KASPERSKY lab

Kaspersky Soluzioni di sicurezza aziendale 2018

#TrueCybersecurity

Kaspersky
Soluzioni di sicurezza aziendale
2018

Cybersecurity in un'Epoca di Trasformazione Digitale

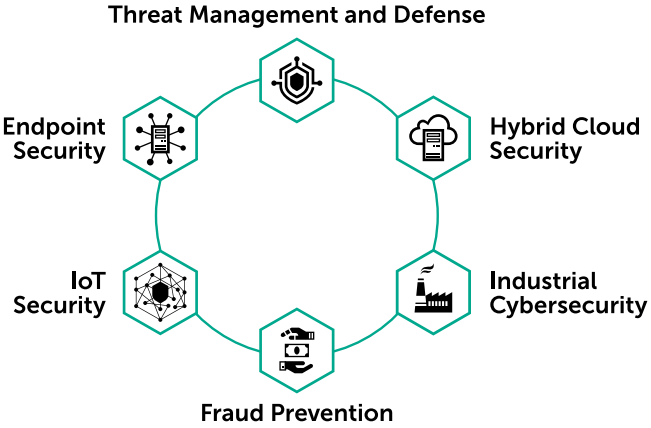
Con l'aumento esponenziale del numero di cyberattacchi, quelli diretti alle infrastrutture aziendali diventano sempre più professionali e altamente personalizzati. Non è più questione di domandarsi se si subirà un attacco, ma quando questo avverrà e con quanta rapidità e completezza sarà possibile ripristinare l'operatività.

Nel frattempo, l'infrastruttura IT aziendale è divenuta più complessa che mai, in quanto si estende al di là del perimetro organizzativo fino ai dispositivi mobili e nei cloud pubblici e provider di terze parti. Mentre la trasformazione digitale apporta enormi benefici in termini di efficienza e flessibilità commerciale, introduce anche nuove sfide per la sicurezza. Garantire la business continuity, proteggere il rendimento finanziario e salvaguardare i dati aziendali e del cliente sono tutte operazioni che impongono uno sforzo considerevole al team responsabile della sicurezza IT, oltre che un dispendio notevole in termini di budget.

Il nuovo Enterprise Portfolio di Kaspersky Lab rispecchia le esigenze di sicurezza delle imprese moderne, creando una piattaforma completa di cybersecurity che combina funzionalità di protezione completamente scalabili per sistemi fisici, virtuali e basati su cloud, tra cui endpoint fissi e mobili, server, reti e hardware e software specializzato.

Una combinazione unica di tecnologie e servizi all'avanguardia permette al team responsabile della sicurezza di prevenire la maggior parte degli attacchi, di individuare nuove minacce prevedendo quelle future e di reagire in maniera tempestiva agli incidenti, contribuendo a garantire la continuità operativa e la conformità normativa.

Il nostro portafoglio consiste nelle soluzioni seguenti, tutte completate da servizi specialistici ad ampio raggio, formazione sulla sicurezza e supporto professionale:



Tali soluzioni si integrano con le tecnologie che le compongono fino a creare un quadro di sicurezza adattivo. In tal modo è possibile prevedere, prevenire, individuare e correggere la maggior parte delle più avanzate minacce di cybersecurity e degli attacchi mirati, promuovendo la business continuity e la resilienza con un impatto minimo sulle prestazioni.

La vera cybersecurity, assistita da una combinazione di Machine learning e di competenza umana e sostenuta da una Threat Intelligence all'avanguardia, offre una protezione delle prestazioni di alto livello unitamente a una visibilità e una gestibilità unificata e al supporto completo della trasformazione digitale.

Battersi per la Libertà Digitale

I dati e la privacy dell'azienda sono sotto attacco da parte di cybercriminali e spie, perciò occorre un partner che non tema di schierarsi con essa nella lotta per la difesa delle risorse aziendali. Da 20 anni, Kaspersky Lab scopre e sconfigge ogni tipo di minaccia informatica, che sia stata creata da dilettanti, cybercriminali o governi, e indipendentemente dalla latitudine. Crediamo che il mondo online debba essere libero dagli attacchi e dallo spionaggio sponsorizzato dallo stato e continueremo a batterci per un universo digitale davvero libero e sicuro.

Collaudato

Kaspersky Lab ottiene abitualmente il massimo dei voti nelle classificazioni e nei sondaggi indipendenti.

- Valutato insieme a **80 noti fornitori** nel settore
- **72 primi posti** in 86 test e revisioni nel 2017
- **Tra i primi 3*** in oltre il 90% di tutte le prove del prodotto
- Nel 2017, Kaspersky Lab ha ricevuto il **Platinum Award** nei Gartner Peer Insight** Customer Choice Awards, nel mercato delle Piattaforme di protezione degli endpoint

Il nostro team di Ricerca e analisi globale ha partecipato attivamente al rilevamento e alla divulgazione di alcuni dei più noti attacchi malware collegati a governi e a organizzazioni statali.

Trasparente

Siamo totalmente trasparenti e semplifichiamo al massimo la comprensione di ciò che facciamo:

- Revisione indipendente del codice sorgente dell'azienda, aggiornamenti del software e regole di rilevamento delle minacce
- Revisione indipendente di processi interni
- Tre centri di trasparenza entro il 2020
- Programmi bug bounty con premi maggiorati fino a 100.000 USD per vulnerabilità rilevata

Indipendente

Essendo una società privata, siamo indipendenti da considerazioni commerciali a breve termine e dall'influenza istituzionale.

Condividiamo competenze, preparazione e conoscenze tecniche con community di sicurezza, fornitori di sicurezza IT, organizzazioni internazionali e forze dell'ordine di tutto il mondo.

Il nostro team di ricerca è distribuito in tutto il mondo e include alcuni degli esperti di sicurezza più rinomati a livello globale. Rileviamo e neutralizziamo ogni forma di APT avanzate, indipendentemente dalla loro origine o dal loro scopo.

* www.kaspersky.com/top3

** https://www.gartner.com/reviews/customerchoice- awards/endpoint-protection-platforms

Sicurezza degli endpoint

La principale piattaforma di protezione multi-layered degli endpoint, basata su tecnologie di Next Gen security

L'ambiente delle minacce sta crescendo in maniera esponenziale, mettendo sempre più a rischio di attacchi zero-day i processi aziendali, i dati riservati e le risorse finanziarie. Per attenuare i rischi per l'organizzazione, occorre essere più astuti, meglio attrezzati e informati rispetto ai cybercriminali che l'hanno presa di mira. Ma esiste una semplice verità: la maggioranza degli attacchi informatici alle aziende iniziano attraverso l'endpoint. Se si riesce a proteggere in modo efficace ogni endpoint aziendale, sia fisso che mobile, si avranno basi solide per una strategia di sicurezza generale.

Nei Gartner Peer Insights Customer Choice Awards 2017 per le Piattaforme di protezione degli endpoint, **siamo stati gli unici fornitori a meritare un Platinum Award***.

*Il logo Gartner Peer Insights Customer Choice è il marchio commerciale di un prodotto di Gartner, Inc. e/o i suoi affiliati, e viene qui usato previa autorizzazione espressa. Tutti i diritti riservati. I premi Gartner Peer Insights Customer Choice Awards (https://www.gartner.com/reviews/customer-choice-awards/endpointprotection-platforms) vengono conferiti grazie alle opinioni soggettive di singoli clienti finali che si basano sulle proprie esperienze, al numero di recensioni pubblicate su Gartner Peer Insights e alla valutazione complessiva di un determinato fornitore sul mercato, come ulteriormente descritto all'indirizzo http://www.gartner.com/reviews-pages/peer-insights-customer-choice-awards/, e non intendono in alcun modo rappresentare le opinioni di Gartner o dei suoi affiliati.

La trasformazione digitale introduce ulteriori rischi

La crescente complessità della maggior parte delle reti IT aziendali può creare divari di visibilità in cui possono annidarsi le minacce.

In media, un attacco mirato può continuare a stare in agguato all'interno dei sistemi target, senza che venga assolutamente rilevato, per 214 giorni.

Durante questo periodo, la minaccia potrebbe continuare a eseguire una serie di attività dannose. È dunque di importanza vitale utilizzare strumenti efficienti in grado di rilevare, rimuovere e correggere rapidamente la minaccia.

Purtroppo, nonostante le solenni affermazioni di alcuni fornitori, non esiste un unico prodotto di sicurezza che rappresenti la soluzione ottimale per garantire la protezione al 100% da ogni tipo di rischio. Analogamente, non esiste nemmeno una soluzione una tantum. La sicurezza IT è un processo di valutazione costante dell'evoluzione dei pericoli, seguito da:

- Adattamento e aggiornamento delle politiche di sicurezza
- Rollout di nuove tecnologie di sicurezza

Tutto questo è mirato alla gestione dei nuovi rischi.

Soluzione per la sicurezza degli endpoint

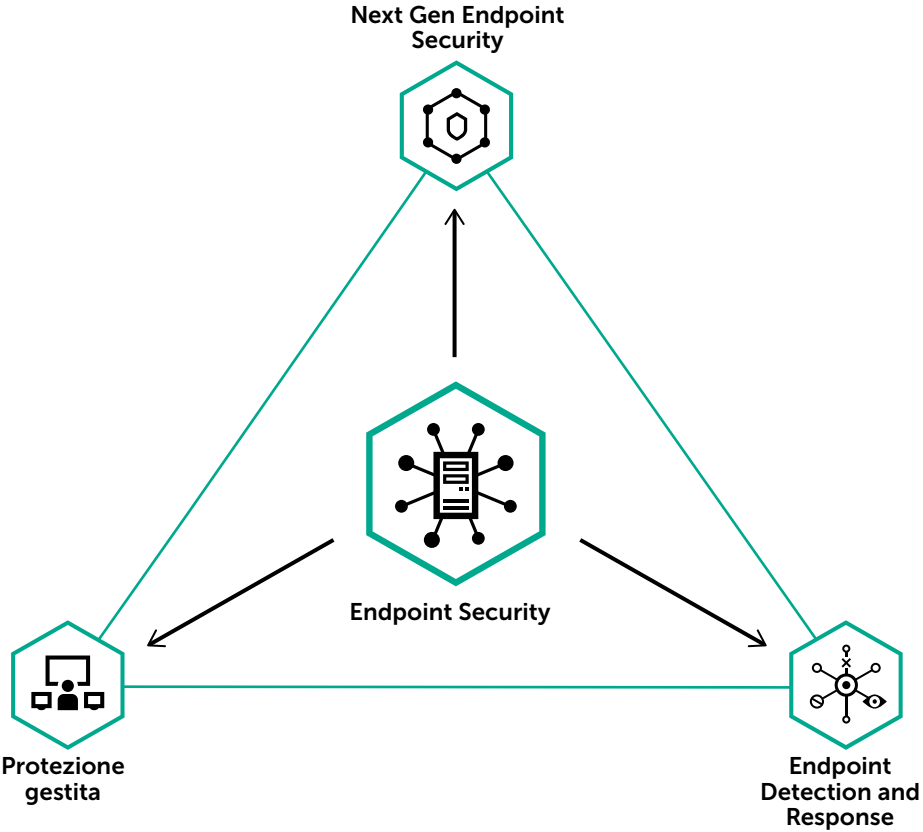
Kaspersky Endpoint Security risponde a queste necessità tramite una piattaforma di sicurezza con protezione multi-layered, affidabile e collaudata. Questa soluzione ben integrata combina eccezionali funzionalità di protezione, rilevamento e risposta agli incidenti, basate su informazioni di sicurezza globale senza pari e su capacità di Machine learning di nuova generazione, per potenziare automaticamente il SOC e migliorare le competenze di attenuazione dei rischi. La protezione per ogni endpoint fisico, virtuale e basato su cloud viene gestita attraverso un'unica console, migliorando l'efficienza e riducendo il TCO.

Questa piattaforma include:

- **Sicurezza degli endpoint Next Gen**
  Protezione completamente scalabile, basata sul nostro pluripremiato motore di Threat Intelligence, che incorpora controlli granulari, programmi anti-ransomware e tecnologie di prevenzione degli exploit.

- **Rilevamento e risposta degli endpoint**
  Scovare gli avversari in maniera proattiva e fermare le minacce prima che possano causare danni costosi, rispondendo in modo rapido ed efficace agli incidenti e alle violazioni dei dati.

- **Protezione gestita**
  Servizio di monitoraggio e di risposta agli incidenti 24 h su 24, fornito da un riconosciuto leader mondiale nelle indagini sulle APT, dedicato a individuare le minacce informatiche per l'organizzazione.



Come colpiscono gli attacchi

La maggioranza degli attacchi è caratterizzata da quattro fasi distinte:

- **Rilevamento**: identificazione dei punti di ingresso appropriati per l'attacco
- **Intrusione**: in un endpoint nella rete aziendale
- **Infezione**: spesso si diffonde in molti punti della rete aziendale
- **Implementazione**: delle azioni dannose dei cybercriminali

Difesa progressiva

Una delle chiavi per affrontare un attacco consiste nell'avere difese capaci di offrire protezione in ciascuna delle quattro fasi.

Prevenzione dell'esposizione al rilevamento
Bloccare l'accesso ai potenziali punti di ingresso

Protezione pre-esecuzione dalle intrusioni
Rilevare le minacce prima che possano causare infezioni

Processi post-esecuzione delle infezioni
Rilevare il comportamento sospetto e contribuire a prevenire l'esecuzione di azioni dannose da parte dell'infezione

Risposta automatizzata dell'implementazione
Aiutare l'azienda vittima a recuperare sistemi e dati e identificare come evitare attacchi simili in futuro

Protezione multi-layered... da un unico fornitore

Forniamo difese per ogni fase di un attacco, e in ciascuna di esse non ci limitiamo a fornire un unico livello, ma più tecniche di difesa. Di conseguenza, i nostri clienti traggono vantaggio dalla protezione multi-layered in ogni fase dell'attacco.

Fase 1 della difesa: prevenzione dell'esposizione
Aiutiamo a bloccare gli attacchi in corrispondenza dei potenziali punti di ingresso.

I nostri livelli di protezione comprendono:

- Filtro di rete
- Filtro dei contenuti cloud-enabled
- Controllo delle porte

Fase 2 della difesa: sicurezza pre-esecuzione
Aiutiamo ad arrestare l'intrusione.

I nostri livelli di protezione e servizi comprendono:

- Protezione avanzata degli endpoint
- Servizi per la reputazione
- Rilevamento pre-esecuzione: basato su Machine learning

Fase 3 della difesa: Runtime Control
Rileviamo in modo proattivo il comportamento sospetto di qualsiasi dispositivo collegato alla rete aziendale, tra cui i dispositivi mobili personali dei dipendenti.

I nostri livelli di protezione comprendono:

- Analisi comportamentale, basata su Machine learning, che comprende:
  – Prevenzione degli exploit
  – Protezione da ransomware
- Controllo dei privilegi di esecuzione

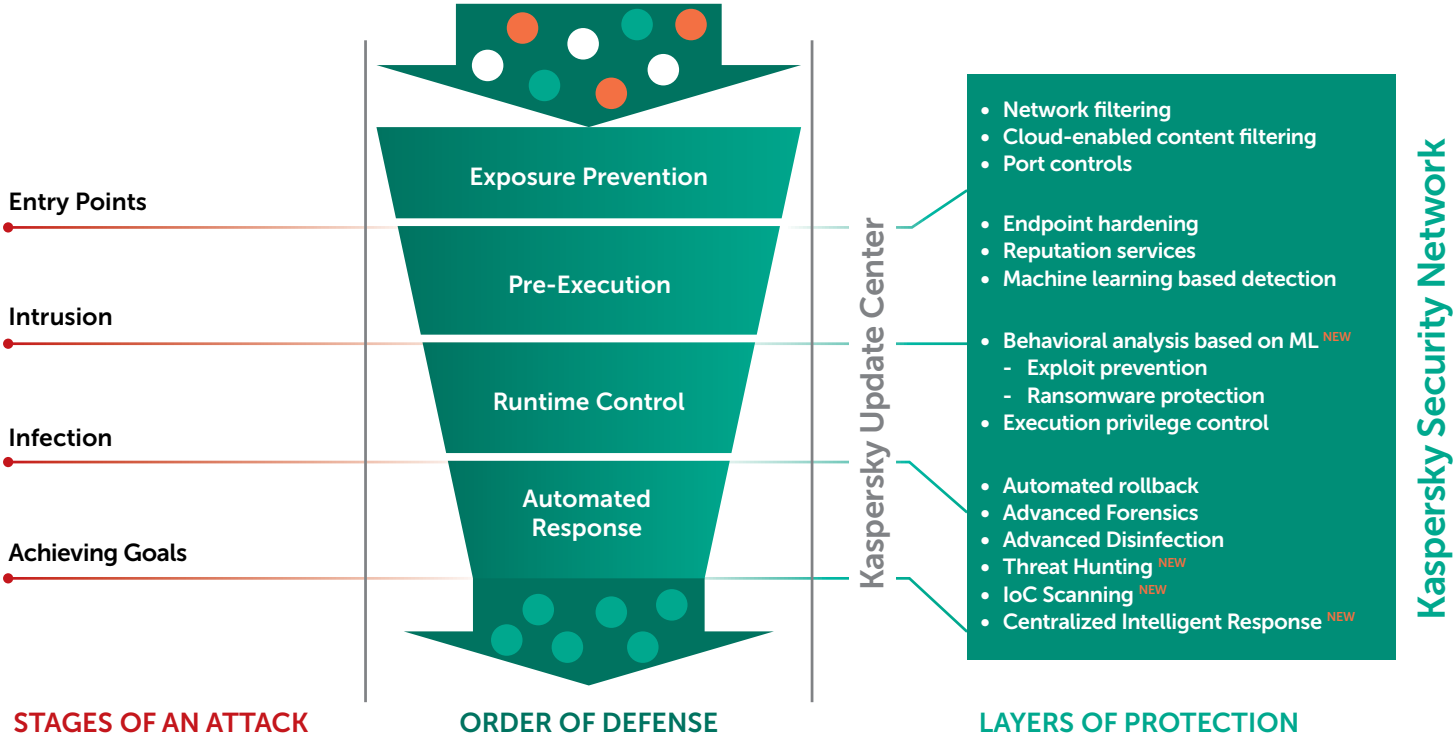
Fase 4 della difesa: risposta automatizzata
Se l'azienda ha subito un attacco, la aiutiamo ad affrontarne le conseguenze più rapidamente.

Le tecnologie e i servizi che offriamo comprendono:

- Rollback automatico, per contribuire al ripristino dello stato dei sistemi precedente all'attacco
- Analisi forense
- Disinfezione avanzata
- Threat Hunting
- Scansione IoC (Indicator of Compromise)
- Risposta intelligente centralizzata

Il nostro meta-layer aiuta le aziende a ottimizzare la protezione dai pericolosi attacchi mirati e dalle APT, rapportando le conclusioni dei singoli livelli di difesa e identificando le minacce che potrebbero passare inosservate attraverso le difese individuali.

Catena di attacchi



Sicurezza dei dispositivi mobili

Sicurezza e gestione integrata a supporto della strategia di sicurezza dei dispositivi mobili

In base al nostro sondaggio del 2017, il 38% delle aziende ha subito exploit o perdite attraverso dispositivi mobili quali principali vettori di attacco.

$1.700.000

Il costo aziendale medio di un incidente di sicurezza che implichi exploit o perdita di dati attraverso dispositivi mobili

Software dannoso, siti Web e attacchi di phishing mirati ai dispositivi mobili continuano a proliferare, mentre le funzionalità dei dispositivi mobili sono in continuo sviluppo. Essendo un importante strumento di produttività a casa e al lavoro, i dispositivi mobili sono bersagli allettanti per i cybercriminali. L'uso crescente dei dispositivi personali a scopi aziendali (BYOD) espande la gamma di tipologie e piattaforme di dispositivi presenti all'interno della rete aziendale, ponendo ulteriori sfide per gli amministratori IT che provano a gestire e controllare le infrastrutture IT.

I dispositivi personali dei dipendenti come rischio aziendale

I dipendenti che adoperano i propri dispositivi mobili per lavoro oltre che per uso personale aumentano le possibilità di violazione della sicurezza IT. Una volta che gli hacker avranno avuto accesso alle informazioni personali non protette su un dispositivo mobile, ottenere l'accesso ai sistemi e ai dati aziendali degli utenti sarà un gioco da ragazzi.

Nessuna piattaforma è sicura

I cybercriminali si servono di vari metodi per ottenere l'accesso non autorizzato ai dispositivi mobili, tra cui applicazioni infette, reti Wi-Fi pubbliche con livelli di sicurezza bassi, attacchi di phishing e messaggi di testo infetti. Quando un utente visita inavvertitamente un sito Web dannoso, o persino un sito Web legittimo infettato da codice dannoso, mette a rischio la sicurezza del proprio dispositivo e dei dati in esso archiviati. Persino la connessione di un iPhone a un Mac per ricaricare la batteria può risultare nella trasmissione di minacce dannose dal Mac all'iPhone (questo è il problema di tutte le piattaforme mobili: Android, iOS e Windows Phone).

La soluzione: Kaspersky Security for Mobile

Kaspersky Security for Mobile risolve questi problemi fornendo funzioni multi-layered di gestione mobile e MTD (Mobile Threat Defense). Queste capacità combinate permettono ai team responsabili della sicurezza di adottare un approccio proattivo alla gestione delle minacce mobili.

È possibile gestire tutte le funzionalità degli endpoint e dei dispositivi mobili dalla stessa console, combattendo efficacemente il cybercrimine aziendale.

La combinazione di crittografia e protezione dal malware consente a Kaspersky Security for Mobile di offrire la protezione proattiva dei dispositivi mobili piuttosto che limitarsi a isolare un dispositivo e i relativi dati.

Protezione avanzata per dispositivi mobili

Le funzionalità anti-malware si combinano alla Threat Intelligence assistita da cloud e al Machine learning per proteggere l'azienda dalle minacce mobili avanzate.

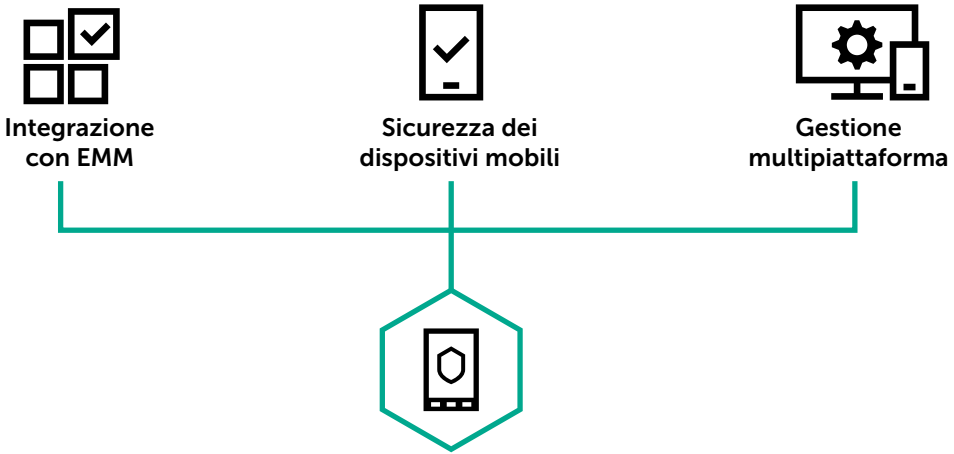
Controllo Web, Anti-Phishing e Anti-Spam

Efficaci tecnologie di controllo Web, anti-phishing e anti-spam proteggono dagli attacchi di phishing e da siti Web, chiamate e messaggi di testo indesiderati.

Integrazione con le piattaforme EMM

Implementazione e gestione della sicurezza dei dispositivi mobili direttamente tramite integrazione con la console EMM (VMware AirWatch, Citrix XenMobile)

Protezione avanzata per dispositivi mobili



Sicurezza per il cloud ibrido

Sicurezza illimitata progettata per ambienti multi-cloud

La nostra soluzione di sicurezza per il cloud ibrido fornisce una protezione multi-layered unificata per ambienti basati su cloud. Ovunque si elaborino e archivino dati aziendali di importanza critica, che sia il cloud pubblico o privato, forniamo una combinazione perfettamente bilanciata di sicurezza continua e agile e migliore efficienza, proteggendo i dati dalle minacce correnti e future più avanzate senza compromettere le prestazioni di sistema.

Il provisioning semplificato si ottiene tramite l'integrazione nativa con le API, assicurando un footprint sulle risorse ridotto al minimo e l'offerta di competenze precise per difendere gli ambienti multi-cloud da ogni forma di minaccia informatica. Tutto questo, grazie all'orchestrazione e alla gestione unificata della sicurezza.

Cybersecurity di nuova generazione per qualsiasi cloud

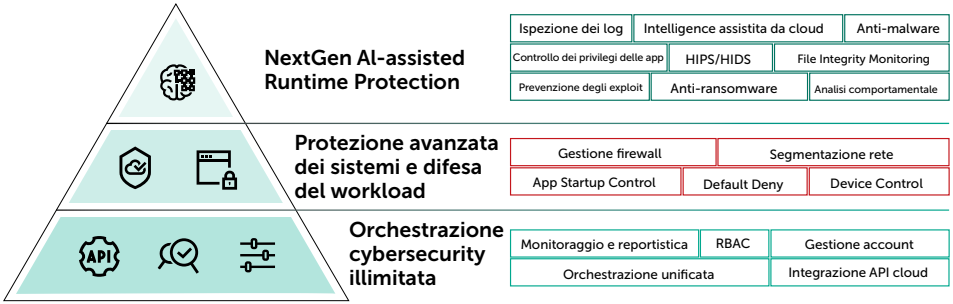
Risponde all'esigenza di proteggere i contenuti distribuiti nei cloud pubblici come parte della responsabilità condivisa per la sicurezza. L'integrazione con le API del cloud ci consente di offrire tecnologie di cybersecurity pluripremiate per ogni workload cloud.

Orchestrazione e trasparenza unificate

Una console di orchestrazione di sicurezza di livello enterprise offre caratteristiche di gestibilità, flessibilità e visibilità illimitate. Un'eccezionale trasparenza significa che l'azienda sa esattamente cosa sta accadendo al di là del livello di sicurezza dell'intero ambiente di cloud ibrido. Tale visibilità, unitamente al provisioning completamente automatizzato delle capacità di cybersecurity, consente l'orchestrazione ininterrotta di una sicurezza migliore e più veloce in tutto il cloud.

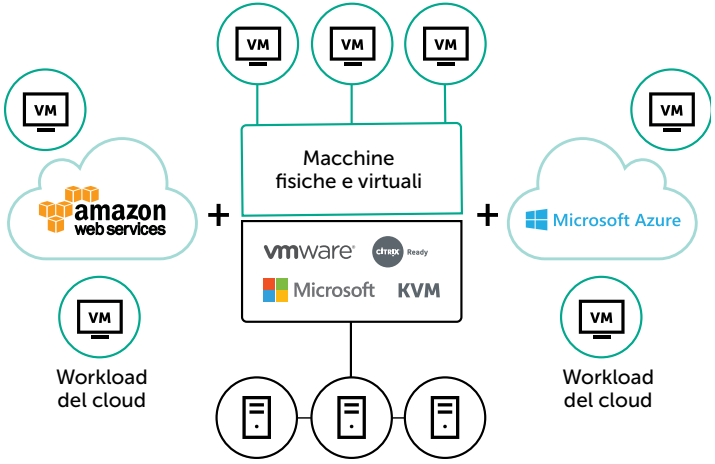
Per ambienti cloud flessibili e sicuri

Sicurezza comprovata per server virtuali e fisici, infrastrutture VDI, sistemi di archiviazione e persino canali dati. Le funzionalità brevettate di architettura e integrazione contribuiscono a implementare la sicurezza informatica nel cuore dell'ambiente IT, pur mantenendo l'efficienza operativa dei sistemi business-critical.



Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security offre tutto ciò che serve per creare un ecosistema di sicurezza informatica perfettamente orchestrato e adattivo, fornendo le capacità precise richieste dai workload multi-cloud e dando comunque priorità all'efficienza delle risorse e all'orchestrazione ininterrotta. Kaspersky Hybrid Cloud Security è stato progettato per proteggere le applicazioni e i dati nei workload fisici, virtuali e nel cloud, garantendo la sostenibilità aziendale e accelerando la conformità attraverso l'intero ambiente di cloud ibrido.



In un data center privato, in cui i workload aziendali vengono eseguiti su server fisici o virtuali o persino in ambienti VDI, occorre affrontare una serie di questioni come parte di una strategia di trasformazione digitale di successo:

- **Accesso ed elaborazione dati sicuri** indipendentemente dalla piattaforma di virtualizzazione o dall'ambiente fisico in cui si eseguono i workload
- **Interoperabilità tra IT e livelli di sicurezza** utilizzando API native per garantire tempi di risposta pari quasi a zero alle minacce avanzate
- **Funzionamento efficiente nell'impiego delle risorse** che migliora le prestazioni IT e mantiene la produttività dei sistemi business-critical

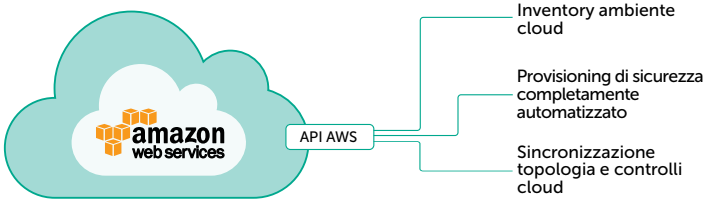
Kaspersky Hybrid Cloud Security offre un'eccellenza comprovata nel proteggere i data center definiti dal software e basati sulle piattaforme di virtualizzazione VMware NSX, Citrix XenServer e XenDesktop, MS Hyper-V e KVM, eliminando la complessità della gestione di ambienti enterprise. L'integrazione con l'IT centrale tramite le API native aiuta a soddisfare i requisiti di sicurezza con un impatto pari quasi a zero sulle prestazioni dei sistemi.

- Sicurezza agentless integrata per VMware NSX for vSphere, che permette ai team di sicurezza e IT di collaborare per una maggiore protezione.
- Protezione Light Agent brevettata per i server virtuali e le infrastrutture VDI con funzionamento efficiente nell'impiego delle risorse e fault-tolerant.
- Tradizionale sicurezza multi-layered per server fisici, che incorpora tecnologie anti-ransomware, prevenzione degli exploit e rilevamento comportamentale.

Cybersecurity automatizzata per cloud pubblici

L'adozione crescente di un modello di servizi in cloud, in cui le risorse del data center privato si espandono immediatamente su richiesta e quando necessario in cloud esterni, offre caratteristiche di flessibilità e agilità senza precedenti, oltre a palesi vantaggi economici. Tuttavia, il modello di responsabilità condivisa per la sicurezza impone la necessità di procurarsi capacità aggiuntive, implementando un livello di sicurezza informatica flessibile che copra l'intero ambiente cloud e protegga i workload di Amazon Web Services (AWS) o Microsoft Azure.

Integrazione con Amazon Web Services (AWS)



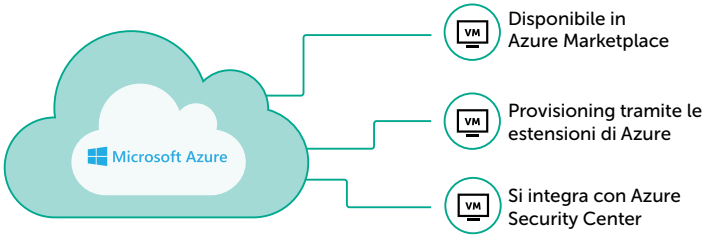
Kaspersky Hybrid Cloud Security aiuta a difendere le risorse nel cloud, rispondendo alla necessità di proteggere tutto quanto viene distribuito nel cloud pubblico come parte della responsabilità condivisa per la sicurezza. Kaspersky Hybrid Cloud Security fornisce una protezione multi-layered che si integra con le API cloud ed è disponibile attraverso i marketplace per offrire tecniche pluripremiate di sicurezza informatica a tutti i workload cloud con maggiore agilità e gestibilità illimitata, per un'eccezionale esperienza di orchestrazione della cybersecurity multi-cloud.

- Cybersecurity all'avanguardia a protezione dei workload nei cloud pubblici, che sfrutta l'integrazione nativa tramite API cloud con Amazon Web Services (AWS) e Microsoft Azure Extensions.
- Completa le capacità di sicurezza cloud-native e aiuta a proteggere le applicazioni, i sistemi operativi, i dati e gli utenti nel cloud, supportando la conformità GDPR.
- L'architettura intelligente e l'integrazione delle API riducono al minimo l'impatto delle risorse, automatizzando l'inventario e il provisioning della sicurezza.

Offre una protezione ancora maggiore

Completiamo gli strumenti cloud-native con una cybersecurity proattiva, la prevenzione degli exploit, il monitoraggio dell'integrità, l'ispezione dei log, i controlli delle app e persino la protezione dei file del runtime assistita dall'intelligenza artificiale e capacità anti-ransomware. Un solo prodotto per combattere qualsiasi forma di minaccia informatica.

Progettato per Microsoft Azure



Sicurezza imbattibile per ogni cloud

L'adozione del cloud non è mai stata così efficace, eppure sicura. Con Kaspersky Hybrid Cloud Security, l'integrazione tramite API native facilita l'inventario dell'infrastruttura del cloud pubblico e il provisioning automatizzato della sicurezza in tutte le istanze in AWS e Microsoft Azure.

Kaspersky Hybrid Cloud Security offre molteplici tecnologie di sicurezza per supportare e semplificare la trasformazione dell'ambiente IT, proteggendo la migrazione dall'ambiente fisico a quello virtuale e nel cloud, mentre la visibilità e la trasparenza garantiscono un'esperienza di orchestrazione di sicurezza impeccabile.

Kaspersky Security for Storage

Kaspersky Security for Storage offre una solida protezione scalabile e ad alte prestazioni per dati sensibili e importanti in NAS (Network Attached Storage) e file server aziendali.

L'integrazione agevole tramite protocolli veloci, tra cui ICAP e RPC, preserva l'efficienza dei sistemi di archiviazione assicurando una protezione affidabile ed efficiente nell'impiego delle risorse e un'esperienza utente ottimizzata. La protezione in tempo reale per i dispositivi NAS include capacità di Self-Defense per una continuità ottimale.

Protezione dei dati affidabile e trasparente

- L'integrazione nativa produce flessibilità, scalabilità e un'eccezionale efficienza operativa, senza alcun impatto negativo sulla produttività e sulle prestazioni dei sistemi di archiviazione dati.
- Le tecnologie innovative offrono le capacità di protezione più avanzate, un'eccezionale tolleranza d'errore e possono persino prevenire gli attacchi ransomware.

Protegge i dati aziendali ovunque siano archiviati

- Si integra in modo nativo con i dispositivi NAS più recenti e funziona sui file server aziendali
- Tutti i file archiviati sono al sicuro, senza alcuna necessità di controllare l'anti-malware negli endpoint o nei dispositivi mobili
- Configurazione flessibile e granulare per i task di scansione anti-malware on-demand e on-access
- Funzionalità di self-defense per un'ottimale continuità operativa

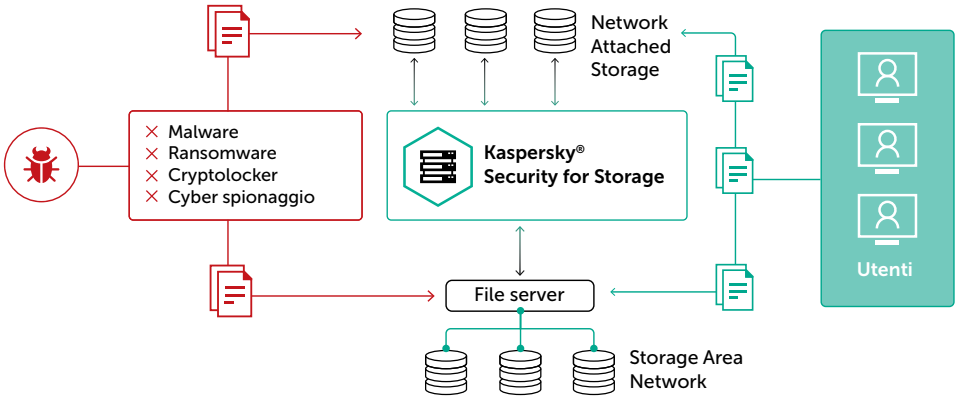
Combatte malware e ransomware

- Il nostro pluripremiato motore di scansione anti-malware difende tutti i file dagli attacchi più avanzati
- Protezione anti-ransomware in tempo reale per i dispositivi NAS di NetApp tramite FPolicy (introdotta da Kaspersky Lab)
- Supporto per una vasta gamma di dispositivi NAS, grazie all'integrazione tramite più protocolli

Offre una sicurezza leggera eppure affidabile

- L'integrazione con le API native implica una maggiore sicurezza con un minore impatto sulla produttività dell'utente finale
- Le funzionalità di bilanciamento e tolleranza di errore garantiscono una protezione continua
- Visibilità completa della sicurezza abilitata a livello di file nell'intera infrastruttura di archiviazione

Kaspersky Security for Storage può essere combinato con Kaspersky Hybrid Cloud Security, applicando la protezione migliore della categoria sui componenti sia fisici che virtuali del data center aziendale.



Kaspersky DDoS Protection

L'impatto finanziario di un singolo attacco DDoS può variare da 106.000 a 1.600.000 USD, a seconda delle dimensioni dell'azienda. Qual è il costo dell'organizzazione di un attacco DDoS? Circa 20 USD...

Il numero di attacchi è oggi inversamente proporzionale al costo del lancio di un attacco DDoS (Distributed Denial of Service). Gli attacchi si sono fatti più sofisticati e difficili da prevedere. La natura mutevole di queste forme di attacco richiede una protezione più rigorosa.

A differenza degli attacchi malware, che tendono a propagarsi automaticamente, gli attacchi DDoS si basano sulla competenza e sull'intuizione umana. L'autore dell'attacco compierà delle ricerche sull'azienda presa di mira, valutandone le vulnerabilità e sceglierà attentamente gli strumenti di attacco più opportuni per conseguire i suoi obiettivi. Quindi, lavorando in tempo reale durante l'attacco, i cybercriminali cambiano costantemente tattica, selezionando diversi strumenti per massimizzare il danno inflitto.

Per difendersi dagli attacchi DDoS, le aziende necessitano di una soluzione che li rilevi prima possibile.

La soluzione: Kaspersky DDoS Protection

Kaspersky DDoS Protection è una soluzione di protezione e mitigazione degli attacchi DDoS che si occupa di ogni fase della difesa aziendale da ogni forma di attacco. Sono disponibili tra opzioni di distribuzione: Connect, Connect+ e Control.

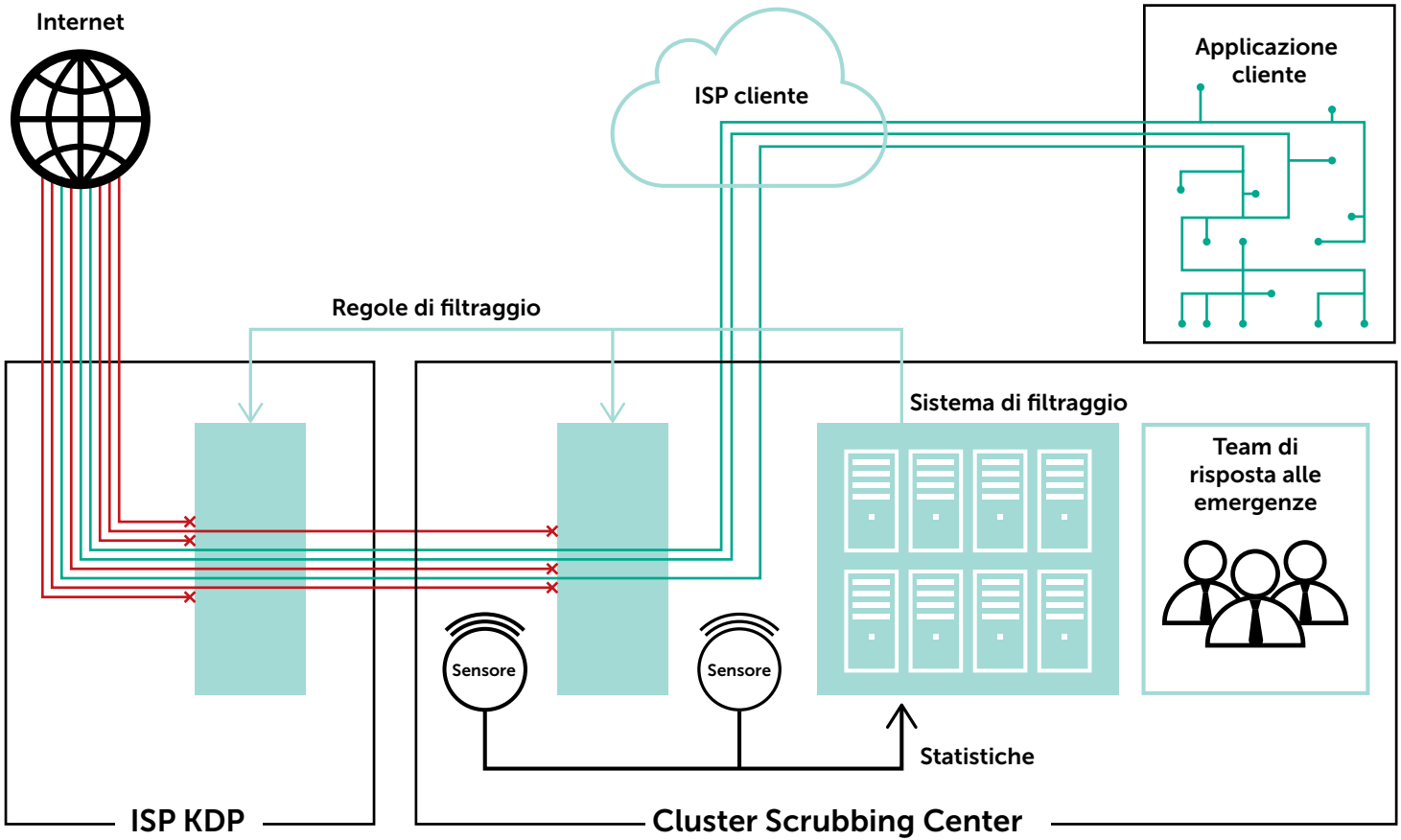
Nel momento esatto in cui viene identificato un possibile scenario di attacco, il Security Operations Center (SOC) di Kaspersky viene allertato. Con Kaspersky DDoS Protection Connect e Connect+, la mitigazione viene avviata automaticamente mentre i tecnici eseguono immediatamente controlli dettagliati per ottimizzare l'operazione, a seconda delle dimensioni, del tipo e della complessità dell'attacco DDoS. Con Kaspersky DDoS Protection Control, si può decidere quando avviare la mitigazione in linea con la propria politica di sicurezza informatica, gli obiettivi commerciali e l'ambiente infrastrutturale.

Grazie alla flessibilità e alla possibilità di impostare diverse configurazioni, possiamo garantire il completo soddisfacimento dei requisiti aziendali e delle risorse online.

Architettura Kaspersky DDoS Protection

Questa soluzione di difesa totale offre:

- Protezione completa per le risorse online business-critical e le infrastrutture di rete
- Opzioni di licenziamento flessibile – Kaspersky DDoS Protection Connect, Connect+ e Control
- Scrubbing center altamente scalabili in tutta Europa
- Intelligence globale sugli attacchi DDoS in tempo reale basata sull'analisi della sicurezza dei Big Data
- Protezione e supporto rapidi 24 ore su 24, 7 giorni su 7, da parte dei team di risposta alle emergenze.


Internet
ISP cliente
Applicazione cliente
Regole di filtraggio
Sistema di filtraggio
Team di risposta alle emergenze
Sensore
Sensore
Statistiche
ISP KDP
Cluster Scrubbing Center

Threat Management and Defense

Protezione e Threat Intelligence avanzate

La protezione delle infrastrutture altamente digitalizzate offre nuove e significative sfide aziendali:

- Alto volume di task manuali richiesto per la risposta agli incidenti
- Carenza di personale nel team responsabile della sicurezza IT e mancanza di competenza di alto livello
- Troppi problemi di sicurezza da elaborare, analizzare, smistare e risolvere in modo efficace in un arco di tempo limitato
- Problemi di attendibilità e conformità nella condivisione dei dati con l'aumento della portata dell'infrastruttura digitale.
- Mancanza di visibilità e problemi di raccolta prove per l'analisi post violazione

Valore commerciale dell'investimento nella gestione e difesa dalle minacce avanzate e mirate:

- Riduzione dei danni finanziari e operativi causati dal cybercrimine
- Riduzione della complessità tramite un'interfaccia di gestione intuitiva e business-oriented
- Riduzione dei costi amministrativi tramite l'automazione dei task e processi semplificati di conformità ai requisiti di sicurezza
- Aumento del ROI grazie all'automazione efficace dei flussi di lavoro senza alcuna interruzione dei processi aziendali
- Attenuazione del rischio posto dalle minacce avanzate tramite il rilevamento rapido

Trasformazione digitale: un nuovo ruolo per la cybersecurity

La trasformazione digitale è un fattore chiave della crescita aziendale e offre alle organizzazioni tantissime nuove opportunità. Tuttavia, allo stesso tempo, implica alcuni rischi associati al garantire la sicurezza dell'infrastruttura IT, unitamente alla conformità e all'utilizzo sicuro dei dati. Gli attacchi mirati e le minacce complesse, tra cui le APT (Advanced Persistent Threat), rappresentano oggi i rischi maggiori che le imprese si trovano ad affrontare. Soluzione unificata che contribuisce a supportare l'innovazione nella trasformazione digitale, **Kaspersky Threat Management and Defense** si adatta alle specifiche dell'organizzazione e ai suoi processi attraverso una combinazione unica di tecnologie di sicurezza e servizi di cybersecurity all'avanguardia, permettendo di creare una metodologia unificata per la protezione aziendale completa dalle minacce avanzate e dagli attacchi mirati.

Supportando lo sviluppo o il potenziamento della strategia aziendale di gestione delle minacce, Kaspersky Threat Management and Defense consente la raccolta automatizzata di informazioni avanzate e prove digitali, semplifica il rilevamento manuale e automatizza l'analisi degli incidenti, grazie anche al Machine learning. Il ricco pool di dati fornito permette di eseguire una complessa indagine sugli incidenti e fornisce il supporto e la competenza necessari a neutralizzare persino le minacce più sofisticate.

Kaspersky Threat Management and Defense è una combinazione unica di tecnologie e servizi all'avanguardia, che supporta l'implementazione di una strategia di sicurezza adattiva, aiutando a prevenire la maggior parte degli attacchi, rilevare rapidamente nuove minacce uniche, rispondere agli incidenti in tempo reale e prevedere le minacce future. Kaspersky Threat Management and Defense include i seguenti componenti:

- **Kaspersky Anti Targeted Attack** combina l'analisi del traffico di rete ed il monitoraggio degli endpoint integrando la nostra Threat Intelligence avanzata e sfruttando tecnologie evolute di Machine learning e sandboxing degli oggetti. Kaspersky Anti Targeted Attack mette in correlazione eventi differenti organizzando secondo priorità gli incidenti per aiutare le organizzazioni a rilevare gli attacchi mirati, le minacce avanzate e i sistemi già compromessi.

- **Kaspersky Endpoint Detection and Response** contribuisce a garantire visibilità sulle minacce lato endpoint, aggregando automaticamente e archiviando a livello centrale i dati dell'analisi forense. Kaspersky Endpoint Detection and Response utilizza la stessa interfaccia di Kaspersky Anti Targeted Attack e lo stesso agent di Kaspersky Endpoint Security, fornendo un approccio sfaccettato alla rivelazione, al riconoscimento e all'individuazione di attacchi mirati complessi. Maggiore attenzione è dedicata al rilevamento delle minacce per mezzo di tecnologie avanzate, in modo da rispondere tempestivamente agli attacchi e prevenendo le azioni dannose tramite l'individuazione delle minacce lato endpoint.

- **Kaspersky Cybersecurity Services** per offrire un'assistenza immediata e professionale quando è in corso un incidente e subito dopo, aiutando a ridurre il rischio di compromissione dei dati e riducendo al minimo i possibili danni finanziari e di immagine. Il nostro portafoglio Cybersecurity Services include un vasto programma di formazione sulla sicurezza, Threat Intelligence aggiornata in tempo reale, rapida risposta agli incidenti, Security Assessment proattivi, servizi di Threat Hunting completamente esternalizzati e supporto Premium 24 ore su 24, 7 giorni su 7.

A seconda dei requisiti specifici del cliente riguardo alle capacità di prevenzione avanzata e le domande della loro infrastruttura specifica, tra cui la necessità di completo isolamento dei dati aziendali, siamo in grado di arricchire ulteriormente la nostra soluzione di gestione e difesa dalle minacce con i prodotti seguenti, offrendo un approccio davvero strategico e integrato alla mitigazione dei rischi e alla prevenzione delle minacce avanzate e degli attacchi mirati:

- **Kaspersky Endpoint Security** è una piattaforma di protezione degli endpoint multi-layered, basata su tecnologie di cybersecurity HuMachine Intelligence, che offre difese flessibili e automatizzate contro le minacce note e sconosciute più avanzate, tra cui gli attacchi fileless e ransomware, avvalendosi di motori di Machine learning, rilevamento di comportamento sospetto, controlli, protezione dei dati e non solo.

- **Kaspersky Secure Mail Gateway** nell'ambito di un approccio preventivo contro gli attacchi mirati fornisce un'eccezionale protezione per il traffico trasmesso attraverso i server di posta contro spam, phishing e minacce malware generiche e avanzate. Kaspersky Secure Mail Gateway funziona efficacemente persino nelle infrastrutture eterogenee più complesse, e indipendentemente da quale modello di recapito posta è in uso: cloud, on-premise, crittografato.

- **Kaspersky Private Security Network** porta on-premise il nostro database di Threat Intelligence per reti e ambienti isolati con rigide restrizioni di condivisione dati, che consente alle imprese di sfruttare la maggior parte dei vantaggi della sicurezza cloud-assisted senza inviare alcun dato all'esterno del perimetro. È la versione personale, locale e completamente privata di Kaspersky Security Network per le imprese. Kaspersky Private Security Network risponde alle preoccupazioni relative alla sicurezza informatica aziendale di importanza critica senza che nemmeno un dato esca dalla rete locale.

Kaspersky Anti Targeted Attack

Mettendo in correlazione gli eventi da più sorgenti, tra cui la rete, gli endpoint e la nostra Threat Intelligence globale, Kaspersky Anti Targeted Attack offre il rilevamento delle minacce complesse praticamente in tempo reale, oltre alla generazione di dati forensi critici per potenziare il procedimento di indagine.

Kaspersky Anti Targeted Attack offre alle organizzazioni:

- Business continuity integrale, conseguita grazie all'implementazione di sicurezza e conformità nei nuovi processi sin dal principio
- Visibilità su Shadow IT e minacce nascoste
- Massima flessibilità, che consente la distribuzione tra ambienti fisici e virtuali, laddove siano necessari visibilità e controllo
- Automazione dei task di indagine e risposta, ottimizzando la redditività dei team di sicurezza, risposta agli incidenti e SOC
- Integrazione con i prodotti di sicurezza esistenti, per migliorare i livelli di sicurezza complessivi e proteggendo l'investimento nella sicurezza legacy

Kaspersky Endpoint Detection and Response

I tradizionali prodotti di sicurezza degli endpoint (ad esempio Kaspersky Endpoint Security) hanno un ruolo fondamentale nella protezione da una vasta gamma di minacce, tra cui ransomware, malware, botnet ecc. Tuttavia, per proteggersi da una gamma ancora più ampia di cyberattacchi avanzati e di avversari intelligenti, le imprese devono oggi implementare ulteriori livelli di protezione a livello endpoint.

Kaspersky Endpoint Detection and Response aiuta le organizzazioni a:

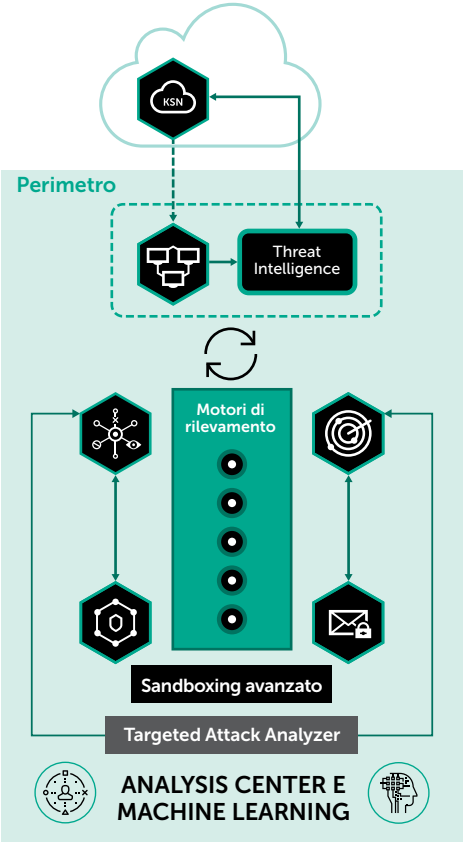
- Automatizzare l'identificazione delle minacce e la risposta senza interruzioni dell'operatività.
- Migliorare la visibilità degli endpoint e il rilevamento delle minacce tramite tecnologie avanzate, tra cui Machine learning, sandboxing, scansione IoC e Threat Intelligence.
- Potenziare la sicurezza informatica con una soluzione aziendale facile da usare per la risposta agli incidenti
- Stabilire processi unificati ed efficaci di Threat Hunting, Incident Management and Response.

Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway è una soluzione automatizzata di prevenzione dalle minacce via email che offre tecnologie avanzate per proteggere il traffico mail di ogni tipo, come parte di un singolo approccio orientato al rilevamento e alla prevenzione degli attacchi mirati. Kaspersky Secure Mail Gateway fornisce innovativi servizi anti-spam e anti-phishing cloud-assisted, una protezione anti-malware con funzionalità zero-day e anti-exploit, tecnologie Threat Intelligence, Machine learning e sandboxing avanzato per fornire un approccio automatizzato multi-layered alla sicurezza della posta elettronica.

Kaspersky Secure Mail Gateway fornisce alle organizzazioni:

- Prevenzione automatizzata di minacce note, sconosciute e future
- Analisi dei file in cloud e basata su firma
- Analisi dei file tramite metodi di Machine learning
- Rapida notifica degli incidenti
- Miglioramento continuo della sicurezza informatica aziendale



Kaspersky Private Security Network

Kaspersky Security Network è una versione locale e completamente privata di Kaspersky Security Network (KSN), che consente alle organizzazioni che non desiderano inviare alcun dato all'esterno del perimetro della rete aziendale di sfruttare la maggior parte dei vantaggi della Threat Intelligence globale basata su cloud.

La tecnologia brevettata Kaspersky Private Security Network:

- Fornisce l'accesso alle statistiche globali di URL e file
- Categorizza URL e file con verdetti specifici per gli oggetti dannosi e inseriti in whitelist
- Riduce al minimo i danni causati da incidenti di cybersecurity tramite la visibilità delle minacce in tempo reale
- Consente di aggiungere i verdetti univoci specifici del cliente e di terze parti (hash dei file)
- Rispetta i rigorosi standard normativi, di sicurezza e privacy.

Cybersecurity Services

Intelligence e competenze, che forniscono un nuovo livello di protezione contro gli attacchi informatici più complessi

Threat Intelligence Portal

Condividendo le informazioni più aggiornate con i propri clienti, Kaspersky Lab offre alle imprese una visione a 360 gradi sui metodi, sulle tattiche e sugli strumenti impiegati dagli autori delle minacce, aiutandoli a proteggersi dalle moderne minacce informatiche. La nostra vasta gamma di servizi di Threat Intelligence aiuta a garantire che il Security Operations Center e/o il team responsabile della sicurezza IT sia perfettamente attrezzato per neutralizzare anche gli attacchi più sofisticati.

- **Threat Data Feeds:**l'azienda può potenziare i controlli di sicurezza (SIEM, IDS, firewall ecc.) e migliorare le funzionalità forensi con i dati più recenti sulle minacce informatiche, disponibili in una vasta gamma di formati e modailtà di utilizzo.
- I **report di intelligence sulle APT** offrono l'accesso esclusivo e proattivo alle descrizioni delle campagne di cyber-spionaggio di alto profilo, tra cui gli IoC (Indicators of Compromise) e le regole YARA.
- I **report di Threat Intelligence finanziari** sono incentrati sulle minacce che prendono di mira in modo specifico gli istituti finanziari, tra cui gli attacchi mirati, gli attacchi a infrastrutture specializzate (ad es. ATM/POS) e strumenti sviluppati o venduti da cybercriminali per attaccare banche, società di gestione pagamenti, Bancomat e sistemi POS.
- **Report sulle minacce personalizzati:** informazioni di Threat Intelligence personalizzati per un'organizzazione o un Pease specifico, derivate da sorgenti di informazione proprietari e open source inclusi Deep e Dark Web
- **Threat Lookup:** un portale Web che offre l'accesso completo a tutte le informazioni di intelligence acquisite da Kaspersky Lab riguardo gli indicatori delle minacce e alle loro relazioni.
- La **CLOUD Sandbox** consente di inviare file sospetti a Kaspersky Lab, ottenere una descrizione dettagliata del comportamento del file con l'aiuto della nostra tecnologia all'avanguardia ed eseguire indagini complete e approfondite basate sulla stretta integrazione con il servizio Kaspersky Threat Lookup.
- **Phishing Tracking:** notifiche in tempo reale sugli attacchi di phishing in corso mirati all'azienda o ai suoi clienti.
- **Botnet Tracking:** notifiche in tempo reale sugli attacchi botnet in corso che minacciano i clienti e la reputazione dell'azienda.

Security Assessment

I servizi di assessment (Kaspersky Security Assessment Services) combinano l'analisi dei nostri specialisti con tecnologie e competenze di ricerca all'avanguardia, al fine di testare i sistemi informatici di qualsiasi livello di complessità negli ambienti real-world.

Penetration Test
Tentativo di compromissione simulato per dimostrare i potenziali vettori di attacco e fornisce una panoramica sull'approccio alla sicurezza aziendale dal punto di vista di un autore dell'attacco.

Application Security Assessment
Una ricerca approfondita, che scova i difetti nella logica dei processi aziendali e le vulnerabilità di implementazione nelle applicazioni di ogni tipo, dalle grandi soluzioni basate su cloud alle applicazioni embedded e per dispositivi mobili.

Security Assessment dei sistemi di pagamento
Analisi completa dei componenti hardware e software dei sistemi di pagamento, mirata a rivelare i potenziali scenari di frode e le vulnerabilità che danno luogo a manipolazioni di transazioni finanziarie.

Security Assessment degli ambienti ICS
Threat modelling specifico del caso e valutazione delle vulnerabilità dei sistemi ICS (Industrial Control System) e dei relativi componenti, che fornisce informazioni approfondite sulla superficie di attacco corrente e il potenziale impatto sul business di un attacco.

Security Assessment dei sistemi di trasporto
Ricerca specializzata incentrata sull'identificazione dei problemi di sicurezza relativi ai componenti mission-critical delle moderne infrastrutture di trasporto, dal settore automobilistico a quello aerospaziale.

Smart Technologies e IoT Security Assessment
Una valutazione dettagliata degli odierni dispositivi altamente interconnessi e della relativa infrastruttura back-end, che rivela le vulnerabilità nel firmware, nella rete e nei livelli applicativi.

Threat Hunting

Tecniche di Threat Hunting proattive eseguite da professionisti esperti e altamente qualificati nel campo della sicurezza, che aiutano a scoprire le minacce avanzate annidate nell'organizzazione.

- **Kaspersky Managed Protection**
  Monitoraggio 24 ore su 24 e analisi continua dei dati relativi alle minacce informatiche eseguiti da esperti di Kaspersky Lab.

- **Targeted Attack Discovery**
  Un'offerta completa che consente l'identificazione proattiva di qualsiasi segno di compromissione corrente o storico e risposta agli attacchi precedentemente non rilevati.

Incident Response

I servizi di risposta agli incidenti di Kaspersky Lab vengono effettuati da analisti e investigatori delle intrusioni informatiche con elevata esperienza. Per la risoluzione dell'incidente di sicurezza possiamo avvalerci della nostra competenza globale.

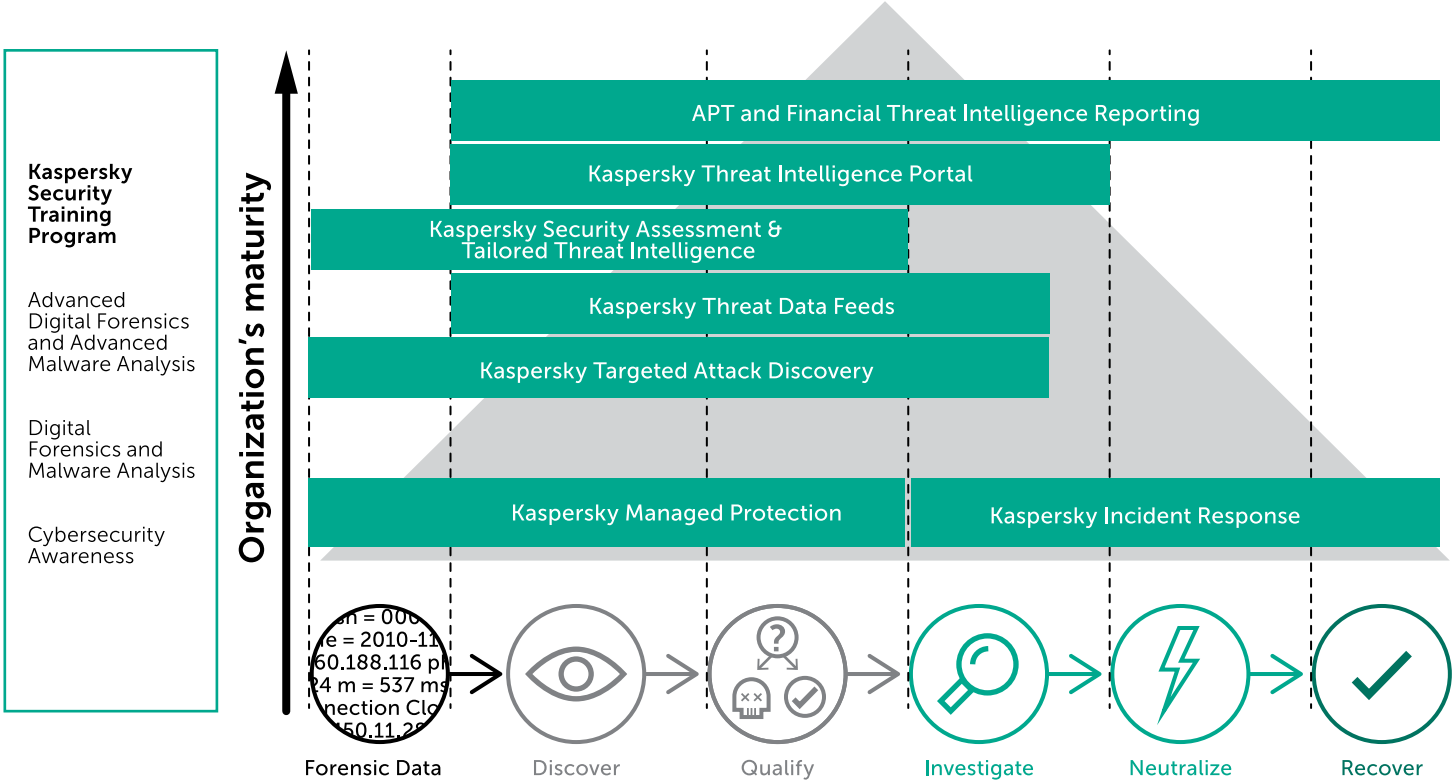
- **Incident Response:** copre l'intero ciclo di indagine sull'incidente per eliminare completamente la minaccia all'organizzazione.
- **Digital Forensics:** analisi delle prove digitali relative a un cybercrimine, creazione di un report completo in cui sono dettagliati tutti i risultati pertinenti.
- **Malware Analysis:** offre all'azienda un quadro completo del comportamento di specifici file malware.

Security Training

Offriamo un portafoglio di corsi che copre ogni aspetto, dai principi fondamentali alle tecniche e agli strumenti avanzati impiegati per l'analisi forense digitale, l'analisi del malware e la risposta agli incidenti, che permette alle organizzazioni di migliorare le proprie conoscenze sulla sicurezza informatica in queste aree.

- **Digital Forensics:** i corsi sono concepiti per colmare le lacune nell'esperienza, attraverso lo sviluppo e il potenziamento delle competenze pratiche nella ricerca di tracce di cybercrimine digitale e nell'analisi di diversi tipi di dati per ripristinare la cronologia e le origini dell'attacco.
- **Malware Analysis and Reverse Engineering:** i corsi forniscono le nozioni necessarie per analizzare il software dannoso, raccogliere gli IoC (indicatori di compromissione), scrivere firme per rilevare malware o computer infetti e ripristinare file e documenti infetti/crittografati.
- **Incident Response:** i corsi forniscono le nozioni relative a ogni fase del procedimento di risposta agli incidenti, dotando i team di cybersecurity dell'approfondita conoscenza necessaria per la remediation degli incidenti.
- **Rilevamento efficiente delle minacce con YARA:** i partecipanti apprenderanno come scrivere le regole YARA più efficaci, come testarle e come migliorarle fino a poter rilevare minacce non altrimenti individuabili usando altri metodi.

Kaspersky Cybersecurity Services



Cybersecurity Awareness

Creare un ambiente informatico aziendale sicuro con un approccio ludico

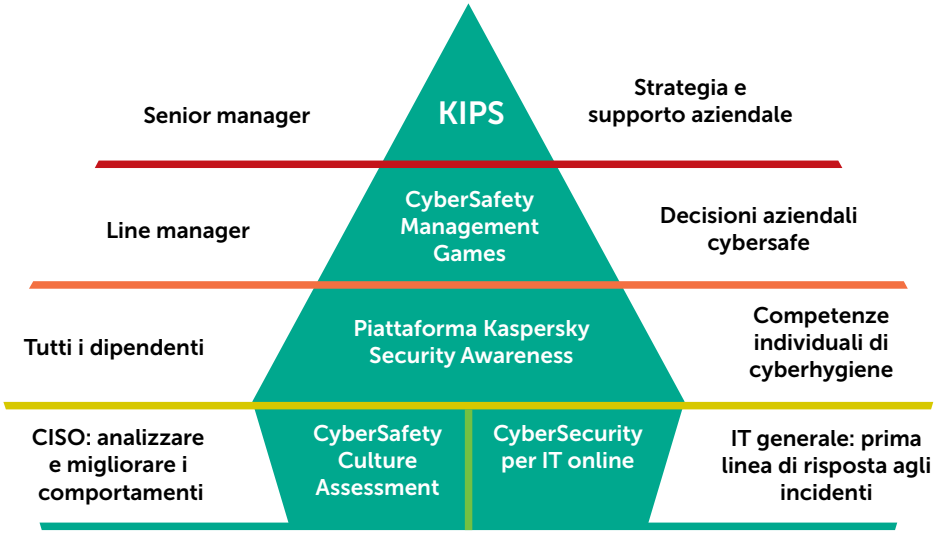
In media, le grandi imprese devono pagare circa 1.155.000 USD per il ripristino dagli attacchi causati da dipendenti negligenti o disinformati, mentre le piccole e medie imprese ne spendono 83.000. Oltre l'80% di tutti gli incidenti informatici è causato dall'errore umano. Gli attacchi di phishing da soli costano fino a 400 USD per dipendente all'anno.

Le grandi imprese perdono milioni nel ripristino dagli incidenti provocati dal personale, ma l'efficacia dei tradizionali programmi di formazione mirati a prevenire questi problemi è limitata. Pertanto, di solito non riescono a generare il comportamento e la motivazione desiderati.

Kaspersky Lab offre una famiglia di prodotti di formazione basata su computer che sfrutta le moderne tecniche di apprendimento e soddisfa tutti i livelli della struttura organizzativa. Il nostro programma di formazione ha già dimostrato la sua efficacia, sia per i clienti che per i partner di Kaspersky Lab:

- Riduzione fino al 90% del numero di incidenti
- Riduzione del 50-60% delle potenziali perdite monetarie associate ai rischi di cybersecurity
- Probabilità fino al 93% che le conoscenze acquisite vengano usate quotidianamente
- L'86% dei partecipanti consiglierebbe il corso ai colleghi

Prodotti di formazione Kaspersky Security Awareness



Approccio vincente

- **Creare un comportamento, e non offrire semplici nozioni**: l'approccio di apprendimento prevede le sessioni ludiche, l'apprendimento sul campo, le dinamiche di gruppo, gli attacchi simulati, i percorsi di apprendimento, il consolidamento automatizzato delle competenze, ecc. Ciò dà origine a modelli comportamentali e produce miglioramenti della sicurezza informatica a lungo termine.

- **Contenuti pratici e affidabili** (basati sull'esperienza del reparto di ricerca e sviluppo di Kaspersky Lab) forniti sotto forma di una serie di esercitazioni interattive ottimizzate per rispondere alle esigenze aziendali e alle preferenze in termini di tempo/formato dei diversi livelli organizzativi: senior manager, line manager, dipendenti generici.

- **Valutazione in tempo reale, gestione dei programma senza problemi**: il software assegna compiti di formazione automatizzati, valutazioni delle capacità e consolidamento tramite simulazioni di ripetuti attacchi di phishing simuato. I corsi possono essere gestiti ed erogati dai partner di Kaspersky Lab oppure dai team di formazione e sviluppo del cliente (i programmi e il supporto Train-The-Trainer sono forniti da Kaspersky Lab).

Come funziona

- La formazione copre una vasta gamma di problemi di sicurezza: dalla violazione dei dati e il ransomware agli attacchi malware basati su Internet, al social networking sicuro e alla sicurezza dei dispositivi mobili.

- La metodologia di apprendimento continuo stimola costantemente le capacità e la motivazione ai livelli più profondi dell'organizzazione.

- I corsi di formazione diretti a diversi livelli e funzioni dell'organizzazione contribuiscono a creare una cultura collaborativa di CyberSafety, condivisa da tutti e condotta dall'alto.

- La formazione prevede strumenti analitici e di reportistica che valutano le competenze dei dipendenti e i progressi di apprendimento, oltre all'efficacia del programma a livello aziendale.

- I piani formativi e le best practice fornite da Kaspersky Lab agevolano l'implementazione del programma e coadiuvano i team di sicurezza IT e T&D del cliente a ottenere il massimo dalle iniziative di Security Awareness.

Cybersecurity industriale

Protezione specializzata per i sistemi di controllo industriale

Nell'era dell'Industria 4.0, la maggior parte delle reti industriali è accessibile attraverso Internet, che sia per scelta o no, questo le espone a specifiche cyber minacce.

Gli attacchi malevoli contro gli ambienti industriali sono significativamente aumentati negli ultimi anni. Il timore per le supply chain che si verifichino delle interruzioni si è classificato al primo posto a livello globale negli ultimi tre anni, mentre il rischio di incidenti informatici è diventata la principale preoccupazione. Per le aziende che operano sistemi infrastrutturali industriali o critici, il rischio non è mai stato maggiore.

La sicurezza industriale ha conseguenze che vanno ben oltre la protezione dell'azienda e della reputazione. In molti casi, occorre fare importanti considerazioni ecologiche, sociali e macroeconomiche quando si parla di proteggere i sistemi industriali dalle minacce informatiche. Ogni infrastruttura critica necessita dei livelli di protezione più elevati possibile contro una crescente gamma di minacce.

Al contempo, gli ambienti industriali necessitano di una soluzione integrata che mantenga la disponibilità dei processi industriali rilevando e prevenendo le azioni (intenzionali o accidentali) che potrebbero interrompere o arrestare servizi vitali.

La soluzione: Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity è un portafoglio di tecnologie e servizi progettati per proteggere ogni livello industriale, tra cui i server SCADA, HMI, le workstation di progettazione, i PLC, le connessioni di rete, senza incidere sulla continuità operativa e sulla coerenza del processo industriale. Impostazioni versatili e flessibili fanno sì che la soluzione possa essere configurata per soddisfare le esigenze e i requisiti unici di singoli impianti industriali.

La soluzione è stata sviluppata per proteggere le infrastrutture critiche, basandosi su una serie di diversi sistemi di controllo industriale. La flessibilità e la portata di Kaspersky Industrial CyberSecurity consente alle organizzazioni di configurare la propria soluzione attenendosi rigorosamente ai requisiti dell'ambiente ICS specifico. La configurazione ottimale delle tecnologie e dei servizi di sicurezza viene stabilita attraverso una revisione completa dell'infrastruttura effettuata dagli esperti di Kaspersky Lab.

L'approccio di Kaspersky Lab alla protezione dei sistemi industriali si basa su oltre un decennio di esperienza nell'individuare e analizzare alcune delle minacce industriali più sofisticate al mondo. La nostra approfondita conoscenza e comprensione della natura delle vulnerabilità di sistema, unita alla nostra stretta collaborazione con le principali forze dell'ordine, agenzie governative e industriali del mondo, tra cui Interpol, Industrial Internet Consortium e vari fornitori ed enti di controllo ICS, ci ha permesso di assumere la leadership nella risposta ai requisiti unici della sicurezza informatica industriale.

Questa soluzione altamente specializzata:

- Rappresenta un approccio olistico alla sicurezza informatica per gli ambienti industriali
- Offre il ciclo completo di servizi di sicurezza, dal cybersecurity assessment all'incident response
- Fornisce tecnologie di sicurezza esclusive, sviluppate specificamente per i sistemi industriali
- Riduce al minimo il tempo di inattività e i ritardi del processo industriale.

Kaspersky Industrial CyberSecurity

Tecnologie

Deep Packet Inspection

Integrazione con altri sistemi

Anti-malware

Integrity Control

Gestione centralizzata

Incident Investigation

Intrusion Detection System

Servizi

Education e intelligence

- Formazione sulla cybersecurity
- Programmi di Awareness
- Threat Intelligence

Servizi di esperti

- Cybersecurity assessment
- Integrazione della soluzione
- Manutenzione
- Incident response

Fraud Prevention

La soluzione avanzata per un'esperienza utente senza problemi e la prevenzione proattiva delle frodi in tempo reale

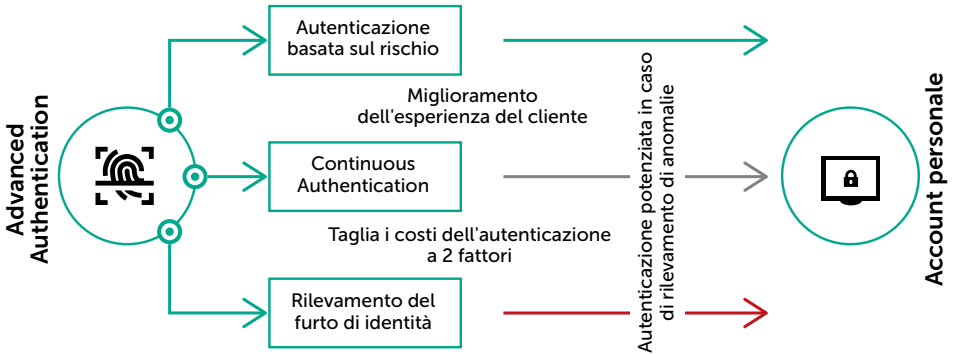
Scegliere il digitale non è solo una tendenza: è una necessità. Poiché molti clienti oggi usano canali mobili e online per le loro esigenze quotidiane, le aziende devono fornire servizi di alto livello con la massima funzionalità. Allo stesso tempo, devono gestire la sicurezza online con un'esperienza senza problemi per il cliente. Ed è qui che entra in gioco Kaspersky Fraud Prevention, permettendo di far crescere e sviluppare i canali online e mobili senza l'ulteriore stress dei problemi di sicurezza e delle questioni di usabilità online.

La gamma complessa di tecnologie avanzate alla base di Kaspersky Fraud Prevention include analisi comportamentale e dei dati biometrici, analisi del dispositivo e dell'ambiente, tutti implementati nell'apposito cloud. Vengono applicate le tecnologie di Machine learning per il rilevamento proattivo di complessi schemi fraudolenti tra i canali Web e mobili. Ciò permette ai sistemi di monitoraggio delle frodi di trarre vantaggio da un processo decisionale più accurato e proattivo, oltre all'uso intelligente e adattivo dell'autenticazione step-up.

La soluzione consiste in due prodotti completi che possono essere utilizzati separatamente oppure assieme, migliorando significativamente i livelli di sicurezza e la protezione dalle frodi oltre a potenziare l'esperienza dell'utente.

Advanced Authentication è stato sviluppato per migliorare l'esperienza dell'utente, tagliare i costi dell'autenticazione a due fattori e rilevare continuamente le attività sospette, consentendo la crescita aziendale e l'aumento dei livelli di sicurezza.

Fin dal momento dell'accesso iniziale, Advanced Authentication analizza continuamente gli eventi, effettuando il calcolo dei livelli di rischio e la generazione dei suggerimenti appropriati alle analisi effettuate.



Automated Fraud Analytics usa una combinazione perfettamente bilanciata di tecnologie all'avanguardia con la Threat Intelligence globale e l'esperienza umana. Queste caratteristiche aiutano a identificare e allertare in anticipo l'organizzazione di possibili attività fraudolente, analizzando dati cruciali per consentire l'assunzione di decisioni accurate e tempestive e l'individuazione di complicati casi di frode.

Gli eventi durante le sessioni utente che incidono su utenti, dispositivi e i rispettivi ambienti trasmettono ai sistemi di gestione delle frodi i dati necessari a un processo decisionale puntuale e accurato. I dettagli relativi agli incidenti generati nell'ambito di Kaspersky Fraud Prevention Cloud sono pronti all'uso e forniscono informazioni approfondite su reali casi di frode, arrivando alla radice del problema.

Oltre alle tecnologie e all'esperienza avanzate, Kaspersky Fraud Prevention offre:

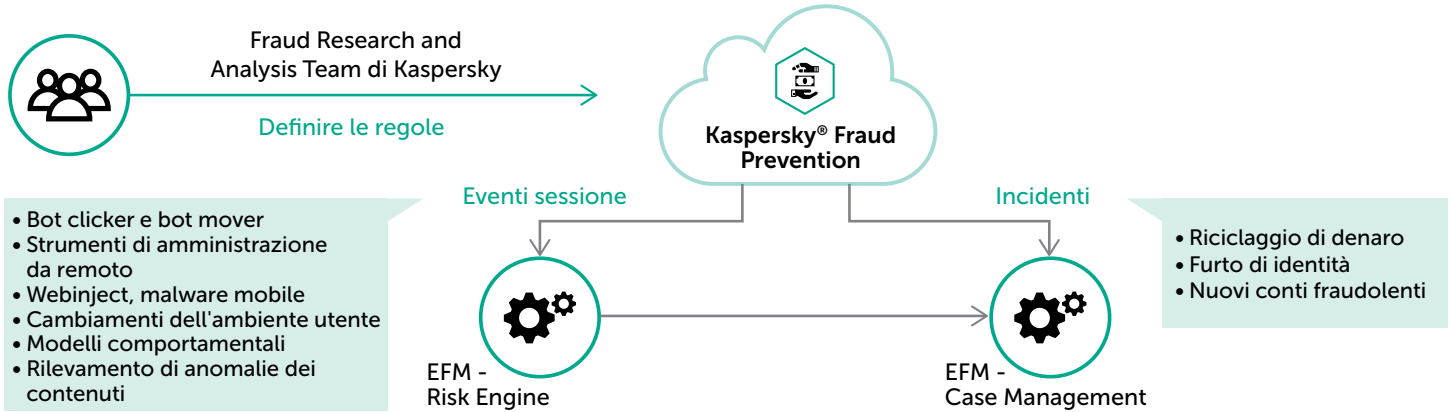
Maintenance Service Agreement: supporto premium per tutte le esigenze di sicurezza per proteggere l'azienda con un'assistenza di prim'ordine da parte dei nostri team locali di tecnici certificati.

Servizi di implementazione: tecnici dedicati che integrano i nostri prodotti con le soluzioni esistenti di sicurezza e prevenzione delle frodi.

Consulenza sulla prevenzione delle frodi: consulenza commerciale che aiuta a creare la giusta strategia di prevenzione delle frodi, a partire da un team di professionisti con varie competenze ed esperienza in più settori.

Vantaggi principali di Kaspersky Fraud Prevention:

- Crescita dei canali online e mobili senza l'ulteriore stress dei problemi di sicurezza e delle questioni di usabilità online
- Controllo dei costi di prevenzione delle frodi e taglio delle perdite dovute alle frodi
- Rilevamento in tempo reale delle frodi avanzate prima dell'esecuzione di qualsiasi transazione
- Potenziamento delle soluzioni di monitoraggio delle frodi aziendali con dati extra



Sicurezza IoT

Come giustificare la fiducia dei clienti proteggendone la privacy

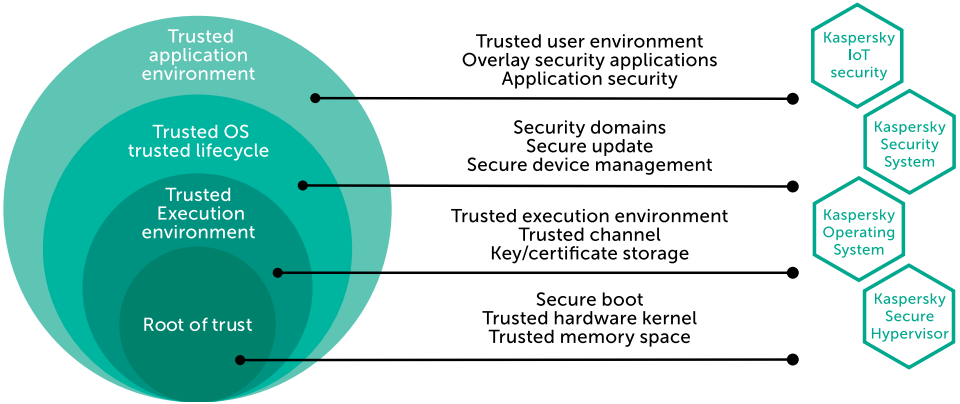
Internet of Things (IoT) è un nuovo modello che sta cambiando il mondo. Potrebbe rendere il nostro mondo più sicuro, migliorare la nostra salute, farci risparmiare tempo e denaro, ridurre gli sprechi e aggiungere una nuova dimensione al controllo della produzione e alla vita in generale.

La cybersecurity è da sempre stata associata alla sicurezza dei dati personali. Nell'era IoT, però, si è trasformata nella sicurezza della privacy. Le violazioni di quest'ultima, quali la sorveglianza remota tramite telecamere intelligenti, multimedia o baby monitor, le interferenze nel funzionamento dei dispositivi domestici, gli arresti imprevisti e il guasto dei servizi di uso quotidiano, sono tutte situazioni inaccettabili per l'utente finale.

Allo stesso tempo, Internet of Things offre incredibili opportunità ai produttori di dispositivi (tra cui componenti hardware e software), ai fornitori di servizi di telecomunicazione e al mercato della System Integration. La mancanza di fiducia nelle soluzioni IoT tra gli utenti finali potrebbe bloccare, o rallentare significativamente, la realizzazione di queste opportunità potenziali. Ecco perché la sicurezza end-to-end delle soluzioni IoT è la priorità principale di tutti coloro che ne sono coinvolti.

Allo stato attuale, i dispositivi periferici IoT e le apparecchiature di telecomunicazione fornite ai clienti possono facilmente incorporare vulnerabiità di sicurezza informatica. L'hardware potrebbe non controllare l'integrità del firmware e i dispositivi vengono talvolta spediti con password preinstallate, inclusa quella dell'amministratore. Altri problemi possono essere rappresentati da impostazioni di sicurezza di rete deboli oppure dall'uso di software obsoleto e vulnerabile. Se poi ci si aggiunge la mancanza di processi di aggiornamento del software, il che significa che i dispositivi vulnerabili possono funzionare per anni senza aggiornamenti, è chiaramente solo una questione di tempo prima che il dispositivo subisca un attacco.

Garanzie di attendibilità a livello di dispositivo



Il principio "chain of trust" forma la base per garantire il funzionamento sicuro di un dispositivo IoT, Inclusi i dispositivi periferici e infrastrutturali (gateway). Questo principio inizia con l'uso di una "root of trust" a livello hardware.

Questa tecnologia esegue l'avvio sicuro di un sistema operativo, incluso il controllo dell'integrità dell'immagine, l'applicazione della crittografia e i meccanismi di archiviazione sicura assistita dall'hardware per le informazioni chiave. L'avvio sicuro è di importanza fondamentale per i dispositivi infrastrutturali IoT critici, ad esempio i gateway, perché garantisce l'avvio del sistema operativo da supporti predefiniti e solo dopo che l'apparecchiatura ha superato specifici controlli di integrità.

Il successivo anello importante nella "chain of trust" è un sistema operativo sicuro in grado di garantire la corretta esecuzione del software non considerato attendibile. I recenti sviluppi nella tecnologia informatica rendono possibile implementare un ambiente a livello di sistema operativo che limita il comportamento delle applicazioni non considerate attendibili.

Il concetto di IoT abbraccia un'enorme varietà di dispositivi, gadget, tecnologie, software e protocolli di comunicazione. Ma questo ambiente eterogeneo genera molti rischi di sicurezza che potrebbero gravemente intralciare qualsiasi aspetto delle nostre vite connesse all'IoT. Kaspersky Lab ha progettato una serie di prodotti che aiutano a ridurre al minimo i rischi associati:

- **Embedded Systems Security**
  L'azienda può rafforzare e proteggere i dispositivi e i computer con sistema operativo di tipo embedded basati su Microsoft Windows con una soluzione creata per ottimizzare la sicurezza per i sistemi low-end con limitata capacità di memoria, che non richiede una manutenzione continua né la connettività a Internet.

- **KasperskyOS**
  Il sistema operativo KasperskyOS è stato progettato per proteggere sistemi embedded diversi e complessi dalle conseguenze del codice dannoso, dai virus e dagli attacchi hacker, attraverso la segregazione e l'applicazione delle policy di sicurezza. KasperskyOS crea un ambiente in cui una vulnerabilità o un codice dannoso non è più un affare di stato. Il componente di protezione Kaspersky Security System controlla le interazioni attraverso l'intero sistema, rendendo inutile lo sfruttamento delle vulnerabilità.

- **Kaspersky Security System**
  Kaspersky Security System è un motore di calcolo in grado di collaborare simultaneamente con diversi tipi di criteri di sicurezza (controllo degli accessi basato su ruoli e obbligatorio, logica temporale, flusso di controllo, type enforcement, ecc.) e può essere personalizzato per soddisfare le esigenze del cliente. Più precisi saranno i criteri, maggiori saranno il controllo e la sicurezza dell'intero sistema.

  Kaspersky Security System può essere usato assieme a KasperskyOS (la configurazione più sicura) oltre che in una soluzione basata su Linux (azioni sicure in un sistema non sicuro).

- **Kaspersky Secure Hypervisor**
  Kaspersky Secure Hypervisor (KSH) viene eseguito sul microkernel di KasperskyOS. Con KSH, i sistemi operativi guest virtualizzati e non attendibili possono essere separati l'uno dall'altro, con la possibilità di controllare le comunicazioni tra di essi dichiarandole attendibili, anche se sono eseguiti fisicamente sulla stessa piattaforma hardware. Un vantaggio aggiuntivo di KSH è la sua capacità di ridurre i costi di manutenzione dell'hardware.

- **Kaspersky Transportation Security Service**
  Modello "Security for Safety" incorporato e basato sulla tecnologia KasperskyOS, comprende un singolo gateway sicuro nelle ECU (Electronic Control Unit) e una gamma di servizi di security assessment che rispondono alle necessità di veicoli connessi attuali e futuri.

- **Secure Communication Unit**
  La Secure Communication Unit (SCU) è un'unità di controllo del communication gateway, connessa a varie subnet e/o controller di gateway a tali subnet all'interno della rete interna dell'automobile. In questo modo, la SCU rappresenta un singolo gateway per le comunicazioni esterne, laddove i dispositivi interni possono comunicare con un dominio o persino tra domini senza usare i servizi SCU. La SCU si basa sul sistema operativo KasperskyOS ed è protetta da Kaspersky Security System. KasperskyOS controlla tutte le interazioni all'interno della SCU a livello più basso e applica i criteri della policy di Kaspersky Security System. Soltanto le interazioni esplicitamente permesse sono possibili.

Sicurezza dei sistemi embedded

Sicurezza all-in-one progettata specificamente per i sistema embedded

Poiché operano con denaro reale e credenziali di carte di credito, i sistemi embedded sono il bersaglio preferito dai cybercriminali, dunque richiedono i livelli di protezione intelligente più elevati e mirati. È quindi necessario applicare tecnologie collaudate come Device Control e Default Deny come prima linea di difesa.

Oggi vediamo sistemi embedded ovunque: in biglietterie automatiche, bancomat, distributori, sistemi POS, attrezzature mediche, e la lista potrebbe continuare.

I sistemi embedded implicano particolari preoccupazioni per la sicurezza perché tendono a essere sparpagliati in giro, difficili da gestire e raramente aggiornati. Tuttavia, i sistemi che utilizzano contanti e le credenziali del cliente devono essere resistenti e a tolleranza d'errore. I dispositivi embedded non devono solo essere protetti dalle minacce dirette, ma devono essere inaccessibili ai cybercriminali o da un autore di un attacco interno in quanto punto di ingresso alla rete aziendale.

Le normative di sicurezza standard per i dispositivi embedded tendono a coprire solo la sicurezza basata su antivirus o l'hardening del sistema, il che non è sufficiente. Un approccio basato unicamente sull'antivirus ha un'efficacia limitata contro le attuali minacce per i sistemi embedded, come è stato ampiamente dimostrato negli attacchi recenti.

Default Deny per applicazioni, driver e librerie, insieme alla funzionalità Device Control, è l'unico approccio che può garantire la sicurezza dei sistemi critici obsoleti ancora in uso.

La soluzione: Kaspersky Embedded Systems Security

Kaspersky Lab ha creato una soluzione di sicurezza specificamente per le organizzazioni che utilizzano sistemi embedded, che ne riflette le funzionalità uniche e i requisiti in termini di sistema operativo, canale e hardware, concentrandosi sulle minacce specifiche sviluppate per questa tipologia di sistemi e supportando completamente la famiglia di prodotti Windows XP.

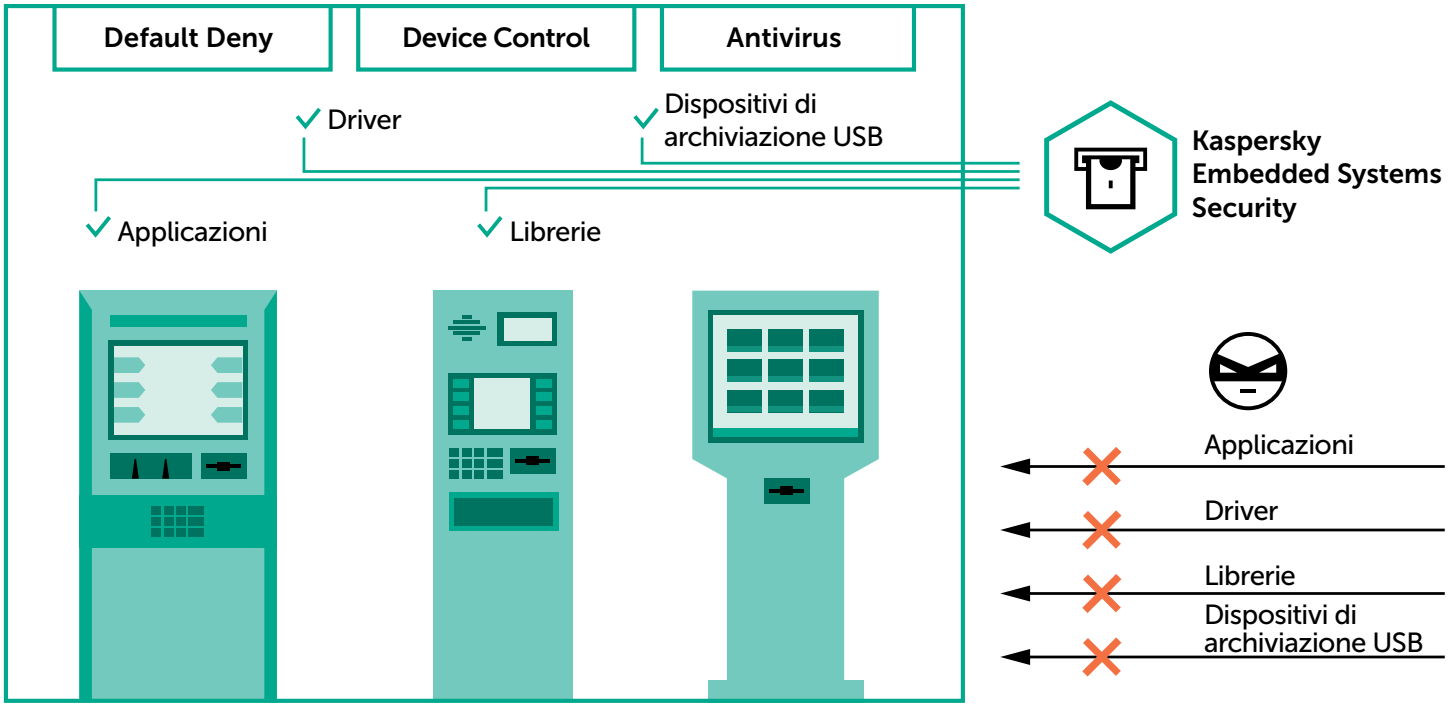
Kaspersky Embedded Systems Security offre una modalità operativa "Default Deny only", in cui i requisiti di sistema partono da 256 Mb di RAM e 50 Mb di spazio su disco rigido su Windows XP per i sistemi hardware low-end.

Viene anche fornita una modalità di scansione on-demand da un modulo antivirus facoltativo, che include la gestione del firewall. Questo modulo si appoggia a Kaspersky Security Network, con funzioni di gestione delle patch se necessario.

Dunque, questa singola soluzione soddisfa dunque tre obiettivi chiave:

- Sicurezza efficiente per i sistemi "difficili da gestire"
- Conformità con i requisiti PCI DSS 5.1, 5.1.1, 5.2, 5.3 e 6.2
- Tempistiche flessibili per la sostituzione di sistemi e hardware obsoleti

La soluzione è stata progettata specificamente per attenuare i rischi per la sicurezza informatica nei sistemi basati su sistemi operativi embedded, proteggendo le superfici di attacco specifiche di queste architetture pur rispettando le considerazioni relative all'efficienza. Una singola console intuitiva offre il controllo e la visibilità necessari a gestire un'efficace sicurezza multi-layered per gli endpoint, i sistemi critici e l'intera infrastruttura IT



Supporto Premium e servizi professionali

Una varietà di servizi che garantisce alle imprese di trarre il massimo beneficio dai prodotti Kaspersky Lab

Supporto Premium

Quando si verifica un incidente di sicurezza, il tempo impiegato per identificare la causa ed eliminarla è di importanza critica. Il rilevamento e la risoluzione rapida di un problema possono far risparmiare alle aziende centinaia di migliaia di dollari. I nostri piani di supporto Premium sono incentrati sul conseguimento di questo preciso obiettivo. Accesso 24 ore su 24 ai nostri esperti, classificazione dei problemi secondo priorità con tempi di risposta garantiti e patch private: tutto quanto necessario a garantire la soluzione tempestiva del problema.

Kaspersky Lab offre una serie di programmi di supporto Premium che trattano i problemi di sicurezza IT con la massima priorità in ogni momento, aiutando a mantenere la continuità delle operazioni, concentrandoci con tutte la forza della nostra esperienza direttamente sulla ricerca del percorso veloce ed efficace per ripristinare le prestazioni completamente e in modo sicuro.

I nostri piani di supporto Premium includono:

- Technical Account Manager dedicato
- Supporto 24 ore su 24, 7 giorni su 7, tramite una linea telefonicaqdedicata
- SLA di risposta agli incidenti
- Avvisi proattivi di nuove minacce

Servizi professionali

La cybersecurity è un grosso investimento. È possibile ottenere il massimo relazionandosi con esperti che comprendono esattamente come ottimizzare l'investimento per soddisfare i requisiti unici della propria azienda.

Attenendosi alle best practice e alle metodologie stabilite, i nostri esperti di sicurezza sono a disposizione per assistervi in ogni aspetto della distribuzione, della configurazione e dell'upgrade dei prodotti Kaspersky Lab nell'intera infrastruttura IT aziendale.

I servizi professionali di Kaspersky Lab garantiscono che la risposta al cambiamento o alla transizione sia agevole, efficace e non causi interruzioni eccessive dell'operatività aziendale.

I servizi professionali di Kaspersky Professional comprendono:

- Implementazione e upgrade
- Configurazione
- Health-Check
- Formazione sul prodotto

Chi è Kaspersky Lab

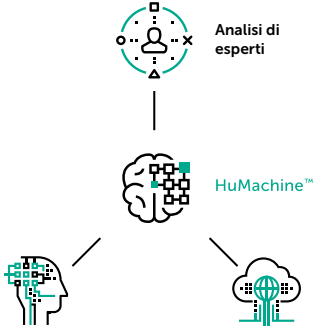
Kaspersky Lab è una delle aziende di cybersecurity a crescita più rapida del mondo e la più grande di proprietà privata.

La nostra indipendenza ci permette di essere più agili, di pensare in maniera differente e di agire più in fretta. Siamo alla ricerca di continue innovazioni, offrendo una protezione efficace, utilizzabile e accessibile. La nostra specialità è lo sviluppo di soluzioni di sicurezza all'avanguardia che ci permettono di stare sempre un passo avanti rispetto alle minacce potenziali, riflettendosi su ognuno dei 400 milioni di utenti e dei 270.000 clienti aziendali.

Oltre a questo, ciò che ci dà una marcia in più rispetto alla concorrenza è il connubio tra la tecnologia avanzata e il nostro impegno nei confronti del cliente.

Visita kaspersky.it/enterprise per scoprire di più sulle competenze uniche di Kaspersky Lab e sulle soluzioni di sicurezza aziendale.

Per le note



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.it/enterprise**
Novità sulle minacce: **www.securelist.com**
Novità sulla sicurezza IT: **https://www.kaspersky.it/blog/b2b//**

#truecybersecurity
#HuMachine

www.kaspersky.it