

Cybersecurity per le piccole e medie imprese

Cosa rende più forte la vostra azienda in crescita

Il 43%* degli attacchi colpisce le PMI

≈ \$70 000*

Da 1 settimana a 6 mesi

Possibili tempi di inattività



Il costo medio di un incidente (perdita di dati, phishing, ransomware, frode, danni alla reputazione)

Cosa sta succedendo e perché è importante per la vostra azienda

Le piattaforme cloud, il lavoro da remoto, i dispositivi mobili, gli strumenti e i servizi online e l'automazione basata sull'intelligenza artificiale semplificano molti aspetti delle operazioni quotidiane, ma ne aumentano anche la complessità e rendono più difficile garantire la sicurezza dei sistemi.



Più strumenti, più punti di accesso

Ogni nuovo servizio apre un'altra potenziale porta d'accesso alla vostra attività



Staff e tempo limitato

I piccoli team IT non possono monitorare tutto, in ogni momento



Lavoro al di fuori del controllo aziendale

L'utilizzo di account e dispositivi personali per lavoro sottrae i dati alla protezione ed espone l'azienda a potenziali sanzioni.



Più attacchi alimentati dall'IA

L'intelligenza artificiale consente attacchi di phishing e furti di password automatizzati a basso costo e su larga scala

Tutti questi fattori minacciano la continuità e la crescita aziendale, portando a:

- potenziali perdite finanziarie,
- violazione dei dati,
- e danni alla reputazione.

Cosa mette a rischio la vostra azienda, dentro e fuori

La maggior parte degli incidenti informatici non inizia con qualcosa di drammatico. Parte da situazioni quotidiane e sfide attuali.

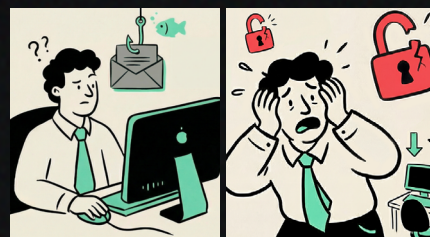
Rischi interni ed esterni



Ransomware



Le operazioni si arrestano completamente



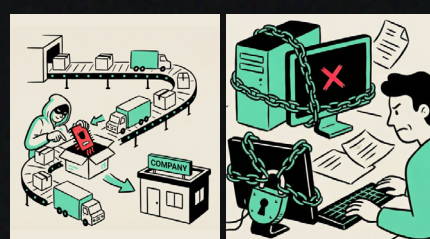
Social engineering

Credenziali rubate, interruzione dell'attività aziendale



Malware e attacchi fileless

Furto di dati, sistemi instabili



Attacchi alla supply chain

Disagi per i clienti e conseguente perdita di fiducia

sfide



Rapida crescita del settore IT

La sicurezza non riesce a stare al passo



Carenza di competenze nella gestione degli incidenti

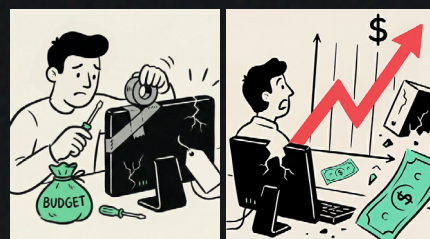
Le decisioni sbagliate peggiorano le situazioni



IT sovraccarico



Minacce non rilevate e risposte ritardate



Budget limitato



Costi di recupero più elevati in seguito

In che modo Kaspersky affronta minacce e sfide


Kaspersky Next
EDR Foundations


Kaspersky
Next EDR
Optimum


Kaspersky
Next XDR
Optimum


Kaspersky Next
MXDR Optimum

	Malware + <i>Minacce comuni</i>	●	●	●	●
	Ransomware	●	●	●	●
	Attacchi fileless	●	●	●	●
	Phishing	●	●	●	●
	Malware sconosciuto <i>Nuove e mirate</i>		●	●	●
	Errore umano		●	●	●
	Terze parti non controllate		●	●	●
	Social engineering			●	●
	Movimento laterale			●	●
	Mancanza di risorse				●
	Business continuity				●

Servizio gestito dagli
esperti di Kaspersky

Cosa significa per voi una sicurezza affidabile

Protezione automatizzata dalle minacce

Protezione integrata contro le minacce di massa, che riduce la necessità di intervento manuale

Minor carico di lavoro per l'IT

Meno attività manuali, meno errori, più tempo per ciò che conta davvero: grazie alla distribuzione semplificata basata sul cloud.

Rilevamento tempestivo delle minacce

Fermate le minacce elusive prima che si trasformino in incidenti

Ripristino rapido in caso di problemi

Meno tempi di inattività significano maggiore stabilità aziendale e minori perdite di fatturato

Protezione contro le tecniche di social engineering

Formazione sulla sicurezza informatica che aiuta i dipendenti a individuare truffe, phishing e manipolazioni

Sicurezza professionale senza bisogno di creare un team

Una protezione efficace senza i costi e le complicazioni derivanti dall'assunzione di specialisti.

Mantenete il ritmo: crescete con fiducia



Pronti per una sicurezza cloud-native pensata su misura per voi?

Ottenete una protezione efficace fin dal primo giorno

Contatti

www.kaspersky.it

© 2026 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio
appartengono ai rispettivi proprietari.