


**SE NÃO É O KASPERSKY
ENDPOINT SECURITY
FOR BUSINESS, NÃO
É UMA PLATAFORMA DE
PROTEÇÃO DE TERMINAIS**

▶ 10 VANTAGENS

**QUE APENAS UMA SOLUÇÃO DE
SEGURANÇA DE PLATAFORMA
INTEGRADA PODE OFERECER**

KASPERSKY lab




O Relatório global de riscos de segurança de TI da Kaspersky Lab revelou que 94% das empresas experienciaram algum tipo de incidente de segurança externo nos últimos 12 meses¹.

À medida que o volume e a sofisticação das ameaças aumenta exponencialmente, as empresas de todas as dimensões desenvolvem um melhor entendimento dos riscos de segurança de TI, em particular dos ataques direcionados e de como podem proteger-se destas ameaças específicas, em vez de adotar uma abordagem aleatória e alargada a uma noção de “malware” generalizada.

Lamentavelmente, muitos fornecedores de segurança de TI continuam a utilizar exatamente esta abordagem aleatória e alargada, comprando novas tecnologias e juntando bases de código díspares, muitas vezes incompatíveis, o que gera complexidade e provoca tantos problemas quantos os que soluciona.

¹ Relatório global de riscos de segurança de TI 2014.



Os dias da segurança de terminais tradicional (antimalware discreto, encriptação e controlos de dispositivos e de rede) estão a chegar ao fim. As plataformas de proteção de terminais (EPP), tecnologias de segurança perfeitamente integradas prometedoras, são a tendência no que diz respeito à segurança de TI, prevenção avançada de ameaças e proteção de dados.

No entanto, existe uma diferença enorme entre “integração” e uma plataforma genuína. Além disso, no que diz respeito à “integração”, existem vários graus de plenitude. Para muitos fornecedores, a “integração” tornou-se apenas um sinónimo de “compatível”.

E, para alguns fornecedores, “compatível” significa improvisar produtos comprados em tantas aquisições como 40 e tentar colocá-los a funcionar com a sua própria base de código, sem considerar a dos seus clientes.

Existem muitos fornecedores que prometem soluções “integradas” mas, se analisarmos mais de perto, veremos que há uma diferença significativa entre “funcionar bem” em conjunto e a verdadeira sinergia que se consegue com o planeamento e desenvolvimento de produtos com base na informação. Alguns fornecedores têm dificuldades em unificar as suas aquisições empresariais e, no entanto, declaram que conseguem fornecer plataformas totalmente integradas.

Comprar qualquer coisa que aparenta ser a próxima grande descoberta não pode fornecer a mesma integridade de visão, ou proteção.

Existem algumas vantagens que apenas uma solução de plataforma verdadeira e profundamente integrada pode oferecer. O Kaspersky Endpoint Security for Business dispõe de um posicionamento único para proporcionar as seguintes vantagens aos administradores de TI:

1. Um servidor, uma consola
2. Arquitetura de agente único*, instalação simples
3. A vantagem de uma política única
4. O efeito da sinergia — maior do que a soma das suas partes
5. Gestão unificada dos direitos de administrador — maior capacidade de auditoria e controlo através de uma consola

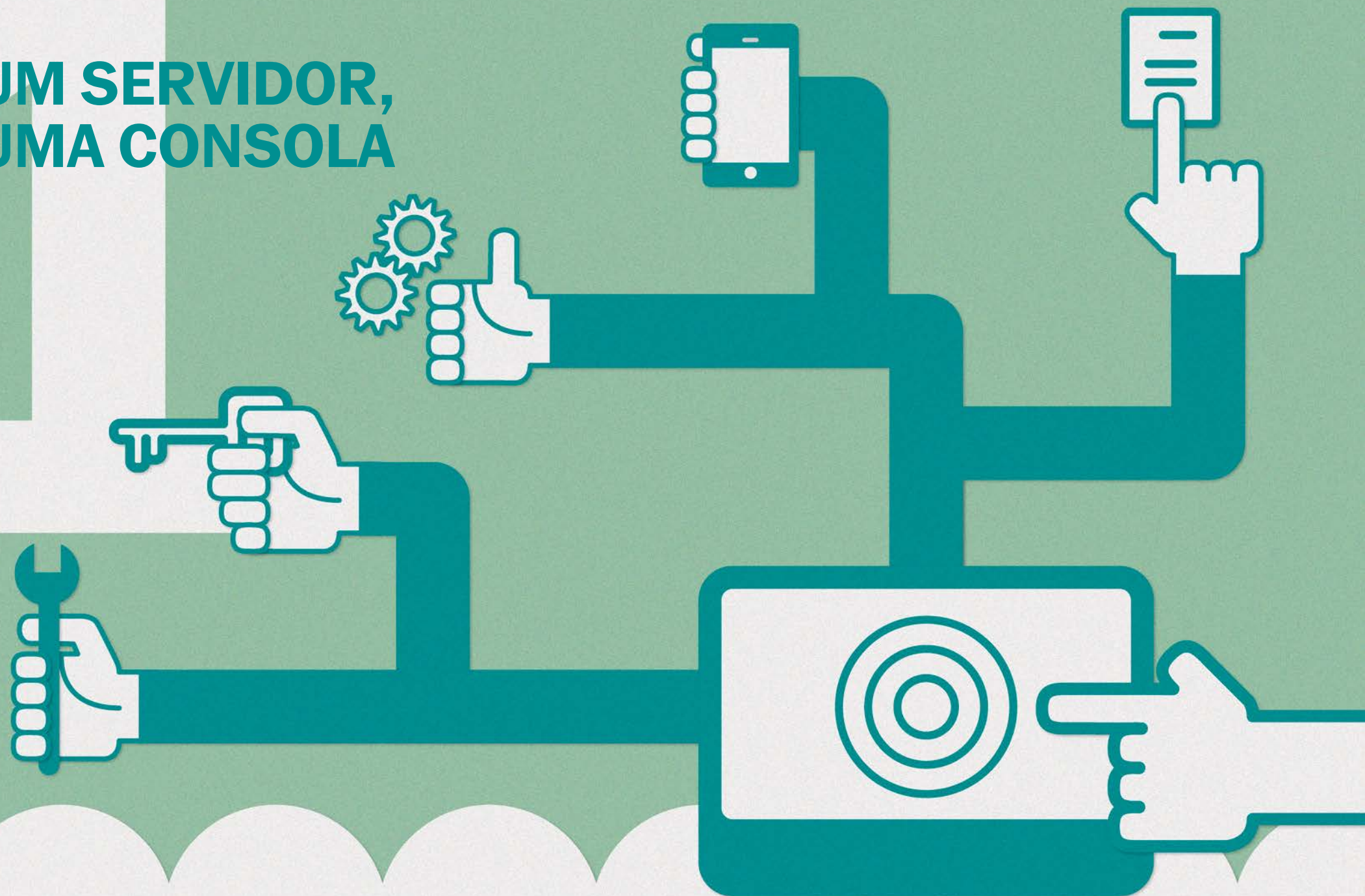


PLATAFORMA DE PROTEÇÃO DE TERMINAIS

6. Estrutura, aspeto e funcionamento comuns — criação de relatórios mais fácil e rápida
7. Uma análise mais clara e aprofundada dos dados — painéis de controlo integrados e criação de relatórios
8. Controlo e gestão unificada de licenças — aumente a eficiência, assuma o controlo
9. A base de código única, concebida internamente, permite uma integração mais profunda
10. Modelo de compra integrado — todas as funcionalidades de que necessita com uma compra única

* Arquitetura de agente único por plataforma (Windows, Linux, Mac).

UM SERVIDOR, UMA CONSOLA



1 UM SERVIDOR, UMA CONSOLA

A solução da Kaspersky Lab é única porque oferece uma consola de administração e servidor de gestão únicos e perfeitamente integrados que cobrem todos os aspetos da segurança de terminais, desde o antimalware à proteção de dados, gestão de dispositivos móveis e gestão de sistemas — o Kaspersky Security Center.

Os relatórios e as políticas de segurança são geridos através de uma única consola, integrada com recursos externos, tais como diretórios LDAP e o Microsoft Exchange. As bases de dados de inventários de hardware e software, bem como as atualizações/vulnerabilidades de software, também estão incluídas, aumentando assim as possibilidades de sinergia e integração, já que os mesmos dados podem ser utilizados para várias funções. Não há necessidade de sincronizar constantemente com diferentes servidores ou conjuntos de dados; tudo é instalado uma só vez, no mesmo servidor, e gerido pela mesma consola.

Estas capacidades de sinergia e integração profunda representam uma vantagem clara em relação às soluções da concorrência, muitas das quais incluem tecnologias adquiridas com várias bases de dados separadas que simplesmente não podem oferecer o mesmo nível de integração da plataforma da Kaspersky.

Vantagens:

- **Implementação rápida e fácil:** um único processo de instalação e configuração do servidor de gestão e da consola proporciona uma funcionalidade completamente integrada, desde o primeiro momento.
- **Hardware de servidor de gestão único:** não terá problemas com diferentes requisitos de hardware, de sistema ou componentes adicionais para cada consola e servidor de administração separado. A Kaspersky requer apenas UM servidor para a maioria das implementações.
- **Software de servidor de gestão único:** infraestrutura fácil de gerir para pequenas empresas, mas ainda assim capaz de se adaptar a implementações de maior dimensão.
 - Alguns produtos requerem a instalação de mais pacotes após a implementação inicial, apenas para oferecerem uma funcionalidade semelhante à da Kaspersky Lab.
 - Para maior comodidade, a plataforma da Kaspersky inclui aplicações adicionais (por exemplo, aquelas requeridas num ambiente Microsoft) como parte do processo de instalação, e a respetiva instalação é autónoma, permitindo-lhe poupar tempo e esforço. Simplesmente funciona.

ARQUITETURA DE AGENTE ÚNICO*, INSTALAÇÃO SIMPLES



* Arquitetura de agente único por plataforma (Windows, Linux, Mac).

2

ARQUITETURA DE AGENTE ÚNICO*, INSTALAÇÃO SIMPLES

A solução da Kaspersky é única porque oferece um agente de terminal que tira partido da integração de código profunda para garantir sinergia e compatibilidade total e fácil entre configurações de hardware e software.

As plataformas de proteção de terminais genuínas possuem uma arquitetura otimizada, reduzindo a complexidade e maximizando a integração através da utilização de um mínimo de agentes discretos para executar tarefas. As funções relacionadas, tais como a análise de vulnerabilidades, as atualizações de aplicações e a aplicação de patches — juntamente com módulos de proteção, como antimalware e encriptação — possuem uma arquitetura de agente único, otimizando o desempenho e reduzindo as tarefas de gestão.

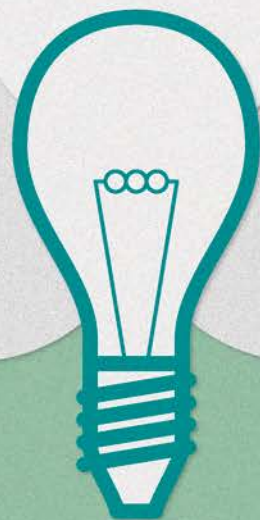
Muitas ofertas da concorrência requerem vários agentes na mesma máquina para funções e funcionalidades tais como a aplicação de patches, o controlo de aplicações ou a encriptação. Isto cria potenciais problemas no que diz respeito à compatibilidade dos agentes e requer testes adicionais.

* Arquitetura de agente único por plataforma (Windows, Linux, Mac).

Vantagens:

- **Poupa tempo na implementação inicial e nas atualizações:** requer apenas o controlo de uma simples tarefa de instalação, sem dependências e sem necessidade de reiniciar o sistema várias vezes.
- **Sem problemas com diferentes requisitos de sistema:** não é nenhum segredo que o crescimento através de aquisições cria problemas de compatibilidade de software. As funcionalidades compradas podem criar novos requisitos de suporte separados, além do software no qual foram integradas. Mas não é agradável descobri-lo apenas depois de iniciar uma implementação... Só uma abordagem de desenvolvimento integrada e orgânica pode garantir a compatibilidade total entre diferentes componentes de software para dispositivos/plataformas de terminais geridas. Isto também significa menos testes de compatibilidade por parte do cliente.
- **Impacto reduzido:** no desempenho do sistema e nas tarefas de gestão.
- **Base para o desenvolvimento de cenários de sinergia:** a integração profunda permite uma maior funcionalidade e flexibilidade. Maiores capacidades sem aumentar o número de recursos.

A VANTAGEM DE UMA POLÍTICA ÚNICA



3

A VANTAGEM DE UMA POLÍTICA ÚNICA

A complexidade é inimiga da segurança, mas gerir todos os aspetos da segurança da informação numa organização envolve, muitas vezes, lidar com múltiplas soluções muito diferentes. Quanto mais conseguir simplificar os processos de gestão, mais clareza e menos riscos obterá.

Uma verdadeira plataforma de proteção de terminais controla a deteção, implementação, configuração de políticas e atualização de terminais em toda a infraestrutura empresarial. O agente único por plataforma do Kaspersky Endpoint Security significa que os administradores podem configurar uma política ativa para um grupo gerido, que abranja todos os componentes necessários sem necessidade de analisar várias políticas ou de correlação.

O “agente de rede” liga o terminal ao servidor de administração, executando tarefas de gestão de sistemas (tais como inventário de software e hardware, análise de vulnerabilidades e gestão de patches), permitindo uma verdadeira flexibilidade e sinergia entre funções.

Vantagens:

- **Gestão simplificada de políticas e tarefas:** graças a um único conjunto de pré-requisitos e parâmetros partilhados; os grupos geridos, as definições de entrega, as notificações e a implementação de políticas são otimizados, eliminando processos e tarefas redundantes para o administrador de TI.
- **Controlo mais fácil da implementação de políticas e tarefas:** o painel de controlo único e os relatórios no momento da implementação e da execução proporcionam uma visualização rápida e abrangente do estado das políticas e da conformidade em toda a rede.
- **Alterações otimizadas de políticas e tarefas:** as modificações são realizadas num único passo. A atribuição automática de políticas pode abranger diversos parâmetros de segurança em simultâneo, desde várias definições de proteção a controlos da Web, aplicações e dispositivos, assim como políticas de encriptação.

**O EFEITO DA
SINERGIA —
MAIOR DO QUE
A SOMA DAS
SUAS PARTES**



4

O EFEITO DA SINERGIA — MAIOR DO QUE A SOMA DAS SUAS PARTES

As funcionalidades de proteção de terminais integradas formam o núcleo da plataforma segura da Kaspersky, facilitando mesmo a implementação de cenários de gestão de segurança complexos e avançados. Uma verdadeira integração proporciona segurança para além das partes constituintes de cada funcionalidade.

Por exemplo:

Para implementar uma proteção abrangente contra ameaças baseadas na Internet, juntamente com tráfego Web baseado em políticas e análises de ficheiros transferidos, as empresas poderiam utilizar a funcionalidade de controlo de aplicações da Kaspersky para impor a utilização de apenas um navegador aprovado pelo departamento de TI.

Este navegador pode, por sua vez, ser adicionalmente protegido através da imposição de patches automáticos para vulnerabilidades de alta prioridade e protegido contra ataques de dia zero com a Prevenção Automática de Exploit. Desta forma, as funcionalidades integradas da Kaspersky oferecem várias camadas de segurança contra um grande número de vetores de ataque: é a isto que nos referimos com “O efeito da sinergia”.

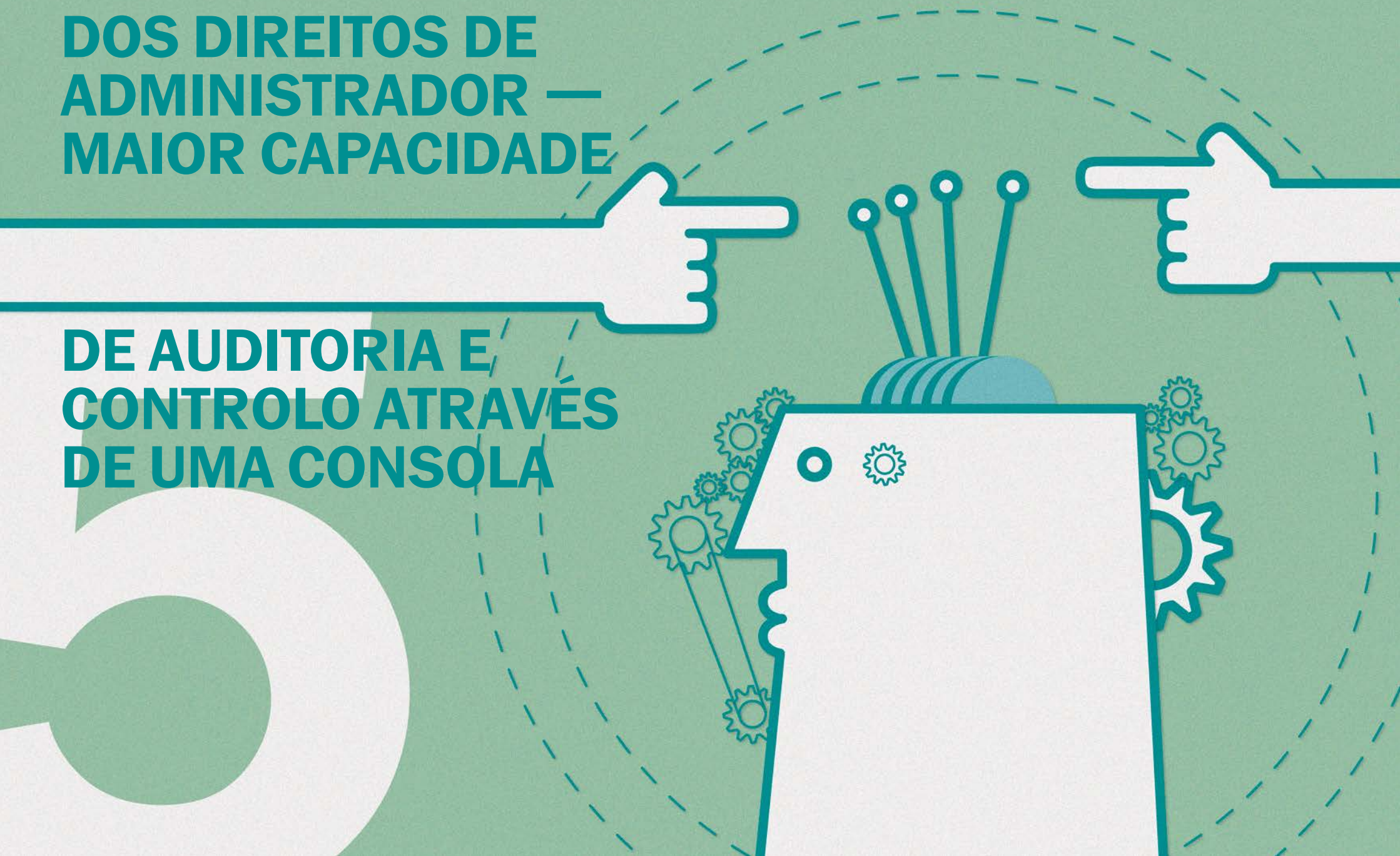
Vantagens:

- **A partilha cruzada de práticas de gestão de segurança e informações recolhidas de diferentes funções, por exemplo:**
 - As informações recolhidas acerca de dispositivos amovíveis são utilizadas para o controlo de dispositivos e encriptação;
 - As informações sobre aplicações são utilizadas no controlo de aplicações e políticas de encriptação;
 - Gestão de dispositivos móveis (MDM) integrada com a segurança de dados no dispositivo;
 - As decisões de gestão de patches podem basear-se na análise de vulnerabilidades.

O efeito da sinergia não se limita aos cenários mencionados acima; a integração de código profunda da Kaspersky garante sinergia e compatibilidade total e fácil entre configurações de hardware e software. Com a plataforma da Kaspersky, a segurança vai para além das partes constituintes de cada funcionalidade.

**GESTÃO UNIFICADA
DOS DIREITOS DE
ADMINISTRADOR —
MAIOR CAPACIDADE**

**DE AUDITORIA E
CONTROLO ATRAVÉS
DE UMA CONSOLA**



5

GESTÃO UNIFICADA DOS DIREITOS DE ADMINISTRADOR — MAIOR CAPACIDADE DE AUDITORIA E CONTROLO ATRAVÉS DE UMA CONSOLA

Departamentos de TI com poucos funcionários são um problema comum para muitas PME e grandes empresas. Os cortes financeiros e o aumento da complexidade de TI significa que os administradores têm de executar mais tarefas e dispõem de menos tempo para o fazer.

A plataforma de proteção de terminais da Kaspersky responde a este desafio proporcionando ferramentas de gestão unificadas para as tarefas de segurança diárias. A integração profunda permite a gestão de registos e o controlo de privilégios a partir de uma única consola. Um registo guarda todas as ações, ao contrário dos produtos da concorrência que, muitas vezes, recolhem dados de consolas e servidores separados.

O registo e a gestão unificada de direitos permitem um controlo mais eficaz e maior informação sobre as ações dos funcionários, contribuindo assim para uma gestão mais eficaz das permissões. O resultado: maior segurança e controlo de auditorias sobre a gestão e as operações de TI. A partir de uma única consola.

Vantagens:

- **Permissões fáceis de definir e controlar:** numa PME típica, em que o técnico de TI trata de tudo, deveria ser fácil realizar todas as tarefas relacionadas com a segurança, como definir permissões de leitura/modificação, acesso, etc.
- **Resposta rápida a incidentes e registo de eventos unificado:** os administradores de TI são humanos; qualquer um pode cometer erros e, no caso de um incidente de segurança, é essencial responder rapidamente. É fundamental dispor de uma funcionalidade que permita a alteração ou o bloqueio rápido de admissões, juntamente com a capacidade de registar essas alterações. Com soluções separadas, incidentes complexos podem requerer a criação de vários processos de análise. A Kaspersky elimina a complexidade, recolhendo todas as alterações de segurança de terminais, políticas e atividades de gestão num único ficheiro de registo, fornecido através da interface de uma única consola de gestão.

**ESTRUTURA,
ASPETO E
FUNCIONAMENTO
COMUNS — CRIAÇÃO
DE RELATÓRIOS MAIS
FÁCIL E RÁPIDA**



6

ESTRUTURA, ASPETO E FUNCIONAMENTO COMUNS — CRIAÇÃO DE RELATÓRIOS MAIS FÁCIL E RÁPIDA

Os administradores sob pressão tirarão partido de qualquer oportunidade para poupar tempo ou tornar uma tarefa mais fácil de realizar. As plataformas de proteção de terminais com funcionalidades integradas unificadas e uma interface comum facilitam a criação de relatórios, as análises e a gestão de incidentes — o Kaspersky Security Center gera uma estrutura de relatório semelhante com um aspeto e funcionamento comuns.

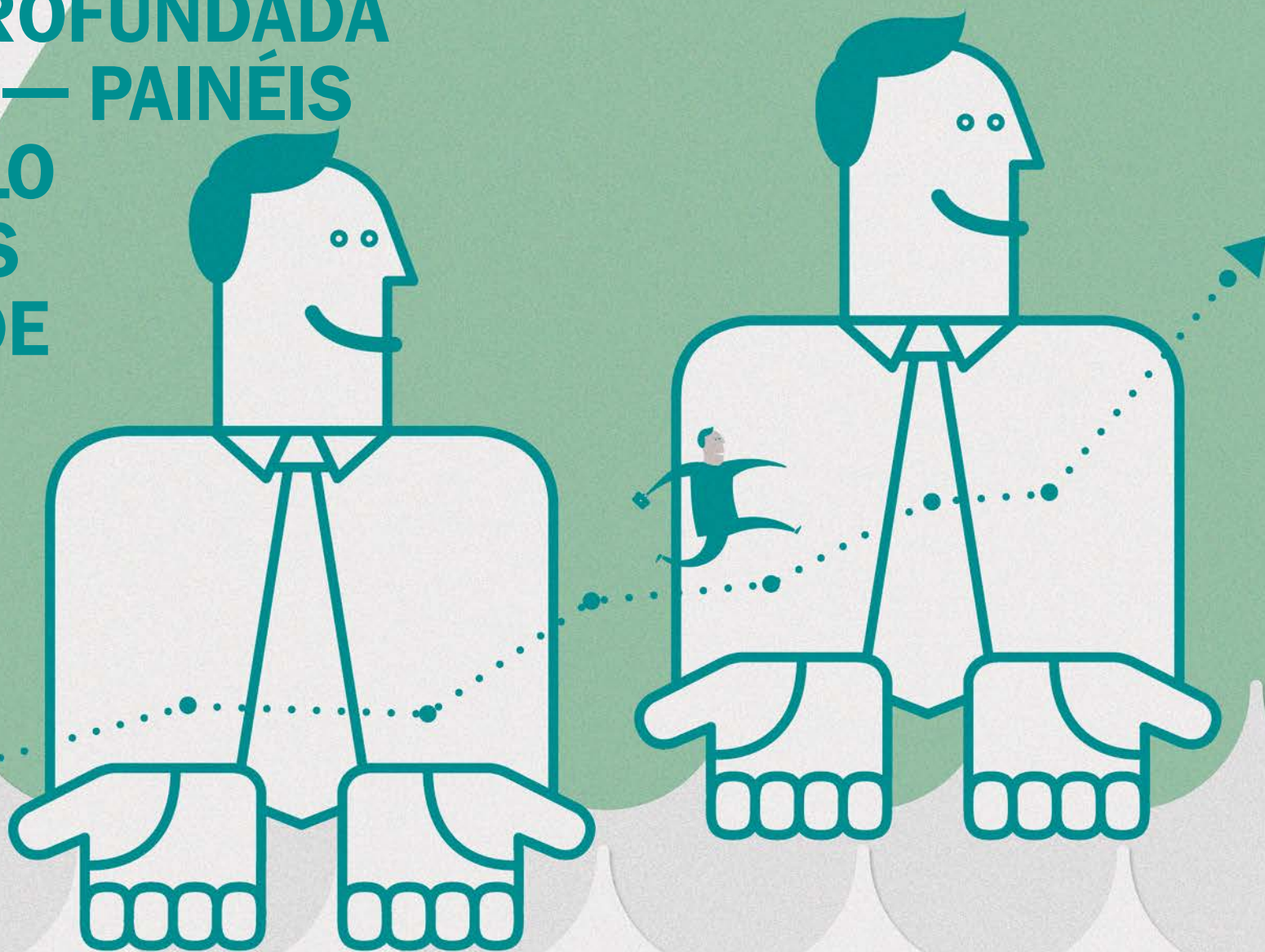
O dia de trabalho de um administrador de TI envolve, normalmente, uma grande variedade de tarefas de rotina essenciais, que necessitam ser monitorizadas e registadas. Num ambiente com várias soluções, isto implica um diverso número de painéis de controlo, que geram relatórios em diferentes formatos, desde PDF a HTML e e-mails diretos. Quem tem tempo para analisar todos esses relatórios e ainda garantir que tudo decorre como deveria?

Neste ambiente, mesmo a mais pequena melhoria em termos de facilidade de utilização ou eficiência pode permitir poupar muito tempo e reduzir a carga de trabalho (para não mencionar o stress) dos administradores de segurança de TI já sobrecarregados. Uma ferramenta de criação de relatórios comum, com um aspeto e funcionamento comuns, pode tornar as tarefas de análise e avaliação mais fáceis, melhorando a gestão de incidentes e apoiando uma abordagem pró-ativa à segurança de TI.

Vantagens:

- **Análises de relatórios mais fáceis e rápidas:** é utilizada a mesma terminologia e estrutura em todos os modelos de relatório. “Computador, PC, nó, máquina” — todos são sinónimos para o mesmo terminal gerido. Todos são utilizados alternadamente nos produtos e na literatura dos fornecedores; adicione suficientes produtos à mistura e as coisas poderão tornar-se confusas. E se cada um dos componentes de segurança no seu ambiente com várias soluções tivesse um problema de linguagem semelhante? E se cada parâmetro de cada um desses componentes tivesse nomes “iguais, mas diferentes”? Em ambientes tão complexos, realizar investigações sobre ameaças ou outros incidentes torna-se muito mais complicado do que o necessário, mesmo para administradores familiarizados com os sistemas. Uma coisa é os administradores aceitarem a complexidade, mas o que acontece quando uma situação envolve investigadores externos, tais como auditores ou entidades reguladoras? Apresente-lhes uma visão geral confusa da sua infraestrutura e poderá passar a impressão errada.
- **Gestão simplificada de incidentes:** reconheça facilmente incidentes semelhantes em diferentes nós da infraestrutura de TI, tais como malware ou violações de políticas.

**UMA ANÁLISE MAIS
CLARA E APROFUNDADA
DOS DADOS — PAINÉIS
DE CONTROLO
INTEGRADOS
E CRIAÇÃO DE
RELATÓRIOS**



7 UMA ANÁLISE MAIS CLARA E APROFUNDADA DOS DADOS — PAINÉIS DE CONTROLO INTEGRADOS E CRIAÇÃO DE RELATÓRIOS

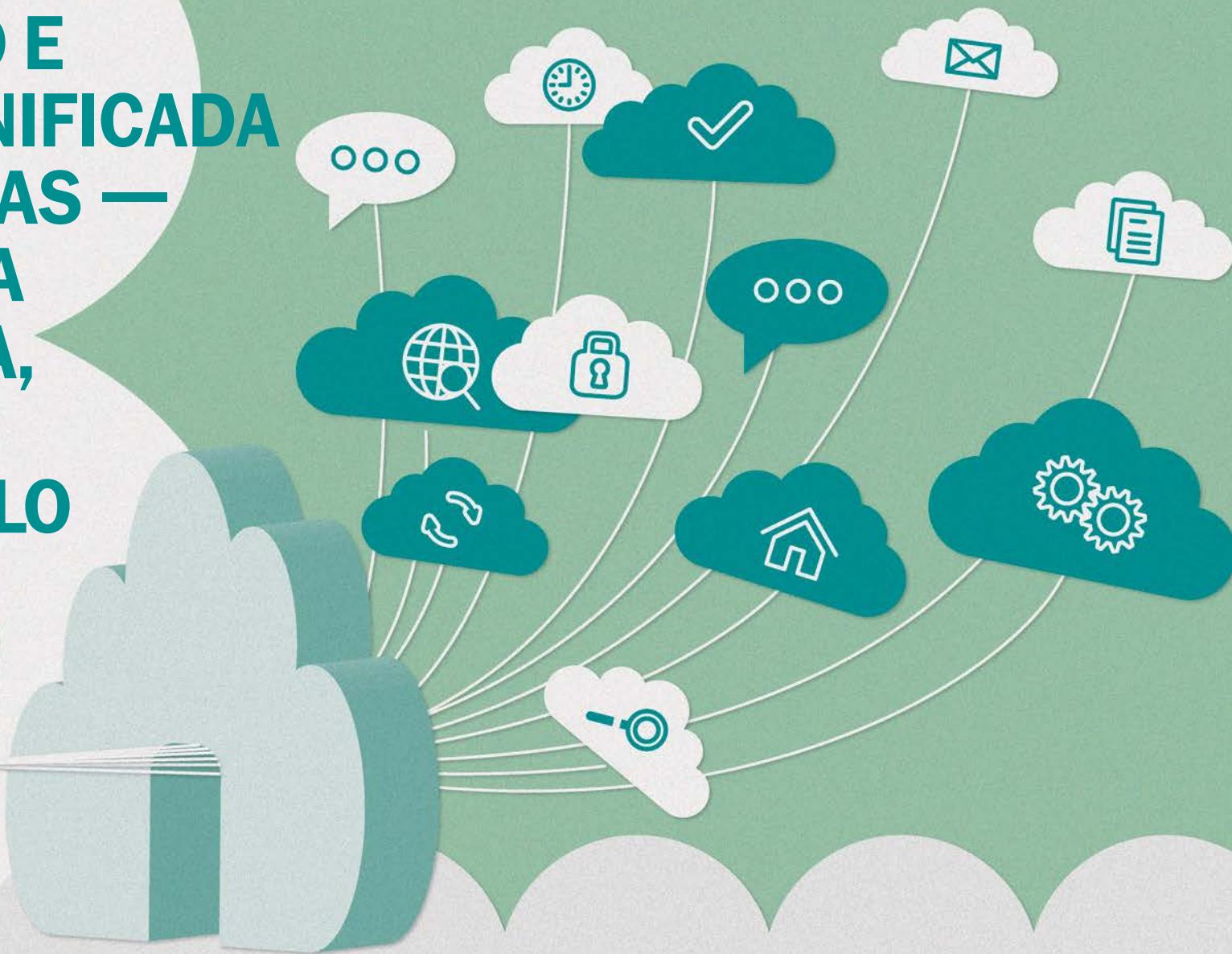
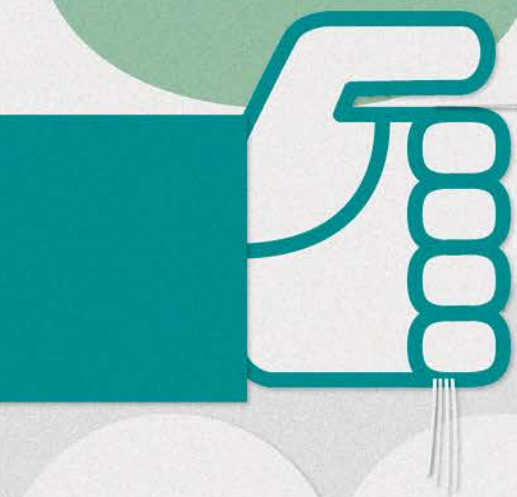
As plataformas de proteção de terminais deveriam proporcionar uma abordagem holística no que diz respeito a painéis de controlo e relatórios. Uma verdadeira integração vai além do aspeto e do funcionamento da interface — por exemplo, clicar num separador “propriedades do terminal” numa consola de administração deve fornecer informações sobre todos os aspetos de segurança do cliente gerido, tais como políticas aplicadas, atualizações de estado e incidentes.

Os painéis de controlo e os relatórios também devem facilitar o processo de investigação e criar uma maior visibilidade do terminal; a integração permite recolher informação através de vários componentes, tornando a tarefa muito mais fácil.

Vantagens:

- **Uma janela única para todos os componentes da segurança de terminais:** um painel de controlo conciso que não implica uma análise demorada, inclui a informação mais importante sobre o estado dos terminais geridos, a execução das tarefas de implementação e o controlo de licenças, bem como eventos de segurança importantes e incidentes.
- **Análise e verificação otimizadas:** verifique relatórios interdependentes para analisar e recolher dados de vários ângulos, incluindo gestão de terminais, análise de vulnerabilidades e aplicação de patches, inventário de hardware e aplicações e contas de utilizador criadas. Visibilidade fácil sobre o estado de proteção e incidentes, incluindo deteção de malware e estado de encriptação dos dados. Isto faz da investigação e das análises de segurança um processo fácil e otimizado.
- **Relatórios executivos de implementação imediata:** a criação de relatórios executivos é um componente fundamental das responsabilidades do administrador de segurança de TI. Criar relatórios abrangentes a partir de várias consolas e conjuntos de dados é moroso e uma verdadeira dor de cabeça. É por esse motivo que a plataforma de segurança de terminais da Kaspersky lhe oferece uma funcionalidade de criação de relatórios executivos desde o início. Não há necessidade de criar relatórios personalizados utilizando ferramentas de terceiros. Assim, fica com mais tempo para se concentrar noutros projetos.

**CONTROLO E
GESTÃO UNIFICADA
DE LICENÇAS —
AUMENTE A
EFICIÊNCIA,
ASSUMA
O CONTROLO**



8

CONTROLO E GESTÃO UNIFICADA DE LICENÇAS — AUMENTE A EFICIÊNCIA, ASSUMA O CONTROLO

Gerir as licenças de todas as soluções de segurança na rede empresarial nunca foi tão fácil. Com a Kaspersky Lab, todas — e queremos dizer mesmo TODAS — as funções são ativadas utilizando uma única licença: segurança de terminais, proteção de dados, gestão de dispositivos móveis e gestão de sistemas.

Esta licença única é facilmente distribuída através da infraestrutura de terminais empresariais, independentemente do respetivo estado ou localização; máquinas físicas ou virtuais em qualquer rede, fixas ou móveis. A funcionalidade de gestão de licenças integrada da Kaspersky permite-lhe fazer um uso mais eficaz daquilo por que está a pagar e, ao mesmo tempo, manter um maior controlo sobre a validade das licenças.

Vantagens:

- **Uma janela única para a auditoria de licenças:** não há necessidade de recorrer a diferentes ferramentas de controlo de licenças para monitorizar e verificar o estado.
- **Utilização eficiente de licenças:** reduza os custos através de uma distribuição flexível num ambiente de TI em constante mudança. Por exemplo, migrar de PC e computadores portáteis tradicionais para dispositivos móveis com funcionalidade semelhante.
- **Atualização fácil da sua solução de segurança:** com a plataforma de proteção de terminais da Kaspersky, pode aumentar a funcionalidade de segurança de acordo com as suas necessidades. Pode começar com a segurança de terminais e ativar funcionalidades tais como a encriptação ou a gestão de sistemas através da adição de uma nova licença.

**A BASE DE
CÓDIGO ÚNICA,
CONCEBIDA
INTERNAMENTE,
PERMITE UMA
INTEGRAÇÃO
MAIS PROFUNDA**



9

A BASE DE CÓDIGO ÚNICA, CONCEBIDA INTERNAMENTE,
PERMITE UMA INTEGRAÇÃO MAIS PROFUNDA

A base de código única da Kaspersky, concebida e mantida internamente, está no núcleo da nossa plataforma de proteção de terminais integrada.

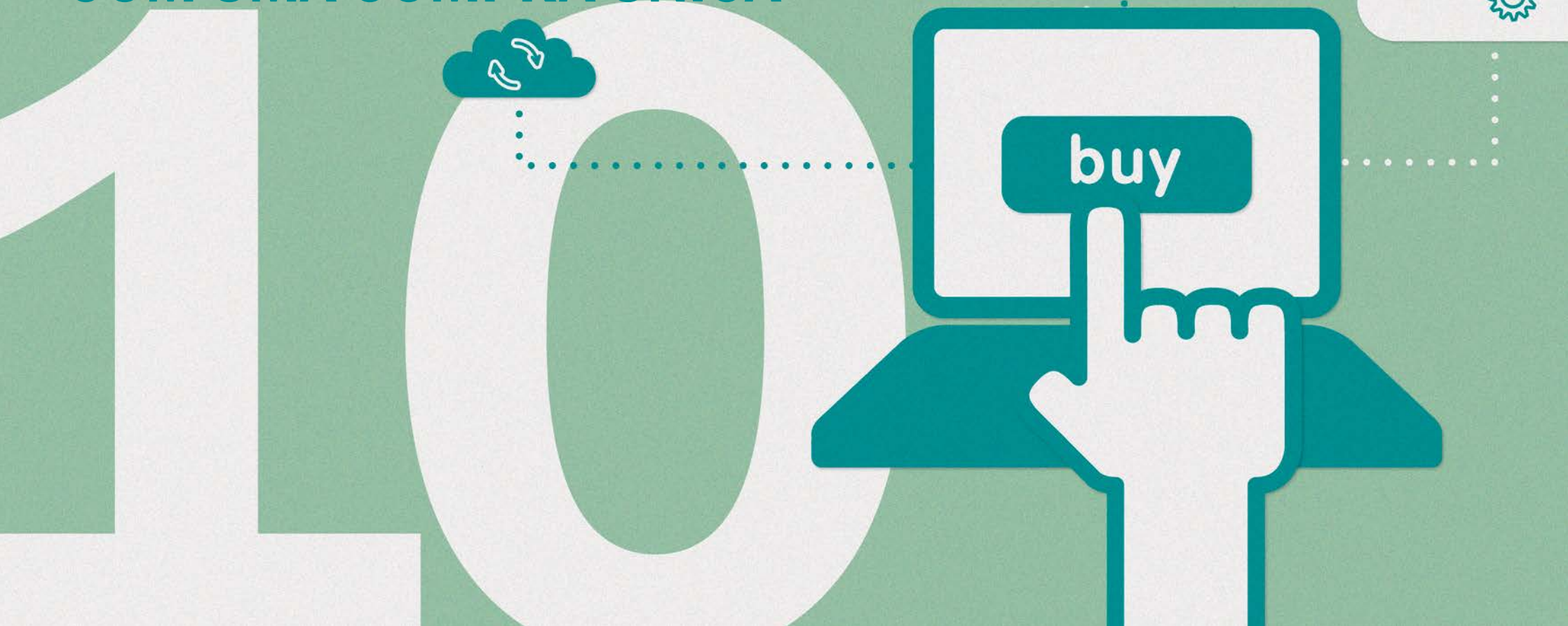
Enquanto outros fornecedores seguirem estratégias de aquisição para aumentar a respetiva oferta de produtos num cenário de ameaças em rápida mudança, a Kaspersky é a única a desenvolver e manter tudo a nível interno. Ao contrário de outros fornecedores, isto permite uma integração profunda a partir do nível de base de código, permitindo-nos oferecer as várias vantagens descritas anteriormente neste documento.

Vantagens:

- Servidor de gestão e consola de administração únicos;
- Arquitetura única de clientes de terminais;
- Políticas únicas e tarefas unificadas;
- Efeito de sinergia da funcionalidade integrada;
- Painéis de controlo e criação de relatórios integrados.

A mesma base de código e processo de desenvolvimento facilita atualizações e aplicações de patches mais rápidas — os utilizadores da Kaspersky podem atualizar uma única aplicação, em vez de duas ou mais aplicações (e os componentes associados), necessárias em muitos produtos da concorrência.

**MODELO DE
COMPRA INTEGRADO
— TODAS AS
FUNCIONALIDADES
DE QUE NECESSITA
COM UMA COMPRA ÚNICA**



10

MODELO DE COMPRA INTEGRADO —
TODAS AS FUNCIONALIDADES DE QUE
NECESSITA COM UMA COMPRA ÚNICA

Uma compra abrange todas as suas necessidades e funções de segurança e basta uma licença para ativar tudo.

Vantagens:

- **Responda a diferentes necessidades com um único pacote:** os utilizadores da Kaspersky podem adquirir diferentes níveis e variantes de funcionalidades integradas, respondendo a diferentes necessidades dos clientes — tudo isto utilizando apenas um pacote de licença. Isto é único.

POR ÚLTIMO...

Com a Kaspersky Lab, os utilizadores obtêm uma plataforma de proteção de terminais genuína, desenvolvida do início ao fim utilizando a mesma base de código e I&D. As nossas tecnologias de vulnerabilidades de software e antimalware são desenvolvidas pelo nosso grupo de investigação interno dedicado, que estuda constantemente de que forma as ameaças modernas penetram nos sistemas para criar proteções mais eficazes.

O grupo de investigação de listas brancas e vulnerabilidade para aplicações da Kaspersky Lab é responsável pela gestão do nosso ecossistema de parceiros e fornecedores, proporcionando uma base de dados constantemente atualizada de software legítimo e, ao mesmo tempo, disponibilizando as informações mais atualizadas sobre os patches disponíveis.

A convergência da segurança de terminais e da tecnologia de gestão de sistemas/clientes é uma tendência em crescimento. A Kaspersky Lab, com o seu processo de desenvolvimento e base de código totalmente internos, desfruta de um posicionamento único para explorar as sinergias óbvias entre as funções de segurança e aquelas tradicionalmente vistas como componentes da gestão de sistemas.

A integração da Kaspersky Lab fornece uma verdadeira plataforma de proteção de terminais. A proteção é ideal, não opcional.

Saiba mais em www.kaspersky.pt/business

CONHEÇA JÁ: AVALIAÇÃO DE 30 DIAS GRÁTIS

Descubra como a nossa segurança premium pode proteger a sua empresa contra malware e cibercrime com uma avaliação sem compromissos.

Registe-se hoje para transferir versões completas de produtos e avaliar o sucesso com que estes protegem a sua infraestrutura de TI, terminais e dados empresariais confidenciais.

30



ACERCA DA KASPERSKY LAB

A Kaspersky Lab é o maior fornecedor privado do mundo de soluções de proteção de terminais. A empresa encontra-se classificada entre os quatro principais fornecedores de soluções de segurança para utilizadores de terminais a nível mundial*. Ao longo dos seus mais de 17 anos de história, a Kaspersky Lab foi sempre uma inovadora na segurança de TI e fornece soluções de segurança digital eficientes para grandes empresas, PME e consumidores. A Kaspersky Lab, cuja sociedade gestora de participações sociais está registada no Reino Unido, opera atualmente em quase 200 países e territórios por todo o mundo, oferecendo proteção a mais de 300 milhões de utilizadores. Saiba mais em www.kaspersky.pt.

* A empresa ocupava o quarto lugar na classificação IDC de Worldwide Endpoint Security Revenue by Vendor, de 2012. A classificação foi publicada no relatório IDC "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC #242618, agosto de 2013). O relatório classificava os fornecedores de software consoante as suas receitas em vendas de soluções de segurança de terminais em 2012.

JUNTE-SE À CONVERSA

#securebiz



Veja-nos no
YouTube



Veja-nos no
Slideshare



Goste de
nós no
Facebook



Visite
o nosso
blogue



Siga-nos
no
Twitter



Junte-se a
nós no
LinkedIn

© 2014 Kaspersky Lab Iberia.

Todos os direitos reservados. As marcas registadas e de serviço são propriedade dos respetivos titulares.

KASPERSKY