, tablets, laptops and other devices – there has never been a greater need for businesses to have total visibility of all devices that attempt to access their network.

## 3.2 SOFTWARE DEPLOYMENT

### The benefits of automation

Manually installing and configuring operating systems and applications on every server, desktop and laptop is very time consuming – especially if the roll-out includes remote or satellite offices.

In the past, if a manual roll-out of software took place over an extended period, problems would arise as a result of different users having access to different software – as some users could be running the latest software, while others were waiting for their computers to be upgraded.

Automating the deployment of operating systems and applications can help to ensure consistency – while also saving time and money.

## 3.3 VULNERABILITIES

### How software vulnerabilities arise

Software is seldom – if ever – free from bugs. Errors exist in the source code of virtually every commercially available software application and operating system.

While some bugs may just introduce an inconvenience that has to be worked around, many software bugs can create major opportunities for malware and cybercriminals to gain access to corporate systems and data… in order to steal sensitive information, steal money, damage a business's reputation or block data or systems until the business makes a ransom payment to the criminal.

Obviously, eliminating these vulnerabilities – in both operating systems and applications – has become an important part of every IT department's day-to-day IT management activities.

### Targeted attacks

Vulnerability exploitation is no longer the result of random attacks. In recent years, there has been a shift from the crude, 'scatter gun' approach – whereby criminals launch broad-based attacks, in the hope of randomly finding a business or organisation that has weak points in its IT infrastructure. Instead, today's highly organised cybercriminals will choose to target specific businesses. Before they launch their attack, the criminals will have completed their research – and will have identified a specific weakness or vulnerability in the targeted company's IT infrastructure.

In some cases, hackers will even compile lists of vulnerabilities that exist within specific businesses' IT environments – and then sell those lists and company names to other criminals.

### The most common method of attack

With all businesses using a wide range of applications for their everyday business operations, it's no surprise that vulnerabilities – within both operating systems and applications – have become the most common way in which malware and criminals attack corporate networks. So it's essential that IT teams monitor all operating systems and applications… and keep them up to date, by applying the latest patches.

## 3.4 PATCH DEPLOYMENT

### Monitoring the availability of patches

When a vulnerability has been identified, one of the biggest issues is ensuring that the time between the release of a new patch and its deployment across the business's IT infrastructure is minimised.

In the past, IT administrators have had to spend time monitoring IT industry news media, in order to find out about new security vulnerabilities within operating systems and applications… while also keeping in touch with vendors for any news about the availability of new patches. This can be very time consuming and can introduce the possibility of information about some critical patches being 'missed' by the business's IT team.

### Problem patches

However, even when a new patch is released, that doesn't necessarily mean that's the end of the problem. In some cases, a patch may adversely affect how an application or operating system runs. In extreme cases, a patch can make an entire system inoperable.

This can leave companies with the dilemma of having to choose between applying the patch – even though its presence may affect the smooth running of key business processes – or continuing to use the application without the benefit of the latest security patch.

Often, IT administrators will test new patches on a separate set of test hardware – to establish whether the patch introduces any severe restrictions on how the application runs.

## 3.5 ACCESS CONTROL

### Deciding who can access the network

For most businesses, there are often guest devices on the corporate network. When partners or customers visit the company, they'll usually bring their laptops and tablets with them – so the business will have to establish policies and controls over how guest devices will be allowed to access the corporate network.

Furthermore, if the business operates a BYOD program, appropriate network access controls will need to be implemented.

Mobile devices and guest devices need to be identified and then checked for the presence of malware. In addition, any user's device should only be allowed to access corporate systems after the business has determined that the device has been configured with the appropriate security software and settings.

# Systems management – the solutions

4.0

## 4.1 GAINING TOTAL VISIBILITY OF YOUR CORPORATE NETWORK

Some systems management solutions are able to scan your entire corporate IT network, identify all components and produce detailed inventories of all hardware and software:

### Hardware inventory

By listing all:

- Servers
- Desktops
- Laptops
- Removable devices – and more

… the inventory helps IT personnel to track the status and history of every hardware item. If the administrator decides that it's necessary, unused devices can be transferred to an archive.

### Software inventory

By listing information about all software that is present on the corporate network, the software inventory supports licence control, the identification of unpatched software and more.

### Empowering the IT team

Total visibility of the hardware and software inventories empowers the IT team to:

- Prioritise management and security tasks
- Eliminate security vulnerabilities
- Adopt a more strategic approach to getting the most out of the company's investment in IT infrastructure

Any 'forgotten' application – including software that is not in active use, but is still present on a workstation or sever – could be the gateway for an attack on the corporate network. With total visibility of all software within the corporate IT network, the IT team will be able to identify unused applications and then either remove them or continue to ensure they are kept up to date – just like any other application.

## 4.2 AUTOMATING THE DEPLOYMENT OF OPERATING SYSTEMS AND APPLICATIONS

Automating the deployment of operating systems and the distribution of application software offers many benefits, including:

- Reducing the load on IT support resources
- Cutting the cost of upgrades and new installations
- Reducing the time taken to complete a roll-out
- Ensuring consistency – so all users receive upgrades within a short period
- Eliminating errors that lead to inconsistencies in configurations

Instead of having to visit every computer in order to deploy the necessary software, the IT administrator prepares one 'master computer' and then copies its image – so that the rest of the nodes can be cloned to include the same 'golden image' of all operating system and application software.

## 4.3 ELIMINATING SOFTWARE VULNERABILITIES

When it comes to eliminating vulnerabilities and managing the deployment of patches and updates, a pre-emptive approach to security is essential. First, it's necessary to conduct an audit of your IT infrastructure – in order to identify every vulnerability in each computer's operating system and applications. Then you should prioritise the deployment of patches – so that you deal with the highest risk vulnerabilities first.

Having identified which software needs to updated – and why – you'll need to know:

- The type of vulnerability that's present
- The danger rating for the vulnerability – low, medium, high or critical
- Which versions of the software are affected
- Which workstations, servers or other devices are affected
- When the vulnerability was identified
- Whether a manufacturer's patch is available

With so many other tasks on your daily agenda, it's essential that all of this information is presented in a clear, concise report that makes it easier for you to decide on the appropriate course of action. In addition, having real-time visibility of your entire IT environment will help you to ensure every instance of the software is updated across your network.

Armed with this information, you'll be able to plan your patch deployment strategy:

- By categorising vulnerabilities according to severity, it's easier to deal with high risk items immediately – while leaving less urgent updates to be implemented outside normal working hours… when there's less demand being placed on network resources.

- For particularly sensitive applications, you should run a regular schedule for updates and patches.

## 4.4 CONTROLLING ACCESS TO THE CORPORATE NETWORK

With visitors bringing mobile devices and laptops onto the company's premises – plus the presence of employees' own devices – effective systems management solutions include flexible tools that enable IT personnel to set policies on:

- Which devices are allowed to access the network
- Exactly what each individual device or group of devices can access on the network – for example, visitors to the business may only need Internet access and will not require access to corporate systems

## 4.5 AVOIDING THE MAYHEM OF MULTIPLE MANAGEMENT CONSOLES

With such a wide range of IT management tasks to cover, many companies are running individual applications for almost every different IT management process that they require. This is both cumbersome and inefficient:

- The IT team has to spend time becoming familiar with every different application's management console.

- During the working day, as the IT support person switches from one management console to another, they constantly have to make sure they are also 'mentally switching' to the conventions, key sequences and terminology that apply to the specific console they are using at that specific time. This repeated changing between different consoles – with each console likely to have a different look & feel and use different conventions – can introduce operational errors… and these errors can affect efficiency and, more importantly, security.

By contrast, there are major benefits to be gained from any solution that enables IT personnel to use a single console to monitor and manage:

- Hardware inventory
- Software inventory
- Operating system and application deployment
- Vulnerability scanning – to identify security vulnerabilities within operating systems and applications
- Patch deployment – to eliminate the security vulnerabilities
- Access Control… and more

Having one centralised console can greatly reduce the amount of time required to perform routine IT management tasks and can also greatly reduce the likelihood of errors.

# Kaspersky Systems Management

5.0

## 5.1 IMPROVED VISIBILITY – OF YOUR ENTIRE NETWORK

### Hardware inventory

Kaspersky Systems Management not only automatically generates an inventory of all hardware in your corporate IT environment, it also automatically discovers any new devices whenever they appear on your network.

The IT administrator is informed about the presence of new devices – via email, events and reports. So the IT team benefits from total visibility of all hardware.

### Software inventory – and licence control

An automatic inventory of all software on the network helps to inform administrators about the use of illegal or undesired software – so that application launches can be automatically blocked and users can be advised that they have contravened the company's policies.

Because the software inventory includes information on purchased licences – for each application – IT personnel can track the usage of applications in order to:

- Prevent the use of unlicensed software
- Renew licences before they expire
- Identify opportunities to reduce the number of software licences

Kaspersky Systems Management makes it far easier to understand:

- What software the business owns
- How much of it the business uses
- How much of it the business needs

### Flexible reports

Administrators can generate a range of reports that help to enable even greater control over hardware that's used on the network. In addition, centralised reports inform administrators about each application's usage history – so IT personnel can monitor and control software usage.

## 5.2 DEPLOYING OPERATING SYSTEMS

### Automated deployment

Kaspersky Systems Management automates the creation and cloning of computer images – in order to save time and optimise the deployment of OS images:

- All of the images that you create are placed into a special inventory that client computers can address during the deployment process.

- Client workstation image deployment can be made with either PXE servers (Preboot eXecution Environment) – that have been previously used on your network – or by using Kaspersky Systems Management's own features.

## 5.3 DISTRIBUTING APPLICATIONS

### Cloud-assisted

Kaspersky Systems Management lets you choose between manual and scheduled deployment of applications – and it supports silent installation mode.

In addition to standard MSI packages, Kaspersky Systems Management also supports deployment through other types of executable files – including exe, bat and cmd.

Using data from the cloud-based Kaspersky Security Network, Kaspersky Systems Management automatically tracks the latest available updates for many of the most commonly used applications – so that you can distribute the most up-to-date version of the applications that you wish to deploy.

### Remote capabilities

For remote offices, the administrator can designate one computer as an update agent for the entire remote office. The installation package is downloaded to the remote office's update agent – and the package is then distributed to all of the remote office's other workstations, from that update agent. This can greatly reduce the amount of traffic on the network.
In addition, Multicast Technology can generate additional savings on network traffic.

Kaspersky Systems Management also helps to enable remote connection to the desktop of any client computer. This can be particularly useful during software deployment projects.

## 5.4 VULNERABILITY ASSESSMENT

Kaspersky Systems Management can scan client workstations for vulnerabilities within the Windows operating system and applications that are running on the workstations. Vulnerability scanning can be performed across the Microsoft database, Secunia and also Kaspersky Lab's own unique database of vulnerabilities.

Kaspersky's vulnerabilities database is a unique element in the company's Vulnerability Assessment technology. Based on continuous research by a dedicated team of Kaspersky experts, the database is compiled using real-time vulnerability and malware information that is gathered from the cloud-based Kaspersky Security Network.

## 5.5 PATCH MANAGEMENT

### Automatic or on demand

Patches can be deployed on demand or automatically. So the entire process – from vulnerability detection to patch deployment – can be automated, while placing minimal load on IT personnel.

When distributing Microsoft updates and hotfixes, Kaspersky Systems Management can act as a Windows Update (WSUS) server. Kaspersky Systems Management will regularly synchronise data on available updates and hotfixes – with Microsoft Windows Update servers – and then automatically distribute them via Windows Update services on client machines across the corporate network… without your IT team having to perform any additional actions.

For non-Microsoft software, information about new software patches is downloaded to Kaspersky Systems Management from Kaspersky Lab's own servers. If a specific update is not available, it can be added manually – and then automatically distributed.

### Reducing network traffic

In order to reduce network traffic, patch distribution can be delayed until after office hours, an update agent can take care of the distribution of patches within remote offices and Multicast technology can be used.

Detailed reports – including information about which workstations are the most vulnerable and why they're vulnerable – help IT administrators to plan and also get an overview of the status of all software across the entire corporate network.

## 5.6 NETWORK ADMISSION CONTROL (NAC)

Kaspersky Systems Management lets administrators create access policies and classify individual devices or groups of devices in order to grant or deny access to the corporate network. For example:

- Devices that are owned by the company – or employee's personal devices – can be:
  - Automatically given access to the network – provided the devices have the latest updates and security patches
  - Updated with the necessary software, updates and patches – before being granted access to the network

- New devices can be automatically recognised as 'guest devices' and can be redirected to the guest portal for authorisation – before they are allowed to access the Internet or the corporate network.

- Security policies can be set in order to block any attempted access by infected devices or devices that contain prohibited software.

# Conclusion

6.0

## 6.1 THE ISSUES

Today's complex corporate IT networks are creating serious operational and security challenges for the vast majority of businesses:

- The variety of endpoints and devices on the corporate network continues to increase
- The range and volume of routine systems management tasks has grown significantly
- IT personnel are finding it difficult to gain visibility of exactly what is on their network
- Coping with vulnerabilities within operating systems and applications can be difficult and time-consuming
- The introduction of mobile devices and BYOD are:
  - Increasing the systems management load
  - Introducing new security issues

**In addition:**

- Malware and cybercriminals have become more sophisticated and accomplished
- Some users will habitually download software – regardless of whether it contains malware or is illegal
- Access to the corporate network has to be tightly controlled – especially for guest devices

## 6.2 THE ANSWERS

Many vendors have developed products that aim to help IT personnel to manage their IT infrastructure. However, not all products cover the complete range of tasks that IT administrators have to tackle on a day-to-day basis. In many cases, this has led to businesses having to use multiple products – with each having its own control console. This reliance on multiple products increases complexity and can lead to gaps in security.

## 6.3 THE KASPERSKY SOLUTION

Kaspersky Systems Management can help IT teams to achieve more from their working day – and their operating budget. Developed for ease of use, Kaspersky's solution:

- Simplifies and automates a vast range of everyday systems management tasks
- Gives clear visibility of all hardware and all software that's present on the corporate network
- Enables remote deployment of software – plus remote troubleshooting

… and all systems management functions can be controlled from one unified management console.

**Kaspersky Systems Management is included in the following products:**

- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

Kaspersky Systems Management can also be purchased as one of Kaspersky's standalone Targeted Security Solutions.

**About Kaspersky**
Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users. Throughout its 15-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for consumers, SMBs and Enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for more than 300 million users worldwide.

Learn more at www.kaspersky.com/business