IF IT'S NOT KASPERSKY ENDPOINT SECURITY 10, IT'S NOT AN ENDPOINT PROTECTION PLATFORM

▶ 10 BENEFITS

THAT ONLY AN INTEGRATED PLATFORM SECURITY SOLUTION CAN BRING

Kaspersky Lab's Global IT Security Risk Report[1] found that while IT security remains the number one concern for IT professionals, only 59 per cent say they feel ready to combat the growing range of threats; just a quarter of respondents said they had a proactive security stance.

The traditional way of addressing these challenges — multiple solutions from multiple vendors, each requiring their own consoles, compatibility and management strategies — has only added to the complexity. IT managers are looking for a more consolidated approach that reduces complexity while simplifying management tasks.

Gartner research shows that the days of traditional endpoint security — discrete anti-malware, encryption, device and network access control — are coming to an end[2]. Endpoint protection platforms (EPP), promising tightly integrated security technologies are the growing trend in data protection.

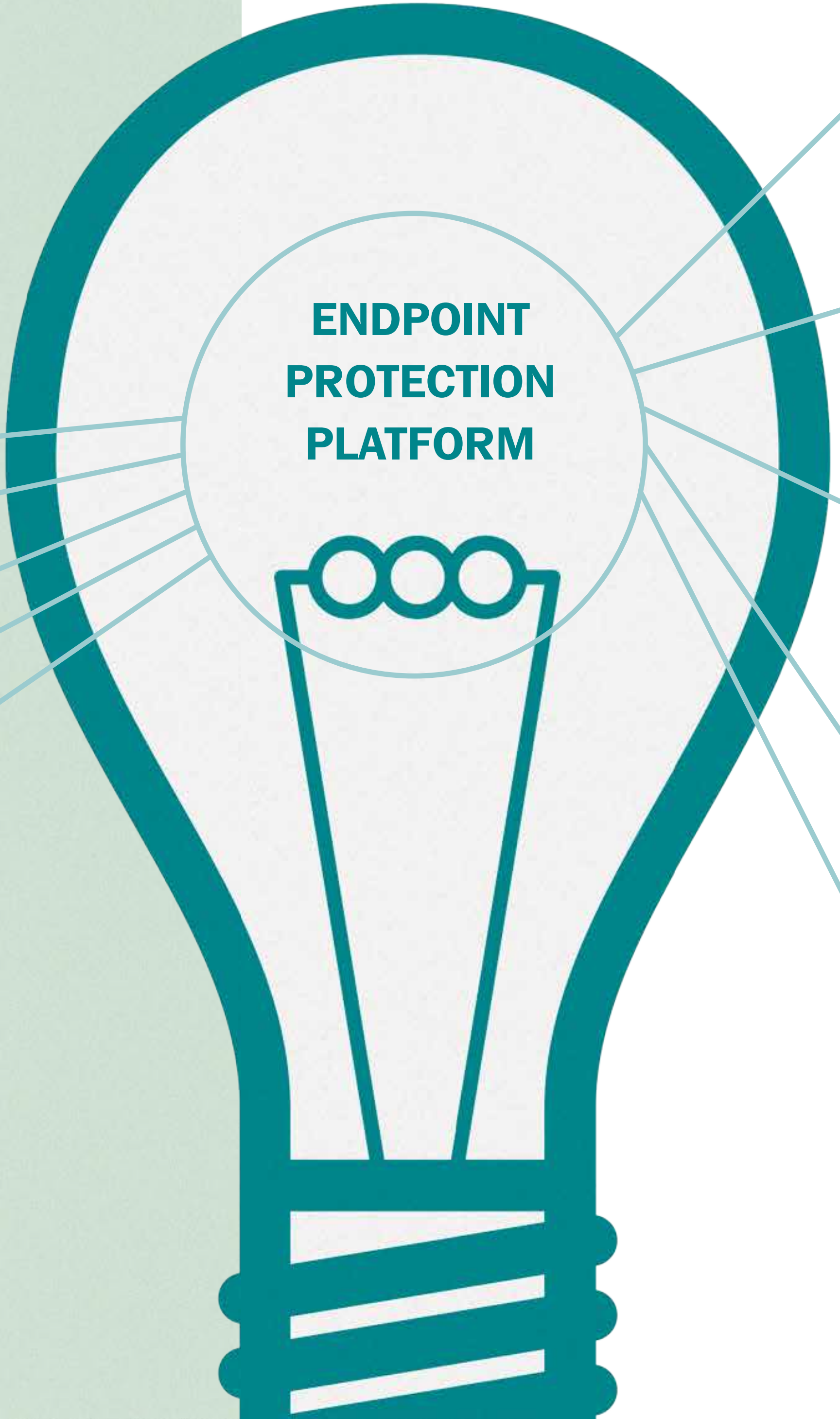
But there's a world of difference between "integration" and a genuine platform. And when it comes to integration, there are varying degrees of completeness. For many vendors, "integration" has become just another word for "compatible".

There are plenty of vendors offering "integrated" solutions, but dig a little deeper and you'll see that there's a significant difference between "playing nicely" together and true synergy.

[1] Global IT Security Risk Report 2012.

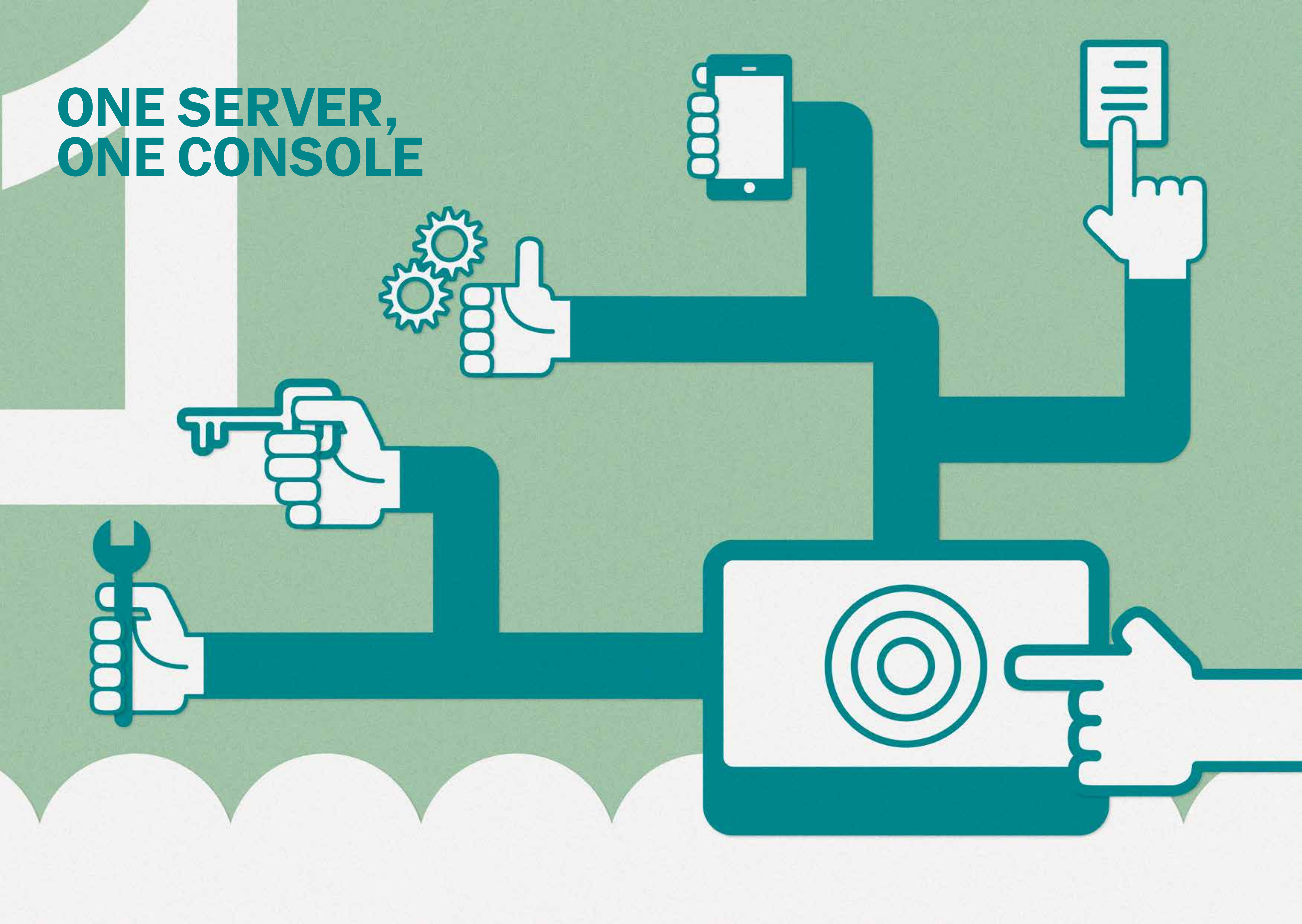
[2] Gartner: Endpoint Protection Platforms: Blending Security, System Management and Data Protection (May 2011)

There are some benefits that only a genuinely, deeply integrated platform solution can bring. Kaspersky Endpoint Security for Business is uniquely placed to deliver the following benefits to IT administrators:



1. One server, one console
2. Single agent architecture, one-step installation
3. The Single Policy Advantage
4. The Synergy Effect — greater than the sum of its parts
5. Unified administrator rights management — increased audit and control capability through one console
6. Common structure, look and feel — faster, easier reporting
7. A clearer, deeper view into data — integrated dashboards and reporting
8. Unified license management and control —drive efficiency, take control
9. Single code base, built in-house, drives deeper integration
10. Integrated purchase model — all the functionality you need in a single purchase

ONE SERVER, ONE CONSOLE



1 ONE SERVER, ONE CONSOLE

Kaspersky Lab's solution is unique in offering a tightly integrated, single management server and administration console that covers every aspect of endpoint security, from anti-malware to data protection, mobile device management and systems management — Kaspersky Security Center 10.

Security polices and reporting are managed through a single console, integrated with external resources such as LDAP directories and Microsoft Exchange. Hardware and software inventory databases as well as software vulnerabilities/updates are also included — driving further integration and synergy possibilities, as the same data can be used across multiple functions. No need to keep synching with different servers or data sets — everything is installed once, on the same server and managed through the same console.

These deep integration and synergy capabilities give a distinct advantage over competing solutions, many of which comprise acquired technologies with multiple, separate databases that simply cannot offer the same depth of integration as Kaspersky's platform.

The benefits:

- **Fast, easy deployment:** One management server, console installation and configuration process delivers completely integrated functionality, right out of the box.

- **Single management server hardware:** No hassle with different hardware, system or additional component requirements for each separate administration server and console. Kaspersky requires only ONE server for most deployments.

- **Single management server software:** Easy-to-manage infrastructure for small business, yet capable of scaling for larger deployments.
  — Some products require further packages to be installed following the initial rollout, just to deliver similar functionality to Kaspersky Lab.
  — For further convenience, Kaspersky's platform includes additional applications (e.g. those required in a Microsoft environment) as part of the installation process and self-install, saving time and aggravation. It just works.

SINGLE AGENT ARCHITECTURE, ONE-STEP INSTALLATION

2 SINGLE AGENT ARCHITECTURE, ONE-STEP INSTALLATION

Kaspersky's solution is unique in offering an endpoint agent that takes advantage of deep code integration to ensure complete, easily achieved compatibility and synergy across hardware and software configurations.

Genuine endpoint protection platforms have streamlined architecture, reducing complexity and deepening integration by using a minimum of discrete agents to run tasks. Kaspersky's solution is unique in offering an endpoint agent that takes advantage of deep code integration to ensure synergy between integrated functions and complete, easily achieved compatibility across hardware and software configurations. Related functions such as vulnerability scanning, application updates and patching — along with protection modules such as anti-malware and encryption — have a single agent architecture — streamlining performance and reducing your management footprint.

Many competing offerings require multiple agents on the same machine for functions and features such as patching application control or encryption. This creates potential problems around agent compatibility and requires additional testing.

The benefits:

- **Saves time on initial deployment and updates:** Just a single installation task to control, with no dependencies and no requirements for numerous re-boots.

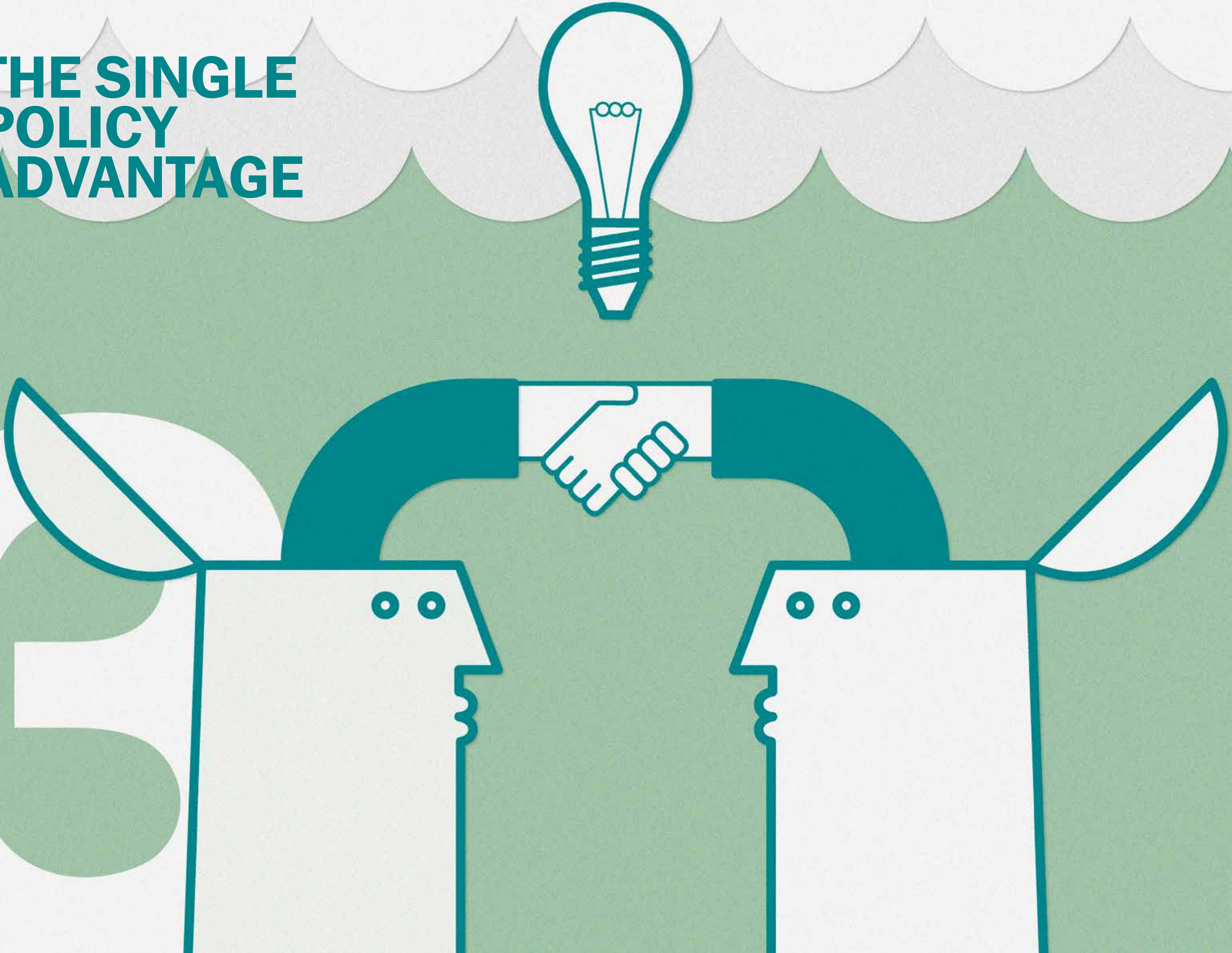
- **No hassle with different system requirements:** It's no secret that growth by acquisition creates software compatibility challenges. Bought-in functionality can create new, separate support requirements in addition to the software it's been bundled with. Too bad you only find this out when you start a deployment… Only an organic, integrated development approach can guarantee seamless compatibility for different software components for managed endpoint platforms/devices. This also means less client-side compatibility testing.

- **Reduced impact:** On system performance and management footprint.

- **Basis for synergy scenarios development:** Deep integration allows for flexibility and greater functionality. Extend capabilities without enlarging the resource footprint.

THE SINGLE POLICY ADVANTAGE

3



3 THE SINGLE POLICY ADVANTAGE

Complexity is the enemy of security, yet managing every aspect of information security across an organisation often involves dealing with multiple, very different, solutions. The more you can simplify management processes, the more clarity and less risk you can have.

A true Endpoint Protection Platform controls discovery, deployment, policy configuration and updating of endpoints throughout the corporate infrastructure. Kaspersky Endpoint Security's single agent architecture means administrators can set one active policy for a managed group, covering anti-malware, firewall, application, encryption, web and device controls.

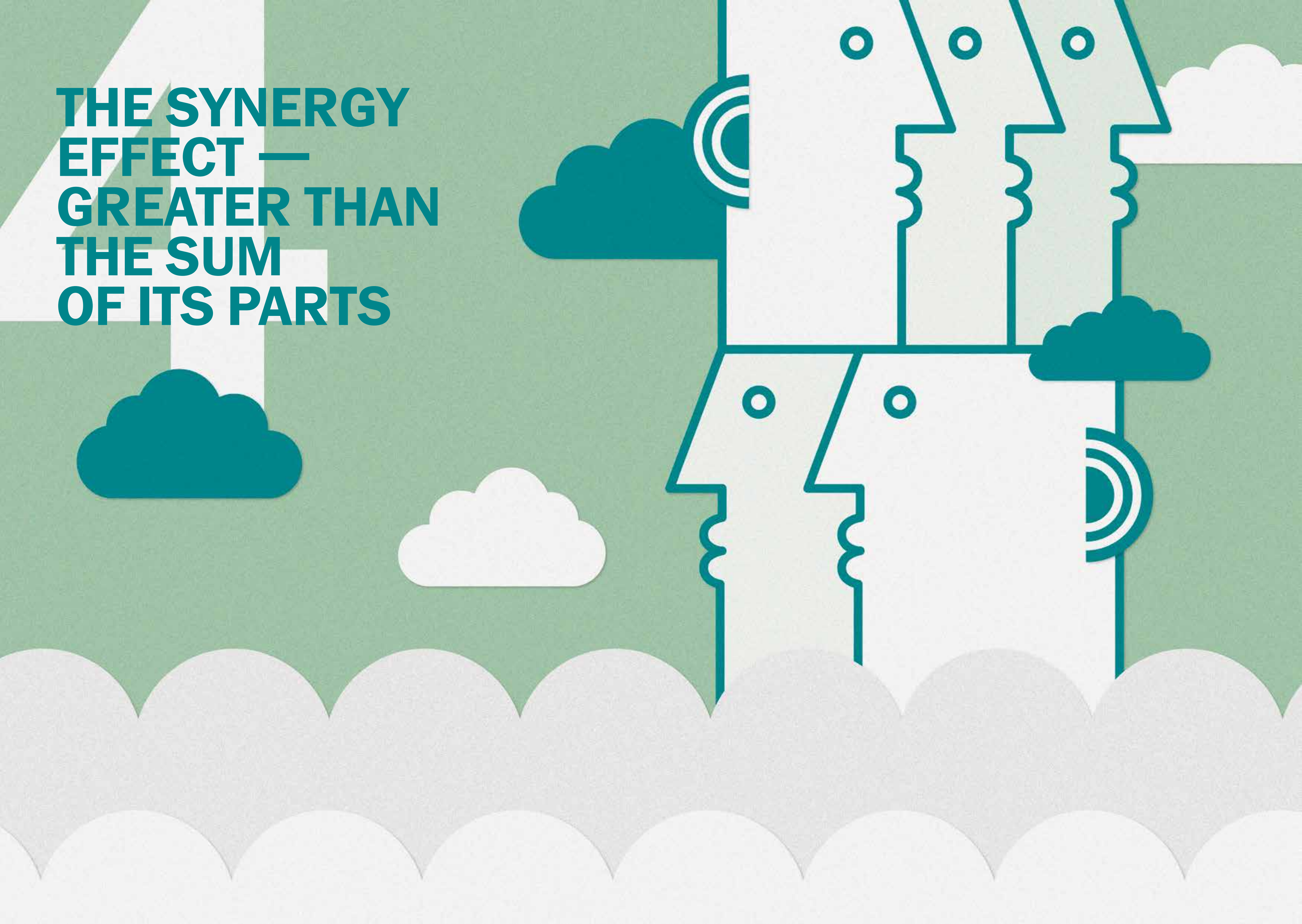
'Network Agent' connects the endpoint with the administration server, performing systems management tasks (such as software and hardware inventory, vulnerability scanning and patch management) or network admission control (NAC) functions, allowing for true flexibility and synergy between functions.

The benefits:

- **Simplified policy and task management:** Thanks to a single set of shared parameters and prerequisites — managed groups, delivery settings, notifications, policy implementation is optimized, eliminating redundant processes and tasks for the IT administrator.
- **Easier control over policy and task implementation:** Single dashboard and reporting on deployment and execution, provides a comprehensive, at-a-glance view of policy status and compliance over the entire network.
- **Streamlined policy and task changes:** Modifications are made in a single step. Automatic policy assignment can cover several security parameters at once, from various protection settings, to application, device and webcontrols, as well as encryption policies.
- **Automatic triggering reduces IT reaction times for incident management:** Based on specific events, such as switching on a dedicated protection policy (including all functions managed by a single policy) if a malware outbreak is detected.

4

THE SYNERGY EFFECT — GREATER THAN THE SUM OF ITS PARTS



4 THE SYNERGY EFFECT — GREATER THAN THE SUM OF ITS PARTS

Integrated endpoint protection features form the core of Kaspersky's secure platform, making even complex, advanced security management scenarios easy to implement. True integration delivers security beyond each feature's constituent parts, for example:

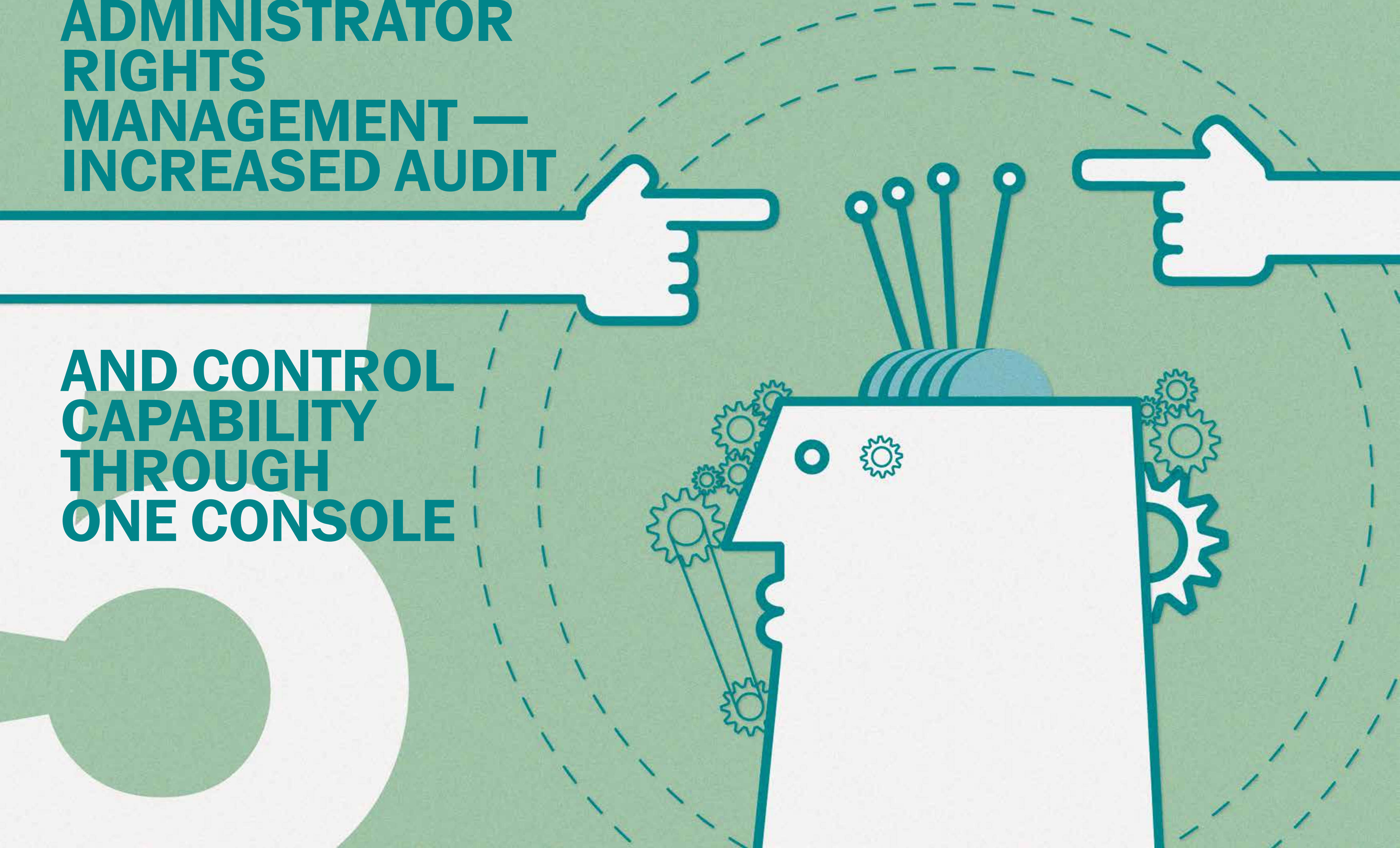
To implement comprehensive protection from Internet-based threats, alongside policy-based web traffic and downloaded file scanning, a business could use Kaspersky's application control feature to enforce the use of only one, IT-approved browser. This browser can, in turn, be further secured by enforcing automatic, high-priority vulnerability patching. To ensure that no updates slip through the cracks, application control can again be used — this time to block outdated or unpatched versions of the browser. In this way, Kaspersky's integrated features provide a canopy of security against a very large attack vector — that's what we mean by The Synergy Effect.

The benefits:

- **Cross-sharing of security management practices and information collected from different functions, for example:**
  — Information collected from the hardware inventory is used for device control and removable device encryption;
  — Software inventory information has input into application control and encryption policies;
  — Mobile device management (MDM) integrated with data security on devices;
  — Update status and scan results, combined with vulnerability assessment data to feed NAC security posture;
  — Patch management decisions can be based on vulnerability assessment.

The Synergy Effect is not limited to the scenarios outlined above — Kaspersky's deep code integration ensures complete, easily achieved compatibility and synergy across hardware and software configurations. With Kaspersky's platform, security is extended beyond each feature's constituent parts.

UNIFIED ADMINISTRATOR RIGHTS MANAGEMENT — INCREASED AUDIT AND CONTROL CAPABILITY THROUGH ONE CONSOLE



5 UNIFIED ADMINISTRATOR RIGHTS MANAGEMENT — INCREASED AUDIT AND CONTROL CAPABILITY THROUGH ONE CONSOLE

Understaffed IT departments are a common problem for many SMBs and enterprises. Economic cutbacks and increased IT complexity mean IT administrators have more tasks to perform and less time to do them in.

Kaspersky's Endpoint Protection Platform addresses this challenge, providing unified management tools for day-to-day security tasks. Deep integration allows privilege control and logs to be managed from just one console. One log records all actions — unlike competitor products, which often have to draw data from separate consoles and servers.

Unified rights management and logging allow for more effective control and insight into staff actions, supporting more effective permissions management. The result: Increased security and audit control over IT operations and management. From one console.

The benefits:

- **Easy to define and control permissions:** In a typical SMB where 'the IT-guy' looks after everything, it should be easy to perform all security-related tasks — including setting permissions for read/modify, access etc.

- **Rapid incident response and unified event log:** IT administrators are only human; mistakes are made and, in the event of a security incident, rapid response is essential. Functionality that enables rapid changing or blocking of admissions is vital, along with the capacity to track those changes. With separate solutions, complex incidents can require the creation of multiple analysis processes. Kaspersky eliminates complexity, covering all changes to endpoint security, policies and management activities in a single log file, provided from a single management console interface.

COMMON STRUCTURE, LOOK AND FEEL — FASTER, EASIER REPORTING

6 COMMON STRUCTURE, LOOK AND FEEL — FASTER, EASIER REPORTING

Under-pressure administrators will take any opportunity they can to save time or make a task easier to perform. Endpoint Protection Platforms with unified, integrated features and a common interface make reporting, analysis and incident management easier — a similar report structure with a common look and feel is generated by Kaspersky Security Center.

An IT administrator's working day typically involves a plethora of routine-yet-vital tasks, all of which need to be monitored and reported on. In a mixed solution environment, this entails a diverse number of dashboards, all generating reports in different formats, from PDF to HTML and direct email. Who has time to look at all that AND make sure everything's running as it should be?

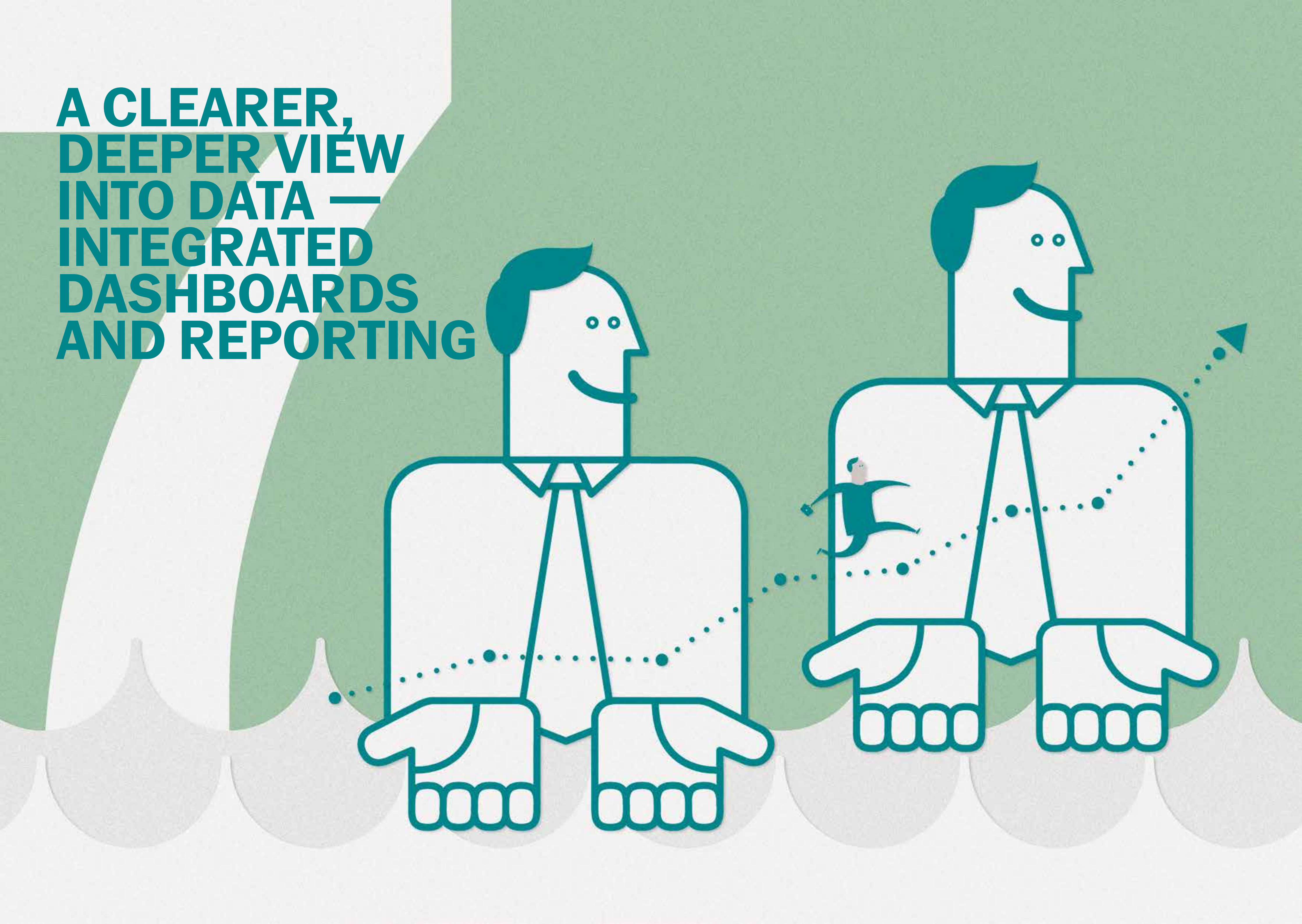
In this environment, even the smallest improvement in usability or efficiency can save a lot of time and reduce the workload (not to mention the stress) on already overloaded IT security administrators. Common reporting with a common look and feel can make analysis and appraisal easier, improving incident management and supporting a proactive approach to IT security.

The benefits:

- **Easier, faster report analysis:** The same terminology and structure is used across report templates. 'Computer, PC, node, machine' — all are synonyms for the same managed endpoint. All are used interchangeably across products and vendor literature; add enough products to the mix, and things can get a little confusing.
  What if each of the security components in your mixed solution environment had a similar language problem? And what if every parameter of every one of those components had 'same, just different' names? In such a complicated environment, conducting investigations into threats or other incidents becomes a lot more complicated than it needs to be — even for administrators that are familiar with the set up. It's one thing for admins to accept complexity, but what about a situation involving external investigators, such as auditors or regulators…? Offer them a confused overview of your infrastructure and you're likely to create the wrong impression.

- **Simplified incident management:** Easily recognize similar incidents across different IT infrastructure nodes, such as malware or policy breaches.

A CLEARER, DEEPER VIEW INTO DATA — INTEGRATED DASHBOARDS AND REPORTING



7 A CLEARER, DEEPER VIEW INTO DATA — INTEGRATED DASHBOARDS AND REPORTING

Endpoint Protection Platforms should provide a holistic approach to dashboards and reporting. True integration goes beyond the look and feel of the interface — for example, clicking on a single "endpoint properties" tab in an administration console should deliver information on all the security aspects of the managed client, such as policies applied, status updates and incidents.

Dashboards and reports should also ease the investigation process and create greater visibility into the endpoint — integration allows for information to be gathered across multiple components, making this much easier.

The benefits:

- **Single pane of glass for all endpoint security components:** A "cup of coffee" dashboard that doesn't take the entire morning to look at, includes most important information about managed endpoints status, deployment tasks execution and license control, as well as major security events and incidents.

- **Streamlined drilling and analysis:** Drill into interdependent reports to analyse and collect data from a variety of angles, including endpoint management, vulnerability assessment and patching, hardware and application inventory and user accounts created. Easy visibility into protection status and incidents, including malware detection and data encryption status. This makes security analysis and investigation a streamlined, easy process.

- **Executive reporting out of the box:** Executive reporting is a core component of an IT security administrator's responsibilities. Creating comprehensive reports from multiple consoles and datasets is time-consuming and a real headache. That's why Kaspersky's Endpoint Security Platform gives you executive reporting functionality right out of the box. No need for customized reports using third-party tools. More time to focus on other projects.

UNIFIED LICENSE MANAGEMENT AND CONTROL — DRIVE EFFICIENCY, TAKE CONTROL

8 UNIFIED LICENSE MANAGEMENT AND CONTROL — DRIVE EFFICIENCY, TAKE CONTROL

Managing licenses for all security solutions across the entire corporate network has never been easier. With Kaspersky Labs, all — and we really do mean ALL — functions are activated using a single license: Endpoint security, data protection, mobile device management and system management.

This single license is easily distributed across the corporate endpoint infrastructure, regardless of state or location; physical or virtual machines on any network, fixed or mobile. Kaspersky's integrated license management functionality allows you to make more effective use of what you're paying for, while keeping tighter control over license validity.

The benefits:

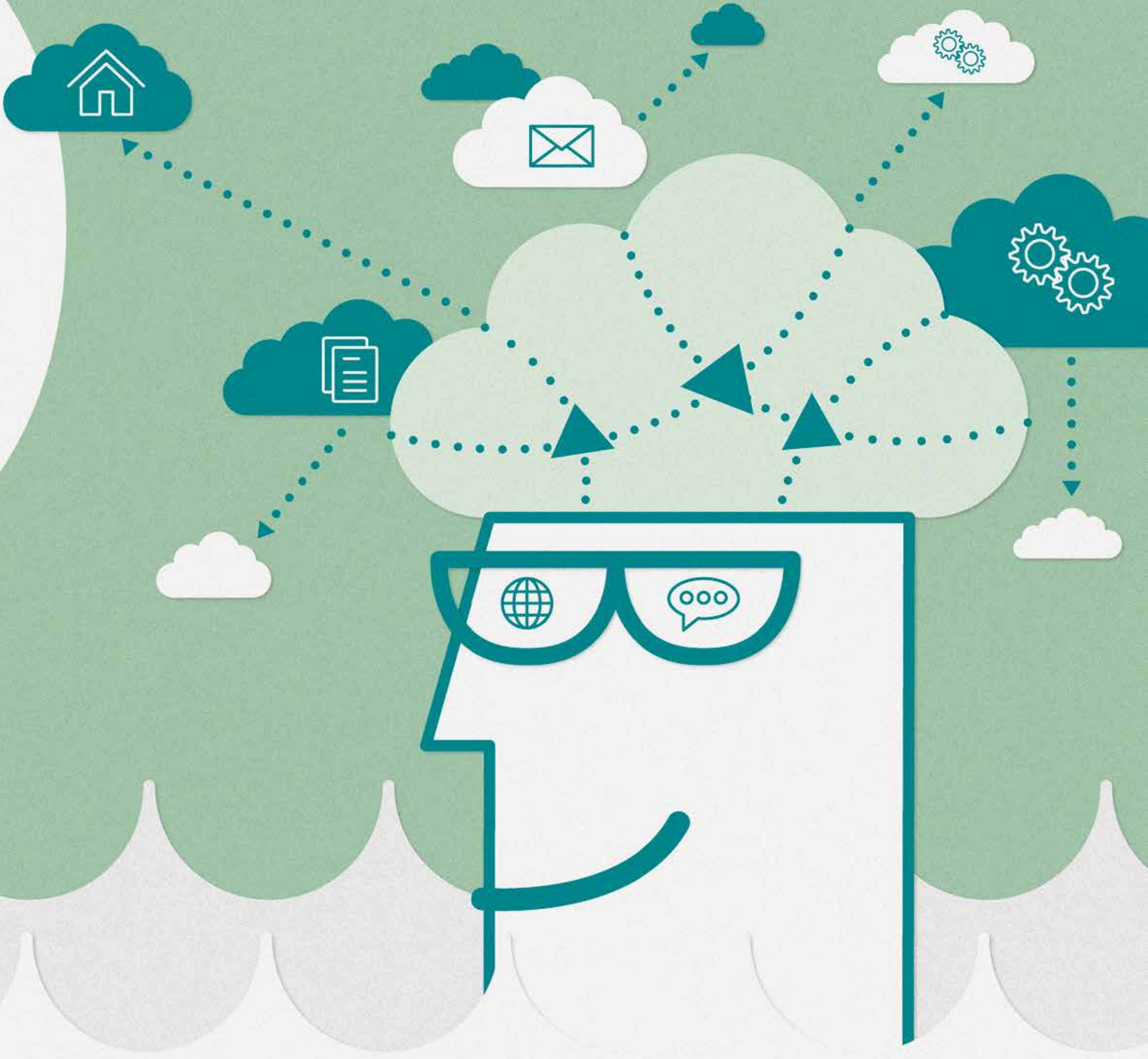
- **Single pane of glass for license auditing:** No need to refer to different license control tools to monitor and check status.

- **Efficient license usage:** Reduce costs through flexible distribution across a changing IT environment. For example, migrating from traditional PCs and notebooks to virtual infrastructure and to mobile devices with concurrent functionality.

- **Easy upgrade of your security solution:** With Kaspersky's Endpoint Protection Platform, you can increase security functionality according to your needs. Begin with endpoint security and simply activate features such as encryption or systems management by adding a new license.

9

SINGLE CODE BASE, BUILT IN-HOUSE, DRIVES DEEPER INTEGRATION



9 SINGLE CODE BASE, BUILT IN-HOUSE, DRIVES DEEPER INTEGRATION

Kaspersky’s single code base, built and maintained in-house, is at the heart of our integrated Endpoint Protection Platform.

Where other vendors have followed acquisition strategies to increase their product offering in a rapidly changing threat landscape, Kaspersky is unique in developing and maintaining everything in-house. Unlike other vendors, this supports deep integration from the code-base level, allowing us to deliver the many benefits described earlier in this document.

The benefits:

- Single management server and administration console;
- Single endpoint client architecture;
- Single policies and unified tasks;
- Synergy effect of integrated functionality;
- Integrated dashboards and reporting.

The same code base and development process facilitates faster updates and patching — Kaspersky users can update a single application, instead of the two or more applications (and the components that go with them) needed in many competing products.

INTEGRATED PURCHASE MODEL — ALL THE FUNCTIONALITY YOU NEED IN A SINGLE PURCHASE

10

10 INTEGRATED PURCHASE MODEL — ALL THE FUNCTIONALITY YOU NEED IN A SINGLE PURCHASE

At time of writing (December 2012), no security product on the market included all functionality — from endpoint security and data protection to mobile device and systems management in one single license purchase. NEW! Kaspersky Security for Business Advanced includes all of this. It has never been so easy!

One order covers all your security needs and functions; one license will activate everything.

The benefits:

- **Address different needs through one package:** Kaspersky users can acquire different levels and flavours of integrated functionality, addressing different customer needs — all using only one license package. This is unique.

FINALLY…

With Kaspersky Lab, users get a genuine Endpoint Protection Platform, developed from beginning to end, using the same code-base and R&D. Our integrated anti-malware and software vulnerability technologies are developed by our in-house, dedicated research group, that constantly studies how modern threats are penetrating systems in order to develop more effective protection.

Kaspersky Lab's own application whitelisting research group manages our ecosystem of partners and vendors, delivering a constantly updated database of legitimate software, while giving the most up-to-date information on available patches.

The convergence of endpoint security and client/systems management technology is a growing trend. Kaspersky Lab, with its entirely in-house code base and development process, is uniquely places to exploit the obvious synergies between security functions and those traditionally seen as components of systems management. Deeper integration of features such as network admission control and patch management with application control and whitelisting creates multiple benefits, drives efficiency and makes for a smaller overall footprint.

Kaspersky Labs integration delivers a true Endpoint Protection Platform. Protection is optimal, not optional.

Learn more at www.kaspersky.com/business