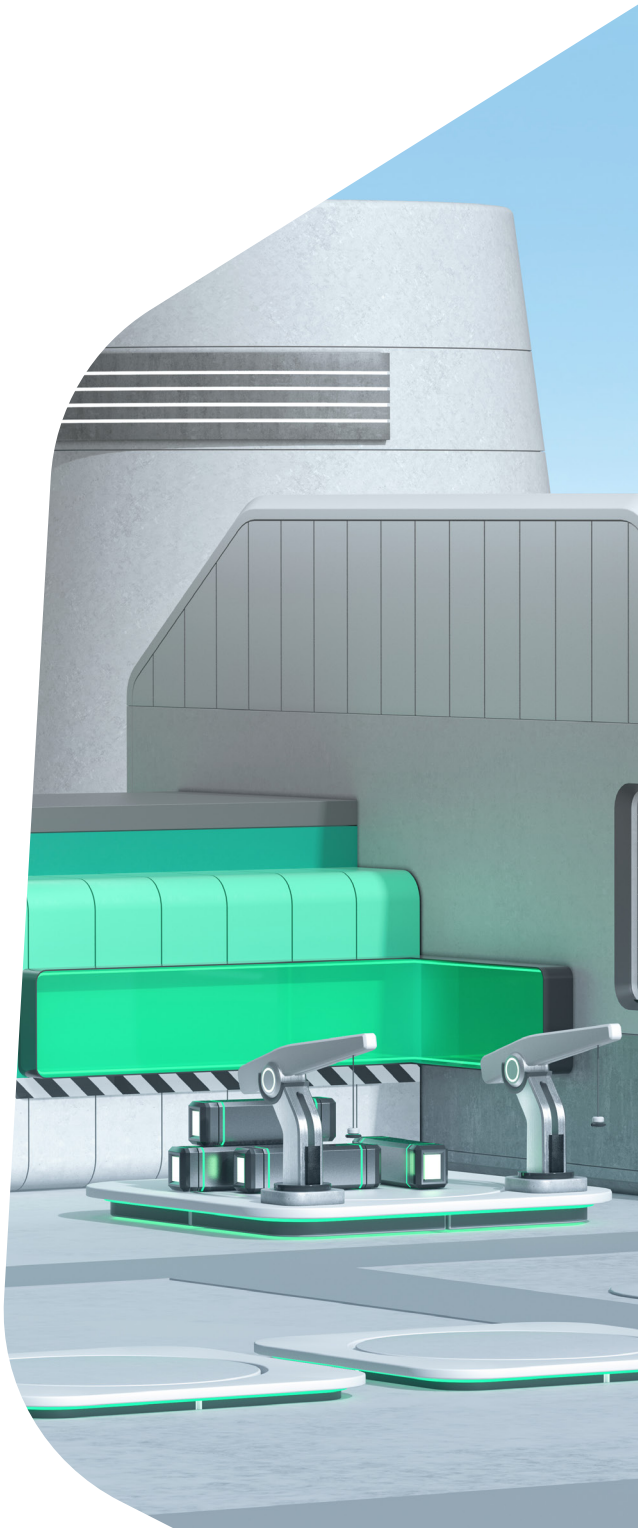
kaspersky

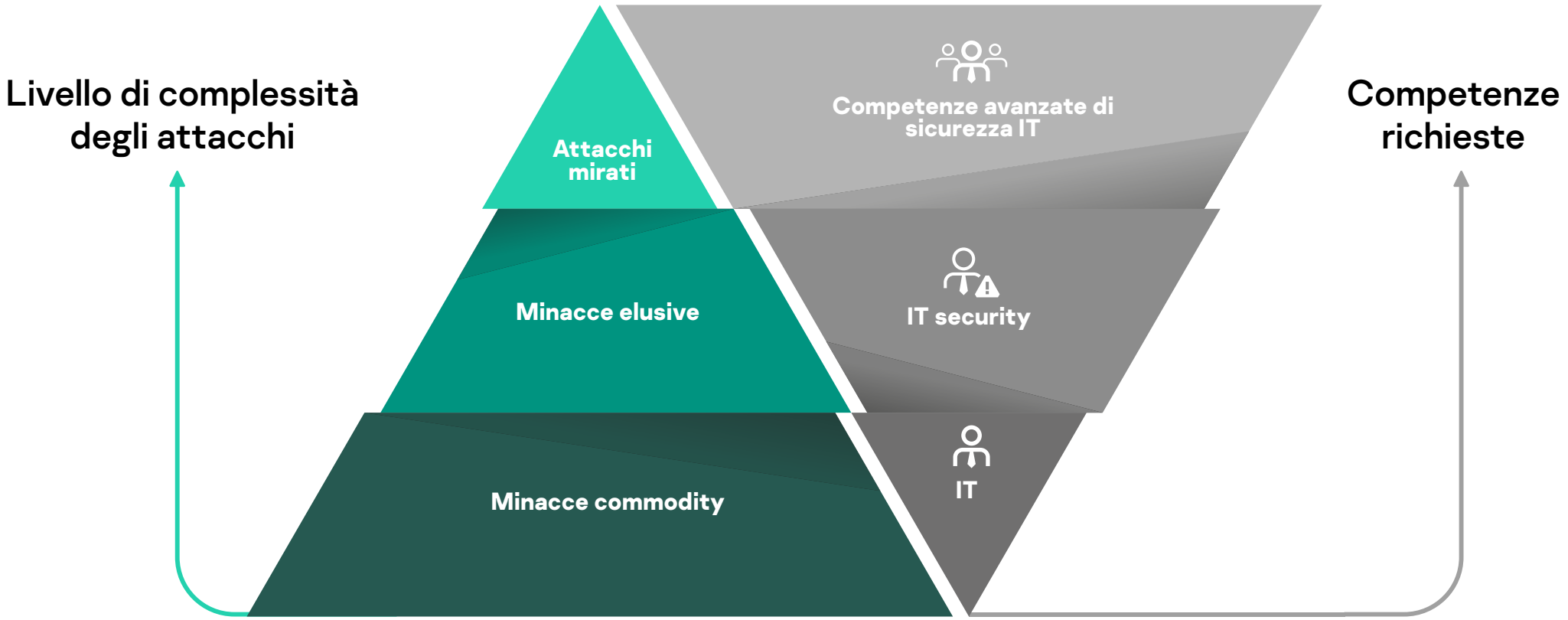
Kaspersky Security per le aziende Enterprise

Il portfolio di soluzioni Kaspersky per aziende Enterprise

La creazione di una solida base di sicurezza IT, attraverso la scelta del prodotto o del servizio più adatto per la propria azienda, rappresenta di sicuro il primo passo da compiere. Tuttavia la chiave per un successo duraturo nel tempo è lo sviluppo di una strategia di Cybersecurity aziendale lungimirante. Il portfolio di soluzioni Kaspersky per aziende Enterprise riflette pienamente le esigenze delle imprese di oggi in termini sicurezza: l'approccio "step by step" risponde perfettamente ai bisogni delle organizzazioni in base ai diversi livelli di maturità tecnologica acquisiti. Tale approccio combina vari livelli di protezione per combattere al meglio qualsiasi tipologia di minaccia informatica, rilevando gli attacchi più complessi, rispondendo in modo rapido ed efficace a qualsiasi tipo di incidente e prevenendo le future minacce.



Tipologia di minacce e competenze necessarie per contrastarle



Pianificazione della sicurezza a breve o a lungo termine

Il processo di evoluzione delle soluzioni di sicurezza tradizionali

Processo decisionale:

- Trend del mercato
- Soluzione di sicurezza isolata
- Approccio ottimale per la gestione delle emergenze
- Basato sulla compliance

Utilizzo di prodotti tradizionali:

- Endpoint Protection Platforms (EPP)
- Firewall / Next Generation Firewall (NGFW)
- Web Application Firewall (WAF)
- Data Loss Prevention (DLP)
- Security Information and Event Management Systems (SIEM)
- Altri prodotti

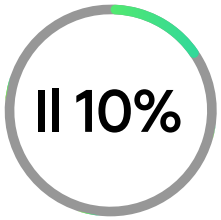
Caratteristiche

- Pianificazione a breve termine della sicurezza
- Utilizzo di tecnologie e funzionalità specifiche
- Protezione della rete a livello perimetrale

Perché falliscono gli approcci tradizionali:

- Crescente complessità del panorama delle minacce
- Complessità delle tecnologie di Cybersecurity
- Il successo della digital transformation delle attività aziendali richiede una strategia di sicurezza informatica a lungo termine

Gli endpoint rappresentano i punti di ingresso più comuni per l'accesso fraudolento all'infrastruttura IT di un'organizzazione, costituiscono l'obiettivo principale dei cybercriminali e la fonte primaria per la raccolta dei dati necessari per condurre indagini particolarmente efficaci in caso di incidenti complessi.

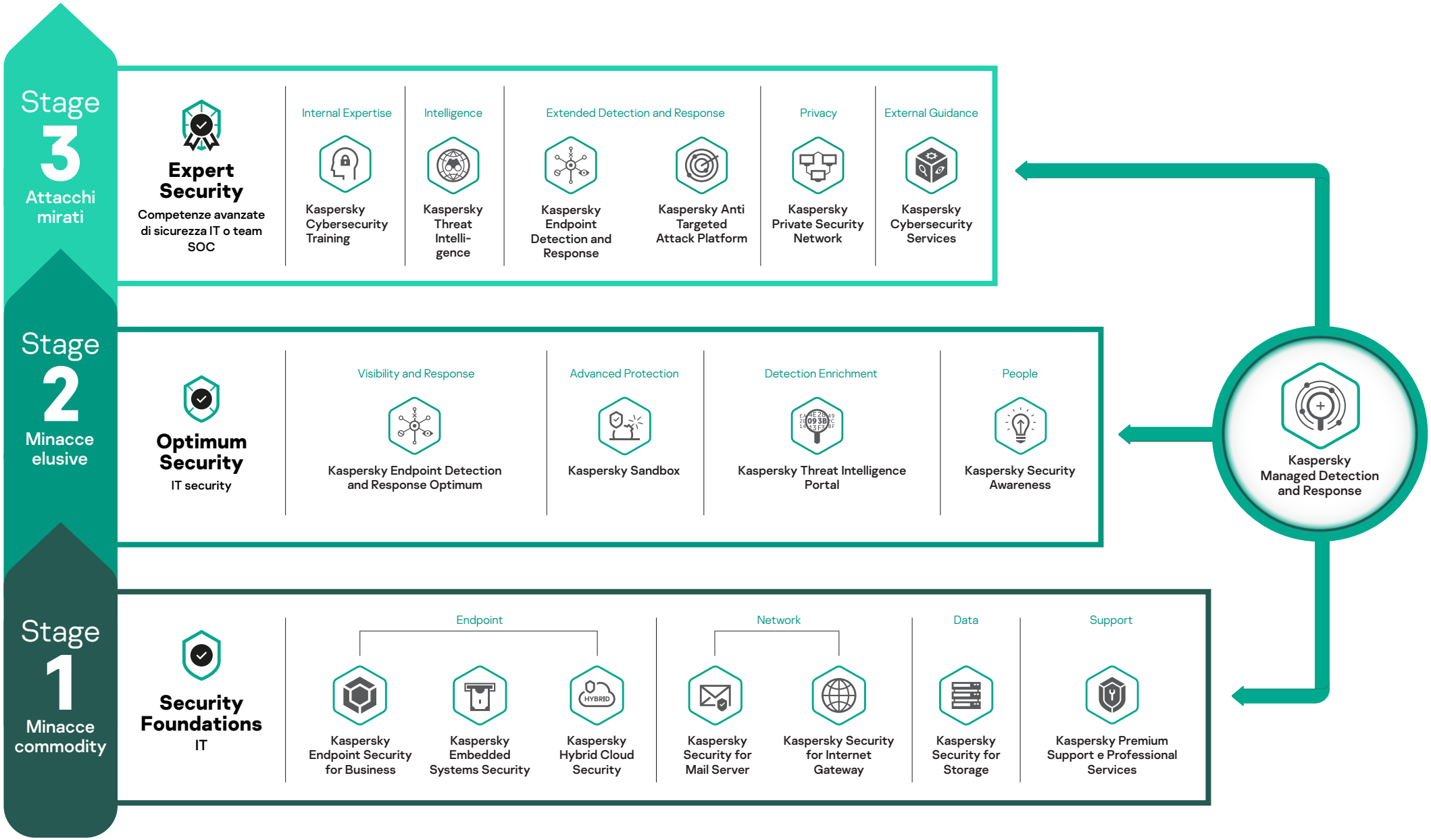


delle aziende rileva gli attacchi quasi istantaneamente

è il costo medio aggiuntivo di un data breach se rilevato dopo sette giorni

Fonte: IT Security Economics 2020 report by Kaspersky

L'approccio step-by- step di Kaspersky alla Cybersecurity



Stage 1
Security Foundations

Blocco automatico della maggior parte delle minacce.

- La base di partenza per aziende di qualsiasi dimensione e complessità, per costruire una strategia integrata di difesa dalle minacce complesse
- Generalmente sufficiente per le piccole imprese che non impiegano specialisti della sicurezza IT

Kaspersky Endpoint Security for Business

La reputazione della vostra azienda deve essere difesa a tutti i costi ed è questo il motivo per cui non ci limitiamo "solo" a proteggere e controllare tutti gli endpoint. Kaspersky Endpoint Security for Business protegge l'organizzazione da tutti i tipi di minacce, da quelle che attaccano il BIOS a quelle fileless. La funzionalità di hardening ottimizza la protezione dei server ad alte performance con controlli specifici che impediscono la perdita di informazioni personali e finanziarie. Queste funzionalità sono inoltre disponibili dal cloud o on-premises per una sicurezza e una gestione flessibili.

È la soluzione ideale se il vostro obiettivo è:

- Impedire ai dipendenti di esporre l'azienda e se stessi ad un attacco
- Ridurre il numero di incidenti negli endpoint che devono essere gestiti manualmente
- Proteggere ambienti diversi con strategie di difesa flessibili e comprovate

2 Competenze richieste

5 Personalizzazione e scalabilità

2 Livello di investimento

Vantaggi per l'azienda

- Riduzione del costo totale di proprietà (TCO) tramite l'automazione della difesa dalle minacce attraverso un prodotto all-in-one
- Garanzia di business continuity, proteggendo qualsiasi dispositivo, ovunque esso sia
- Mantenimento del rispetto dei requisiti di conformità pur garantendo la più totale flessibilità per esternalizzare la gestione della sicurezza IT

Use case

- Riduzione del rischio di esposizione agli attacchi con la tecnologia di protezione degli endpoint più premiata in assoluto
- Garanzia che l'infrastruttura IT sia aggiornata e gestita dalla console cloud-based oppure on-premises
- Migrazione da soluzioni di terze parti in modo semplice e veloce
- Aggiunta di nuove tecnologie, tra cui EDR e altre funzionalità, senza necessità di installare software aggiuntivo oltre all'endpoint agent
- Protezione dei dati garantendo piena conformità legale tramite la gestione integrata della crittografia, inclusa la cancellazione e il controllo dei dispositivi in remoto per vari sistemi operativi

Kaspersky Hybrid Cloud Security

Hybrid Cloud Security è una soluzione di sicurezza che semplifica e protegge la digital transformation dell'impresa, nel momento stesso in cui l'organizzazione implementa ambienti virtuali o trasferisce il proprio workload nel cloud. La tecnologia brevettata Light Agent riduce in modo significativo l'utilizzo delle risorse hypervisor. L'integrazione nativa con una vasta gamma di piattaforme di virtualizzazione, container e di cloud pubblico garantisce una visibilità completa e il controllo sull'intera infrastruttura. Un set completo di tecnologie di sicurezza, gestite attraverso un'unica console, assicura una gestione semplificata dei rischi in ambienti IT diversi tra loro.

È la soluzione ideale se il vostro obiettivo è:

- Virtualizzare i workload di server e desktop
- Spostare o mantenere le infrastrutture nei cloud pubblici (IaaS)
- Integrare i passaggi di sicurezza nelle pipeline DevOps
- Sfruttare in modo sicuro i container

Vantaggi per l'azienda

- Riduzione al minimo dei danni finanziari e reputazionali, riducendo la superficie di attacco e il tempo di permanenza dell'attaccante
- Ottimizzazione dei costi IT liberando fino al 30% delle risorse dell'hypervisor
- Supporto alla compliance, soddisfando i principali requisiti di sicurezza
- Garanzia di un'efficace collaborazione tra il team IT e i team DevOps, riducendo il livello di rischio e l'eventualità di inattese falle di sicurezza

Use case

- Garanzia di visibilità completa e controlli sistematici sui processi di deployment a livello di cloud e data center
- Sicurezza per ambienti VDI, VMWare e Citrix
- Protezione dei workload su cloud per istanze AWS, Azure e Google Cloud, con deployment automatizzato e visibilità completa tramite integrazione API nativa
- Sicurezza per DevOps con la protezione del container, le interfacce di integrazione della pipeline e l'API di gestione

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security è una soluzione specializzata multilivello, progettata per proteggere i dispositivi integrati basati su Windows e gli endpoint meno recenti che eseguono sistemi operativi non supportati ce non più aggiornabili. Application Control fa parte delle funzionalità anti-malware opzionali che includono inoltre la prevenzione degli exploit, la protezione dalle minacce di rete, il monitoraggio dell'integrità e altri livelli di sicurezza per una protezione ottimale su misura per tutti gli endpoint

È la soluzione ideale se il vostro obiettivo è:

- Proteggere bancomat, sistemi PoS, apparecchiature sanitarie o qualsiasi altro sistema integrato di livello non industriale
- Ottimizzare la sicurezza dei sistemi che eseguono hardware e sistemi operativi obsoleti, inclusi gli endpoint meno recenti
- Integrare la sicurezza della vostra infrastruttura nell'ecosistema di sicurezza basato su Kaspersky

2 Competenze richieste

5 Personalizzazione e scalabilità

2 Livello di investimento

Vantaggi per l'azienda

- Processi aziendali senza interruzioni in aree in cui l'impatto di un attacco a livello finanziario, legale e reputazionale potrebbe essere impattante
- Possibilità di non dover eseguire necessariamente l'upgrade, continuando a utilizzare in sicurezza gli endpoint insostituibili specifici per un determinato scenario
- Piena conformità attraverso meccanismi di protezione affidabili, compresi quelli specificamente raccomandati dalle autorità di regolamentazione

Use case

- Configurazione dello scenario di sicurezza più efficace per il sistema, in base al relativo utilizzo e al livello di efficienza, scegliendo tra una serie di layer e scenari di sicurezza
- Protezione duratura e gestione facilitata dove le operazioni di manutenzione frequenti sono impossibili
- Contrasto degli attacchi interni: un grave rischio per i dispositivi integrati che non possono essere attaccati tramite e-mail o Web.
- Protezione dei dispositivi con scarsa connettività a Internet

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server impedisce alle minacce email-based (crimeware, ransomware, phishing e spam) di raggiungere i vostri endpoint, principale obiettivo di social engineering e malware. L'implementazione dell'intelligenza artificiale cloud-based e dei modelli basati sul machine learning on-premises garantiscono tassi di rilevamento elevati con un numero di falsi positivi estremamente basso, consentendo di far fronte a minacce sofisticate mail-based, tra cui Business Email Compromise (BEC). Lo spam viene bloccato in modo efficace prima che possa colpire la vittima.

È la soluzione ideale se il vostro obiettivo è:

- Consolidare le capacità per far fronte agli attacchi distribuiti in massa e altamente mirati che utilizzano la posta elettronica come vettore
- Coprire una vasta gamma di scenari di sicurezza e-mail che coinvolgono diverse piattaforme e schemi di deployment

3 Competenze richieste

4 Personalizzazione e scalabilità

2 Livello di investimento

Vantaggi per l'azienda

- Riduzione degli effetti dannosi degli attacchi basati su malware e social engineering effettuati via e-mail
- Aumento della produttività del personale, annullando le distrazioni indotte dallo spam
- Diminuzione dei workload di sicurezza IT/IT e ottimizzazione dei costi operativi
- Riduzione al minimo del rischio legale e reputazionale legato al controllo dei contenuti inviati tramite e-mail

Use case

- Consolidamento delle difese dell'infrastruttura a livello di server di posta, grazie al blocco delle minacce prima che raggiungano gli utenti e gli endpoint
- Potenziamento della sicurezza del gateway esistente senza aggiungere falsi positivi
- Potenziamento delle strutture Kaspersky-based di rilevamento delle minacce avanzate con un contesto aggiuntivo e con funzionalità di risposta automatizzate a livello di gateway

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway, con la sua applicazione principale Kaspersky Web Traffic Security, offre una solida protezione a livello di gateway contro le minacce informatiche web-based (malware, ransomware, miner, phishing e siti Web dannosi). Consente inoltre di controllare l'utilizzo del World Wide Web, limitando l'accesso a risorse Web specifiche in linea con i criteri aziendali e limitando il trasferimento di determinati tipi di file.

È la soluzione ideale se il vostro obiettivo è:

- Impedire alle minacce web-based di compromettere gli endpoint
- Ridurre il rischio di infezione e aumentare la produttività complessiva applicando controlli all'utilizzo di Internet
- Ridurre il carico di lavoro dei team di sicurezza IT/IT bloccando automaticamente le minacce web-based nel punto di ingresso

Vantaggi per l'azienda

- Riduzione al minimo delle interruzioni delle attività e dell'impatto della gestione della sicurezza all'interno della rete
- Aumento dell'efficienza della sicurezza IT/IT e ottimizzazione dei costi operativi
- Protezione dalle minacce online basate sul social engineering
- Miglioramento della produttività dei dipendenti, controllando l'accesso online a risorse Web specifiche

Use case

- Consolidamento delle difese basate sugli endpoint a livello di gateway
- Integrazione e potenziamento della sicurezza del gateway Web esistente, senza ulteriori falsi positivi
- Protezione dei dispositivi critici che soffrono di una protezione completa per motivi aziendali o legati all'utilizzo.
- Potenziamento delle strutture Kaspersky-based di rilevamento delle minacce avanzate con modalità di risposta automatizzate a livello di gateway

2 Competenze richieste

5 Personalizzazione e scalabilità

2 Livello di investimento

Kaspersky Security for Storage

Gli storage connessi, facilmente accessibili, possono di fatto divenire una sorgente di infezione per l'intera infrastruttura IT e un comodo bersaglio per le più pericolose minacce informatiche, quali i ransomware. Kaspersky Security for Storage salvaguarda i dati aziendali e previene la diffusione delle minacce tramite rete grazie a un solido ed efficace set di tecnologie di protezione basate su criteri di Threat Intelligence globale. Comprende funzionalità esclusive, come Remote Anticryptor, abilitate attraverso l'integrazione con le API del sistema di storage.

È la soluzione ideale se il vostro obiettivo è:

- Proteggere gli storage connessi dagli attacchi esterni e dalla diffusione delle infezioni
- Salvaguardare i dati importanti dagli attacchi ransomware negli storage connessi
- Gestire la sicurezza dei data storage insieme a endpoint e server protetti dalle soluzioni Kaspersky

Vantaggi per l'azienda

- Mantenimento della business continuity, prevenendo i malware outbreak che utilizzano gli archivi come punti di diffusione
- Garanzia della compliance, offrendo mezzi affidabili di protezione per l'archiviazione regolamentata dei dati
- Riduzione dei problemi operativi attraverso una gestione unificata con altre soluzioni di protezione Kaspersky per server ed endpoint

Use case

- Protezione di NAS, DAS, SAN o di qualsiasi combinazione di queste soluzioni utilizzate nell'infrastruttura
- Protezione sia del server che degli storage utilizzati per ospitare la soluzione di sicurezza, grazie ad un unico prodotto
- Prevenzione della perdita di dati causata dall'esecuzione remota di strumenti di criptaggio

3 Competenze richieste

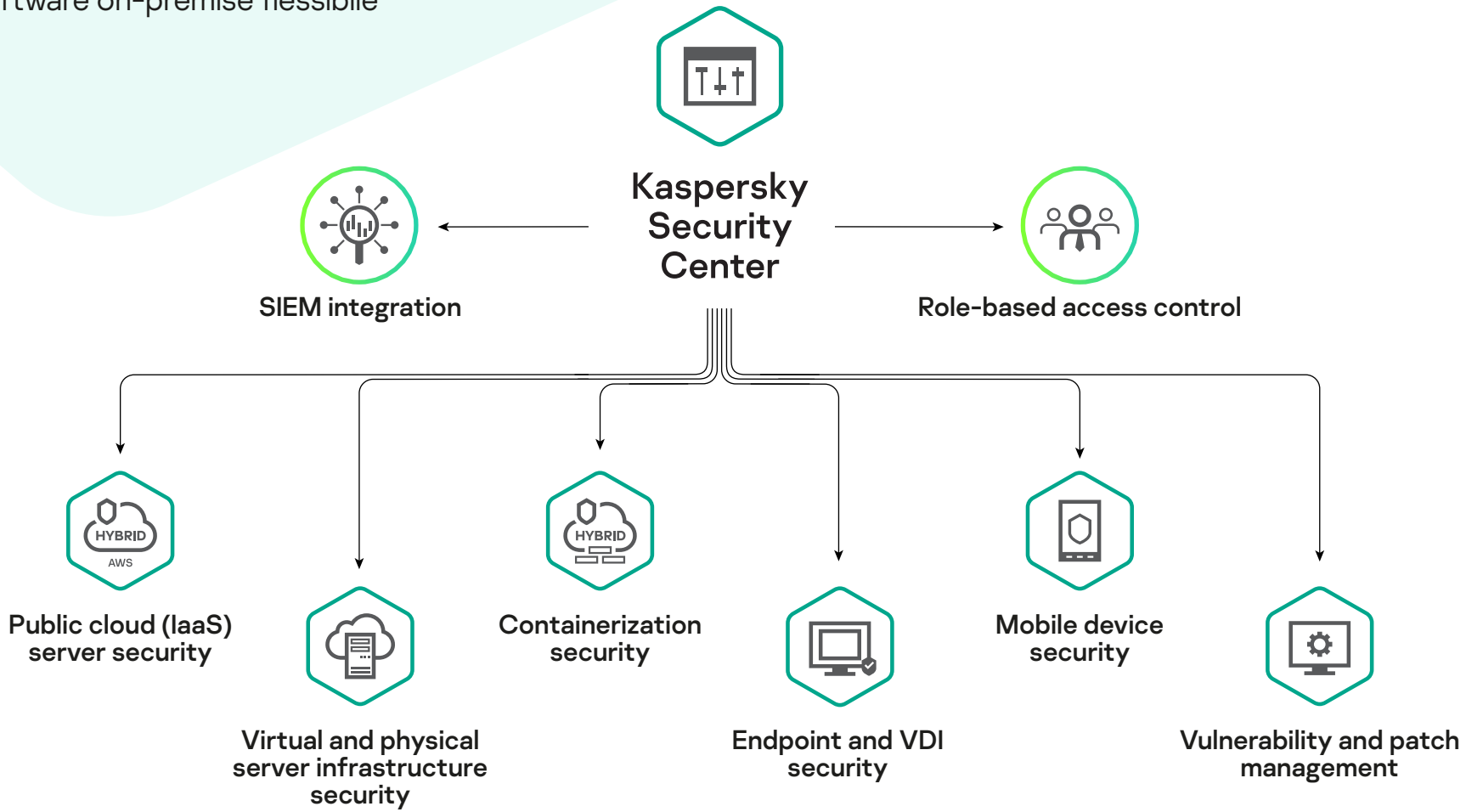
4 Personalizzazione e scalabilità

3 Livello di investimento

Singola console di gestione della sicurezza

Kaspersky Security Center per la gestione dei multiple workload e il controllo policy-based, fornito sotto forma di:

- Offerta SaaS scalabile
- Software on-premise flessibile



Kaspersky Premium Support (MSA)

Quando si verifica un incidente di sicurezza, il tempo impiegato per identificare la causa ed eliminarla è fondamentale. Rilevare e risolvere rapidamente un simile problema può far risparmiare alle aziende significative somme di denaro. I nostri pacchetti di assistenza Maintenance Service Agreement (MSA) sono specificamente concepiti per realizzare tale obiettivo. Accesso H 24 ai nostri esperti, prioritizzazione e contestualizzazione del problema, con tempi di risposta garantiti e patch private: tutto il necessario per assicurare che il problema sia risolto nel più breve tempo possibile.

È la soluzione ideale se il vostro obiettivo è:

- Avere la certezza che i vostri sistemi IT siano protetti non soltanto da tecnologie di sicurezza leader di settore, ma anche dalle competenze degli esperti Kaspersky

Vantaggi per l'azienda

- Assicura la business continuity grazie ad esperti dedicati, immediatamente disponibili a farsi carico del problema di sicurezza riscontrato e pronti a fornire la relativa soluzione nel più breve tempo possibile
- Significativa riduzione dei costi derivanti dall'incidente di sicurezza attraverso l'accesso a una linea di assistenza tecnica prioritaria, con tempi di risposta garantiti e disponibilità di patch private
- Un Technical Account Manager dedicato agisce in qualità di vostro rappresentante all'interno di Kaspersky; l'esperto in questione è autorizzato a mobilitare tutte le competenze necessarie per risolvere rapidamente il problema

Use case

- Risoluzione rapida delle criticità direttamente da parte di specialisti in grado di fornire, in tempi brevi, la soluzione più adeguata
- Protezione completa con misure proattive su misura per il vostro sistema
- Riduzione del tempo impiegato dalle risorse interne per la manutenzione e la risoluzione dei problemi

Kaspersky Professional Services

La sicurezza informatica è un investimento fondamentale. Potete ottenerne i massimi vantaggi collaborando con esperti che sanno esattamente come ottimizzare la soluzione di sicurezza per soddisfare pienamente le esigenze specifiche della vostra azienda. Operando secondo best practice e metodologie consolidate, i nostri esperti di sicurezza sono disponibili per assistervi in qualunque aspetto relativo a implementazione, configurazione e upgrade dei prodotti Kaspersky sull'intera infrastruttura IT aziendale.

È la soluzione ideale se il vostro obiettivo è:

- Ottimizzare e personalizzare la vostra soluzione Kaspersky per soddisfare le best practice di sicurezza informatica

1 Competenze richieste

5 Personalizzazione e scalabilità

3 Livello di investimento

Vantaggi per l'azienda

- Massimizzazione del ROI (ritorno sugli investimenti) delle soluzioni di sicurezza implementate, assicurando un livello di performance al 100% delle loro capacità
- Riduzione dei costi per il personale IT interno
- Riduzione minima dell'impatto esercitato dall'implementazione della nuova soluzione di sicurezza sulle attività aziendali quotidiane e riduzione dei costi complessivi di implementazione
- Gestione di qualsiasi problema critico in modo rapido ed efficace

Use case

- Riduzione dei rischi correlati a una tipologia di implementazione che può diminuire il livello di protezione, incidere negativamente sulla produttività aziendale e persino condurre a tempi di inattività
- Riduzione al minimo del rischio di tempi di inattività attraverso controlli periodici della configurazione dei prodotti, garantendo la presenza dei meccanismi di difesa più aggiornati
- Riduzione del periodo di "know-how" del prodotto, consentendo di trarre subito tutti i vantaggi

Stage 2
Optimum Security

Rilevamento avanzato e risposta centralizzata

Permette a piccoli team, dedicati alla sicurezza informatica, di affrontare le minacce in grado di eludere la prevenzione automatica, con una soluzione basata sulle risorse che si sviluppa a partire da Security Foundations

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response (EDR) Optimum supporta le organizzazioni, con competenze di base in materia di Cybersecurity, ad affrontare le minacce elusive. Include le funzionalità di protezione di Kaspersky Endpoint Security for Business Advanced ed è gestito da Kaspersky Security Center. Il prodotto fornisce un toolkit di facile utilizzo, basato sull'analisi semplificata delle cause principali, sulla scansione IoC (Indicator of Compromise) e sulle opzioni di risposta automatizzate o "in un solo clic".

È la soluzione ideale se il vostro obiettivo è:

- Aumentare la visibilità delle minacce su tutti gli endpoint
- Ridurre il tempo medio di risposta
- Ottimizzare le risorse di sicurezza IT e aumentare l'efficienza

3 Competenze richieste

4 Personalizzazione e scalabilità

3 Livello di investimento

Vantaggi per l'azienda

- Riduzione al minimo dei rischi a livello finanziario, reputazionale e di altro tipo associati alle minacce che eludono la protezione preventiva
- Ottimizzazione dei workload del personale e dell'utilizzo delle risorse attraverso un flusso di lavoro semplificato con funzionalità di automazione
- Potenziamento dell'efficienza con uno strumento accessibile e attento ai costi che non richiede competenze approfondite e tempi di apprendimento eccessivi

Use case

- Visibilità granulare degli avvisi di sicurezza degli endpoint
- Ulteriore analisi della minaccia rilevata nell'host per rivelarne l'entità e la root cause
- Possibilità di scoprire se si è sotto attacco analizzando gli IoC importati da terze parti
- Risposta automatica alle minacce in pochi clic al momento del rilevamento o durante le indagini

Kaspersky Managed Detection and Response Optimum

Kaspersky Managed Detection and Response Optimum offre una funzione di sicurezza IT completa, attraverso un'implementazione pronta all'uso rapida e scalabile che non richiede di investire in personale o competenze extra. I modelli brevettati di machine learning, l'intelligence sulle minacce costante ed esclusiva, nonché la ricerca delle minacce tramite indicatori di attacco (IoA) proprietari, assicurano una difesa costante dell'organizzazione da minacce complesse che utilizzano tattiche, tecniche e procedure note.

È la soluzione ideale se il vostro obiettivo è:

- Stabilire e migliorare la capacità di rilevare e rispondere tempestivamente ed efficacemente alle minacce attraverso un monitoraggio continuo 24 ore su 24, 7 giorni su 7
- Ridurre rapidamente la vulnerabilità dell'azienda alle minacce avanzate, senza richiedere al team di sicurezza di dedicare molto tempo per potenziare le proprie competenze e acquisire familiarità con le nuove soluzioni

Vantaggi per l'azienda

- Consapevolezza di essere costantemente protetti anche dalle minacce più avanzate
- Riduzione dei costi complessivi della sicurezza, senza la necessità di assumere e formare esperti di sicurezza informatica interni per affrontare le diverse eventualità.

Use case

- Approccio sistemico alla protezione prevenendo, rilevando, cercando e rispondendo automaticamente alle minacce che prendono di mira le vostre reti
- Reazione rapida agli incidenti, mantenendo il pieno controllo di tutte le azioni di risposta
- Visibilità completa in tempo reale su tutti i rilevamenti, le risorse coperte e il relativo stato di protezione corrente

2 Competenze richieste

5 Personalizzazione e scalabilità

4 Livello di investimento

Kaspersky Sandbox

Kaspersky Sandbox vi protegge automaticamente dalle minacce nuove e sconosciute, progettate per aggirare la protezione degli endpoint. È complementare a Kaspersky Endpoint Security for Business e aiuta le organizzazioni ad aumentare in modo significativo i livelli di protezione di endpoint e server contro minacce come malware sconosciuti, nuovi virus, ransomware ed exploit zero-day senza la necessità di assumere nuovo personale di sicurezza.

È la soluzione ideale se il vostro obiettivo è:

- Potenziare le difese contro le minacce elusive
- Automatizzare il rilevamento avanzato
- Ottimizzare i workload del personale e i requisiti relativi alle competenze

1 Competenze richieste

3 Personalizzazione e scalabilità

2 Livello di investimento

Vantaggi per l'azienda

- Riduzione dei rischi per la sicurezza IT e garanzia della business continuity
- Protezione dalle minacce nuove e sconosciute senza influire sulle performance degli endpoint o sulla produttività degli utenti
- Riduzione al minimo dei costi relativi alle operazioni manuali, automatizzando i task quotidiani
- Ottimizzazione dei costi per la protezione avanzata dalle minacce degli uffici remoti

Use case

- Semplificazione dell'analisi in-depth tramite il rilevamento delle minacce elusive e sconosciute
- Risposta automatica su tutti gli endpoint protetti
- Offload dell'analisi dei comportamenti che richiedono un'ampia quantità di risorse nella sandbox per non influire sulla produttività e potenziare la sicurezza degli endpoint sottoposti a un carico elevato
- Integrazione con soluzioni di terze parti tramite API
- Risparmio di tempo grazie alla semplice installazione e al funzionamento completamente automatico della sandbox, senza la necessità di competenze avanzate in ambito IT o di sicurezza informatica

Kaspersky Security per le aziende Enterprise

Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal riunisce tutte le conoscenze acquisite sulle minacce informatiche in un unico ed efficace servizio Web. Consente di controllare gli indicatori di minacce sospette, che si tratti di un file, di un hash file, di un indirizzo IP o di un'URL. Il portale analizza gli oggetti con una serie di tecnologie avanzate di rilevamento delle minacce come il rilevamento reputazionale tramite Kaspersky Security Network, modelli di machine learning strutturale e rilevamento dinamico avanzato mediante Kaspersky Cloud Sandbox che indica se un oggetto si trova nell'area "Good", "Bad" o "Not Categorized". I dati contestuali forniti consentono di stabilire le priorità e rispondere alle minacce in modo più efficace.

È la soluzione ideale se il vostro obiettivo è:

- Ottenere l'accesso gratuito a una fonte di intelligence sulle minacce
- Assegnare la priorità agli incidenti in modo più efficace
- Accelerare le indagini e il rilevamento delle minacce

Vantaggi per l'azienda

- Possibilità di adottare un'unica soluzione anche per l'intelligence sulle minacce
- Mantenimento efficace della protezione sulle reti tramite l'accesso immediato a dati sicuri e attendibili

Use case

- Convalida o definizione delle priorità per gli avvisi o gli incidenti che rappresentano una reale minaccia in base all'impatto e ai livelli di rischio
- Identificazione immediata degli avvisi che devono essere inoltrati al team di risposta agli incidenti
- Separazione delle minacce reali da quelle non effettive e individuazione della destinazione delle risorse limitate per la risposta agli incidenti
- Eliminazione della necessità di eseguire ricerche complicate in diversi database per trovare informazioni dettagliate su una particolare osservazione o su un determinato attacco
- Individuazione di minacce precedentemente non rilevate

3 Competenze richieste

4 Personalizzazione e scalabilità

0 Livello di investimento

Kaspersky Security Awareness

Kaspersky Security Awareness include una serie di prodotti di formazione computer-based basati sul gioco, definendo le competenze in materia di Cybersecurity dei dipendenti e motivandoli a mantenere comportamenti sicuri, a tutti i livelli della struttura organizzativa. La soluzione comprende:

- Kaspersky Interactive Protection Simulation & CyberSafety Management Games – per incentivare e motivare il coinvolgimento
- Gamified Assessment Tool – per definire il giusto starting point per il percorso di formazione più appropriato
- Online Learning Platform & Cybersecurity for IT Online – per acquisire competenze pratiche
- [Dis]connected – un gioco educativo per consolidare le nuove competenze acquisite.

È la soluzione ideale se il vostro obiettivo è:

- Ridurre il numero di incidenti causati dalla negligenza dei dipendenti
- Sviluppare una comprensione adeguata delle misure di sicurezza informatica per il personale, a tutti i livelli
- Sensibilizzare la sicurezza informatica all'interno dell'organizzazione con soluzioni pronte all'uso

2 Competenze richieste

4 Personalizzazione e scalabilità

3 Livello di investimento

Vantaggi per l'azienda

- Riduzione del numero di incidenti causati dagli attacchi di Social Engineering garantendo la business continuity e riducendo al minimo l'impatto di un incidente
- Coinvolgimento e motivazione delle persone
- Aumento della cultura sulla sicurezza informatica nell'organizzazione

Use case

- Adozione, da parte dei dipendenti, delle competenze e delle conoscenze necessarie per imparare a mantenere un comportamento sicuro
- Mantenimento di un atteggiamento corretto nei confronti dei problemi di sicurezza informatica
- Possibilità per i dipendenti di ottenere risultati migliori nei task quotidiani senza esporre l'azienda a rischi informatici

Stage 3
Expert Security

Reazione immediata ad attacchi complessi e APT

Difesa a 360 gradi, basata sull'intelligence delle minacce, guida degli esperti e trasferimento di competenze che permettono ai team di sicurezza IT esperti di affrontare minacce complesse e attacchi mirati.

Kaspersky Security per le aziende Enterprise

Kaspersky Endpoint Detection and Response

Un efficace strumento EDR, ricco di funzionalità per gli esperti di sicurezza IT che consente visibilità completa, rilevamento delle minacce a livello premium e la possibilità di analizzare in maniera approfondita gli eventi. Il vostro processo di indagine è alimentato da analisi retrospettive, indicatori di attacco (IoA) proprietari e mappatura MITRE ATT & CK, oltre che dalla ricerca proattiva delle minacce e dall'accesso a Kaspersky Threat Intelligence. Potrete scoprire l'intera sequenza di intrusione, comprendere la complessità degli attacchi basati su più fasi e rispondere in modo appropriato e veloce!

È la soluzione ideale se il vostro obiettivo è:

- Consolidare la protezione degli endpoint
- Migliorare ulteriormente le capacità interne di risposta agli incidenti, riducendo continuamente il tempo medio di rilevamento e risposta
- Potenziare le operazioni di ricerca proattiva delle minacce

4 Competenze richieste

3 Personalizzazione e scalabilità

4 Livello di investimento

Vantaggi per l'azienda

- Controllo sulle risorse più importanti
- Mitigazione del rischio informatico e riduzione dei danni finanziari e operativi causati dagli incidenti sugli endpoint
- Riduzione dei costi operativi associati alla sicurezza IT, semplificando l'analisi e la risposta agli incidenti
- Garanzia di conformità ai requisiti normativi

Use case

- Rilevamento efficace (con funzionalità comprovate attraverso la valutazione MITRE) e risposta rapida agli attacchi avanzati
- Esecuzione di analisi retrospettive e indagini efficaci sui dati aggregati a livello centralizzato
- Centralizzazione della gestione degli incidenti con indagini e risposte guidate
- Ricerca delle minacce nascoste, attraverso funzionalità automatizzate e proattive
- Kaspersky EDR fa parte di Kaspersky Anti Targeted Attack Platform, in un contesto di una soluzione Extended Detection and Response

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform combina il rilevamento delle minacce avanzato a livello di rete con funzionalità EDR, fungendo da soluzione Extended Detection and Response per fornire una protezione APT all-in-one basata sulla nostra intelligence sulle minacce e sul framework MITRE ATT&CK. I vostri specialisti di sicurezza IT dispongono di tutti gli strumenti necessari per gestire un rilevamento delle minacce multidimensionale di livello superiore, intraprendere indagini efficaci, cercare in modo proattivo le minacce e fornire una risposta rapida e centralizzata, attraverso un'unica soluzione.

È la soluzione ideale se il vostro obiettivo è:

- Estendere le difese contro gli attacchi più sofisticati attraverso un unico ed efficace sistema
- Ottenere una visibilità completa a livello aziendale
- Ridurre il tempo medio di rilevamento o risposta
- Arricchire il Security Operations Center
- Migliorare la strategia di sicurezza preservando la privacy

5 Competenze richieste

3 Personalizzazione e scalabilità

5 Livello di investimento

Vantaggi per l'azienda

- Mitigazione del rischio informatico e riduzione dei danni a livello finanziario, reputazionale e operativo causati da attacchi mirati complessi
- Riduzione dei costi operativi della sicurezza IT, semplificando e automatizzando i processi di gestione degli incidenti
- Garanzia di conformità ai requisiti normativi

Use case

- Protezione di più punti di ingresso da potenziali minacce a livello di rete ed endpoint
- Rilevamento rapido di minacce avanzate che eludono le tecnologie preventive esistenti
- Ricerca delle minacce nascoste, attraverso funzionalità automatizzate e proattive
- Informazioni tempestive sulle minacce rilevate per un'indagine più approfondita da parte dei team di sicurezza
- Risposta centralizzata agli incidenti complessi attraverso scenari automatizzati ad ampio raggio

Managed Detection and Response Expert

Affidate a Kaspersky i processi di selezione e indagine degli incidenti che richiedono di tempo e risorse. Tutte le caratteristiche e le funzionalità di Kaspersky Managed Detection and Response Optimum combinate con la ricerca gestita delle minacce che utilizzano tattiche, tecniche e procedure sconosciute. Accesso diretto agli analisti SOC di Kaspersky, fino a 3 mesi di retention dei dati non elaborati, accesso privilegiato a Kaspersky Threat Intelligence e un'API che consente l'integrazione con sistemi di ticketing di terze parti, riducendo in modo significativo la gestione dei flussi di lavoro.

È la soluzione ideale se il vostro obiettivo è:

- Sgravare il lavoro del team di sicurezza IT interno, che potrà concentrarsi sugli incidenti critici che ne richiedono effettivamente il coinvolgimento
- Migliorare ulteriormente l'efficienza del team di sicurezza, aumentando le best practice interne con l'esperienza consolidata di Kaspersky

Vantaggi per l'azienda

- Tutti i vantaggi di un Security Operations Center, senza la necessità di crearne uno proprio
- Massimo valore dalle soluzioni di sicurezza Kaspersky
- Riduzione dei costi di sicurezza complessivi e degli investimenti futuri, aumentando istantaneamente la capacità di sicurezza IT senza la necessità di formare personale specializzato internamente

Use case

- Rilevamente continuo, assegnazione delle priorità, funzioni di indagine e risposta su misura
- Consulenza con i nostri esperti per ottenere supporto su ogni tipo di minaccia, comprese le più recenti
- Possibilità di ricerca retrospettiva delle minacce utilizzando le funzionalità di Intelligence avanzata
- Potenziamento delle indagini sugli incidenti interrogando l'intera Knowledge Base di Kaspersky sulle minacce e sulle relative relazioni

2 Competenze richieste

5 Personalizzazione e scalabilità

5 Livello di investimento

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence fornisce un contesto ricco e significativo per tutto il ciclo di gestione degli incidenti. Le nostre informazioni esclusive e immediatamente fruibili possono essere fornite in diverse forme, supportando una perfetta integrazione con i flussi di lavoro di sicurezza esistenti. Il portfolio comprende: feed di intelligence sulle minacce, report specifici in base al settore e alla minaccia e un repository consultabile con petabyte di dati su minacce, oggetti legittimi e le relative relazioni.

È la soluzione ideale se il vostro obiettivo è:

- Ottimizzare le capacità di prevenzione e rilevamento
- Passare da una strategia di sicurezza reattiva ad una proattiva
- Migliorare il programma di intelligence sulle minacce
- Consentire un processo decisionale di sicurezza strategica più completo

Vantaggi per l'azienda

- Riduzione del turnover del personale addetto alla sicurezza IT, anticipando le necessità degli analisti
- Incremento dell'efficienza operativa in ambito di sicurezza, riducendo al minimo le interruzioni dell'attività e l'impatto degli incidenti
- Ottimizzazione del ROI ottimizzando l'investimento nella sicurezza IT con il panorama delle minacce specifico

Use case

- Incremento della sicurezza con dati sulle minacce informatiche continuamente aggiornati e machine-readable
- Miglioramento dell'assegnazione delle priorità agli avvisi, determinando quelli più critici che richiedono l'inoltro ai team di risposta agli incidenti
- Potenziamento delle indagini guidate, analizzando le relazioni tra le minacce rilevate
- Giustificazione del budget per la sicurezza IT, presentando scenari di rischio chiari e pertinenti

4 Competenze richieste

5 Personalizzazione e scalabilità

5 Livello di investimento

Kaspersky Cybersecurity Training

Lo sviluppo delle competenze è fondamentale per le aziende che devono far fronte a un volume crescente di minacce in continua evoluzione. Il personale addetto alla sicurezza IT deve essere esperto nelle tecniche di attacco avanzate, fondamentali per una gestione della sicurezza e nelle strategie di mitigazione, tra cui: il reverse engineering, la creazione di regole YARA e l'utilizzo di digital evidence. Il servizio Kaspersky Cybersecurity Training consente di trasferire al team di sicurezza interno tutte le conoscenze necessarie per affrontare al meglio il panorama delle minacce in costante evoluzione.

È la soluzione ideale se il vostro obiettivo è:

- Aumentare i livelli delle competenze interne in materia di sicurezza IT
- Consolidare l'operatività del Security Operations Center
- Sviluppare capacità interne di ricerca delle minacce

Vantaggi per l'azienda

- Miglioramento delle capacità del team SOC nella mitigazione di potenziali danni, causati da incidenti di sicurezza, in modo più rapido ed efficace
- Risparmio di tempo e denaro dedicati alla ricerca di personale competente che dovrà integrarsi nello scenario aziendale
- Mantenimento e motivazione del personale interno promuovendo lo sviluppo delle competenze.

Use case

- Miglioramento della risposta agli incidenti attraverso l'analisi del malware, per una piena comprensione della minaccia e una risposta più efficace
- Conservazione di log ed evidenze sui sistemi host o di rete per rivelare la root cause di un incidente e per prevenire incidenti simili in futuro evitando azioni legali
- Processi di risposta agli incidenti scalabili, rapidi ed efficaci per garantire la risoluzione ottimale di fronte a un'ampia gamma di minacce

4 Competenze richieste

3 Personalizzazione e scalabilità

4 Livello di investimento

Kaspersky Cybersecurity Services

Kaspersky Cybersecurity Services fornisce l'accesso illimitato all'esperienza di Kaspersky nella risposta agli incidenti di sicurezza delle informazioni, nell'individuazione di tentativi di compromissione passati e in corso, nonché nell'esecuzione di valutazioni di sicurezza a livello aziendale specifiche del settore per colmare le lacune di sicurezza prima che vengano sfruttate prevenendo attacchi futuri. La collaborazione con gli esperti di Kaspersky consente ai team di sicurezza IT interni di ottenere una maggiore efficienza nella lotta a minacce sempre più sofisticate.

È la soluzione ideale se il vostro obiettivo è:

- Avere un partner esperto in grado di intervenire in caso di incidente
- Verificare che i sistemi di rilevamento e prevenzione esistenti siano adeguati
- Adottare un approccio proattivo alla sicurezza

Vantaggi per l'azienda

- I danni causati dagli incidenti, per quanto complessi, vengono ridotti al minimo grazie all'accesso continuo a solide competenze in materia di sicurezza IT
- Riduzione significativa dei potenziali costi per i tempi di inattività
- Supporto conforme alle normative, al fine di evitare sanzioni e multe

Use case

- Ripristino rapido ed efficace dei sistemi e delle attività aziendali
- Rilevamento dei tentativi di compromissione e mitigazione dell'impatto degli incidenti prima che diventi evidente
- Miglioramento della sicurezza delle infrastrutture specifiche del settore
- Valutazione delle capacità di difesa e individuazione dei punti deboli che dovranno essere sanati

3 Competenze richieste

5 Personalizzazione e scalabilità

4 Livello di investimento

Kaspersky Private Security Network

Kaspersky Private Security Network consente alle aziende di sfruttare la maggior parte dei vantaggi della Threat Intelligence globale, basata su cloud, senza divulgare alcun dato al di fuori del perimetro controllato. Si tratta, per l'organizzazione, di una versione di Kaspersky Security Network personale, locale e completamente privata.

È la soluzione ideale se il vostro obiettivo è:

- Proteggere un'azienda attenta alla privacy, con criteri rigorosi relativamente all'uscita dei dati dai confini dell'infrastruttura IT
- Soddisfare le più severe normative sulla protezione dei dati
- Facilitare la circolazione dell'intelligence sulle minacce all'interno dell'organizzazione per rafforzare la protezione e accelerare i tempi di risposta

Vantaggi per l'azienda

- Supporto della business continuity attraverso un rilevamento e una risposta efficienti, supportati dalla condivisione interna delle informazioni
- Aumento dell'efficienza operativa riducendo il più possibile i falsi positivi
- Piena conformità ai requisiti normativi inerenti alla sicurezza di sistemi e ambienti isolati

Use case

- Protezione dell'infrastruttura isolata, anche air gap, senza compromettere l'efficacia del rilevamento delle minacce
- Organizzazione efficace per lo scambio di dati sulle minacce
- Integrazione delle soluzioni Kaspersky, per il rilevamento avanzato delle minacce esistenti, con qualsiasi altra soluzione B2B Kaspersky tramite la rete di intelligence sulle minacce interna

5 Competenze richieste

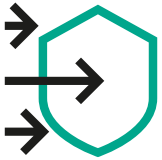
5 Personalizzazione e scalabilità

5 Livello di investimento

Aspetti da tenere in considerazione quando si definisce una strategia di Cybersecurity a lungo termine

Un approccio "isolato" alla sicurezza informatica mette a rischio le aziende

I costi crescenti causati da violazioni della rete aziendale e data breach generano forti pressioni finanziarie sulle imprese che intendono attuare la digital transformation, questo è il motivo per cui la sicurezza informatica rappresenta una problematica così rilevante. Per ottenere risultati soddisfacenti le aziende devono rendere la Cybersecurity parte integrante della strategia complessiva dell'impresa, affinché svolga un ruolo chiave nella gestione dei rischi e nella pianificazione a lungo termine.



La sicurezza informatica non è un punto di arrivo, è una continua evoluzione

Il piano di sicurezza di un'azienda deve essere regolarmente rivisto e adeguato alle nuove conoscenze e ai nuovi strumenti. Si dovrebbe sottoporre ad analisi approfondita ogni singolo incidente di sicurezza, con lo scopo di creare nuove procedure e nuove misure di gestione dell'attacco, prevenendo incidenti simili in futuro. Le difese esistenti devono essere continuamente migliorate.

Awareness, comunicazione e cooperazione sono la chiave per il successo in un mondo di cyberminacce in rapida e continua evoluzione

Oltre l'80% di tutti gli incidenti informatici è riconducibile a errori umani. Si rivela pertanto di vitale importanza la formazione del personale ad ogni livello, al fine di accrescere la security awareness all'interno dell'organizzazione e fornire le giuste motivazioni a tutti i dipendenti affinché prestino la dovuta attenzione alle minacce informatiche e alle contromisure da intraprendere, nonostante ritengano che ciò non faccia parte delle loro responsabilità in ambito lavorativo.

Un approccio mentale proattivo, di tipo "rilevamento e risposta", è il modo migliore per contrastare le attuali minacce IT, in continua evoluzione

I sistemi di prevenzione tradizionali dovrebbero agire in piena armonia con le nuove tecnologie di rilevamento avanzato, con l'analisi delle minacce, con le attuali capacità di risposta e con le tecniche predittive per la sicurezza. Questo aiuta a creare un sistema di Cybersecurity in grado di adattarsi continuamente e rispondere in modo puntuale alle nuove sfide che affrontano le aziende.

Perché scegliere Kaspersky

La più testata. La più premiata

Kaspersky ha ottenuto più primi posti in test indipendenti rispetto a qualsiasi altro vendor di sicurezza.
I riconoscimenti continuano ad arrivare anno dopo anno.
www.kaspersky.com/top3

Il logo GARTNER PEER INSIGHTS CUSTOMERS' CHOICE è un marchio commerciale e un marchio di servizio di Gartner, Inc. e/o delle relative affiliate ed è usato nel presente documento con autorizzazione. Tutti i diritti riservati. I premi Gartner Peer Insights Customers' Choice vengono attribuiti sulla base di opinioni soggettive dei singoli utenti finali espresse in recensioni, valutazioni e dati applicati secondo una metodologia documentata; non rappresentano le opinioni di, né equivalgono all'approvazione di, Gartner o delle relative affiliate.

Kaspersky è stata ancora una volta nominata Customers' Choice for Endpoint Protection Platforms da Gartner Peer Insights.

Kaspersky ha ottenuto il riconoscimento Customers' Choice in 'Gartner Peer Insights 'Voice of the Customer': EDR Solutions'

Kaspersky è stata nominata Gartner Peer Insights Customer's Choice of 2020 per le soluzioni Secure Web Gateway

Proven.
Transparent.
Independent.

Qualità Kaspersky confermata dalla valutazione MITRE ATT&CK

MITRE | ATT&CK®

Massima trasparenza

Con l'attivazione del nostro primo Transparency Center, l'elaborazione dei dati statistici viene eseguita in Svizzera e la loro riservatezza è garantita. Nessun altro vendor può assicurare un tale livello di privacy.

kaspersky