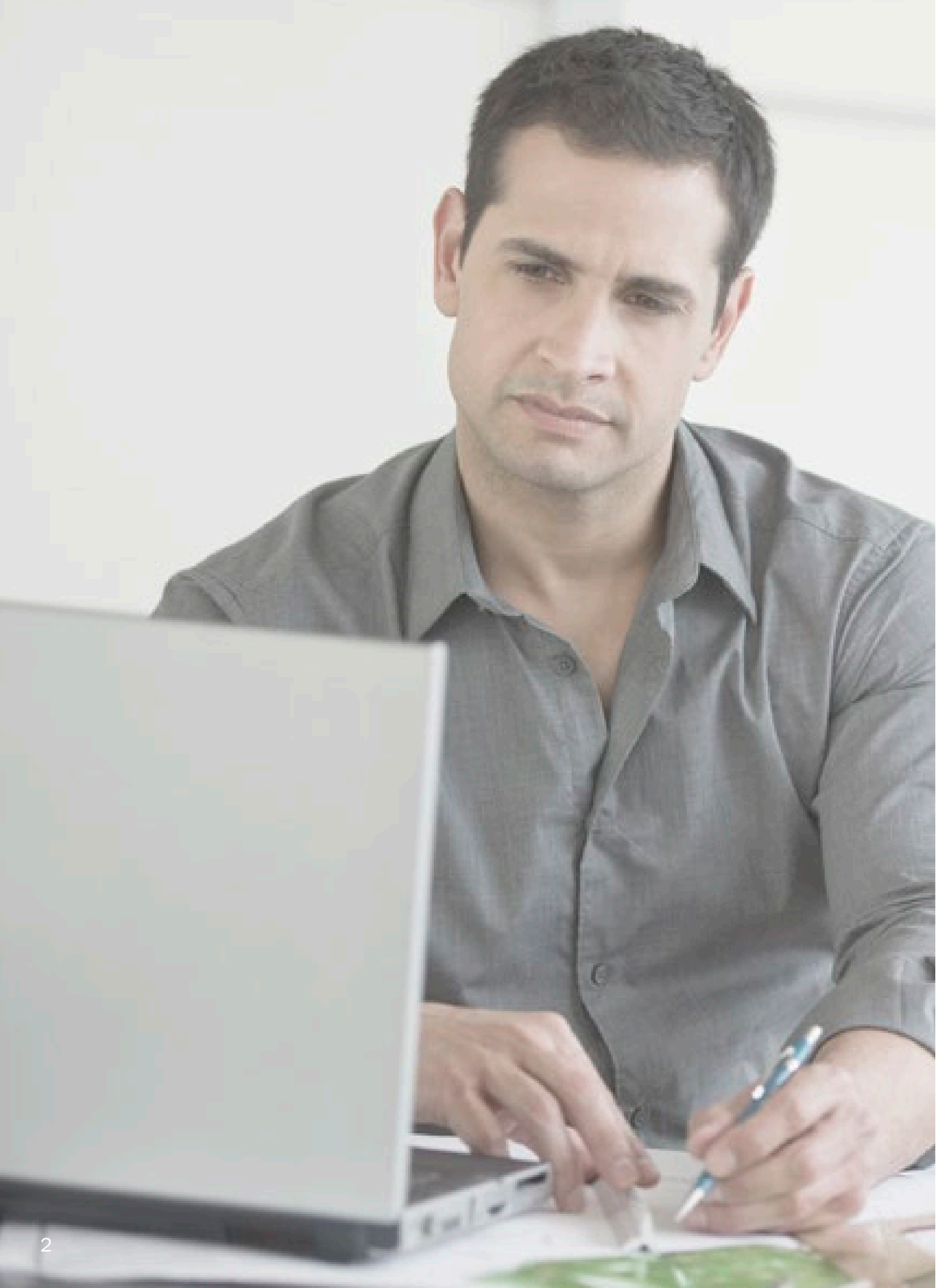
PRACTICAL GUIDE

BE THE ONE WHO PUTS SECURITY ON THE AGENDA

Advice to help you align IT security to your business goals

Empower business through security
kaspersky.com/business
#securebiz

KASPERSKY lab



CONTENTS

PUT SECURITY ON THE AGENDA

DRIVING NEW EFFICIENCIES

In today's fast moving business environment, companies that are quick to adopt new technologies can establish a significant advantage over their competitors. The latest IT developments – together with continually improving business applications – can help all sizes of business to:

- Boost the efficiency of their day-to-day business processes
- Improve their levels of customer service
- Accelerate time-to-market
- Work more closely with suppliers and business partners
- Adapt to changing requirements within their target markets

… all while spending less.

By contrast, companies that are slow to harness the potential offered by new business processes – that are enabled by new technologies – may find that they're constantly lagging behind their peers in terms of efficiency… and that could have a very negative impact on their profit margins.

ENSURING NEW TECHNOLOGIES DON'T BRING NEW RISKS

In particular, companies are benefiting from technology that enables greater mobility – including 'Bring Your Own Device' (BYOD) initiatives – and both server and desktop virtualization programs. However, in common with any form of business change, new technologies can also introduce new challenges… including security risks that have the potential to cause severe damage to the business.

Advanced security solutions are available to protect every element of the corporate IT network – but only if the business takes the necessary time to select the right solution for each potential security issue. Furthermore, care needs to be taken to select only efficient security products that deliver comprehensive protection, without placing undue load on IT systems and IT administration staff… or hampering business agility.

If security isn't on the agenda for every new technology project in your business, there's a real risk that the company may later have to deal with the loss of valuable data, 'leakage' of customers' confidential information, disruption to business-critical processes, compliance issues, financial penalties, loss of reputation and much more.

MEET MAX – INTREPID IT & SECURITY SPECIALIST

As the IT Manager for a business with 150 employees, Max devotes his working life to managing every aspect of the company's IT systems and services – physical, virtual and mobile. He's also responsible for keeping all servers, desktops and mobile devices – plus sensitive corporate data – safe and secure.

With so many tasks to 'juggle' – and tight budget constraints to comply with – Max is always looking for IT solutions that simplify support, automate everyday tasks and help control costs.

Max's bosses do not totally understand the day-to-day challenges that he faces – they just know everything has to run smoothly. However, they also realise that the company's ongoing success is increasingly reliant on IT. Max's ability to introduce new technologies and IT services that enable improved business processes is crucial, all while he also continues to do his day-to-day job and ensure that valuable company information is protected.

A MESSAGE FROM MAX

"From bitter experience… I know that new technologies can introduce new security risks. I've learnt to include security considerations at the start of every project. That way, we can assess the risks, consider whether our existing security technologies are adequate and – if necessary – adapt our security policies."

ENABLING BUSINESS – NOT DISABLING BUSINESS

More than ever before, 'business agility' is essential to a company's ongoing success. Today, many of the factors that can directly affect a business's profitability are subject to more rapid change than was typical even just a few years ago, including:

- Changes in customers' behaviour and requirements
- Changes in the levels of service that your competitors are offering – and customers are beginning to demand

Manufacturing businesses are under pressure to release new products quickly, while retailers and service companies are constantly trying to find ways to reduce operating costs in order to remain competitive.

Obviously, keeping abreast of new technologies – that can help the business rise to these challenges – is essential. However, although IT is likely to play a central role in enabling key processes and boosting efficiency, it's worth remembering that your corporate IT network is there to serve the business. Any technologies that negatively impact your day-to-day business operations – or delay the introduction of efficient, new processes – are not serving your business as well as they should be.

It's exactly the same with IT security. While it's vitally important that you protect your systems – and the confidential data that's stored within them – complex, poorly-integrated security products are no longer suitable for modern, agile, efficient businesses.

IT security needs to take care of protection – without 'disabling' business agility by:

- Slowing down essential processes
- Restricting the business's ability to introduce new technologies that enable new processes
- Being unable to scale adequately, as the business grows

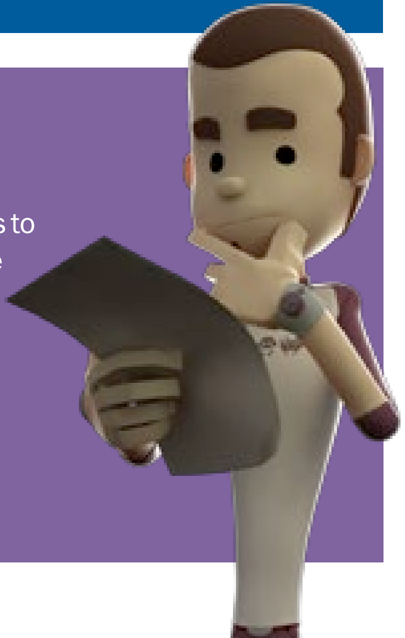
"The proliferation of security products placed on a single device has become daunting to acquire and manage, and equally expensive. In response, many organizations now purchase a single product that can handle multiple security requirements. Security suites/ platforms have the advantage of being easier to install than multiple applications and easier to manage, provided they can be managed with a single console."

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS
JANUARY 2013, IDC #IS01V, VOLUME: 1

A MESSAGE FROM MAX

"In the past, I've spent too long trying to work with inflexible security products that require us to 'bend' our business processes to fit in with the product's own limitations.

"Over the years, I've concluded that the best security software product is one that's able to 'wrap' its protective layers around our key business processes."



CHANGES THAT ARE TOTALLY OUTSIDE YOUR CONTROL

While IT can be a positive force in enabling change that boosts efficiency and profit margins – there's also a less desirable change happening in the business environment. The volume and sophistication of malware and targeted attacks is accelerating – and cybercriminals are becoming more organised and professional in their attempts to steal money, gain access to valuable information or cause disruption.

The direct costs of recovering from an attack – including penalties from regulators – can be substantial. However, the indirect costs – including loss of reputation, legal claims from customers and suppliers that have had confidential information subjected to unauthorised access, loss of intellectual property that gave the business its competitive edge and more – could be even more significant.

KEY CONSIDERATIONS TO HELP YOU CHOOSE AN EFFECTIVE SECURITY SOLUTION

ANTI-MALWARE IS THE ESSENTIAL FIRST STAGE IN YOUR DEFENCES

Anti-malware software is still a vitally important element in a company's IT defences. Good anti-malware solutions don't just rely on signature-based protection, they also include:

- Heuristic analysis
- Cloud-enabled, real-time supply of data about new and emerging threats

Signature-based protection is reliant on security vendors analysing each new malware program that they discover – and then delivering updates to the malware databases held on endpoint devices – but there's a period during which your corporate IT network could be highly vulnerable. Even if the period between the launch of the new malware program and the availability of the new signature update is only a few hours, it still means your systems are vulnerable… unless your security software includes additional protection technologies.

Heuristic analysis provides a more proactive response to the emergence of new malware. In the absence of a malware signature, heuristic analysis can detect many previously unknown malware items – or new variants of an existing malware threat.

The third essential element of modern anti-malware protection is delivered from the cloud. By adding cloud-based services – that deliver real-time data about new malware and other threats – security vendors can greatly enhance the corporate IT network's ability to combat the latest malware attacks.

BUT IS ANTI-MALWARE ENOUGH AGAINST NEW, COMPLEX THREATS?

Although anti-malware is a vitally important component in your defences – and solutions that combine signature-based, heuristic and cloud-assisted technologies deliver higher levels of protection than previous solutions – it's very unwise to rely on just anti-malware to defend your business and its reputation.

Unfortunately – with cybercriminals using more sophisticated techniques to compromise business security – anti-malware simply isn't enough to guarantee the security of your systems and data.

For today's threats, it's essential that businesses use a security product that delivers a multi-layered system of security technologies, including:

- Anti-malware
- Application Control – with dynamic Whitelisting
- Device Control
- Web Control
- Vulnerability Assessment
- Patch Management
- Data Encryption

…plus specialist security technologies to protect mobile devices, virtualized environments and more.

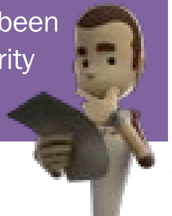
"Traditional endpoint security is synonymous with antimalware. It's no secret that signature-based anti-malware technologies have not fared that well with today's modern malware. As a result, enterprise IT is moving away from point anti-malware technologies and moving to deploy layered defence with a portfolio of measures that include not just anti-malware but also host-based firewall/IPS, application control, device and media control, and endpoint encryption."

THE FORRESTER WAVE™: ENDPOINT SECURITY, Q1 2013
ENDPOINT SECURITY SUITES TAKE CENTER STAGE IN THE ENTERPRISE
FORRESTER RESEARCH, INC
4TH JANUARY 2013

A MESSAGE FROM MAX

"Security breaches don't just damage the business – they can also result in penalties for the senior management team.

"In many regions, regulatory bodies can apply a range of penalties – including fines and / or prison terms – for directors of any business that has been negligent over its security measures."



CONTROLS – PROTECTING YOUR BUSINESS AGAINST YOUR USERS' SECURITY ERRORS

APPLICATION CONTROL AND DYNAMIC WHITELISTING

There are many ways in which unauthorised applications can appear on your corporate network – and some of those unwanted applications could present a security risk:

- Users may deliberately download applications over the Internet
- Users may download applications onto their desktops, from removable storage devices

Naturally, if you aren't given a chance to check and approve these applications, how do you know that they are malware-free… and how can you ensure their presence on your network isn't causing licensing issues?

Security vendors have developed Application Control features that make it easy for you to control which applications are permitted to launch on your network. Application Control tools can give you the ability to manage:

- Which applications are allowed to run (whitelisting)
- Which applications are blocked (blacklisting)
- How authorised applications are allowed to behave, while they're running (application privilege control)

Most Application Control tools will let you choose between operating a Default Allow or a Default Deny policy:

- **Default Allow** – choose this option if you wish to allow any application to launch, unless the application is included on your blacklist of programs that are blocked
- **Default Deny** – choose this policy to make sure all applications are blocked from launching, unless an application is included on your whitelist of safe programs and is permitted to run

The Default Deny option can be particularly powerful in helping to prevent malware from launching and also preventing users from running applications that are not relevant to their job. However, a Default Deny policy is far easier to run if your security vendor helps you to assess the security of common applications – by analysing programs in the vendor's own 'whitelisting laboratory'.

> "Protection from highly targeted, new and low-volume attacks requires a more proactive approach that is grounded in solid operations management processes, such as vulnerability analysis, patch management and application control capabilities. In particular, application control, which restricts execution to known good applications, is proving to be effective in demanding security environments, and is especially effective when combined with support for trusted change and supplemented with cloud-based file reputation services."
>
> MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS
> 8TH JANUARY 2014
> GARTNER, INC.

DEVICE CONTROL

Removable storage devices – including USB flash drives, SD cards and external hard disk drives – can be used to steal confidential data or to download malware onto the corporate network. So their use needs to be tightly controlled.

Device Control features can make it easy for you to identify which devices are authorised for use on your corporate network – and which are unauthorised devices that employees or contractors are using to connect to your systems. In addition, Device Control lets you:

- Block specific types of device – such as all removable storage
- Block all devices that use a specific type of bus – for example all USB devices
- Block individual devices – according to their unique identifiers
- Enforce encryption when you're copying files to a removable device
- Set up device restrictions for specific times of day

USB DEVICE HELPS TO ENABLE HIGH-PROFILE ATTACK

One of the most notorious attacks against a critical infrastructure owner is believed to have been launched via a simple USB flash drive. Stuxnet, a cyber-sabotage worm, is thought to have been downloaded from a USB device onto systems within a nuclear facility.

WEB CONTROL

Giving your employees uncontrolled access to the Internet can affect your business's security and productivity.

Even if your employees are visiting legitimate websites, in the course of their everyday work tasks – how can you be sure those sites are safe? There are many cases of cybercriminals hacking genuine websites, so innocent visitors are subject to 'drive-by' downloads – whereby malware is automatically downloaded onto the user's device. Obviously, this creates the opportunity for the malware item to spread across your corporate IT network.

Quite apart from the security risks that the Internet can present, surfing the Web can also be a major distraction that can affect employee productivity.

Some security solutions include flexible Web Control features that let you:

- Completely block access to specific sites or categories of websites – such as gambling or sites with adult content
- Completely block access to sites that enable illegal or unauthorised downloads – including unlicensed applications
- Limit access to social networking sites – such as only allowing access during lunch breaks
- Use the latest information – delivered in real time from the cloud – in order to warn users about infected or dangerous sites and help to prevent 'drive-by' infections

PREVENTING THE EXPLOITATION OF VULNERABILITIES

One of the most common ways for cybercriminals to gain access to computers and mobile devices is via vulnerabilities within operating systems or applications. These vulnerabilities normally arise from 'bugs' in the code of the application or operating system (OS). As soon as the hacker community has identified a new bug and worked out how to exploit it, news of the vulnerability quickly spreads – and a growing number of new attacks can be unleashed.

With most modern businesses relying on a wide range of software applications – and possibly several different versions of an OS – it can be very difficult for IT departments to keep up with all the latest vulnerabilities and to establish whether the software developers have issued any fixes or patches for those vulnerabilities. In addition, there's the onerous task of having to prioritise the distribution of the necessary patches – and then implement them.

VULNERABILITY ASSESSMENT

Although Vulnerability Assessment is normally associated with systems management – rather than security – it is vitally important in helping you to defend your corporate IT network against attacks. So it's essential to choose a security or systems management solution that automatically scans your network for vulnerabilities.

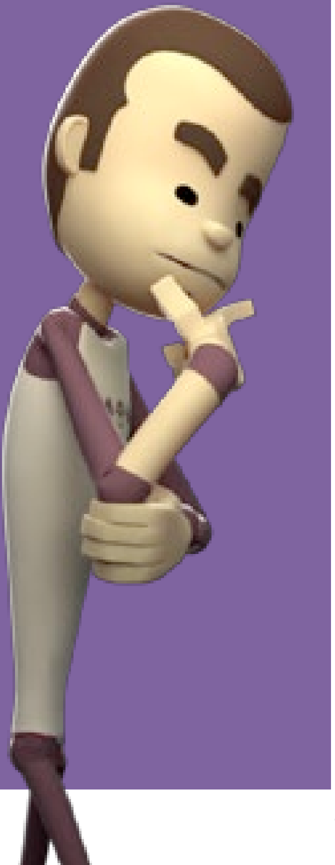
PATCH MANAGEMENT

Obviously, identifying the OS and application vulnerabilities that are present on your corporate IT network is just the first stage. You then need to prioritise and implement the latest software patches and updates. Again, this can be regarded as a systems management activity – but it's a task that can greatly improve your security and it's one that good security or systems management software can help you to automate.

A MESSAGE FROM MAX

"As the markets for IT security and IT management software have matured, fully-integrated security and systems management solutions have begun to emerge. The days of having to take 'point solutions' from different vendors and then try to get them to work together are well and truly over… thankfully!

"However, it's worth checking on the reality behind any vendor's claims about integration. If a vendor has 'bolted on' new functionality – simply by buying another vendor's solution – that can introduce problems. Try to make sure that there's more than just a 'veneer of integration' that is merely there to hide a whole host of operational issues."



DATA ENCRYPTION

If an employee loses a laptop, USB flash drive or a removable hard disk, sensitive business data could fall into the wrong hands – and that could be very costly. However, if the data has been encrypted, the loss of the device needn't lead to the loss of any confidential data that's in a readable form. After it has been encrypted, the data can only readily be 'decoded' – into a readable form – by using the necessary decryption algorithm.

Despite being available for many years, data encryption is not used by all businesses. Part of the blame lies with the lack of usability of some of the commercially available encryption products. Many have proven to be too complex to configure and manage, or have adversely affected IT performance.

In the past, this has led many companies to abandon the use of encryption – in favour of maintaining performance and productivity. However, security vendors have responded to the demand for more efficient solutions and it's now possible to buy encryption products that are easy to use.

MOBILITY BRINGS EVEN MORE RISKS

Mobile devices have revolutionised the ways in which businesses and their remote workers can interact and get more out of their working day.

Smartphones are much more than just simple phones. Because they're powerful computers that are capable of storing a lot of confidential corporate data – together with access codes and passwords for your corporate network – you need to protect them in the same way that you secure your desktops and servers.

However, the portability of smartphones, tablets and laptops also introduces additional security risks. All of these devices are outside your traditional security perimeter. They can easily be lost or stolen and that can result in unauthorised users gaining access to your corporate network.

BYOD ADDS MORE COMPLICATIONS

Bring Your Own Device (BYOD) initiatives offer many benefits for businesses and employees. However, the fact that employees will be using devices that contain both confidential business information and the user's personal data can introduce risks.

Furthermore, if employees are free to use almost any mobile device, the task of managing how all of those different devices are allowed to access your business systems – and ensuring they each have effective security software installed on them – can be particularly tricky.

Choosing a mobile security solution that includes extensive mobile device management (MDM) features is essential.

VIRTUALIZED ENVIRONMENTS ARE VULNERABLE TOO

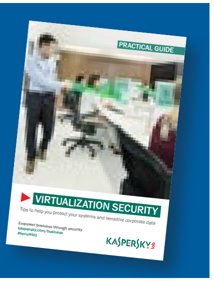
Virtualized server and desktop environments can help businesses to control hardware acquisition costs and reduce maintenance, energy and licensing costs. In addition, because virtual machines can be rapidly deployed, virtualization can enhance business agility – by ensuring new IT services can be delivered to the business, without unnecessary delays.

Despite the common myth that virtual machines are somehow more secure than physical servers and desktops, all virtual machines need to be protected – just like physical hardware. However, the security technologies that are used to protect virtual environments can be very different from the security products that defend physical IT infrastructure.

Running a traditional, agent-based security solution on each virtual machine will severely limit the consolidation ratio that you can achieve – which means your virtualization project will generate a lower return on investment. Instead, it's best to choose a security solution that has been optimised for virtual environments. These can eliminate the need to have identical anti-malware databases and security agents on every virtual machine.

FIND OUT MORE…
…about the challenges of securing virtualized environments.
Get Kaspersky's latest report:

Practical Guide – Virtualization Security
Tips to help you protect your systems and sensitive corporate data



THE CASE FOR SECURITY THAT'S TIGHTLY INTEGRATED WITH SYSTEMS MANAGEMENT

Because well-executed vulnerability assessment and patch management features can have such a positive effect on the overall security of your systems, there's a strong argument for choosing a security solution that includes these and other systems management functions.

Many businesses run separate security software and systems management software packages – from different vendors. However, this can make security and systems management more complex to configure and control – and that can:

- Add to the burden on IT administration
- Create gaps in corporate security

By contrast, a solution that combines security and systems management functionality – within one product, developed by one vendor – can simplify both sets of tasks.

Some combined security and systems management solutions also have one unified management console for all tasks. This can bring major benefits for IT administrators:

- There's only one set of features to learn
- There's no need to keep switching between different consoles for security and systems management
- Single policies can be implemented – to cover both security and systems management issues

A MESSAGE FROM MAX

"At first sight, the need to use two or three different management consoles – to manage individual security and management technologies from different vendors – may seem like a trivial task for a professional IT administrator.

"However, in practice, it's surprisingly time-consuming and can easily lead to errors – especially when you're under pressure to react quickly to a security issue."

HOW KASPERSKY LAB CAN HELP… INTEGRATED SECURITY AND SYSTEMS MANAGEMENT

In addition to award-winning anti-malware – plus flexible control technologies, data encryption, mobile security and virtualization security – Kaspersky has integrated systems management and mobile device management (MDM) technologies… so you can manage your IT security and your IT infrastructure from one product and one management console.

> "The latest Kaspersky Endpoint Security for Business (KESB) platform demonstrates the company's ability to develop issues-based offerings challenging resource, management and cost complexities in this category. IDC positions Kaspersky Lab as a Leader in the Western Europe Endpoint Security Software IDC MarketScape."
>
> IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS
> JANUARY 2013, IDC #IS01V, VOLUME: 1

> Kaspersky is recognised as 'A Leader' in the Gartner Magic Quadrant for Endpoint Protection Platforms.
>
> MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS
> 8TH JANUARY 2014
> GARTNER, INC.

ADVANCED ANTI-MALWARE PROTECTION

Kaspersky's latest anti-malware technologies deliver a powerful combination of:

- Signature-based protection
- Proactive technologies
- Cloud-assisted delivery of protection against new malware

… for Mac, Linux and Windows platforms – plus a wide range of mobile devices, including Android, iOS, Windows Phone, Windows Mobile, BlackBerry and Symbian.

With Kaspersky's Urgent Detection System database continually being updated with information about new malware discoveries, Kaspersky's advanced anti-malware technologies defend businesses against the latest threats and attacks – even before a new malware signature has been released.

In addition, Kaspersky's System Watcher technology monitors the behaviour of applications that are running on your endpoints. If System Watcher detects suspicious behaviour, the application will be blocked and malicious changes automatically rolled back.

Kaspersky continues to innovate by introducing new anti-malware technologies – including Automatic Exploit Prevention (AEP), which monitors systems to identify behaviours that are commonly performed by malware that tries to exploit vulnerabilities within the operating system or applications. AEP effectively blocks exploits – to protect systems against Zero-Days.

FLEXIBLE CONTROL TOOLS

APPLICATION CONTROL

Kaspersky's Application Control tools give you granular control over how applications are allowed to run on your corporate network – so you can easily implement a Default Deny or Default Allow policy:

- Default Deny lets you block all programs, except those on your whitelist
- Default Allow blocks only blacklisted applications – and lets all other programs run

DYNAMIC WHITELISTING

Kaspersky is the only security vendor that has established its own Whitelist Lab that assesses commonly used applications and checks them for security risks. Updates for Kaspersky's dynamic whitelist of applications are automatically downloaded from the cloud-based Kaspersky Security Network – to make it easier to run a Default Deny policy, using up-to-date information on applications.

Whereas some vendors may update their whitelist of applications on an infrequent basis, Kaspersky's dynamic whitelisting delivers superior protection.

DEVICE CONTROL

Kaspersky's Device Control features help you to control the use of removable devices – so you can guard against the security risks that unauthorised devices can introduce. It's easy to:

- Control access privileges – for specific types of device, a specific bus or an individual device
- Define time periods when your Device Control policies apply – for example, to prevent devices accessing your corporate network outside your normal office hours

WEB CONTROL

Web Control tools simplify the task of monitoring and filtering each employee's web usage. Kaspersky makes it quick and simple to manage controls that permit, prohibit, limit or audit users' access to specific websites or categories of websites – including games, gambling or social networking sites.

Kaspersky also assesses the reputation of websites and delivers warnings – in real time, from the cloud – to help users avoid dangerous sites and prevent drive-by infections.

> "Because of its extensive security strength and an attractive price point, we expect many organizations to short-list Kaspersky when considering an endpoint security product."
>
> THE FORRESTER WAVE™: ENDPOINT SECURITY, Q1 2013
> ENDPOINT SECURITY SUITES TAKE CENTER STAGE IN THE ENTERPRISE
> FORRESTER RESEARCH, INC
> 4TH JANUARY 2013

VULNERABILITY SCANNING AND PATCH MANAGEMENT

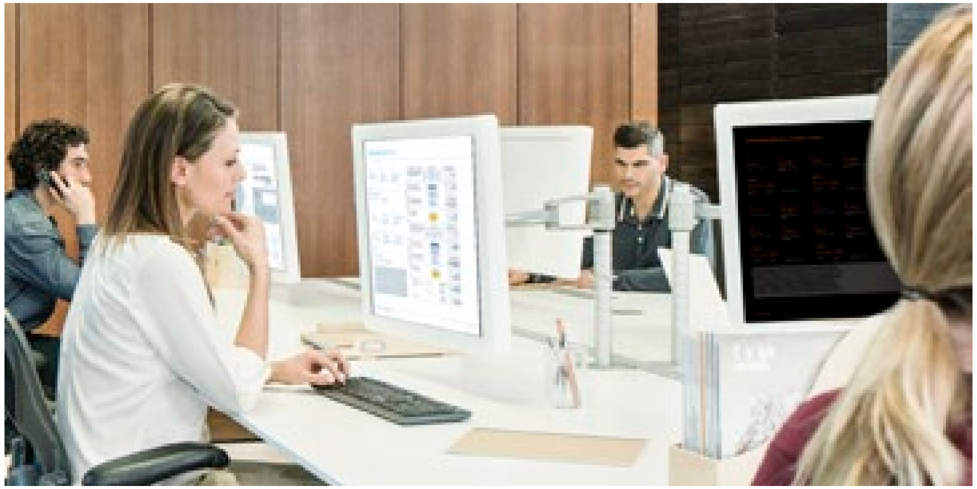
The Kaspersky Systems Management application includes automatic vulnerability scanning – plus patch distribution functionality – to help you maintain the stability and security of your corporate network.

VULNERABILITY SCANNING

Kaspersky technologies scan your endpoints to find security vulnerabilities that result from unpatched operating systems and applications. In addition to Kaspersky's own vulnerabilities database, the scanner also works with Secunia's and Microsoft's databases.

AUTOMATING PATCH DISTRIBUTION

All vulnerabilities that are identified during a scan are 'colour coded', to help you decide on patch priorities. Kaspersky technologies can automatically distribute urgent patches across your network and you can schedule non-urgent software updates for outside normal office hours.



EASY-TO-USE DATA ENCRYPTION

Kaspersky's encryption tools provide both:

- Full disk encryption (FDE) – which operates on the physical sectors of the disk, for an 'encrypt everything at once' strategy
- File level encryption (FLE) – which encrypts individual files or folders, to enable secure sharing of data between employees and trusted partners

While an AES encryption algorithm – with 256 bits of key length – delivers strong encryption, all encryption and decryption processes are totally transparent to your users. Instead, your IT administrators set up simple policies that control which files and disks are automatically encrypted. Furthermore, the encryption and decryption processes have no significant impact on IT performance.

For encryption on mobile devices, Kaspersky gives you the ability to manage the encryption facilities that are resident within many common mobile platforms.

MOBILE SECURITY AND MOBILE DEVICE MANAGEMENT

Kaspersky was one of the very first vendors to offer antivirus solutions for mobile devices. Today, the company is a leader in providing both advanced anti-malware agents and efficient Mobile Device Management (MDM) capabilities in one integrated solution.

Kaspersky's mobile security technologies protect a wide range of mobile platforms – including Android, iOS, Windows Phone, Windows Mobile, BlackBerry and Symbian – against the latest malware threats. Because Kaspersky combines signature-based protection, proactive defences and cloud-based technologies, mobile devices benefit from multi-layered anti-malware.

CONTROL TOOLS

Application Control makes it easy to manage which applications are allowed to run on any mobile devices too. It's easy to implement a 'default deny' policy that only lets whitelisted applications run or implement a 'default allow' policy – that only blocks blacklisted applications.

Web Control tools let you block malicious websites and websites that don't conform to your corporate security or Internet usage policies.

SEPARATING CORPORATE DATA AND PERSONAL DATA – FOR MORE SECURE BYOD INITIATIVES

Kaspersky's containerisation technology makes it easy to separate corporate data and personal information on a user's mobile device. A special container holds corporate applications and you can enable the encryption of corporate data. If an employee leaves the company, you can remotely run a selective wipe procedure that deletes all corporate data from their mobile device.

DEALING WITH A LOST OR STOLEN MOBILE DEVICE

If a mobile device is lost or stolen, Kaspersky's remotely-operated features let you:

- Lock the mobile device
- Delete corporate data or all data on the device
- Find the device's approximate location

Even if a thief changes the SIM in the device, Kaspersky's SIM Watch technology will send you the new phone number – so you can still access the remote lock, find and data wiping features.

SIMPLIFYING MOBILE MANAGEMENT

Kaspersky's extensive mobile device management MDM capabilities simplify the deployment of Kaspersky's mobile security agent and any other applications you wish to distribute – either over the air (OTA) or via a tether – and they include support for both Microsoft Exchange ActiveSync and Apple MDM Server.

A CHOICE OF VIRTUALIZATION SECURITY TECHNOLOGIES

With security solutions for a wide range of virtual environments – including VMware, Citrix and Microsoft – Kaspersky Security for Virtualization lets you choose from two virtualization security approaches, that have been developed to help minimise the impact on consolidation ratios and help you boost your return on investment.

KASPERSKY SECURITY FOR VIRTUALIZATION I AGENTLESS

For VMware-based virtual environments, Kaspersky Security for Virtualization I Agentless works through VMware vShield – to give you the ability to protect every virtual machine on a virtual host, by installing a single virtual machine that's dedicated to security (Virtual Security Appliance or VSA).

In addition to providing file-level anti-malware protection and network-level protection – via Kaspersky's Network Attack Blocker technology – Kaspersky Security for Virtualization I Agentless also benefits from real-time threat data from the Kaspersky Security Network.

KASPERSKY SECURITY FOR VIRTUALIZATION I LIGHT AGENT

With one dedicated virtual security appliance installed on the host and a small software agent – called a light agent – installed on each guest virtual machine, Kaspersky Security for Virtualization I Light Agent delivers a higher level of security than agentless virtualization solutions offer. However, it still uses much less processing power and storage capacity than are required to run a traditional, agent-based security product – thanks to it offloading anti-malware tasks and the malware definition database to the Virtual Security Appliance.

In addition to advanced anti-malware protection and network-level protection, Kaspersky Security for Virtualization I Light Agent also includes Application Control, Device Control and Web Control toolsets.

HIGH CONSOLIDATION RATIOS – AND HIGH AVAILABILITY

Whether you choose Kaspersky Security for Virtualization I Agentless or Kaspersky Security for Virtualization I Light Agent, there's no need to reboot any machines – or put the host server into maintenance mode – when you're deploying your Kaspersky security solution.

This is vitally important for any data centre or business that needs to achieve 'five nines' (99.999%) uptime.

COMBINING SECURITY AND SYSTEMS MANAGEMENT

MANAGING HARDWARE, SOFTWARE AND LICENCES

By automatically discovering all hardware and software in your corporate IT network – and recording all items within hardware and software inventories – Kaspersky gives you detailed visibility of all of your IT assets. This helps you to:

- Monitor the security status of your systems
- Apply the necessary security settings
- Identify breaches of licence conditions

OPERATING SYSTEM DEPLOYMENT

Kaspersky helps to optimise the deployment of operating systems, by providing automatic features for creating and cloning computer images that can be stored in a special inventory – ready for access during deployment.

APPLICATION PROVISIONING

Kaspersky helps you to simplify the distribution of applications – by helping to deploy software on command or according to your schedule.

REMOTE DEPLOYMENT OF SOFTWARE… PLUS TROUBLESHOOTING

Whenever you need to install software at a remote office, Kaspersky lets you use one local workstation as the update agent for the entire remote site. In addition, remote access helps to simplify troubleshooting.

NETWORK ACCESS CONTROL

With technologies that automatically discover all devices on your corporate network, Kaspersky makes it easier for you to:

- Control which devices are allowed to access your network
- Check that each device complies with your corporate security policies
- Block network access for devices that don't have the necessary security software running on them

A SINGLE, UNIFIED MANAGEMENT CONSOLE

Kaspersky security technologies and systems management functionality can be configured and controlled from one management console that gives IT administrators a 'single pane of glass' view.

By eliminating the need to run several different – and incompatible – consoles, Kaspersky Security Center reduces complexity and saves time for your IT department.

It simplifies a vast array of administration and security tasks, across physical, mobile and virtual environments – so you benefit from:

- Greater visibility of every endpoint on your corporate IT network
- A simple interface into Kaspersky's security, MDM and systems management features
- Detailed control over users' activities – including how they use applications, devices and the Web

KASPERSKY'S PROVEN RECORD OF INNOVATIONS AND ACHIEVEMENTS

Among its many awards, accolades and recognitions, Kaspersky has received the Product of the Year Award 2013 – from the independent testing lab, AV-Comparatives – after the company's Internet Security solution consistently demonstrated the best results in testing throughout 2013.

The AV-Comparatives test program is considered the most comprehensive in the industry – and the Product of the Year Award is based on the total ranking during a full year of tests. Kaspersky Internet Security was selected because the product showed a solid lead in all the tests it underwent. Kaspersky is also a previous winner of the AV-Comparatives' Product of the Year Award – having won in 2011 and also tied for the top spot in 2012.

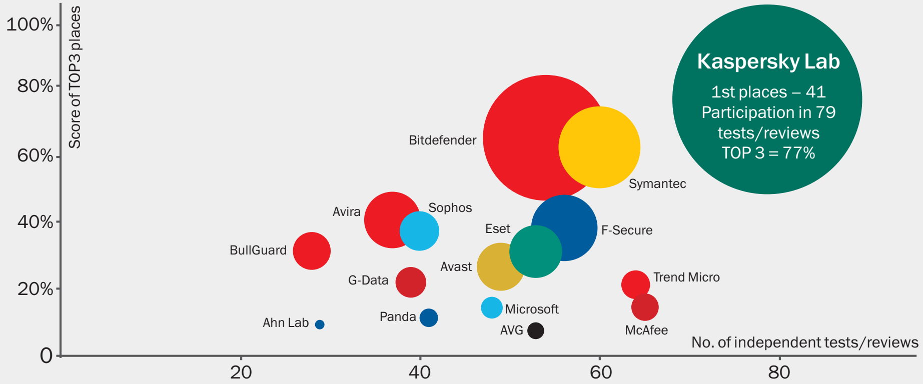
Because Kaspersky Endpoint Security for Business employs the same core anti-malware protection technologies that are used in Kaspersky Internet Security, your business can benefit from Kaspersky's award winning protection.

Other awards and achievements include:

- 'Information Security Vendor of the Year' award – SC Magazine Awards Europe 2013
- 'Information Security Team of the Year' award – SC Magazine Awards Europe 2013
- Excellence Award winner – SC Magazine Awards 2013
- Kaspersky Endpoint Security for Windows was awarded highest prize in Enterprise Antivirus Protection April – June 2013 test by Dennis Technology Labs
- The greatest number of gold and platinum awards – across all testing categories – from the third-party Anti-Malware Test Lab, since 2004
- More than 50 pass scores on the rigorous VB100 testing regimen, since 2000
- The Checkmark Platinum Product Award from West Coast Labs

MORE TOP 3 POSITIONS THAN ANY OTHER VENDOR

In 2013, Kaspersky Lab products participated in 79 independent tests and reviews. Our products were awarded 41 first places and received 61 top-three finishes.



Notes:
- According to summary of results of independent tests in 2013 for corporate, consumer and mobile products
- Summary includes tests conducted by the following independent test labs and magazines:
  - Test labs: Anti-Malware.ru, AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, TollyGroup, VB100
  - Magazines: CHIP Online, ComputerBild, Micro Hebdo, PC Magazine, PCWorld, PC Welt
- In the above graph, the size of each bubble is related to the number of 1st places achieved

MAX'S STRATEGY TIPS FOR PUTTING SECURITY ON THE AGENDA

> "With the relentless increases in the volume and sophistication of malware and other threats, security has to be on the agenda for every business's IT strategy."

- Take time to 'step back' from your everyday IT routine and devote some effort to evaluating your current IT security measures. Assess whether they're adequate to meet today's challenges.
- Choose IT security that is as flexible and scalable as possible – and avoid using any product that restricts the agility of your business.
- Remember there's a lot more to IT security than just anti-malware. Look for security solutions that offer additional protection – including Application Control, Device Control, Web Control, data encryption and more.
- With increasing use of mobile devices, don't forget that smartphones and tablets are capable of storing vast amounts of confidential business data. Make sure all mobile devices that access your corporate network and business information are running appropriate security software. Deploy Mobile Device Management (MDM) to help you monitor and control the mobile devices on your network.
- Before launching a Bring Your Own Device initiative (BYOD), assess how it could affect business security. Consider security technologies that will allow you to separate corporate data and the user's personal data on their mobile device.
- Virtualized environments are no safer than physical servers and desktops – they all need protection. However, take care over your choice of security products for your virtual infrastructure – the wrong security technology could adversely affect consolidation ratios.
- Because software vulnerabilities are one of the most common ways in which malware and cybercriminals access computers and networks, make sure your systems management software includes vulnerability assessment and patch distribution capabilities. Although these are systems management functions, they can have a dramatic effect on your security.
- Choosing a product that combines security and systems management can simplify tasks and allow you to set integrated policies… and that could save you a lot of time.
- For IT security – and systems management software – ease of use is much more than just a convenience. If your security and systems management software is complex and difficult to manage, there's a far greater risk of errors and security gaps.

> "Kaspersky Lab focuses on what it does very well: Endpoint security. The high scoring for capability and strategic criteria recognizes the organic development within the company that ensures, where possible, the various components for workstations, laptops, mail, collaborative servers and Internet gateways utilize the same code base for ease of updates and continuity in the event of a product failure."
>
> **IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS JANUARY 2013, IDC #IS01V, VOLUME: 1**

Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organisation and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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 more than 16-year history, Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide.

Learn more at kaspersky.com/business

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.

© 2014 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Mac and Mac OS are registered trademarks of Apple Inc. Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. IBM, Lotus, Notes and Domino are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, Windows Server and Forefront are registered trademarks of Microsoft Corporation in the United States and other countries. Android™ is a trademark of Google, Inc. The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.