KASPERSKY lab

Next Generation security per proteggere l'azienda da qualsiasi tipo di cyber minaccia.

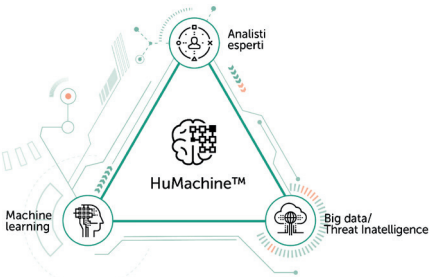
www.kaspersky.com/business
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Protezione come parte della strategia di business continuity

La tecnologia rappresenta una componente fondamentale per l'azienda: o si rimane al passo o si rischia di rimanere bloccati. Tuttavia la tecnologia può anche aiutare i criminali; l'endpoint è il primo obiettivo e la fonte della maggior parte dei problemi. Nel solo ultimo anno più del 38% delle imprese ha subito un cyberattacco, mentre il 39% degli attacchi mirati a endpoint protetti è andato a buon fine. In una situazione di questo tipo, le aziende hanno la necessità di doversi difendere dai cybercriminali che le attaccano.

Fino a quando ci saranno gli essere umani dietro ai cyberattacchi, per contrastarli sarà necessario l'intelletto umano e le tecnologie più innovative. La protezione di Kaspersky Lab è fondata sulla nostra Threat Intelligence globale combinata con algoritmi di machine learning, basata sulla competenza umana dei migliori specialisti del settore. Definiamo questa combinazione efficiente HuMachine™, parte intrinseca del DNA dei nostri prodotti.



Nel 2017, Kaspersky Lab ha vinto il primo premio **Platinum di Gartner Peer Insights per le piattaforme di protezione degli endpoint.** Questo premio è sicuramente il riconoscimento più prestigioso nel mercato delle piattaforme di protezione degli endpoint. Le nostre applicazioni endpoint hanno raggiunto la percentuale più alta (90%) di primi tre posti nell'ambito di test indipendenti rispetto a qualsiasi altro fornitore.

Un investimento per il futuro

L'impatto finanziario medio di una sola violazione dei dati per le piccole e medie imprese è di 86,5 mila dollari, mentre per le grandi imprese è pari a 992 mila dollari. La Next Generation security non è più sufficiente: solo una soluzione multilivello in grado di proteggere sia i diversi layer tecnologici che funzionali dell'infrastruttura IT aziendale può fornire la protezione necessaria. La reale sicurezza dell'endpoint combina diverse tecniche e tecnologie intelligenti per proteggere le aziende da qualsiasi tipo di cyberminaccia, su qualsiasi piattaforma. Se si è in grado di proteggere l'intera rete IT, è possibile garantire la business continuity.

Proteggi le risorse più preziose grazie alle applicazioni basate su HuMachine™

L'investimento e il budget dedicato alla sicurezza IT potrebbero non seguire la crescita aziendale. Le risorse devono essere ottimizzate per soddisfare le sfide odierne e future.
Kaspersky Endpoint Security for Business, sfruttando la HuMachine™ intelligence, protegge da ransomware, exploit e cyberminacce avanzate.
La nuova soluzione, ottimizzando il consumo di risorse, integra potenti controlli di sicurezza, gestione centralizzata delle patch e delle vulnerabilità rilevate sulle macchine gestite, crittografia integrata e possibilità di controllo da un'unica console in tutta la rete aziendale.

Sicurezza agile e flessibile

Il prodotto è pensato per funzionare in qualsiasi ambiente IT, utilizzando un set completo di tecnologie comprovate e Next generation.
I sensori incorporati e l'integrazione con Kaspersky Endpoint Detection and Response (EDR) consentono l'acquisizione e l'analisi di grandi volumi di dati per identificare i cyberattacchi più avanzati e sofisticati.

Sicurezza e versatilità per gli MSP

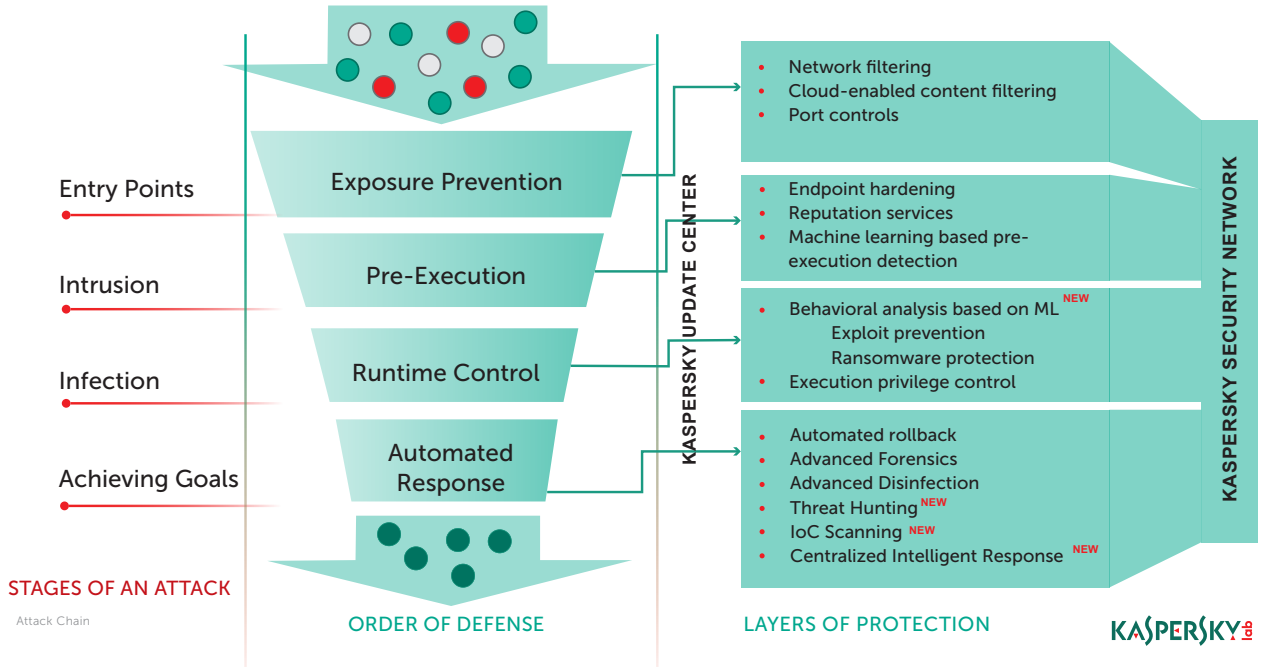
Per consentire agli MSP (Managed Service Providers) di aggiungere valore alla sicurezza IT delle proprie offerte, la soluzione include: Multitenancy integrata, prevenzione delle minacce avanzate, sicurezza dei dispositivi mobili, crittografia dei dati, gestione centralizzata delle patch e delle vulnerabilità rilevate sulle macchine gestite.

Footprint ridotto; prestazioni elevate

La nostra sicurezza più premiata e più testata basata su HuMachine garantisce una protezione ottimale con il minimo impatto sulle risorse del PC. I componenti signatureless assicurano che le minacce vengano rilevate anche senza aggiornamenti frequenti.

Protezione completa

Kaspersky Endpoint Security for Business utilizza diverse tecnologie Next generation (hardening degli endpoint, analisi dei comportamenti basata su machine learning, prevenzione degli exploit, ecc.) per neutralizzare la maggior parte delle minacce prima che possano giungere a una fase più avanzata. I file sospetti all'origine dell'attacco, oltre all'endpoint, vengono rilevati e bloccati.



Le tecnologie avanzate unitamente al nostro approccio multilivello sono la combinazione perfetta tra prestazioni e protezione efficace, occupando un ruolo cruciale nei nostri prodotti che così raggiungono uno dei più alti tassi di rilevamento del settore, come dimostrato in modo continuativo da test indipendenti.

Più livelli di protezione per

- Windows, Linux o Mac
- Android e altri dispositivi mobili
- Dispositivi rimovibili
- Server Windows e Linux
- Server di posta
- Gateway Web
- Collaboration server

Difesa senza precedenti contro

- Exploit
- Ransomware
- Malware mobile
- Minacce sconosciute
- Minacce fileless
- PowerShell e altri gli attacchi basati su script
- Minacce sul web
- Minacce distribuite via e-mail
- Attacchi di phishing
- Spam

Protezione anti-ransomware e anti-exploit

Basate su fonti di threat intelligence in tempo reale, le nostre tecnologie si evolvono costantemente. Parliamo per esempio di protezione degli endpoint dagli exploit più recenti e da ransomware e minacce avanzate, nonchè del mantenimento della sicurezza di dati e cartelle condivise.

Protezione dal furto degli account

L'analisi comportamentale implementa un meccanismo di protezione della memoria che salvaguarda i processi fondamentali per il sistema e impedisce il furto di credenziali utente e amministratore.

Protezione dagli attacchi attraverso le applicazioni

Il modulo Application Control, basato su whitelisting dinamico, riduce in maniera significativa l'esposizione agli attacchi zero-day, fornendo il controllo totale sul software che può essere mandato in esecuzione. L'Application Control intercetta il lancio di file eseguibili, DLL e controlla gli script eseguiti da diversi interpreti. L'analisi comportamentale e la prevenzione degli exploit monitorano il comportamento delle applicazioni, bloccano attività potenzialmente dannose e proteggono dallo sfruttamento e dall'uso di applicazioni legittime da parte dei malware. Le applicazioni approvate e affidabili continuano ad essere eseguite senza interruzioni.

Neutralizzazione dei rootkit

Gli utenti malintenzionati utilizzano rootkit e bootkit per nascondere le proprie attività alle soluzioni di protezione. La tecnologia anti-rootkit, parte della protezione Next Generation e multilivello di Kaspersky Lab, consente di rilevare e neutralizzare anche le infezioni nascoste più in profondità.

Identificazione di un maggior numero di attacchi e intrusioni, anche tra i più avanzati

I sensori incorporati e l'integrazione con Kaspersky Endpoint Detection and Response consentono l'acquisizione e l'analisi di grandi volumi di dati senza alcun impatto sulla produttività dell'utente. La soluzione offre la possibilità di effettuare azioni di threat hunting avanzate per la ricerca di evidenze di intrusioni, come gli indicatori di compromissione (IoC).

Prevenzione degli attacchi via rete

I malware che utilizzano tecniche di attacco basate su buffer-overrun possono modificare un processo già in esecuzione in memoria, e in questo modo riescono ad eseguire codice malevolo. La soluzione consente di identificare gli attacchi di rete e gli exploit e di fermarli subito.

Manutenzione e supporto

Fornendo supporto in più di 200 paesi, da 35 uffici in tutto il mondo, il nostro impegno è 24 ore su 24, 7 giorni su 7 e viene incluso nei nostri pacchetti di assistenza Maintenance Service Agreement (MSA). I team dedicati ai servizi professionali sono sempre pronti a garantire che l'utente ottenga il massimo dalla soluzione Kaspersky Lab, fornendo assistenza durante il setup iniziale e il supporto in caso di incidenti critici.

Prova gratuita

Scopri perché solo la True Cybersecurity combina la flessibilità e la semplicità d'uso con la **HuMachine™** intelligence per proteggere l'azienda da qualsiasi tipo di minaccia. Visita il nostro sito web e richiedi una prova gratuita di 30 giorni della versione completa di **Kaspersky Endpoint Security for Business**. Al termine del periodo di prova, se si decide di acquistare, sarà sufficiente acquistare la licenza. Dal momento che l'applicazione è già in esecuzione sull'endpoint durante la prova, non sarà necessario eseguire altre operazioni.

Oltre la protezione endpoint: pronti per il futuro

Semplificazione di inventario e patching

La discovery dei dettagli hardware e software delle macchine e la gestione del patching tempestivo delle vulnerabilità rappresentano attività tediose e dispendiose in termini di tempo. Lo sfruttamento delle vulnerabilità per le quali non sono state applicate le patch è uno dei modi più comuni utilizzati dai cybercriminali per attaccare l'infrastruttura IT attraverso un singolo endpoint. Andando oltre la semplice distribuzione remota di nuovo software di terze parti, le attività di vulnerability assessment e patch management automatizzate basate su una intelligence attiva 24 ore su 24 permettono di mantenere aggiornato il software potenzialmente vulnerabile consentendo agli amministratori IT di dedicarsi ad altre attività.

Condivisione sicura dei dati attraverso la crittografia

La crittografia con certificazione FIPS 140-2, completamente trasparente per l'utente, protegge i dati riservati sui dispositivi fissi e portatili. La tecnologia integrata consente di applicare in maniera centralizzata le policy di crittografia dei dati aziendali a livello di file, disco o dispositivo removibile e di poter condividere in maniera sicura i dati attraverso la rete.

Supporto per l'accesso ai dati in mobilità e da remoto

I dati sono diventati accessibili in qualsiasi momento. La soluzione offre protezione anche dalle minacce che mirano ai dati a cui si deve accedere in mobilità, nonché dai tentativi di sfruttare le vulnerabilità dei dispositivi mobili, in modo da utilizzarli come punti di accesso all'infrastruttura IT. Il modulo Device Control protegge dalle conseguenze dovute alla perdita dei dati su dispositivi portatili non crittografati o non approvati e al caricamento di dati infetti sul dispositivo.

Ottimizzazione dell'efficienza: gestione di tutte le piattaforme

Una singola console offre visibilità e controllo completi su ogni workstation, server e dispositivo mobile, ovunque si trovi. La soluzione è estremamente scalabile e fornisce funzionalità di accesso e controllo delle licenze, trouble-shooting remoto sulle postazioni e controllo dell'utilizzo della rete. La gestione centralizzata è completata grazie all'integrazione con Active Directory, dashboard di monitoraggio integrate e profilazione degli accessi utente.

Regolazione dell'accesso ai dati sensibili e dispositivi di registrazione

La nostra soluzione restringe i privilegi delle applicazioni in base ai livelli di affidabilità assegnati, limitando l'accesso a risorse come i dati crittografati. Lavorando con il database di reputazione locale e cloud (KSN), il modulo Host Intrusion Prevention System (HIPS) controlla le applicazioni e controlla l'accesso a risorse di sistema critiche, dispositivi di registrazione audio e video.

Blocco delle minacce Web prima che possano raggiungere gli endpoint

Bloccando la maggior parte delle minacce a livello gateway, riduciamo in maniera significativa l'impatto del fattore umano e delle specifiche di sicurezza della workstation, impedendo al malware di raggiungere gli endpoint.

Un gateway sicuro rimane la prima linea di difesa per la maggior parte degli scenari di protezione aziendale, nonostante l'aumento dell'accesso ai dati in mobilità durante i processi di lavoro. Le nostre tecnologie di sicurezza filtrano il traffico che passa attraverso il gateway, bloccando automaticamente le minacce in entrata prima che raggiungano gli endpoint e i server. In questo modo si riduce notevolmente il rischio di sfruttamento della vulnerabilità e diminuiscono notevolmente i costi operativi per il personale di sicurezza IT.

Aumento della produttività e riduzione delle minacce

L'anti-spam Next generation e supportato dal cloud di Kaspersky Lab rileva anche lo spam più sofisticato e sconosciuto minimizzando la perdita di comunicazioni preziose a causa di falsi positivi. Riducendo le perdite di tempo, le risorse e i rischi associati allo spam bloccandolo subito, è possibile risparmiare risorse preziose. La protezione include più livelli di sicurezza proattiva, inclusi machine learning e threat intelligence assistita dal cloud, per filtrare gli allegati dannosi e i malware noti o sconosciuti nella posta in arrivo.

Collaborazione sicura

Le nostra protezione per piattaforme Microsoft SharePoint® include funzionalità anti-malware e di content/file filtering, per consentire alle aziende di applicare i criteri di collaborazione interni e impedire l'archiviazione di contenuti inappropriati sulla rete aziendale.

Kaspersky Endpoint Security for Business permette agli amministratori di, monitorare, controllare e proteggere l'ambiente IT. Gli strumenti e le tecnologie Next generation sono sviluppati in maniera intelligente attraverso livelli progressivi, per rispondere alle crescenti esigenze di sicurezza e IT.

Kaspersky® Total Security for Business

Le aziende con ambienti IT complessi, con un mix di infrastrutture di nuova generazione e legacy, hanno bisogno di perfezionare la sicurezza per i diversi sistemi. La nostra soluzione di sicurezza più completa per endpoint, infrastruttura e collaboration server consente di ottenere una protezione adeguata al patrimonio IT.

Kaspersky® Endpoint Security for Business Advanced

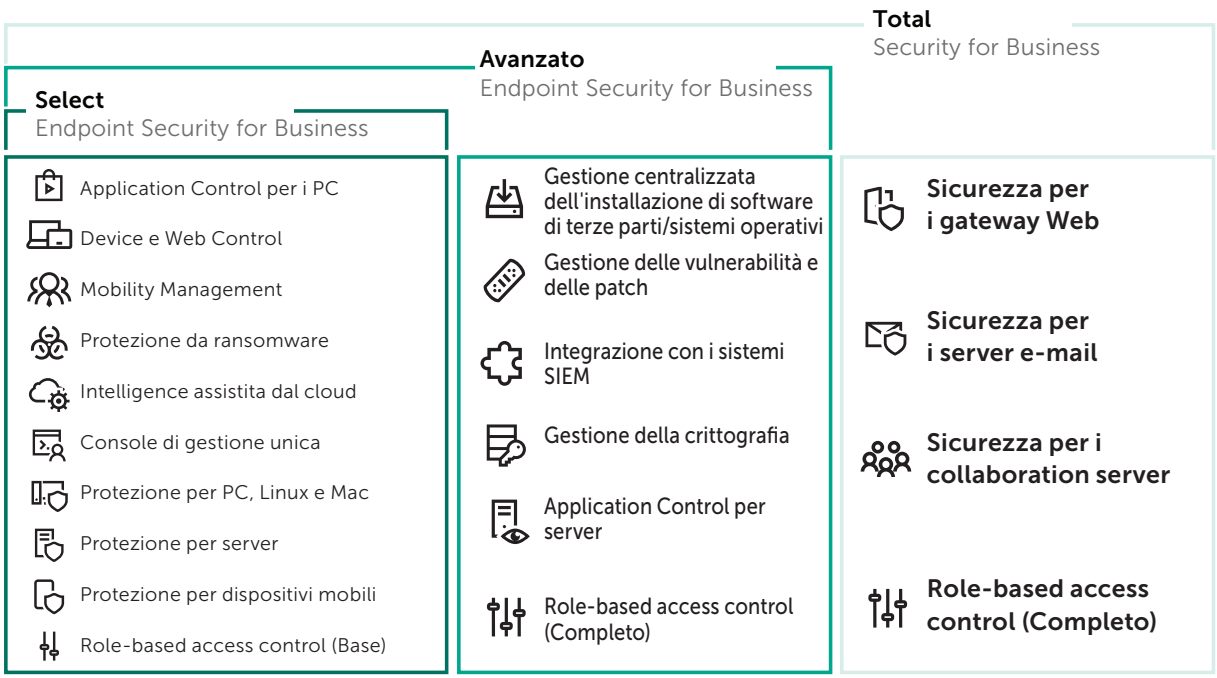
Kaspersky Endpoint Security for Business Advanced garantisce un livello di sicurezza efficace per proteggere la vostra azienda. Inoltre, garantisce copertura per tutti gli endpoint e server, offre livelli di sicurezza aggiuntivi per proteggere i dati sensibili ed eliminare le vulnerabilità e contribuisce anche a semplificare le attività di gestione dei sistemi.

Kaspersky® Endpoint Security for Business Select

In un mondo sempre più digitale, è necessario proteggere tutti i server, i laptop e i dispositivi mobili. Offriamo una sicurezza Next generation che permette di proteggere ogni endpoint aziendale, in un'unica soluzione con una console di gestione flessibile.

Qual è la versione più adatta a voi?

Qualsiasi siano le esigenze IT e di sicurezza, **Kaspersky Endpoint Security for Business** è la soluzione ideale.



Aggiunta di ulteriori tecnologie di sicurezza in base alle esigenze

L'automazione e la centralizzazione dell'individuazione delle vulnerabilità del software e della gestione delle patch offre una protezione contro le minacce più pericolose, incluso il ransomware. Per i clienti **Kaspersky Endpoint Security for Business Select**, questo modulo è disponibile con **con l'Add-on Kaspersky Vulnerability and Patch Management**.

Anche per i clienti Select, **con l'Add-on Kaspersky Encryption** consente di gestire la crittografia a livello full disk e file, utilizzando algoritmi di encryption avanzati per l'accesso immediato ai dati, con il supporto al Single Sign-On e alle smart card/token, per l'autenticazione a due fattori. Il modulo consente inoltre di crittografare i file e le cartelle archiviati su unità rimovibili.

Per una sicurezza ancora maggiore e senza alcuna ulteriore complessità, è sufficiente attivare la funzionalità richiesta dal Kaspersky Security Center.

Perché aggiornare la protezione degli endpoint?

Resta aggiornato con le tecnologie più recenti, flessibili e veloci: un server, un'unica console e un singolo agente.

Supporto ai processi aziendali grazie alla profonda integrazione di più moduli

Niente costi nascosti e licenze separate: tutte le funzionalità di cui hai bisogno in in un'unica soluzione

Auditing e capacità di controllo migliorate con role-based access control

In Kaspersky Lab, siamo in grado di sviluppare e perfezionare internamente tutte le tecnologie, così tutte le nostre applicazioni sono più stabili ed efficienti. Il nostro dipartimento R&D è impegnato quotidianamente per ricercare e sviluppare nuove innovazioni tecnologiche da includere nei nostri prodotti. Alcuni esempi:

- Machine learning multilivello: utilizzando metodi di Machine learning in fasi diverse della killchain sugli endpoint e nel cloud.
- Ricerca attiva delle minacce come risultato dell'integrazione tra la protezione degli endpoint e le soluzioni Endpoint Detection & Response o Anti Targeted Attack.
- L'esclusiva modalità cloud per la protezione dei componenti garantisce una copertura ottimale con il minimo impatto sulle risorse del PC e sulla connessione ad Internet.
- Supporto ai container di Microsoft Windows Server, sicurezza del traffico in uscita e gestione del firewall.
- Funzionalità di Device Control e anti-bridging.
- Application Control migliorato con categoria Certificati attendibili e Modalità di test per le policy.
- La nuova interfaccia utente mette in evidenza la protezione multi-livello, indicando lo stato della protezione e l'efficacia delle ultime tecnologie di Kaspersky Lab in azione.

True Cybersecurity: il nostro DNA

Kaspersky Lab offre potenti soluzioni di cybersecurity utilizzando una threat intelligence di livello mondiale intrinseca nel nostro DNA e influenza tutto ciò che facciamo. In qualità di società indipendente siamo più agili, pensiamo *"out of the box"* e agiamo più rapidamente.

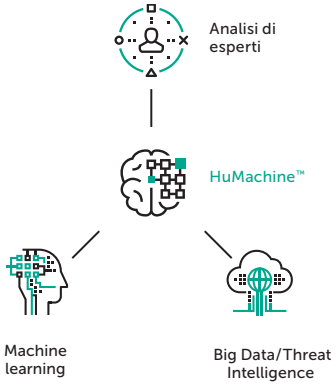
- **La nostra competenza è a tutti i livelli**, a partire dal nostro CEO, Eugene Kaspersky.
- **Il nostro Global Research & Analysis Team (GReAT)**, un gruppo d'elite di esperti di sicurezza, ha scoperto molti dei più pericolosi attacchi mirati e minacce malware al mondo.
- La nostra **Global Transparency Initiative** è l'ulteriore prova del nostro impegno per la protezione dei clienti dalle cyberminacce, indipendentemente dalla loro origine o scopo.

Rispetta i requisiti GDPR grazie alla True Cybersecurity

Kaspersky Lab aiuta i propri clienti a comprendere gli aspetti del GDPR legati alla cybersecurity. Le nostre soluzioni consentono ai clienti di ridurre i rischi di violazione dei dati e di prevenire gli incidenti di sicurezza. Inoltre, supportiamo i DPO dei clienti grazie a una maggiore visibilità dell'infrastruttura.

The bigger picture – Kaspersky IT Security Solutions for Business

La protezione degli endpoint, anche se critica, è solo l'inizio. Sia che si utilizzi una strategia di sicurezza avanzata o basata su un'unica sorgente di intelligence, Kaspersky Lab offre una vasta gamma di prodotti che collaborano tra di loro o lavorano indipendentemente così da poter scegliere in maniera autonoma la propria strategia di sicurezza. Maggiori informazioni sul nostro sito web.



Kaspersky Lab
Trovate il partner più vicino: **www.kaspersky.it/buyoffline**
Kaspersky per le aziende: **www.kaspersky.com/business**
True Cybersecurity: **www.kaspersky.com/true-cybersecurity**
Novità sulla sicurezza IT: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.it

KESB_Product_Datasheet_Next_Generation_Endpoint_Protection_Customer_0218_IT_GLB