KASPERSKY ENDPOINT SECURITY FOR BUSINESS – DIE INTEGRIERTE ENDPOINT-PROTECTION-PLATTFORM

10 VORTEILE,

DIE IHNEN NUR EINE INTEGRIERTE PLATTFORM-SICHERHEITSLÖSUNG BIETET

KASPERSKY lab

Im Bericht von Kaspersky Lab zu globalen IT-Risiken wird festgestellt, dass es in 94 % der Unternehmen in den letzten 12 Monaten zu einer Art von externem Sicherheitsvorfall gekommen ist[1].

Da Umfang und Raffiniertheit der Bedrohungen exponentiell anwachsen, entwickeln Unternehmen aller Größenordnungen ein besseres Verständnis für IT-Sicherheitsrisiken, insbesondere für gezielte Angriffe, und wie sie sich vor bestimmten Bedrohungen schützen können, anstatt einen unsystematischen, sehr breit gefassten Ansatz für eine allgemeine Vorstellung von „Malware“ einzusetzen.

Bedauerlicherweise verfolgen viele IT-Sicherheitsanbieter nach wie vor einen solchen unmethodischen, breit gefassten Ansatz. Sie kaufen dann Fremdtechnologien ein, kombinieren unterschiedliche, oft inkompatible Codebasen und schaffen so Komplexität und zusätzliche Probleme.

[1] Global IT Security Risk Report 2014.

Die Tage der herkömmlichen Endpoint-Sicherheit mit getrennten Komponenten für Anti-Malware, Verschlüsselung, Geräte und Netzwerk sind gezählt. Endpoint Protection-Plattformen (EPPs), die nahtlos miteinander integrierte Sicherheitstechnologien versprechen, sind ein wachsender Trend in den Bereichen IT-Sicherheit, Schutz vor hoch entwickelten Bedrohungen und Datensicherheit.

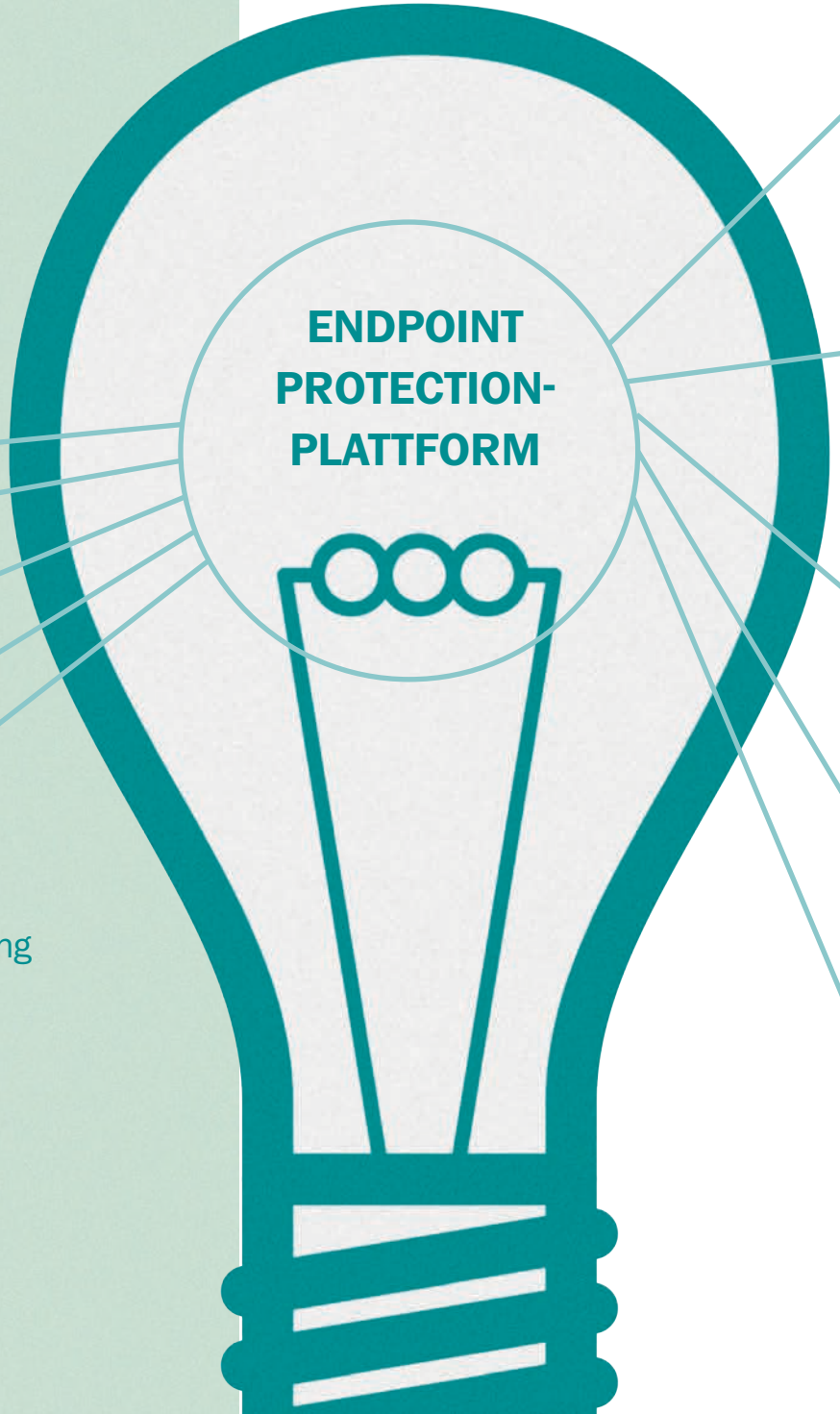
Es besteht jedoch ein gewaltiger Unterschied zwischen „Integration“ und einer echten Plattform. Zudem sind bei der Integration verschiedene Integrationstiefen möglich. Für viele Hersteller ist „Integration“ mittlerweile gleichbedeutend mit „kompatibel“.

Und für einige von ihnen heißt „kompatibel“, Produkte aus nicht weniger als 40 Übernahmen zusammenzuschustern und dann zu versuchen, diese mit der eigenen Codebasis ans Laufen zu bringen – ganz zu schweigen von der des Kunden.

Es gibt eine Vielzahl von Herstellern, die „integrierte“ Lösungen anbieten. Wenn Sie aber etwas genauer hinschauen, werden Sie erkennen, dass zwischen „miteinander harmonieren“ und echter Synergie ein gewaltiger Unterschied besteht. Schwierigkeiten, erworbene Technologien zu vereinheitlichen, behaupten aber, ihre Plattformen seien umfassend integriert.

Lediglich nur das aufzukaufen, was angeblich das nächste „große Ding“ sein soll, führt einfach nicht zu demselben umfassenden Überblick – oder Schutz.

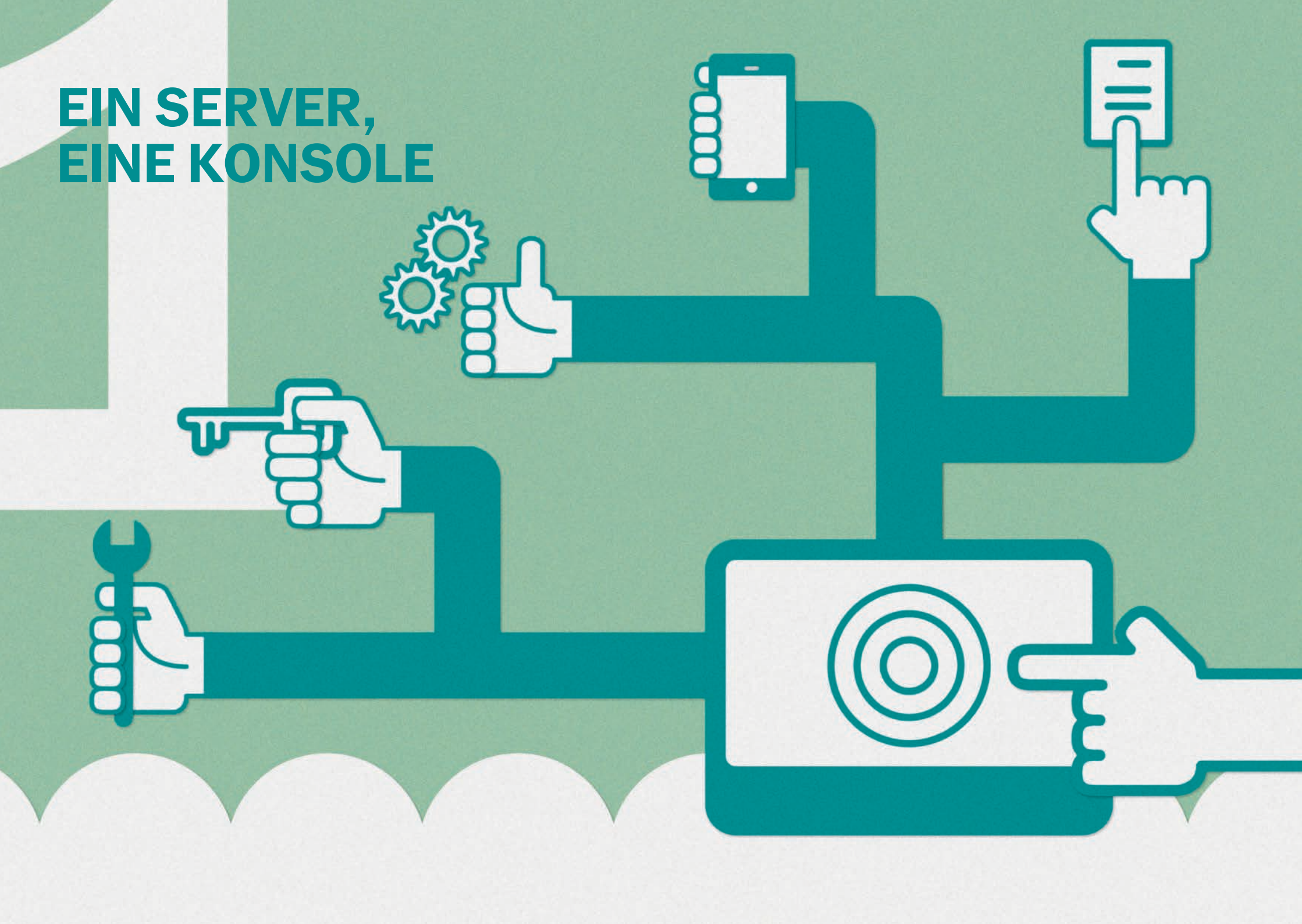
Es gibt eine Reihe von Vorteilen, die nur eine echte, tiefgreifend integrierte Plattformlösung mit sich bringt. Kaspersky Endpoint Security for Business bietet IT-Administratoren die folgenden, einzigartigen Vorteile:



1. Ein Server, eine Konsole
2. Architektur mit einem Agent*, einfache Installation
3. Der Vorteil einer einzigen Richtlinie
4. Der Synergie-Effekt: Mehr als die Summe der Einzelteile
5. Einheitliche Verwaltung von Administratorrechten – erweiterte Überwachung und Steuerung von einer Konsole aus
6. Einheitlicher Aufbau, einheitliche Funktionsweise – schnelleres, einfacheres Reporting
7. Klare, detaillierte Datensichten – integrierte Dashboards und Reporting-Funktionen
8. Einheitliche Lizenzverwaltung und-steuerung – mehr Effizienz und Kontrolle
9. Einheitliche, intern entwickelte Codebasis für tiefgreifendere Integration
10. Integriertes Anschaffungsmodell – alle benötigten Funktionen mit einem Kauf

* Architektur mit einem Agent pro Plattform (Windows, Linux, Mac)

EIN SERVER, EINE KONSOLE



1 EIN SERVER, EINE KONSOLE

Kaspersky Lab bietet als einziger Hersteller eine Lösung mit nahtlos integrierter Verwaltungskonsole und nur einem Management-Server, die von Anti-Malware über Datenschutz bis hin zu Mobile Device Management und Systems Management alle Aspekte der Endpoint Security abdeckt: Kaspersky Security Center.

Sicherheitsrichtlinien und Reporting werden über eine einzelne Konsole verwaltet, die mit externen Ressourcen, z. B. LDAP-Verzeichnissen und Microsoft Exchange, integriert ist. Ebenfalls eingebunden sind Datenbanken der Hardware- und Software-Bestände sowie Updates für Software-Schwachstellen, um die Integration und Synergie-Effekte zu verstärken, da dieselben Daten für unterschiedliche Funktionen genutzt werden können. Es besteht keine Notwendigkeit, verschiedene Server oder Datenbestände zu synchronisieren – alles wird nur einmal auf demselben Server installiert und über eine Konsole verwaltet.

Diese tiefgreifende Integration und die daraus resultierenden Synergie-Effekte liefern einen deutlichen Vorteil gegenüber Konkurrenzlösungen, die oft hinzugekaufte Technologien mit mehreren, separaten Datenbanken enthalten, mit denen der Grad an Integration, den die Plattform von Kaspersky Lab bietet, einfach nicht zu erreichen ist.

Die Vorteile:

- **Schnelles, unkompliziertes Deployment:** Ein einziger Installations- und Konfigurationsprozess für Management-Server und Konsole sorgt für nahtlos integrierte Funktionalität, die umgehend zur Verfügung steht.

- **Eine Management-Server-Hardware:** Keine Probleme aufgrund unterschiedlicher Anforderungen für Hardware-, System- oder Zusatzkomponenten für die einzelnen Verwaltungsserver und die jeweilige Konsole. Kaspersky Lab benötigt für die meisten Deployments nur EINEN Server.

- **Einzelne Management-Server-Software:** Benutzerfreundliche Infrastruktur für Kleinunternehmen, die für größere Deployments skaliert werden kann.
  - Bei einigen Konkurrenzprodukten müssen nach dem ersten Rollout zusätzliche Softwarepakete installiert werden, um ähnliche Funktionen wie Kaspersky Lab zu bieten.
  - Die Plattform von Kaspersky Lab umfasst außerdem zusätzliche Programme (z. B. Programme für eine Microsoft-Umgebung), die während der Konfiguration automatisch installiert werden und so Zeit und Aufwand sparen. Es funktioniert einfach.

ARCHITEKTUR MIT EINEM AGENT*, EINFACHE INSTALLATION

* Architektur mit einem Agent pro Plattform (Windows, Linux, Mac)

2 ARCHITEKTUR MIT EINEM AGENT*, EINFACHE INSTALLATION

Die Lösung von Kaspersky Lab bietet als einzige einen Endpoint-Agent, der dank der tiefgreifenden Codeintegration in der Lage ist, eine umfassende Kompatibilität und Synergie für alle Hardware- und Software-Konfigurationen zu garantieren.

Echte Endpoint Protection-Plattformen besitzen eine optimierte Architektur, die reduzierte Komplexität und eine tiefgreifendere Integration ermöglicht, da zur Aufgabenausführung nur ein Minimum an separaten Agents eingesetzt wird. Zugehörige Funktionen, z. B. Vulnerability Scanning, Updates und Patching von Programmen sowie Schutzmodule wie Anti-Malware und Verschlüsselung besitzen eine Architektur mit nur einem einzigen Agent, wodurch die Leistung optimiert und Ihr Verwaltungsaufwand reduziert wird.

Bei vielen Konkurrenzlösungen ist eine Vielzahl von Agents auf demselben System erforderlich, um Funktionen wie Patching, Programmkontrolle oder Verschlüsselung bereitzustellen.
Dies kann zu Problemen mit der Agent-Kompatibilität führen und zusätzliche Tests erforderlich machen.

* Architektur mit einem Agent pro Plattform (Windows, Linux, Mac)

Die Vorteile:

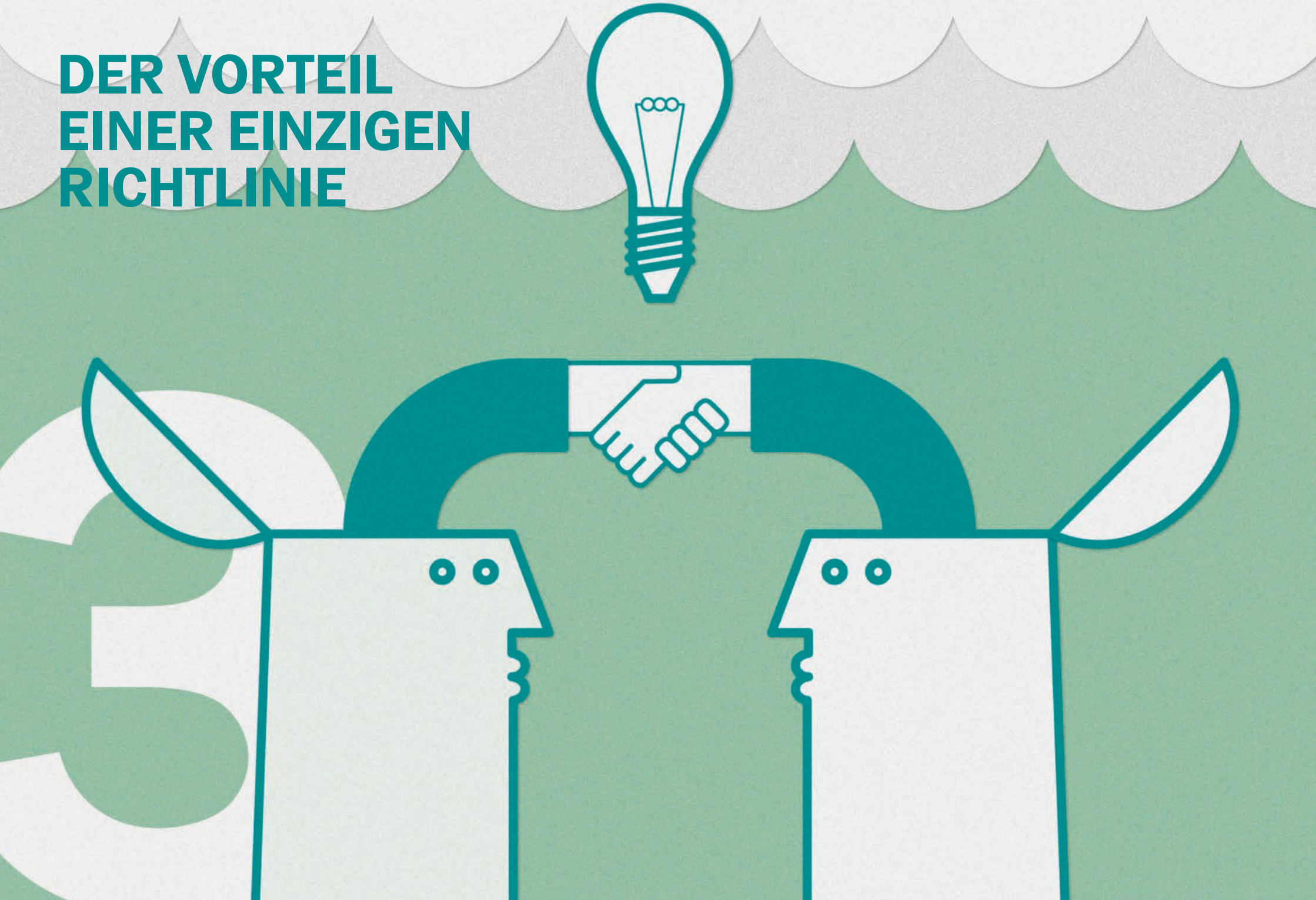
- **Spart Zeit bei Deployment und Updates:** Ein einfacher Installationsvorgang, ohne Abhängigkeiten oder häufige Neustarts.

- **Kein Kopfzerbrechen wegen unterschiedlicher Systemanforderungen:**
  Es ist kein Geheimnis, dass bei Wachstum durch Übernahmen Kompatibilitätsprobleme entstehen können. Durch hinzugekaufte Funktionen können neue, separate Anforderungen entstehen, die über die des Softwarepakets, in das sie integriert sind, hinausgehen. Zu dumm, wenn Sie das erst während des Deployments feststellen … Nur ein organischer, integrierter Entwicklungsansatz garantiert nahtlose Kompatibilität der unterschiedlichen Softwarekomponenten für verwaltete Endpoint-Plattformen/-Geräte. Dies bedeutet außerdem weniger clientseitige Kompatibilitätstests.

- **Geringe Auswirkung:** Auf Systemleistung und Verwaltungsaufwand.

- **Grundlage für die Entwicklung von Synergie-Szenarien:**
  Tiefgreifende Integration ermöglicht Flexibilität und reichhaltigere Funktionalität. Erweiterte Funktionalität ohne zusätzliche Ressourcenbelastung.

DER VORTEIL EINER EINZIGEN RICHTLINIE



3 DER VORTEIL EINER EINZIGEN RICHTLINIE

Obwohl Komplexität eine Gefahr für die Sicherheit ist, erfordert eine umfassende Verwaltung der Informationssicherheit in einem Unternehmen oft den Umgang mit einer Vielzahl sehr unterschiedlicher Lösungen. Wenn es Ihnen gelingt, die Verwaltungsvorgänge einfacher zu gestalten, haben Sie mehr Klarheit und sind in der Lage, Risiken zu minimieren.

Eine echte Endpoint Protection-Plattform ermöglicht es Ihnen, Erkennung, Deployment, Richtlinienkonfiguration und das Update von Endpoints innerhalb der gesamten Infrastruktur eines Unternehmens zu steuern. Dank nur eines Agent pro Plattform können Administratoren bei Kaspersky Endpoint Security eine aktive Richtlinie für eine verwaltete Gruppe festlegen, durch die alle erforderlichen Komponenten abgedeckt werden, ohne dass eine Vielzahl von Richtlinien geprüft und zugeordnet werden muss.

Der „Network Agent“ stellt die Verbindung zwischen Endpoint und dem Verwaltungsserver her, führt Systems-Management-Vorgänge (z. B. Software- und Hardware-Inventur, Vulnerability Scanning und Patch Management) aus und ermöglicht so echte Flexibilität und Synergie zwischen den Funktionen.

Die Vorteile:

- **Vereinfachte Richtlinien- und Aufgabenverwaltung:** Dank eines Satzes aus gemeinsam genutzten Parametern und Bedingungen – verwaltete Gruppen, Bereitstellungsoptionen, Benachrichtigungen – wurde die Richtlinienumsetzung optimiert, wodurch redundante Arbeitsgänge für den IT-Administrator entfallen.

- **Einfachere Kontrolle der Richtlinien- und Aufgabenumsetzung:** Ein Dashboard mit Reporting zu Deployment und Ausführung bietet einen umfassenden Überblick über den Richtlinienstatus und die Einhaltung der Vorgaben im gesamten Netzwerk.

- **Optimierung von Richtlinien- und Aufgabenänderungen: Änderungen werden in einem Schritt vorgenommen.** Durch die automatische Richtlinienzuweisung werden mehrere Sicherheitsparameter gleichzeitig abgedeckt, z. B. unterschiedliche Schutzeinstellungen, Programm-, Geräte- und Web-Kontrollen oder die Verschlüsselungsrichtlinien.

DER SYNERGIE-EFFEKT: MEHR ALS DIE SUMME DER EINZELTEILE

4 DER SYNERGIE-EFFEKT: MEHR ALS DIE SUMME DER EINZELTEILE

Der integrierte Endpoint-Schutz bildet den Kern der Sicherheitsplattform von Kaspersky Lab und ermöglicht eine einfache Umsetzung selbst bei komplexen, erweiterten Sicherheitsszenarien. Echte Integration bietet Sicherheit, die über die Funktionen der einzelnen Teile hinausgeht. Hier ein Beispiel:

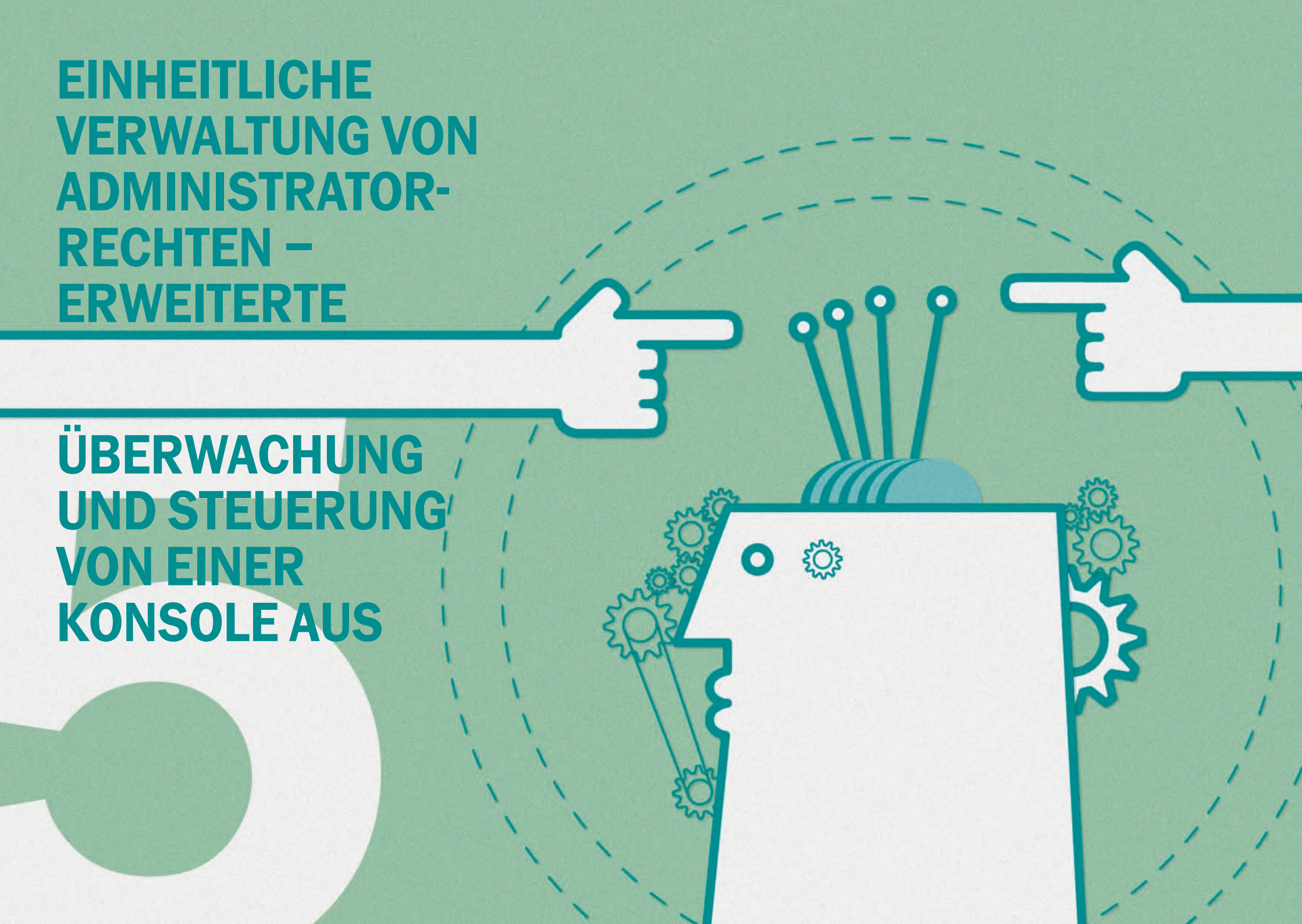
Um einen umfassenden Schutz vor Bedrohungen aus dem Internet zu gewährleisten, könnte ein Unternehmen zusätzlich zu richtlinienbasiertem Webverkehr und dem Scannen heruntergeladener Dateien die Programmkontrollfunktion von Kaspersky Lab verwenden, um die Nutzung eines einzelnen, von der IT-Abteilung genehmigten Browsers durchzusetzen. Dieser Browser lässt sich wiederum durch automatisches, priorisiertes Vulnerability Patching noch weiter absichern und kann durch automatischen Exploit-Schutz effektiv vor Zero-Day-Attacken geschützt werden. Auf diese Weise bilden die miteinander integrierten Funktionen von Kaspersky Lab einen echten Schutzschirm, um einer Vielzahl von Angriffsmöglichkeiten vorzubeugen. Dies ist gemeint, wenn wir vom Synergie-Effekt reden.

Die Vorteile:

- **Gemeinsame Nutzung von Sicherheitsmanagement-Praktikenund der von den verschiedenen Funktionen erfassten Informationen. Beispiele:**
  - — Die Informationen aus der Hardware-Bestandsaufnahme werden für die Gerätekontrolle und die Verschlüsselung von Wechseldatenträgern verwendet.
  - — Informationen aus der Software-Bestandsaufnahme werden für die Programmkontrolle und für Verschlüsselungsrichtlinien genutzt.
  - — Mobile Device Management (MDM) wird mit der Datensicherheit auf Geräten integriert.– Update-Status und Scan-Ergebnisse bilden zusammen mit dem Vulnerability Assessment die Grundlage für die NAC-Sicherheitsstellung.
  - — Patch Management-Entscheidungen können auf dem Vulnerability Assessment basieren.

Der Synergie-Effekt ist nicht auf die oben erläuterten Szenarien beschränkt – Kaspersky Lab ist dank der tiefgreifenden Codeintegration in der Lage, eine umfassende Kompatibilität und Synergie für alle Hardware- und Software-Konfigurationen zu gewährleisten. Plattformen von Kaspersky Lab bieten Sicherheit, die über die Funktionen der einzelnen Teile hinausgeht.

EINHEITLICHE VERWALTUNG VON ADMINISTRATOR-RECHTEN – ERWEITERTE ÜBERWACHUNG UND STEUERUNG VON EINER KONSOLE AUS



5 EINHEITLICHE VERWALTUNG VON ADMINISTRATORRECHTEN – ERWEITERTE ÜBERWACHUNG UND STEUERUNG VON EINER KONSOLE AUS

Unterbesetzte IT-Abteilungen sind in kleinen und mittelständischen Unternehmen ein häufig anzutreffendes Problem. Budgetkürzungen und eine Steigerung der Komplexität in der IT haben dazu geführt, dass IT-Administratoren immer weniger Zeit für eine ständig wachsende Zahl von Aufgaben haben.

Die Endpoint Protection-Plattform von Kaspersky Lab stellt sich dieser Herausforderung mit einheitlichen Verwaltungstools zur Ausführung alltäglicher Sicherheitsvorgänge. Dank der tiefgreifenden Integration können Programmberechtigungen und Protokolle von einer Konsole aus verwaltet werden. Ein Protokoll für alle Vorgänge – im Gegensatz zu Konkurrenzprodukten, die Daten aus verschiedenen Konsolen und Servern abrufen müssen.

Die einheitliche Rechteverwaltung und Anmeldung ermöglicht eine effektive Kontrolle und Analyse der Aktivitäten von Mitarbeitern und bildet die Grundlage für eine wirksamere Verwaltung von Berechtigungen. Das Ergebnis: Verbesserte Sicherheit und Kontrolle von IT-Betrieb und -Management. Alles mit einer einzigen Konsole.

Die Vorteile:

- **Einfache Festlegung und Steuerung von Berechtigungen:** In einem typischen Mittelstandsbetrieb, in dem sich der „IT-Mensch“ um alles kümmern muss, sollte die Ausführung der sicherheitsrelevanten Vorgänge möglichst einfach sein, einschließlich der Lese-/Schreibberechtigungen, Zugriffsrechte usw.

- **Schnelle Vorfallsreaktion und einheitliches Ereignisprotokoll:** IT-Administratoren sind auch nur Menschen, denen Fehler unterlaufen, und bei einem Sicherheitsvorfall kommt es auf ein rasches Eingreifen an. Eine Funktion, mit der sich Berechtigungen umgehend ändern oder sperren lassen, sowie die Möglichkeit, diese Änderungen nachzuverfolgen, ist deshalb von essenzieller Bedeutung. Bei getrennten Lösungen können komplexe Sicherheitsvorfälle eine Vielzahl von Analysevorgängen erforderlich machen. Kaspersky Lab reduziert die Komplexität, da alle Änderungen der Endpoint-Sicherheit, Richtlinien und Verwaltungsaktivitäten in einer einzigen Protokolldatei erfasst werden, die über die zentrale Verwaltungskonsole abgerufen werden kann.

EINHEITLICHER AUFBAU, EINHEITLICHE FUNKTIONSWEISE – SCHNELLERES, EINFACHERES REPORTING

6 EINHEITLICHER AUFBAU, EINHEITLICHE FUNKTIONSWEISE – SCHNELLERES, EINFACHERES REPORTING

Vielbeschäftigte Administratoren nutzen jede Chance, um Zeit einzusparen oder einen Vorgang zu vereinfachen. Endpoint Protection-Plattformen mit einheitlichen, integrierten Funktionen und einer gemeinsamen Schnittstelle vereinfachen Reporting, Analyse und Vorfallmanagement – Kaspersky Security Center generiert Berichte mit einheitlichem Aufbau und Layout.

Der Arbeitsalltag eines IT-Administrators besteht aus einer Vielzahl unerlässlicher Routineaufgaben, die alle überwacht und protokolliert werden müssen. Bei einer gemischten Lösung ist hierzu eine Vielzahl von Dashboards erforderlich, die Berichte in unterschiedlichen Formaten generieren, z. B. als PDF, HTML oder direkt als E-Mail. Wer hat schon die Zeit, sich all dies anzuschauen UND sicherzustellen, dass alles ordnungsgemäß läuft?

In einer solchen Umgebung können schon die kleinsten Verbesserungen von Funktionalität oder Effizienz zu Zeitersparnissen führen und die Arbeitsbelastung von IT-Sicherheitsadministratoren verringern. Einheitliches Reporting mit einem einheitlichen Layout vereinfachen Analyse und Auswertung, verbessern das Vorfallmanagement und ermöglichen einen proaktiven Umgang mit der IT-Sicherheit.

Die Vorteile:

- **Einfachere, schnellere Berichtsauswertung: Berichtsvorlagen garantieren eine einheitliche Terminologie und einen gleichbleibenden Aufbau.** „Computer, PC, Knoten, Rechner“ sind alles Bezeichnungen, die für denselben verwalteten Endpoint verwendet werden können. All diese Begriffe werden in verschiedenen Produkten und in den zugehörigen Herstellerdokumentationen synonym verwendet, was das Ganze ein wenig verwirrend machen kann. Wie sähe es aus, wenn bei jedem der Sicherheitskomponenten Ihrer gemischten Lösung ein ähnliches sprachliches Problem besteht? Und wenn jede dieser Komponenten zwar dieselben Parameter verwendet, diese aber unterschiedliche Bezeichnungen haben? In einer derart komplexen Umgebung gestalten sich die Untersuchungen von Bedrohungen oder Vorfällen um einiges schwieriger, als sie es eigentlich sein müssten, und das selbst für Administratoren, die mit der Konfiguration vertraut sind. Es ist eine Sache, wenn Administratoren mit Komplexität zurechtkommen müssen, aber wie sieht es in Fällen aus, in denen externe Ermittler, beispielsweise Prüfer oder Behörden, involviert sind? Wenn Sie diesen externen Personen einen konfusen Überblick über Ihre Infrastruktur vermitteln, entsteht möglicherweise der falsche Eindruck.

- **Vereinfachtes Vorfallmanagement:** Einfache Erkennung ähnlicher Vorfälle innerhalb verschiedener IT-Infrastrukturknoten, z. B. Malware und Richtlinienverletzungen.

KLARE, DETAILLIERTE DARSTELLUNG– INTEGRIERTE DASHBOARDS UND REPORTING-FUNKTIONEN

7 KLARE, DETAILLIERTE DARSTELLUNG – INTEGRIERTE DASHBOARDS UND REPORTING-FUNKTIONEN

Endpoint Protection-Plattformen sollten bei Dashboards und Reporting einen ganzheitlichen Ansatz verfolgen. Wahre Integration geht über Aussehen und Bedienung der Benutzeroberfläche hinaus. Wenn Sie beispielsweise in der Verwaltungskonsole auf eine der Registerkarten für die Endpoint-Eigenschaften klicken, sollten Sie Informationen zu allen Sicherheitsaspekten des verwalteten Clients erhalten, z. B. angewendete Richtlinien, Status, Updates und Vorfälle.

Dashboards und Berichte sollten darüber hinaus dazu beitragen, Untersuchungen zu vereinfachen und einen besseren Einblick in die einzelnen Endpoints gewähren. Da bei echter Integration Informationen von einer Vielzahl von Komponenten erfasst werden, gelingt dies viel einfacher.

Die Vorteile:

- **Eine Verwaltungskonsole für alle Endpoint-Sicherheitskomponenten:** Ein Dashboard, das alle wichtigen Informationen zum Status der verwalteten Endpoints, zu Deployment-Vorgängen, Lizenzkontrolle sowie zu allen relevanten Sicherheitsereignissen und -vorfällen übersichtlich zusammenfasst.

- **Optimierte Detailansichten und Analysefunktionen:** Nutzen Sie ineinander greifende Berichte, um Daten, einschließlich Endpoint-Verwaltung, Vulnerability Assessment und Patching, Hardware- und Software-Bestand und den erstellten Benutzerkonten, aus verschiedenen Blickwinkeln zu analysieren. Transparenter Überblick über Schutzstatus und Vorfälle, einschließlich Malware-Erkennung und Verschlüsselungsstatus. Auf diese Weise können Sicherheitsanalysen und Überprüfungen optimiert und vereinfacht werden.

- **Systemeigenes Executive Reporting:** Das Executive Reporting ist eine der Kernaufgaben von IT-Sicherheitsadministratoren. Das Erstellen umfassender Berichte auf Grundlage mehrerer Konsolen und Datenbestände kann sich als sehr zeitaufwändig und umständlich erweisen. Aus diesem Grund besitzen Endpoint Security-Plattformen von Kaspersky Lab systemeigene, sofort einsetzbare Executive Reporting-Funktionen.
  Es besteht keine Notwendigkeit, Berichte mithilfe externer Tools aufzubereiten oder anzupassen. Ihnen bleibt also mehr Zeit, sich auf andere Projekte zu konzentrieren.

EINHEITLICHE LIZENZVERWALTUNG UND -STEUERUNG – MEHR EFFIZIENZ UND KONTROLLE

8 EINHEITLICHE LIZENZVERWALTUNG UND -STEUERUNG – MEHR EFFIZIENZ UND KONTROLLE

Die Verwaltung der Lizenzen für alle Sicherheitslösungen im gesamten Unternehmensnetzwerk war noch nie so einfach. Bei Kaspersky Lab werden alle – und das heißt wirklich alle – Funktionen über eine einzige Lizenz aktiviert: Endpoint-Sicherheit, Datenschutz, Mobile Device Management und System Management.

Diese Lizenz lässt sich mühelos auf die einzelnen Endpoints im Unternehmen verteilen, unabhängig von Status oder Standort, physischen oder virtualisierten Maschinen, in jedem Netzwerk, egal ob kabelgebunden oder drahtlos. Die integrierte Lizenzverwaltungsfunktion von Kaspersky Lab erlaubt Ihnen eine effektivere Nutzung der von Ihnen bezahlten Ressourcen und ermöglicht gleichzeitig eine striktere Kontrolle über die Lizenzgültigkeit.

Die Vorteile:

- **Eine Konsole für die Lizenzüberwachung:** Für Überwachung und Prüfung des Lizenzstatus sind keine unterschiedlichen Kontrolltools erforderlich.

- **Effiziente Nutzung von Lizenzen: Kostenreduzierung durch flexiblen Einsatz innerhalb einer sich ständig wandelnden IT-Umgebung.** Ein Beispiel wäre die Umstellung von herkömmlichen PCs und Notebooks auf eine virtualisierte Infrastruktur und mobile Geräte bei gleichbleibender Funktionalität.

- **Einfaches Upgrade Ihrer Sicherheitslösung:** Mit der Endpoint Protection-Plattform von Kaspersky Lab können Sie den Umfang der Sicherheitsfunktionen bedarfsgerecht erweitern. Beginnen Sie mit der Endpoint-Sicherheit, und aktivieren Sie dann weitere Features, wie Verschlüsselung oder Systems Management, einfach durch Hinzufügen einer neuen Lizenz.

EINHEITLICHE, INTERN ENTWICKELTE CODEBASIS FÜR TIEFGREIFENDERE INTEGRATION

9 EINHEITLICHE, INTERN ENTWICKELTE CODEBASIS FÜR TIEFGREIFENDERE INTEGRATION

Unsere einheitliche, intern bei Kaspersky Lab entwickelte und gepflegte Codebasis bildet das Herzstück unserer integrierten Endpoint Protection-Plattform.

Im Gegensatz zu anderen Anbietern, die ihre Produktpalette angesichts einer sich dynamisch verändernden Bedrohungslage anhand von Übernahmen erweitern müssen, wird die gesamte Codebasis bei Kaspersky Lab intern entwickelt. Dies ermöglicht eine tiefgreifende Integration, die schon an der Codebasis ansetzt, und bildet die Grundlage für die vielen, in diesem Dokument vorgestellten Vorteile.

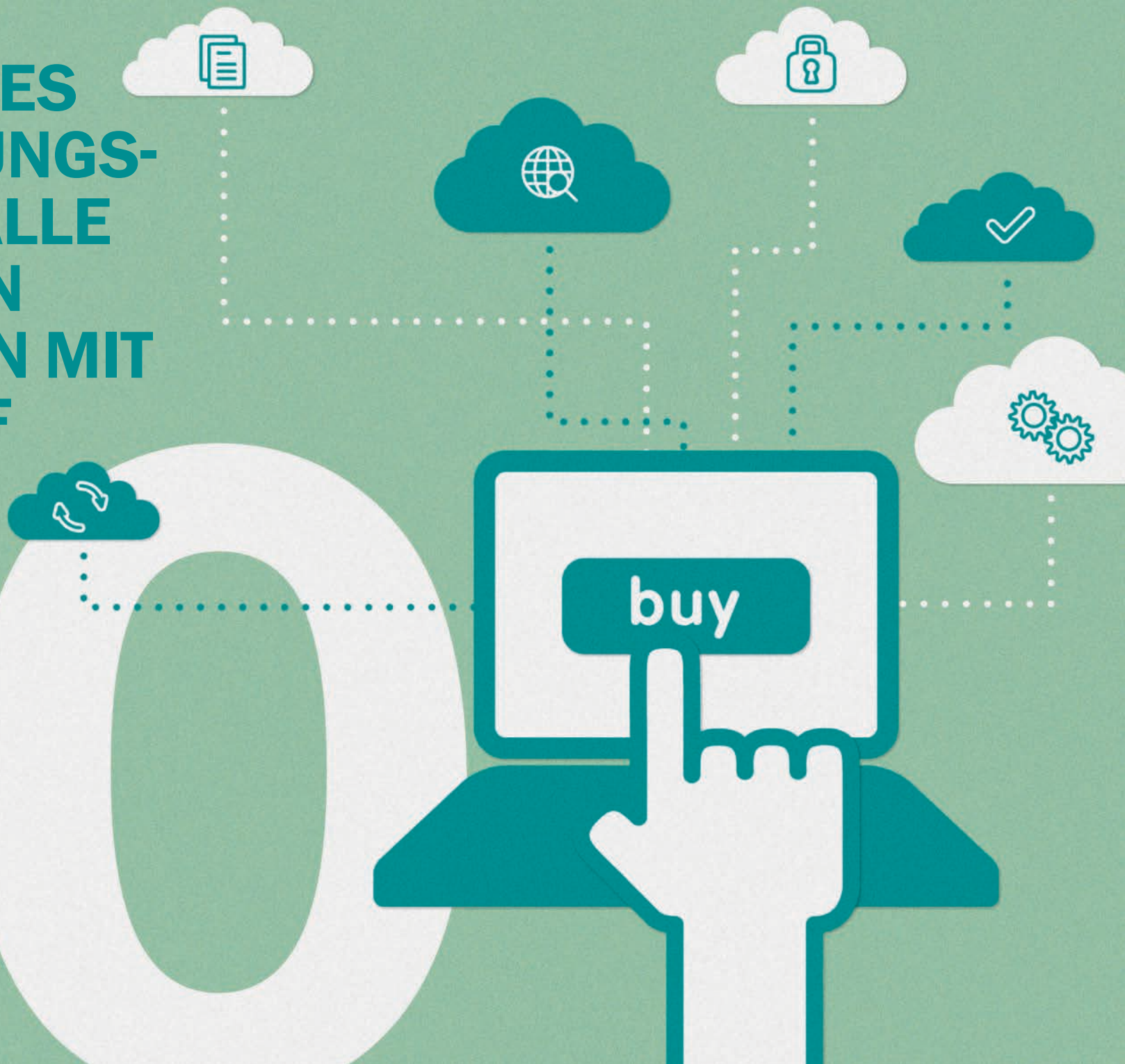
Die Vorteile:

- Ein Management-Server und eine Verwaltungskonsole
- Client-Architektur mit einem einzigen Endpoint
- Einzelne Richtlinien und vereinheitlichte Abläufe
- Synergie-Effekt durch integrierte Funktionalität
- Integrierte Dashboards und Reporting

Eine einheitliche Codebasis und einheitliche Entwicklungsprozesse ermöglichen schnellere Update- und Patching-Vorgänge. Benutzer von Kaspersky-Produkten müssen nur ein einziges Programm aktualisieren, anstatt zwei oder noch mehr Programme (einschließlich der zugehörigen Komponenten), wie bei vielen Konkurrenzprodukten.

INTEGRIERTES ANSCHAFFUNGS-MODELL – ALLE BENÖTIGTEN FUNKTIONEN MIT EINEM KAUF

10



10 INTEGRIERTES ANSCHAFFUNGSMODELL – ALLE BENÖTIGTEN FUNKTIONEN MIT EINEM KAUF

Mit einer Bestellung decken Sie sämtliche Sicherheitsanforderungen und -funktionen ab, die Sie dann über eine einzige Lizenz aktivieren können.

Die Vorteile:

- **Erfüllt unterschiedliche Anforderungen mit einem Paket:** Zur Erfüllung unterschiedlicher Kundenanforderungen stehen für die integrierten Funktionen verschiedene Levels und Varianten zur Verfügung – und das mit einem einzigen Lizenzpaket. Das kann kein anderer Hersteller bieten.

ZU GUTER LETZT …

Unsere Kunden erhalten eine echte Endpoint Protection-Plattform, die von Anfang bis Ende auf Grundlage derselben Codebasis und unter Nutzung einheitlicher Forschungsergebnisse von Kaspersky Lab entwickelt wurde. Die integrierten Anti-Malware-Technologien und Verfahren zum Vulnerability Scanning von Software werden von einem speziellen, internen Forschungsteam entwickelt, das laufend analysiert, wie moderne Schadsoftware in Systeme eindringt, um effektivere Schutzmechanismen zu entwickeln.

Ein internes Team, das unsere Programm-Whitelists zusammenstellt und Schwachstellen analysiert, ist für die Verwaltung unseres Partner- und Lieferantennetzwerks zuständig und veröffentlicht eine laufend aktualisierte Datenbank mit vertrauenswürdiger Software sowie aktuelle Informationen zu verfügbaren Patches.

Die Bündelung von Endpoint-Sicherheit und Client/Systems Management-Technologien ist ein anhaltender Trend. Mit einer komplett intern entwickelten Codebasis ist Kaspersky Lab bestens aufgestellt, die offenkundigen Synergien zu nutzen, die sich zwischen Sicherheitsfunktionen und den Komponenten ergeben, die traditionell dem Systems Management zugerechnet wurden.

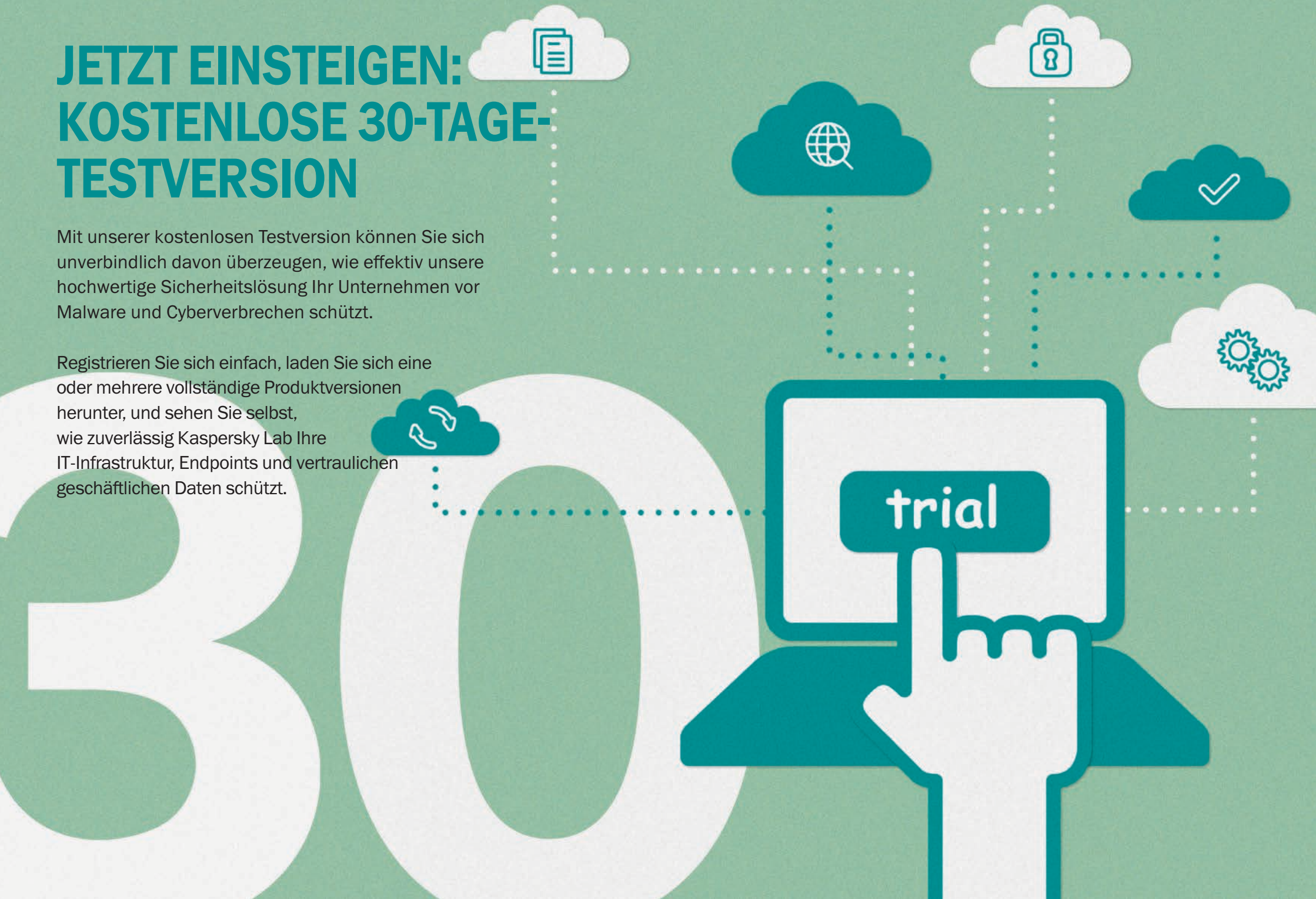
Die hervorragende Integration von Kaspersky Lab ermöglicht eine echte Endpoint Protection-Plattform. Unser Schutz ist optimal, nicht optional.

Weitere Informationen erhalten Sie unter:
www.kaspersky.de/business-security.

JETZT EINSTEIGEN: KOSTENLOSE 30-TAGE-TESTVERSION

Mit unserer kostenlosen Testversion können Sie sich unverbindlich davon überzeugen, wie effektiv unsere hochwertige Sicherheitslösung Ihr Unternehmen vor Malware und Cyberverbrechen schützt.

Registrieren Sie sich einfach, laden Sie sich eine oder mehrere vollständige Produktversionen herunter, und sehen Sie selbst, wie zuverlässig Kaspersky Lab Ihre IT-Infrastruktur, Endpoints und vertraulichen geschäftlichen Daten schützt.



ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer*. In seiner 17-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Der Hauptsitz des Unternehmens ist in Großbritannien registriert. Kaspersky Lab ist zurzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 300 Millionen Anwendern weltweit.
Weitere Informationen erhalten Sie unter: **www.kaspersky.de**.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2012“ den vierten Rang. Die Rangfolge wurde im IDC-Bericht „Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares“ (IDC Nr. 242618, August 2013) veröffentlicht. In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2012 eingestuft.

DEM GESPRÄCH BEITRETEN

#securebiz

Auf YouTube ansehen

Auf Slideshare ansehen

Werden Sie unser Fan auf Facebook

Lesen Sie unseren Blog

Folgen Sie uns auf Twitter

Treten Sie uns auf LinkedIn bei

KASPERSKY lab