SE NON È KASPERSKY ENDPOINT SECURITY FOR BUSINESS NON È UNA PIATTAFORMA DI PROTEZIONE DEGLI ENDPOINT

# 10 VANTAGGI

## CHE SOLO UNA SOLUZIONE DI SICUREZZA INTEGRATA PUÒ OFFRIRE

KASPERSKY lab

Il rapporto sui rischi IT globali di Kaspersky Lab ha messo in evidenza come il 94% delle aziende abbia subito un incidente di sicurezza esterna in varie forme negli ultimi 12 mesi[1].

Con l'aumento esponenziale del volume e della complessità delle minacce, le aziende di tutte le dimensioni stanno sviluppando una migliore comprensione dei rischi legati alla sicurezza IT, in particolare degli attacchi mirati, e di come possono proteggersi da minacce specifiche anziché adottare un approccio generale e casuale a una nozione generalizzata di "malware".

Purtroppo molti fornitori di sicurezza IT continuano a portare avanti questo schema casuale e generalizzato, proponendo nuove tecnologie e mettendo insieme codebase disparati, spesso incompatibili, con il risultato di creare una complessità maggiore e di provocare tanti problemi quanti ne risolvono.

I giorni della sicurezza tradizionale degli endpoint (anti-malware, crittografia, controllo di dispositivi e controllo di accesso alla rete) sono ormai al tramonto. Le piattaforme di protezione endpoint (EPP, Endpoint Protection Platform), con la loro promessa di tecnologie di sicurezza fortemente integrate, rappresentano il trend in crescita per la sicurezza IT, la prevenzione avanzata delle minacce e la protezione dei dati.

Sussiste però una grandissima differenza tra il concetto di "integrazione" e una vera e propria piattaforma. Quando si tratta di integrazione, poi, esistono livelli diversi di completezza. Per molti fornitori, la parola "integrazione" è diventata solo un sinonimo di "compatibilità".

Alcuni invece per "compatibilità" intendono la combinazione di prodotti diversi ottenuti con una quarantina di acquisizioni e il tentativo di farli funzionare con la propria codebase, senza pensare a quella dei clienti.

Esiste una pletora di fornitori che promettono soluzioni "integrate", ma basta esaminare un po' più a fondo per scoprire la differenza notevole tra un "funzionamento discreto" di questi componenti e una vera sinergia che deriva da roadmap di prodotti e da uno sviluppo basato sull'approfondimento. Alcuni fornitori si affannano per unificare i prodotti delle aziende acquisite, dichiarando al tempo stesso di poter offrire piattaforme realmente integrate.

Acquistare tutto quello che ha l'aspetto dell'Ultimo ritrovato non significa poter fornire la stessa completezza di visione o di protezione.

[1] Rapporto sui rischi IT globali per la sicurezza 2014.

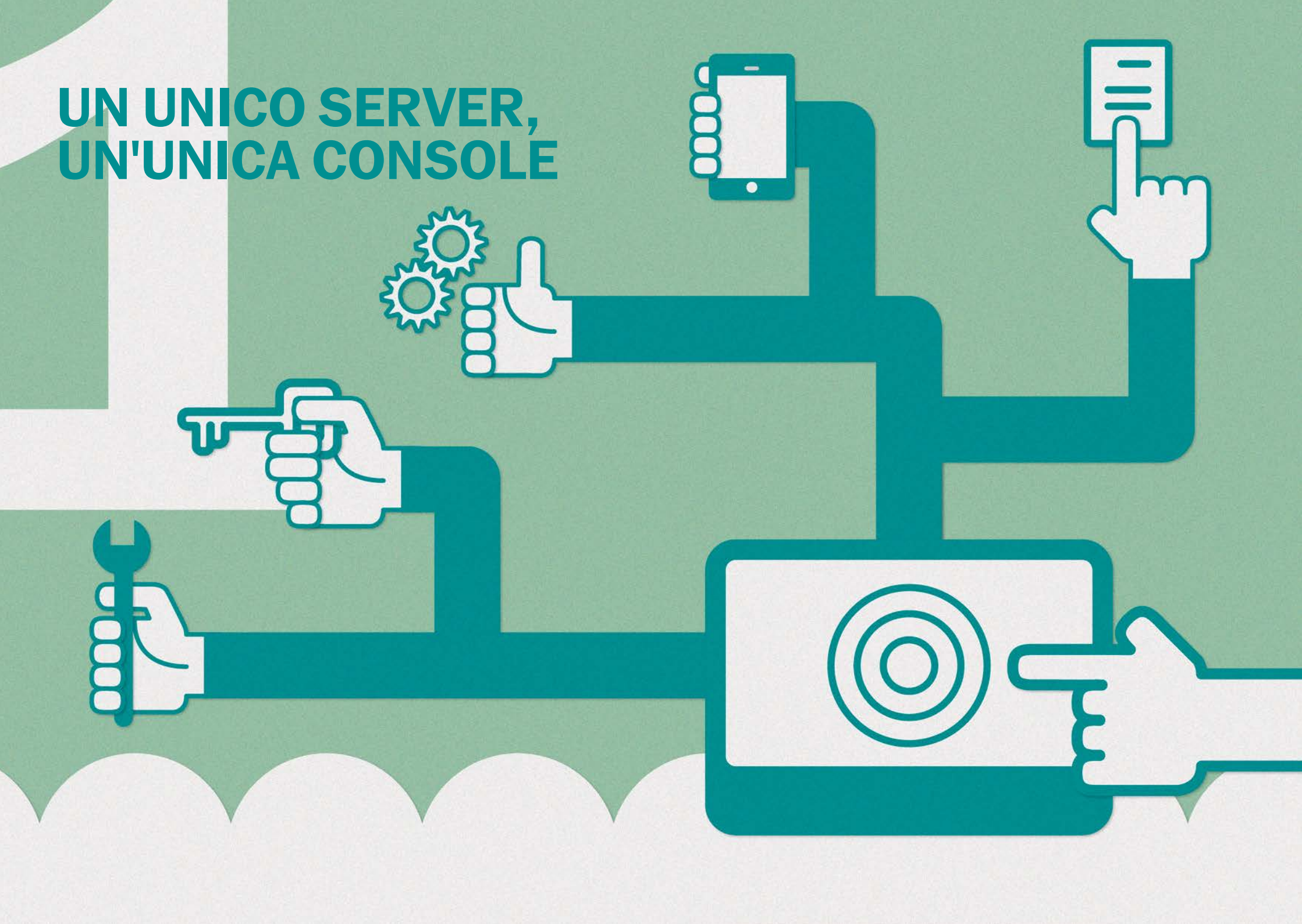
Ecco alcuni dei vantaggi che solo una soluzione di piattaforma realmente e profondamente integrata può offrire. Kaspersky Endpoint Security for Business è l'unico in grado di offrire questi vantaggi agli amministratori IT:

1. Un unico server, un'unica console
2. Architettura con un unico agente*, semplicità di installazione
3. Il vantaggio del criterio unico
4. L'effetto sinergia, maggiore della somma delle parti
5. Gestione unificata dei diritti di amministratore: maggiore capacità di controllo e verifica tramite un'unica console


6. Struttura e aspetto familiari: reporting più rapido e più facile
7. Visualizzazione più chiara e approfondita dei dati: dashboard e reporting integrati
8. Gestione e controllo unificati delle licenze: maggiore efficienza, migliore controllo
9. Un'unica codebase, creata internamente, per un'integrazione più approfondita
10. Modello di acquisto integrato: tutte le funzionalità necessarie in un unico acquisto

* Architettura con un unico agente per piattaforma (Windows, Linux, Mac).

# UN UNICO SERVER, UN'UNICA CONSOLE



# 1 UN UNICO SERVER, UN'UNICA CONSOLE

La soluzione di Kaspersky Lab è la sola capace di offrire un unico server di gestione e un'unica console di amministrazione strettamente integrati, capaci di coprire ogni aspetto della sicurezza degli endpoint, dall'attività anti-malware alla protezione dei dati, dalla gestione dei dispositivi mobili alla gestione dei sistemi: parliamo di Kaspersky Security Center.

I criteri e i report di sicurezza vengono gestiti tramite un'unica console, integrata con risorse esterne come le directory LDAP e Microsoft Exchange. Sono compresi anche i database di inventari hardware e software e le vulnerabilità/gli aggiornamenti software, da cui scaturiscono ulteriori possibilità in termini di integrazione e sinergia, grazie all'opportunità di utilizzo degli stessi dati per più funzioni. Non c'è necessità di mantenere la sincronizzazione con server o data set diversi, perché tutto viene installato una sola volta, sullo stesso server, e gestito tramite la stessa console.

Queste capacità di profonda integrazione e sinergia offrono un netto vantaggio rispetto alle soluzioni della concorrenza, che in maggioranza si basano su tecnologie acquistate con più database separati e semplicemente non possono dare la stessa profondità di integrazione della piattaforma Kaspersky.

## I vantaggi:

- **Rapidità e facilità di implementazione:** l'unicità del server di gestione, del processo di installazione e configurazione della console offre una funzionalità totalmente integrata, pronta per l'uso.

- **Unicità dell'hardware del server di gestione:** non esiste più il problema dei requisiti di hardware, sistema o componenti aggiuntivi diversi per ogni console e server di amministrazione separato. Kaspersky richiede UN UNICO server per la maggioranza delle implementazioni.

- **Unicità del software del server di gestione:** ecco un'infrastruttura di facile gestione per le piccole aziende, pronta per l'espansione nel caso di implementazioni di maggiori dimensioni.
  — Alcuni prodotti richiedono l'installazione di pacchetti aggiuntivi dopo il rollout iniziale, e questo solo per offrire funzionalità simili a quelle di Kaspersky Lab.
  — Per maggiore praticità, la piattaforma Kaspersky include altre applicazioni (ad esempio quelle richieste in un ambiente Microsoft) come parte del processo di installazione e di auto-installazione, risparmiando tempo e complicazioni. E tutto questo funziona.

# ARCHITETTURA CON UN UNICO AGENTE*, SEMPLICITÀ DI INSTALLAZIONE

* Architettura con un unico agente per piattaforma (Windows, Linux, Mac).

## 2 ARCHITETTURA CON UN SINGOLO AGENTE*, SEMPLICITÀ DI INSTALLAZIONE

La soluzione di Kaspersky è la sola capace di offrire un agente per gli endpoint con una profonda integrazione del codice per garantire una compatibilità completa e facile da raggiungere insieme alla sinergia delle configurazioni hardware e software.

Le piattaforme realmente finalizzate alla protezione degli endpoint presentano un'architettura semplificata, per ridurre la complessità e approfondire l'integrazione usando un numero minimo di agenti discreti per eseguire le operazioni. Le funzioni correlate come la scansione delle vulnerabilità, gli aggiornamenti delle applicazioni e le patch, insieme ai moduli di protezione come anti-malware e crittografia, hanno un'architettura con un unico agente, il che semplifica le prestazioni e riduce l'impatto della gestione.

Molte offerte della concorrenza richiedono più agenti sulla stessa macchina per funzionalità come l'applicazione di patch, il controllo delle applicazioni e la crittografia. In questo modo si creano potenziali problemi di compatibilità degli agenti e sono necessari test aggiuntivi.

* Architettura con un unico agente per piattaforma (Windows, Linux, Mac).

# I vantaggi:

- **Risparmio di tempo per l'implementazione iniziale e gli aggiornamenti:** solo una semplice operazione di installazione da controllare, senza dipendenze e senza necessità di numerosi riavvii.

- **Nessuna complicazione dovuta ai diversi requisiti di sistema:** non è un segreto che la crescita per acquisizioni crei problemi di compatibilità del software. La funzionalità dei componenti acquisiti può creare nuovi requisiti di supporto in aggiunta a quelli del software in cui sono stati inclusi. Peccato che tutto questo si scopra solo quando si avvia l'implementazione... Solo un approccio organico e integrato di sviluppo può garantire la compatibilità assoluta dei diversi componenti software per le piattaforme e i dispositivi degli endpoint gestiti. Tutto ciò si traduce in una riduzione dei test di compatibilità sul lato client.

- **Impatto ridotto:** sulle prestazioni di sistema e sulla gestione.

- **Base per lo sviluppo di scenari di sinergia:** la profonda integrazione consente flessibilità e migliore funzionalità. Si estendono così le capacità senza aumentare l'impatto per le risorse.

# IL VANTAGGIO DEL CRITERIO UNICO

# 3 IL VANTAGGIO DEL CRITERIO UNICO

La complessità è nemica della sicurezza, tuttavia la gestione di ogni aspetto della sicurezza dei dati in un'organizzazione spesso richiede l'uso di numerose soluzioni diverse. Più si semplificano i processi di gestione, più si può aumentare la chiarezza e ridurre i rischi.

Un'autentica piattaforma di protezione degli endpoint controlla il rilevamento, l'implementazione, la configurazione dei criteri e l'aggiornamento degli endpoint in tutta l'infrastruttura aziendale. Grazie all'agente unico per piattaforma di Kaspersky Endpoint Security, gli amministratori possono impostare un criterio attivo per un gruppo gestito per tutti i componenti richiesti, senza dover esaminare o correlare più criteri.

Il "Network Agent" collega l'endpoint al server di amministrazione eseguendo operazioni di gestione del sistema (ad esempio inventario software e hardware, scansione delle vulnerabilità e gestione delle patch), consentendo così una reale funzionalità e una sinergia tra funzioni.

## I vantaggi:

- **Gestione semplificata dei criteri e delle operazioni:** Grazie a un unico set di parametri e prerequisiti condivisi (gruppi gestiti, impostazioni di distribuzione, notifiche) si ottimizza l'implementazione dei criteri, eliminando i processi e le operazioni ridondanti per l'amministratore IT.

- **Controllo semplificato dell'implementazione di criteri e operazioni:** l'unicità di dashboard e report sull'implementazione e l'esecuzione offre una vista completa e immediata dello stato e della conformità dei criteri per l'intera rete.

- **Modifiche semplificate dei criteri e delle operazioni:** le variazioni vengono eseguite in un unico passaggio. L'assegnazione automatica dei criteri può coprire numerosi parametri di sicurezza in una sola volta, dalle diverse impostazioni di protezione ai controlli delle applicazioni, dei dispositivi e del web, come i criteri di crittografia.

# L'EFFETTO SINERGIA, MAGGIORE DELLA SOMMA DELLE PARTI

# 4 L'EFFETTO SINERGIA, MAGGIORE DELLA SOMMA DELLE PARTI

Le funzionalità di protezione integrata degli endpoint costituiscono le attività principali della piattaforma sicura Kaspersky, semplificando l'implementazione di scenari di gestione della sicurezza avanzati e complessi. L'integrazione autentica offre una sicurezza che va oltre le parti componenti ogni funzionalità, ad esempio:

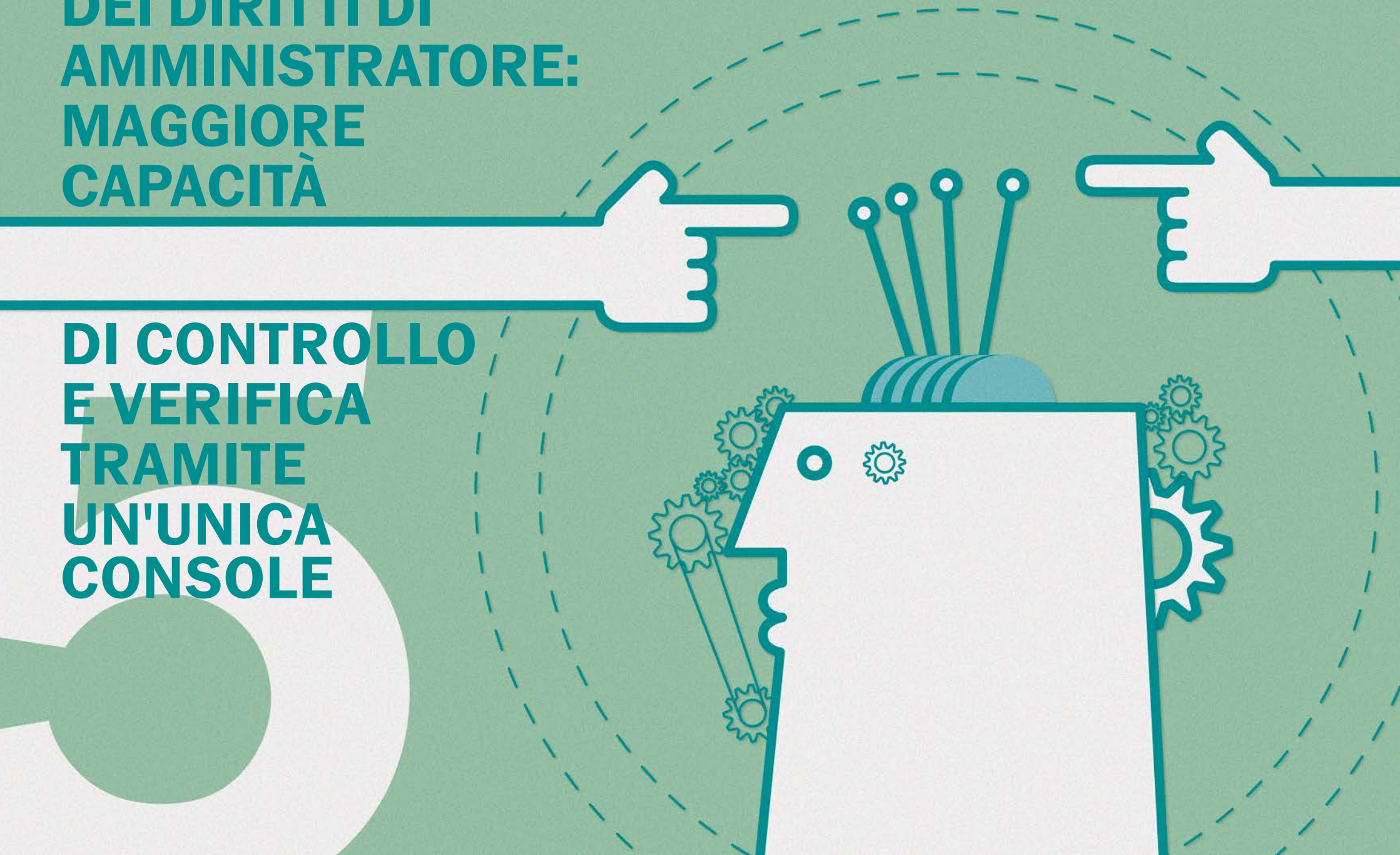
Per implementare una protezione completa dalle minacce di Internet, il controllo del traffico del web basato sui criteri e la scansione dei file scaricati, un'azienda potrebbe usare la funzione di controllo delle applicazioni di Kaspersky per applicare l'uso di un solo browser approvato dal reparto IT.
Questo browser, a sua volta, potrebbe essere ulteriormente protetto applicando le patch per la vulnerabilità ad alta priorità e salvaguardato dagli attacchi "zero-day" tramite la Prevenzione automatica degli exploit. In questo modo, le funzioni integrate di Kaspersky forniscono una copertura di protezione da un vettore di attacco importante: questo è quello che si intende per "Effetto sinergia".

## I vantaggi:

- **Cross-sharing delle pratiche di gestione della sicurezza e delle informazioni raccolte dalle diverse funzioni, ad esempio:**
  - — Le informazioni raccolte sui dispositivi rimovibili vengono utilizzate per il controllo e la crittografia dei dispositivi;
  - — Le informazioni sulle applicazioni considerano quanto viene inserito nei criteri di controllo e crittografia delle applicazioni;
  - — L'integrazione di Mobile device management (MDM) con la sicurezza dei dati nei dispositivi;
  - — Le decisioni di gestione delle patch possono essere basate sulla valutazione delle vulnerabilità.

L'Effetto Sinergia non è limitato agli scenari sopra descritti: l'integrazione profonda del codice di Kaspersky garantisce una compatibilità completa e facile da raggiungere insieme alla sinergia delle configurazioni hardware e software. Con la piattaforma Kaspersky, la sicurezza viene estesa oltre le parti costitutive di ciascuna funzione.

# GESTIONE UNIFICATA DEI DIRITTI DI AMMINISTRATORE: MAGGIORE CAPACITÀ DI CONTROLLO E VERIFICA TRAMITE UN'UNICA CONSOLE



## 5 GESTIONE UNIFICATA DEI DIRITTI DI AMMINISTRATORE: MAGGIORE CAPACITÀ DI CONTROLLO E VERIFICA TRAMITE UN'UNICA CONSOLE

Il personale limitato dei reparti IT è un problema comune per le piccole e medie imprese come per le grandi aziende. I tagli alle spese e la maggiore complessità della gestione IT si traducono in un maggior numero di operazioni che gli amministratori IT devono svolgere in meno tempo.

La piattaforma di protezione degli endpoint di Kaspersky affronta questa problematica fornendo strumenti di gestione unificata per le operazioni di sicurezza giornaliere. La profonda integrazione consente di gestire il controllo dei privilegi e i registri da una sola console. Tutte le azioni vengono riportate in un solo registro, a differenza dei prodotti della concorrenza, che spesso devono andare a procurarsi i dati da console e server separati.

La registrazione e la gestione unificata dei diritti consentono un controllo più efficace e una migliore visione delle azioni del personale, che supportano una gestione più funzionale delle autorizzazioni. Il risultato? Maggiore sicurezza e controllo delle verifiche sulle operazioni e sulla gestione IT. Tutto questo da un'unica console.

# I vantaggi:

- **Facilità di definizione e controllo delle autorizzazioni:** nella tipica piccola/media impresa, dove un solo informatico si occupa di tutto, dovrebbe essere facile eseguire tutte le operazioni correlate alla sicurezza, inclusa l'impostazione delle autorizzazioni di lettura/modifica, accesso e così via.

- **Risposta rapida agli incidenti e registro eventi unificato:** anche gli amministratori IT sono esseri umani: possono sbagliare e, nell'eventualità di un incidente di sicurezza, la rapidità della risposta è fondamentale. Una funzionalità che consente la modifica o il blocco rapido degli accessi è vitale, insieme alla capacità di monitorare queste modifiche. Con soluzioni separate, gli incidenti complessi possono richiedere la creazione di processi di analisi multipli. Kaspersky elimina la complessità, riportando tutte le modifiche alla sicurezza, le attività relative ai criteri e alla gestione, in un unico file di registro fornito da una singola interfaccia della console di gestione.

# STRUTTURA E ASPETTO FAMILIARI: REPORTING PIÙ RAPIDO E PIÙ FACILE

# 6 STRUTTURA E ASPETTO FAMILIARI: REPORTING PIÙ RAPIDO E PIÙ FACILE

Gli amministratori, sempre sotto pressione, colgono ogni opportunità per risparmiare tempo o semplificare un'operazione. Le piattaforme di protezione degli endpoint, con le funzionalità unificate e integrate e un'interfaccia comune, facilitano il reporting, l'analisi e la gestione degli incidenti: Kaspersky Security Center genera una struttura di report uguale, di aspetto uniforme.

La giornata lavorativa dell'amministratore IT in genere comprende una quantità di operazioni di routine, anche se vitali, e tutte vanno monitorate e documentate. In un ambiente di soluzioni miste, le dashboard sono molteplici, e ciascuna genera report di formati diversi, da PDF ad HTML all'email diretta. Ma chi ha il tempo di guardare tutti questi documenti E di accertarsi che tutto funzioni come dovrebbe?

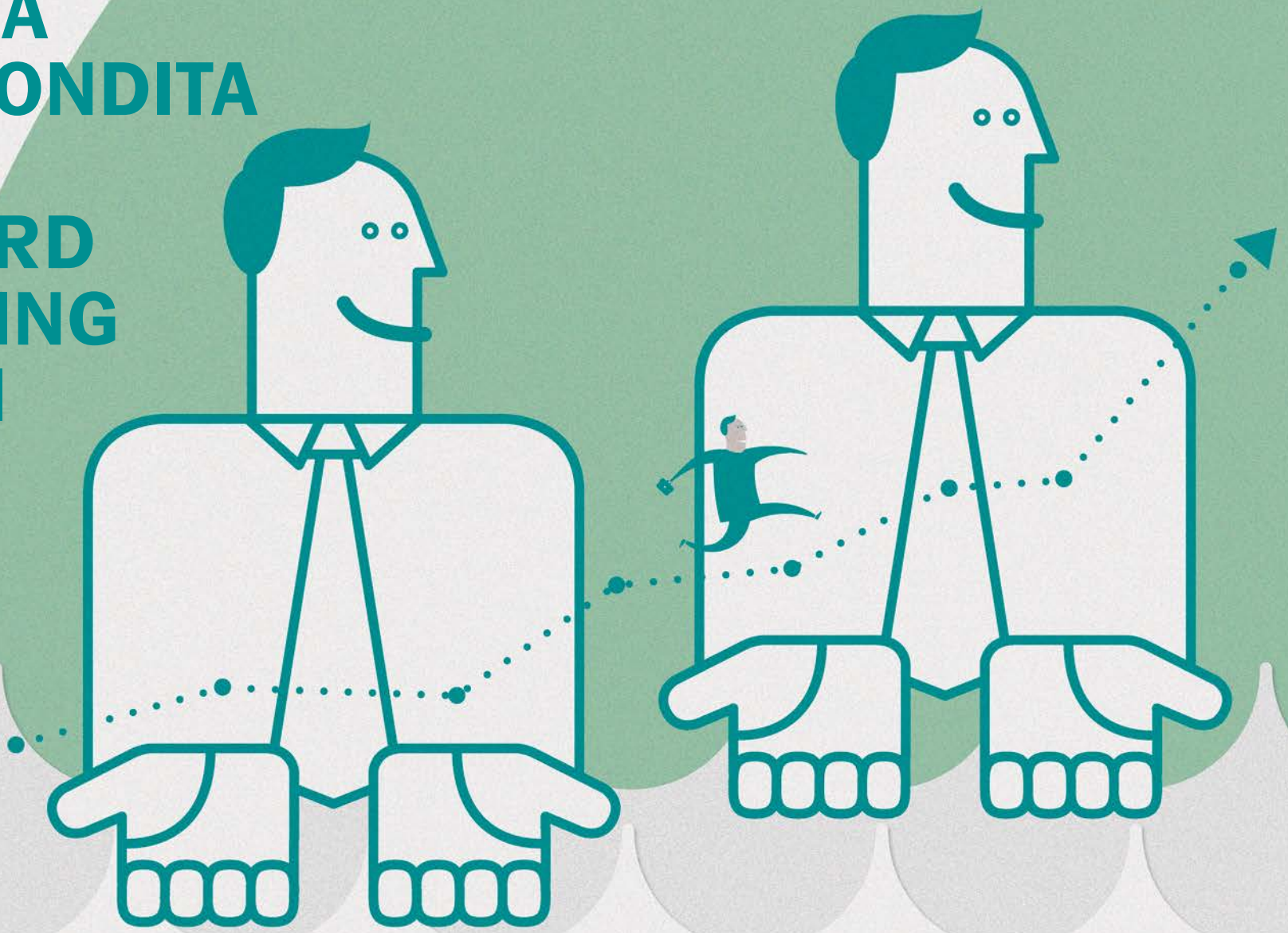
In questo ambiente, anche il minimo miglioramento in termini di praticità o di efficienza può fare risparmiare molto tempo e ridurre il carico di lavoro (per non parlare dello stress) che grava sugli amministratori della sicurezza IT, già fortemente messi alla prova. La generazione di report con lo stesso aspetto familiare può facilitare l'analisi e la valutazione, migliorando la gestione degli incidenti e consentendo un approccio proattivo alla sicurezza IT.

## I vantaggi:

- **Analisi dei report più facile e rapida:** tutti i modelli di report usano la stessa terminologia e la stessa struttura. "Computer, PC, nodo, macchina" sono tutti sinonimi dello stesso endpoint gestito; vengono usati in modo intercambiabile nei prodotti e nella documentazione dei fornitori: aggiungete prodotti alla combinazione, e le cose possono diventare piuttosto complicate. E se ognuno dei componenti della sicurezza dell'ambiente di soluzioni miste avesse un problema linguistico di questo tipo? E se ogni parametro di ciascuno di questi componenti avesse nomi "uguali o leggermente diversi"? In un ambiente tanto complicato, investigare sulle minacce o su altri incidenti diventa molto più difficile del necessario, anche per gli amministratori che conoscono bene le configurazioni. Gli amministratori possono gestire questa complessità, ma se la situazione coinvolge persone esterne come auditor o autorità di regolamentazione…? Offrendo a queste persone una visione confusa dell'infrastruttura si darà probabilmente un'impressione sbagliata.

- **Gestione semplificata degli incidenti:** facilità di riconoscimento di incidenti simili nei diversi nodi dell'infrastruttura IT, ad esempio malware o violazione di criteri.

# VISUALIZZAZIONE PIÙ CHIARA E APPROFONDITA DEI DATI: DASHBOARD E REPORTING INTEGRATI



## 7 VISUALIZZAZIONE PIÙ CHIARA E APPROFONDITA DEI DATI: DASHBOARD E REPORTING INTEGRATI

Le piattaforme di protezione degli endpoint dovrebbero fornire un approccio olistico alle dashboard e al reporting. Un'integrazione autentica va oltre l'aspetto dell'interfaccia: ad esempio, facendo clic su un'unica scheda "proprietà endpoint" di una console di amministrazione si dovrebbero ottenere informazioni su tutti gli aspetti della sicurezza del client gestito, quali criteri applicati, aggiornamenti di stato e incidenti.

Le dashboard e i report dovrebbero anche facilitare il processo investigativo e offrire una maggiore visibilità dell'endpoint: l'integrazione permette di raccogliere le informazioni dei diversi componenti, facilitando enormemente questa funzionalità.

# I vantaggi:

- **Una sola posizione per tutti i componenti della sicurezza degli endpoint:** una dashboard funzionale che permette un rapido controllo dei dati include le informazioni più importanti sullo stato degli endpoint gestiti, sull'esecuzione delle operazioni di implementazione e sul controllo delle licenze, oltre agli eventi di sicurezza e agli incidenti più critici.

- **Drilling e analisi facilitati:** il drilling dei report interdipendenti consente di analizzare e raccogliere dati da numerosi punti di vista, tra cui la gestione degli endpoint, la valutazione delle vulnerabilità e l'applicazione delle patch, l'inventario dell'hardware e delle applicazioni e gli account utente creati. Questo vuol dire grande visibilità dello stato di protezione e degli incidenti, compresi il rilevamento del malware e lo stato di crittografia dei dati. È così che l'analisi e l'investigazione della sicurezza si trasformano in un processo facile e lineare.

- **Reporting esecutivo pronto per l'uso:** il reporting esecutivo è uno dei componenti fondamentali delle responsabilità di un amministratore della sicurezza IT. Creare report completi partendo da console e dataset diversi è complicato e richiede molto tempo. È per questo che la piattaforma Kaspersky Endpoint Security offre la funzionalità di reporting esecutiva pronta per l'uso. Così non servono report personalizzati ottenuti usando strumenti di terze parti,  e rimane più tempo da dedicare ad altri progetti.

# GESTIONE E CONTROLLO UNIFICATI DELLE LICENZE: MAGGIORE EFFICIENZA, MIGLIORE CONTROLLO

# 8

## GESTIONE E CONTROLLO UNIFICATI DELLE LICENZE: MAGGIORE EFFICIENZA, MIGLIORE CONTROLLO

Gestire le licenze per tutte le soluzioni di sicurezza dell'intera rete aziendale non è mai stato tanto facile. Con Kaspersky Labs, tutte, ma veramente TUTTE le funzioni vengono attivate con un'unica licenza: sicurezza degli endpoint, protezione dei dati, gestione dei dispositivi mobili e gestione del sistema.

Questa unica licenza viene distribuita con facilità in tutta l'infrastruttura degli endpoint aziendali, indipendentemente dalla loro ubicazione, dal fatto che si tratti di macchine fisiche o virtuali su qualsiasi rete, fissa o mobile. La funzionalità di gestione integrata delle licenze Kaspersky consente di usare in modo più efficace ciò che è stato acquistato, mantenendo al contempo un migliore controllo della validità delle licenze.

## I vantaggi:

- **Un'unica postazione per la verifica delle licenze:** non occorre passare a strumenti diversi di controllo delle licenze per monitorarne e controllarne lo stato.

- **Uso efficiente delle licenze:** riduzione dei costi tramite la distribuzione flessibile in un ambiente IT in continua trasformazione. Ad esempio, questo potrebbe essere il caso del passaggio da PC e notebook tradizionali a dispositivi mobili con funzionalità equivalenti.

- **Aggiornamento facile della soluzione di sicurezza:** la piattaforma di protezione degli endpoint di Kaspersky permette di aumentare la funzionalità della sicurezza in base alle proprie esigenze. A partire dalla sicurezza degli endpoint, basta attivare funzionalità come la crittografia o la gestione dei sistemi aggiungendo una nuova licenza.

# UN'UNICA CODEBASE, CREATA INTERNAMENTE, PER UN'INTEGRAZIONE PIÙ APPROFONDITA

# 9

## UN'UNICA CODEBASE, CREATA INTERNAMENTE, PER UN'INTEGRAZIONE PIÙ APPROFONDITA

La codebase unica di Kaspersky, creata e gestita internamente, è il cuore della piattaforma integrata per la protezione degli endpoint.

Mentre altri fornitori si sono affidati a strategie di acquisizione per incrementare l'offerta di prodotti in un panorama di minacce in rapida evoluzione, Kaspersky è l'unica azienda che sviluppa e gestisce tutto internamente. Grazie a questo, Kaspersky è in grado di supportare l'integrazione approfondita a partire dal livello di codebase, e di offrire i molti vantaggi descritti precedentemente in questo documento.

## I vantaggi:

- Unico server di gestione e unica console di amministrazione;
- Un'unica architettura per i client degli endpoint;
- Unici criteri e operazioni unificate;
- Effetto sinergia della funzionalità integrata;
- Dashboard e reporting integrati

L'uso della stessa codebase e dello stesso processo di sviluppo consente una più rapida applicazione degli aggiornamenti e delle patch: gli utenti Kaspersky possono aggiornare una sola applicazione, anziché le due o più (e relativi componenti) di molti prodotti della concorrenza.

# MODELLO DI ACQUISTO INTEGRATO: TUTTE LE FUNZIONALITÀ NECESSARIE IN UN UNICO ACQUISTO

10

## 10 MODELLO DI ACQUISTO INTEGRATO: TUTTE LE FUNZIONALITÀ NECESSARIE IN UN UNICO ACQUISTO

Un solo ordine per tutte le esigenze e funzionalità di sicurezza: una sola licenza per attivare tutto.

# I vantaggi:

- **La risposta alle diverse esigenze in un solo pacchetto:** gli utenti Kaspersky possono acquisire livelli e tipologie differenti di funzionalità integrate, per rispondere ad esigenze diverse, tutto con un solo pacchetto di licenza. E questo non lo offre nessun altro.

# PER CONCLUDERE...

Con Kaspersky Lab, gli utenti ricevono una autentica piattaforma per la protezione degli endpoint, sviluppata dall'inizio alla fine con la stessa codebase e lo stesso team di ricerca e sviluppo. Si tratta di tecnologie integrate antimalware e di rilevamento delle vulnerabilità software sviluppate dal nostro gruppo interno di ricerca che studia costantemente la modalità di penetrazione dei sistemi da parte delle moderne minacce per sviluppare una protezione sempre più efficace.

Il gruppo di Kaspersky Lab per il whitelisting delle applicazioni e la ricerca sulle vulnerabilità gestisce un ecosistema di partner e fornitori, offrendo un database di software attendibile che viene aggiornato costantemente e dando al contempo le informazioni più aggiornate sulle patch disponibili.

Quella della convergenza tra tecnologia di sicurezza degli endpoint e di gestione di client e sistemi è una tendenza in crescita. Kaspersky Lab, con una codebase e un processo di sviluppo svolto interamente all'interno, ha una posizione unica nello sfruttamento delle sinergie ovvie tra le funzioni di sicurezza e quelli che tradizionalmente vengono considerati componenti della gestione dei sistemi.

L'integrazione di Kaspersky Lab fornisce un'autentica piattaforma di protezione degli endpoint. La protezione deve essere ottimale e non opzionale.

Ulteriori informazioni sul sito Web **www.kaspersky.it/business**

# INIZIA SUBITO: PROVA GRATUITA PER 30 GIORNI

Scopri come la nostra eccellente sicurezza sia in grado di proteggere la tua azienda dal malware e dal cybercrimine con una prova non vincolante.

Registrati oggi stesso per scaricare le versioni complete dei prodotti e valutare l'efficacia della loro protezione per l'infrastruttura IT, gli endpoint e i dati aziendali riservati.

## INFORMAZIONI SU KASPERSKY LAB

Kaspersky Lab è il maggior fornitore privato di soluzioni per la protezione degli endpoint al mondo. L'azienda è tra i primi quattro fornitori mondiali di prodotti di sicurezza per utenti endpoint*. Da più di 17 anni Kaspersky Lab è pioniere della sicurezza IT e offre soluzioni efficaci per la sicurezza digitale a grandi aziende e piccole e medie imprese e a privati. Kaspersky Lab, la cui società madre ha sede legale nel Regno Unito, è attualmente presente in quasi 200 Paesi e territori a livello globale e offre soluzioni di protezione a oltre 300 milioni di utenti in tutto il mondo.
Ulteriori informazioni sul sito Web: **www.kaspersky.it/business**

* La società ha conseguito il quarto posto nella classifica 2012 di IDC relativa ai fornitori del settore della sicurezza degli endpoint con il maggior fatturato. La valutazione è stata pubblicata nel report IDC "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, agosto 2013)". Nella relazione viene stilata una classifica di fornitori software basata sui ricavi ottenuti dalla vendita di soluzioni per la sicurezza degli endpoint nel 2012.

## PARTECIPA ALLA CONVERSAZIONE

#securebiz

Guardaci su YouTube


Visualizzaci su Slideshare


Metti il tuo Mi piace su Facebook


Leggi il nostro blog


Seguici su Twitter


Collegati su LinkedIn



KASPERSKY lab