



# La risposta alla mitigazione del rischio della cybersecurity in un'era di trasformazione digitale

**La trasformazione digitale è fondamentale per la crescita aziendale e l'efficacia istituzionale in tutto il mondo. Tuttavia, mettere in sicurezza l'infrastruttura dell'organizzazione digitale rappresenta una sfida notevole. Le minacce avanzate e gli attacchi mirati agli elementi della rete unici, nascosti e inerti fino a quando non vengono attivati, si aggiungono ai fattori di rischio che circondano la trasformazione digitale, mettendo a repentaglio la crescita aziendale e le iniziative di sviluppo. Mentre le tecniche utilizzate dai criminali informatici si evolvono costantemente e si concentrano sempre più su ambienti mirati, troppe organizzazioni si affidano ancora alle tecnologie di sicurezza convenzionali per proteggersi dalle minacce attuali e future.**

## Trasformazione digitale: un nuovo ruolo per la cybersecurity

La cybersecurity, insieme alla conformità e all'utilizzo dei dati, è diventata una priorità strategica fondamentale per le attività digitali. Le organizzazioni sono alla ricerca di approcci per la sicurezza che facilitino una maggiore attenzione alle esigenze aziendali.

### Nuove sfide per le imprese:

- Elevato volume di attività manuali necessario per la risposta agli incidenti
- Il personale del team responsabile della sicurezza IT è insufficiente e mancano competenze di alto livello
- Troppi eventi di sicurezza da elaborare, analizzare, smistare e a cui rispondere efficacemente entro un periodo di tempo limitato
- Problemi di fiducia e di condivisione dei dati sulla conformità, di pari passo con l'ampliamento dell'infrastruttura digitale
- Mancanza di visibilità e difficoltà di raccolta delle prove per l'analisi successiva alla violazione

### Vantaggi per l'azienda

- Riduzione dell'entità dei danni finanziari e operativi causati dal cybercrimine
- Riduzione della complessità attraverso un'interfaccia di gestione semplice e orientata al business
- Riduzione dei costi amministrativi grazie all'automazione delle attività e alla semplificazione dei processi di conformità con la sicurezza
- Incremento del ROI attraverso l'automazione dei flussi di lavoro, senza alcuna interruzione della business continuity e dei processi aziendali
- Rischio mitigato dalle minacce avanzate grazie al rilevamento rapido

## Una soluzione unificata per accelerare la trasformazione digitale

Kaspersky Threat Management and Defense include una combinazione unica di tecnologie di sicurezza leader nel settore e di supporto e servizi di cybersecurity che si adattano notevolmente alle specifiche della singola organizzazione e adottano un approccio strategico, fornendo processi unificati per la protezione contro le minacce avanzate e gli attacchi mirati unici.



### Prodotti

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Endpoint Security for Business
- Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky (Private) Security Network

### Servizi

- Kaspersky Cybersecurity Training
- Portale Kaspersky Threat Intelligence
- Kaspersky Managed Detection and Response
- Kaspersky Incident Response

### Assistenza

- Kaspersky Maintenance Service Agreement
- Kaspersky Security Account Manager
- Kaspersky Professional Services

Comprovata come la soluzione  
più efficace del settore



Gartner Peer Insights  
**Customers' Choice**  
per le soluzioni  
**Endpoint Detection &  
Response, 2020**

**MITRE | ATT&CK®**

Qualità di rilevamento confermata  
dalla valutazione MITRE ATT&CK



Breach Response Test  
di SE Labs: **Premi AAA**



Advanced Threat  
Defense Test di ICSA  
Labs (terzo trimestre  
2019): **percentuali  
di rilevamento del  
100%, con zero falsi  
positivi**



**Top Player nel report Radicati APT  
Protection Market Quadrant 2020**

## Il giusto equilibrio tra tecnologie e servizi

Per potenziare le competenze dei team, Kaspersky offre anche un'ampia gamma di programmi formativi, nonché dati di Threat Intelligence con cui arricchire i risultati delle investigation. Grazie al nostro servizio Managed Detection and Response, le risorse di sicurezza IT possono essere preservate trasferendo a noi i task di elaborazione degli incidenti oppure richiedendo a Kaspersky valutazioni esperte e competenze esclusive per la ricerca delle minacce. Qualunque siano le esigenze di sicurezza della vostra azienda, oggi o in futuro, abbiamo la soluzione che fa per voi.

### Difese potenziate ampliando le prospettive

Kaspersky Anti Targeted Attack Platform basato su Kaspersky EDR protegge i molteplici più punti di ingresso sia a livello di rete che di endpoint e offre funzionalità estese di rilevamento e risposta. L'esperto di sicurezza IT può fare affidamento su un toolkit completo per la discovery multilivello delle minacce, un'investigation approfondita, un threat hunting proattivo e un incident response centralizzata per attacchi complessi. Si integra perfettamente con Kaspersky Endpoint Security for Business e condivide un singolo agente con Kaspersky EDR, Kaspersky Hybrid Cloud Security e con Kaspersky Security for Mail Server e Kaspersky Security for Internet Gateway per fornire risposte automatizzate a livello di gateway. La struttura all-in-one di questa soluzione riduce in modo significativo il tempo che i team di sicurezza IT devono dedicare alla protezione, grazie all'automazione delle difese a livello di rete e di endpoint e alla rappresentazione contestuale degli incidenti in un'unica console web.

### Una soluzione di sicurezza affidabile che fornisce completa privacy

Per le aziende con rigidi criteri di privacy, l'analisi degli oggetti viene eseguita in loco senza flusso di dati in uscita tramite l'integrazione con Kaspersky Private Security Network. In questo modo si ottengono aggiornamenti in tempo reale della reputazione in entrata, preservando al contempo il completo isolamento dei dati aziendali.

### Potenziamento dei team SOC

Per contrastare le minacce informatiche più sofisticate e adattarsi alle sfide legate a un ambiente in continua evoluzione, i team SOC devono poter contare su tecnologie avanzate, potenziate da Threat Intelligence e personale dotato di tutte le competenze necessarie. Il risultato è un insieme di difese dagli attacchi ATP più complessi e da campagne mirate. Kaspersky Threat Management and Defense offre un arsenale completo di tecnologie e servizi avanzati per potenziare l'efficacia del vostro SOC.

### Kaspersky Managed Detection and Response

Se siete alla ricerca di competenze complete nella ricerca delle minacce, potete ampliare le vostre risorse con le skill e l'esperienza dei nostri rilevatori di minacce, i quali:

- Analizzeranno i dati raccolti nel vostro ambiente
- Notificheranno rapidamente al team responsabile della sicurezza aziendale eventuali rilevamenti di attività dannose
- Forniranno consigli su come rispondere all'incidente e risolvere la problematica

Novità sulle minacce informatiche: [www.securelist.it](http://www.securelist.it)  
IT Security News:  
<https://www.kaspersky.it/blog/category/business/>  
Sicurezza IT per piccole e medie imprese:  
[www.kaspersky.it/small-to-medium-business-security](http://www.kaspersky.it/small-to-medium-business-security)  
Sicurezza IT per le aziende Enterprise:  
[kaspersky.it/enterprise-security](http://kaspersky.it/enterprise-security)

**www.kaspersky.it**

2020 AO Kaspersky Lab.  
I marchi registrati e i marchi di servizio appartengono  
ai rispettivi proprietari.



Offriamo tecnologie di protezione comprovate. Siamo indipendenti. Siamo trasparenti. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia possa migliorare le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Soluzioni di Cybersecurity Kaspersky, per un futuro più sicuro.

Per saperne di più:  
[www.kaspersky.it/about/transparency](http://www.kaspersky.it/about/transparency)



**Proven.  
Transparent.  
Independent.**