

# Kaspersky Next

Sicurezza all'avanguardia

**Chi siamo**



Siamo un'azienda internazionale che si occupa di cybersecurity



Operiamo in

200

paesi e territori



34

Uffici regionali di rappresentanza



**Nord America**  
Messico  
Stati Uniti

**Sud America**  
Brasile

**Africa**  
Sudafrica

**Australia**

**Europa**  
Austria  
Repubblica Ceca  
Danimarca  
Francia  
Germania  
Israele  
Italia  
Paesi Bassi  
Polonia  
Portogallo  
Romania  
Russia (HQ)  
Spagna  
Svizzera  
Regno Unito

**Asia**  
Cina  
Hong Kong  
India  
Giappone  
Kazakistan  
Malaysia  
Singapore  
Corea del Sud  
Turchia  
EAU

**Centri di trasparenza**  
Zurigo, Svizzera  
Madrid, Spagna  
San Paolo, Brasile  
Kuala Lumpur, Malaysia

# Clienti protetti in ogni settore



>250,000

Clienti corporate in tutto il mondo



> 400.000.000

Utenti protetti in tutto il mondo

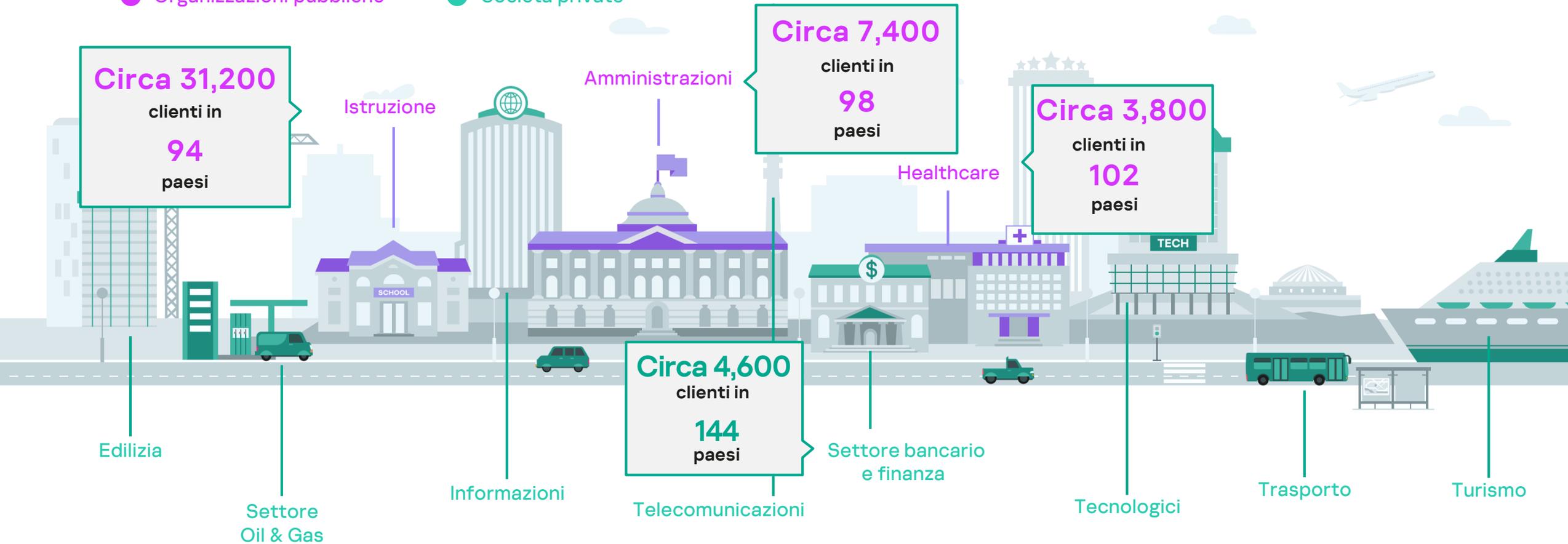


L'80%

Delle nostre operazioni è su scala internazionale

● Organizzazioni pubbliche

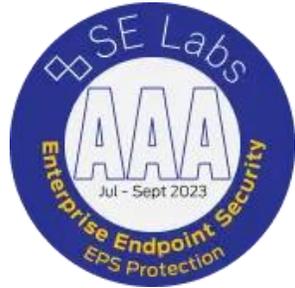
● Società private



# Scegliete Kaspersky come partner di cybersecurity di fiducia



Per saperne di più



Per saperne di più



Per saperne di più



Per saperne di più



Per saperne di più



Per saperne di più

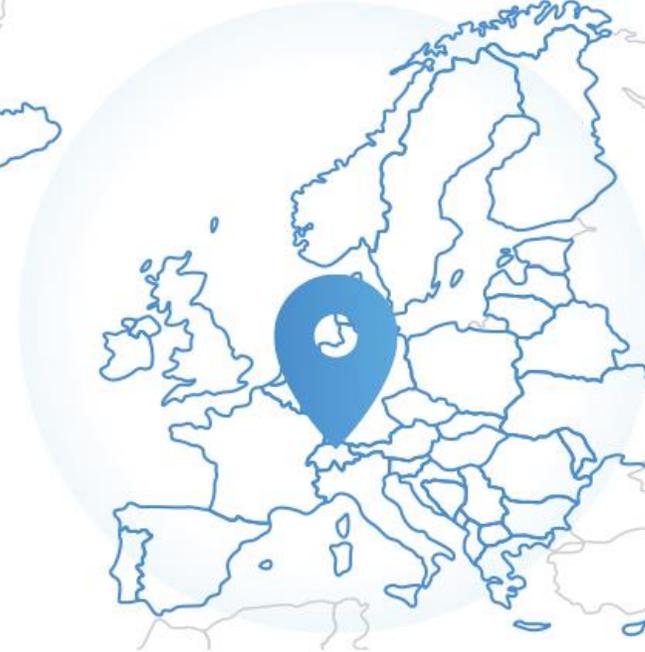


Per saperne di più



Per saperne di più

## DATA STORAGE AND PROCESSING IN SWITZERLAND



### Protezione dei dati

Elaborazione dei dati legati alle cyberminacce e archiviazione in Svizzera per:

- Europa
- US
- Canada
- America Latina
- Medio Oriente
- APAC

### Trasparenza

Codice sorgente, aggiornamenti e documentazione sono disponibili per la consultazione nei nostri

- Transparency Center:
- Zurigo, Svizzera
  - Madrid, Spagna
  - Kuala Lumpur, Malaysia
  - San Paolo, Brasile
  - ...e altri 7!

### Integrità e sicurezza

Abbiamo completato le seguenti revisioni indipendenti:

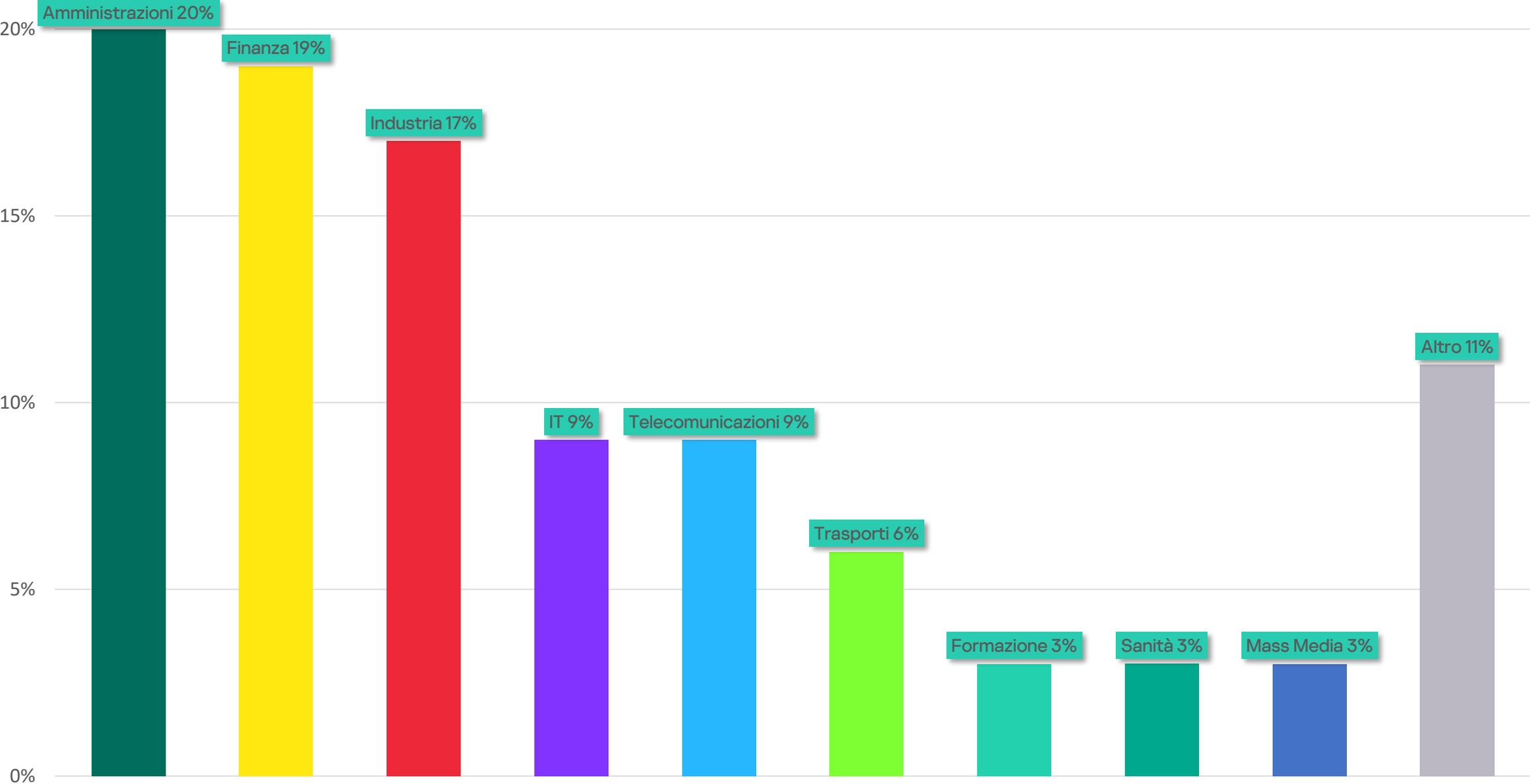
- Controllo SOC2
- Certificazione ISO 27001

[www.kaspersky.com/transparency-center](http://www.kaspersky.com/transparency-center)

# Lo stato della cybersecurity

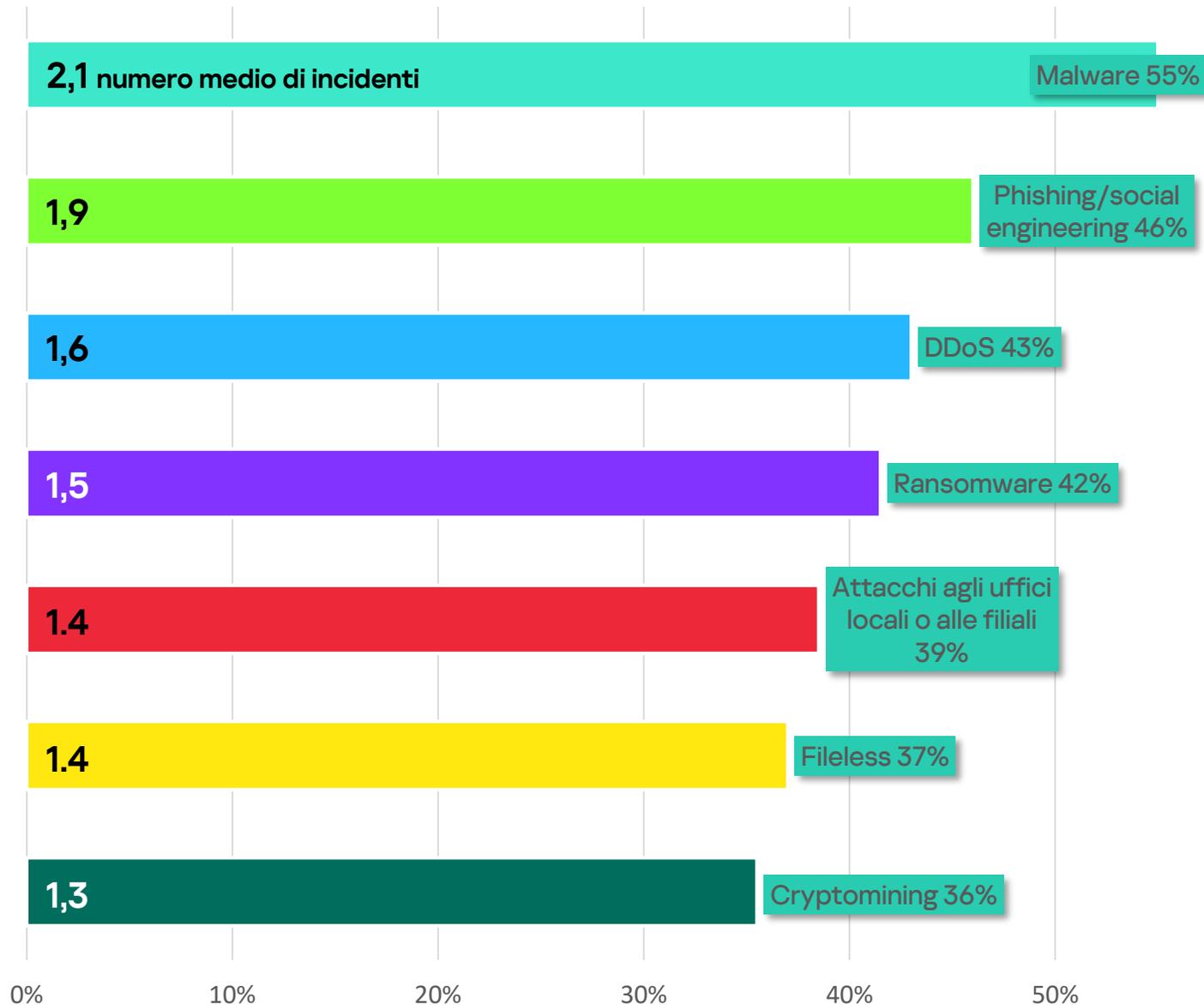
# Tutti vengono attaccati

Fonte: [Incident response analyst report, Kaspersky, 2022](#)



# Una continua raffica di attacchi

Fonte: IT Security Economics 2022, Kaspersky, 2022



In media, dovrete gestire circa

# 4,7

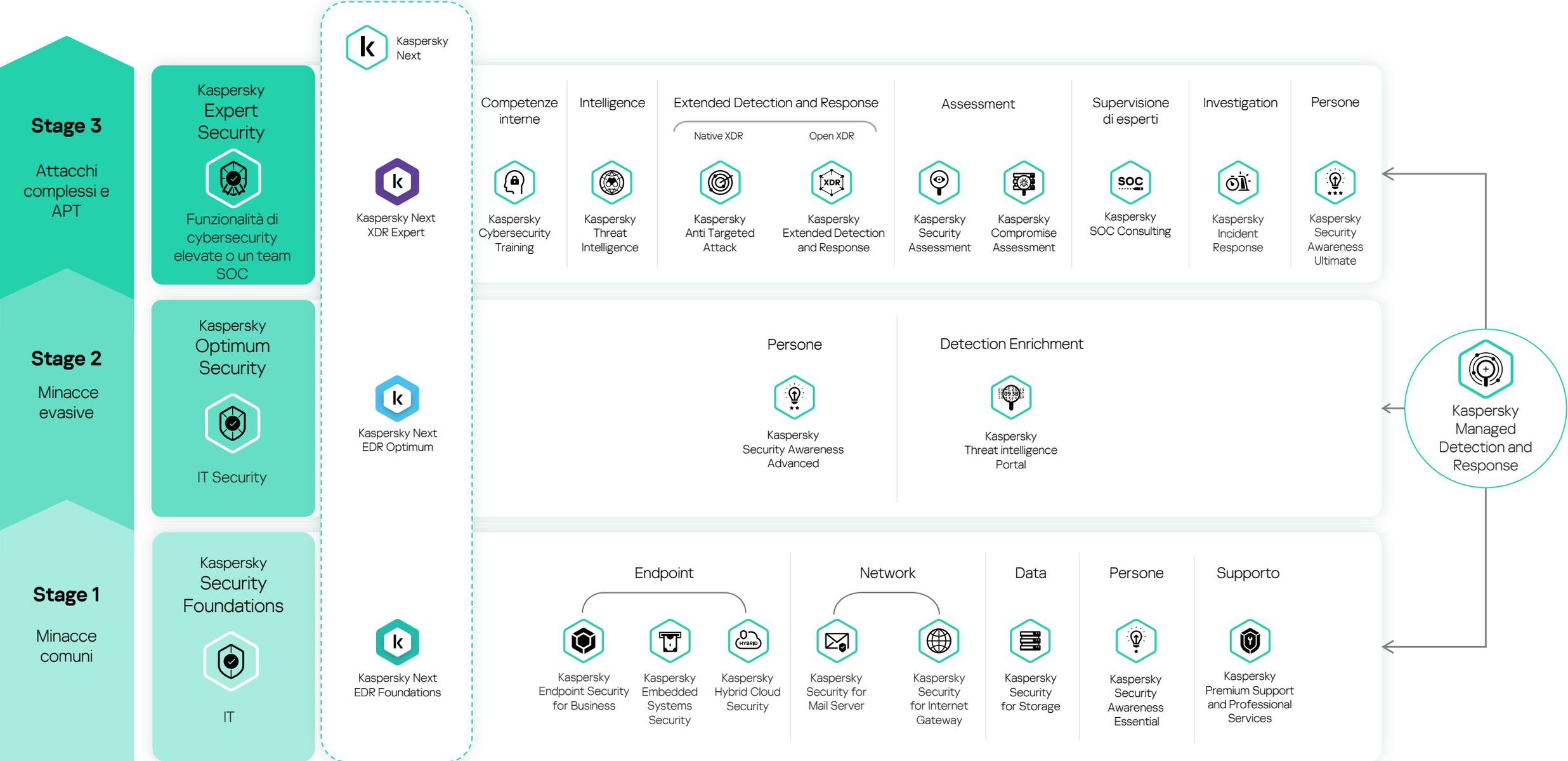
incidenti all'anno

Fonte: SOC Modernization and the Role of XDR, Enterprise Security Group, 2022



**Che cos'è  
Kaspersky  
Next?**

# L'approccio passo-passo di Kaspersky





## Kaspersky Next



### Kaspersky Next EDR Foundations

#### Solida sicurezza per tutti

Proteggi tutti gli endpoint

#### Se occorrono

- Efficiente protezione degli endpoint
- Controlli della sicurezza di base
- Massima automazione



### Kaspersky Next EDR Optimum

#### Create le vostre difese

Aumentate la sicurezza con investigation e response essenziali

#### Se occorrono

- Ottimizzate le capacità di risposta e la visibilità
- Sicurezza cloud aumentata
- Controlli di livello enterprise



### Kaspersky Next XDR Expert

#### Equipaggiate i vostri esperti

Proteggete la vostra azienda dalle minacce più avanzate e complesse

#### Se occorrono

- Rilevamento delle minacce avanzate
- Integrazione seamless
- Potenti strumenti di threat hunting



**Kaspersky Next  
EDR Foundations**

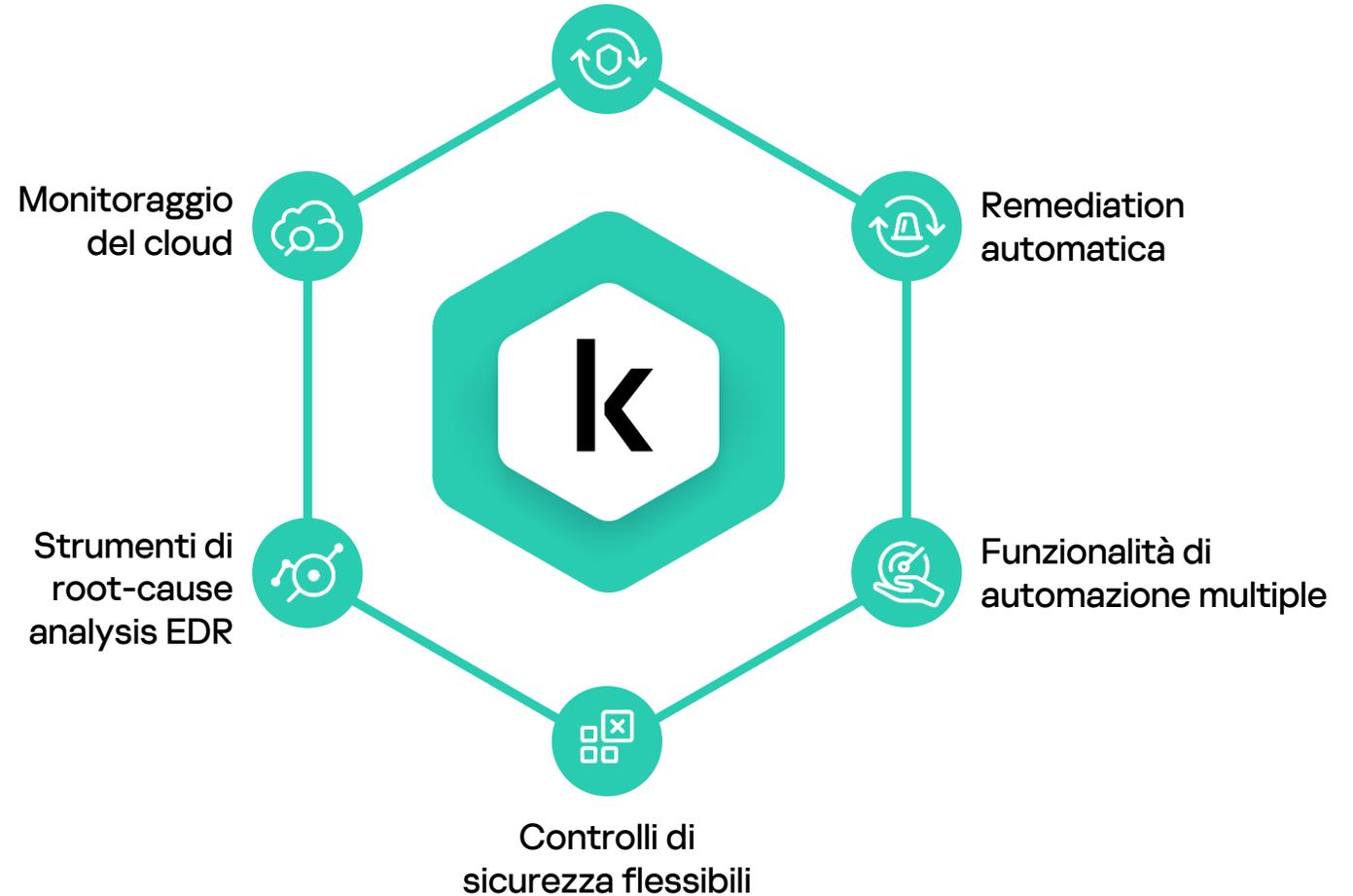
## Sicurezza robusta per tutti

Proteggi tutti gli endpoint

### Se occorrono...

- Efficiente protezione degli endpoint
- Controlli di sicurezza standard
- Massima automazione

Protezione degli endpoint  
potente e basata su machine learning





**Kaspersky Next  
EDR Optimum**

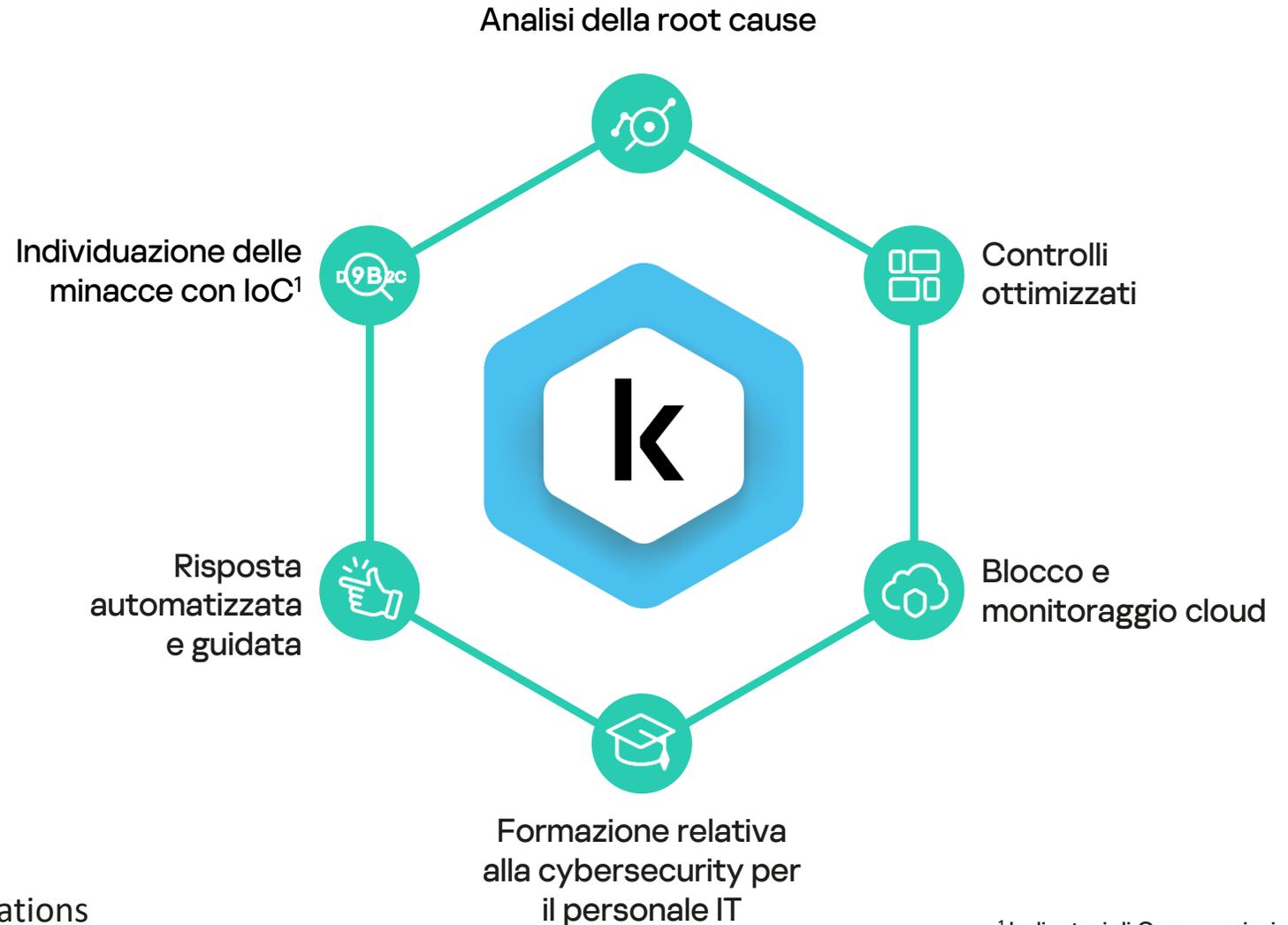
## Create le vostre difese

Aumentate la sicurezza con investigation e response essenziali

### Se occorrono...

- Ottimizzate le capacità di risposta e la visibilità
- Sicurezza cloud aumentata
- Controlli di livello Enterprise

Include  
le funzionalità di Kaspersky Next EDR Foundations



<sup>1</sup> Indicatori di Compromissione



**Kaspersky Next  
XDR Expert**

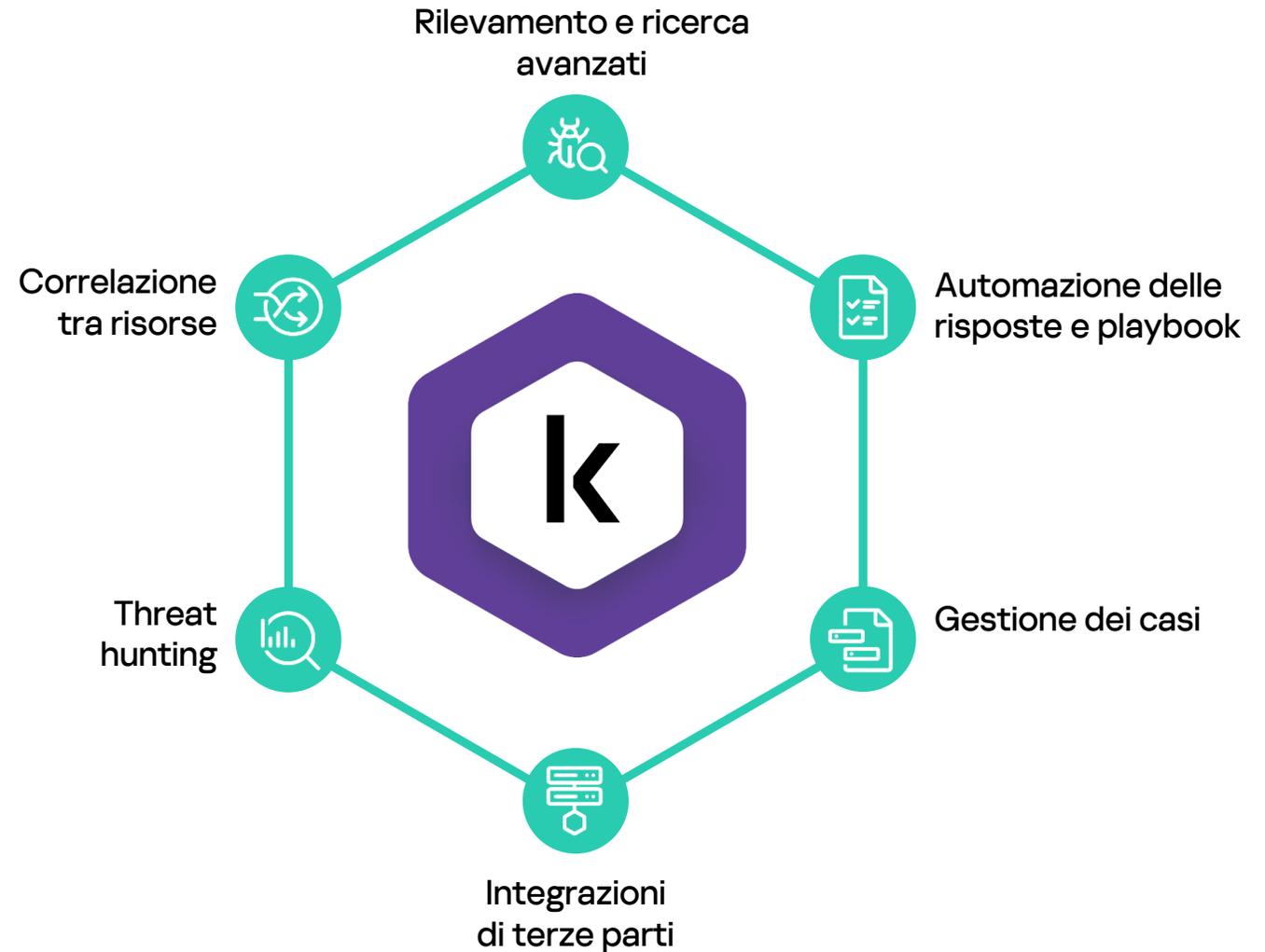
## Equipaggiate i vostri esperti

Proteggete la vostra azienda dalle minacce più avanzate e complesse

### Se occorrono

- Rilevamento delle minacce avanzate
- Integrazione seamless
- Potenti strumenti di threat hunting

Include  
le funzionalità di Kaspersky Next EDR Optimum



# Confronto dei livelli

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
<b>Protezione endpoint</b> Anti-Virus File, Anti-Virus Web e Anti-Virus Posta, protezione di rete, AMSI, Prevenzione degli exploit, Remediation, rilevamento del comportamento, HIPS	✓	✓	✓
<b>Gestione della sicurezza</b> Firewall, controlli di applicazioni, dispositivi e Web, Cloud Discovery	✓	✓	✓
<b>Gestione e protezione dei device mobili</b> Protezione, controlli e gestione	✓	✓	✓
<b>Scenari IT</b> Valutazione vulnerabilità, gestione patch, cancellazione dei dati, inventario software/hardware, installazione sistema operativo e app di terze parti, connessione remota	✗ valutazione vulnerabilità, inventario software/hardware	✓	✓
<b>Encryption</b> Cifratura e gestione della cifratura		✓	✓
<b>Protezione Cloud</b> Cloud Discovery, sicurezza per MS O365, Data Discovery	✗ solo Cloud Discovery	✓	✓
<b>Formazione</b> Formazione relativa alla cybersecurity per gli amministratori IT		✓	✓
<b>Funzionalità EDR essenziali</b> Root Cause Analysis, scansione IoC, risposta endpoint	✗ solo Root-Cause Analysis	✓	✓
<b>Funzionalità EDR avanzate</b> Raccolta dei dati di telemetria, ricerca delle minacce, rilevamento IoA (Indicatore di attacco), mappatura MITRE ATT&Ck			✓
<b>Funzionalità XDR essenziali</b> Aggregazione degli avvisi, gestione dei casi, sandbox, integrazione AD, integrazione TI			✓
<b>Funzionalità XDR avanzate</b> Correlazione incrociata, connettori di terze parti, playbook, grafico di indagine, gestione dei log e data lake			✓

Fate riferimento agli elenchi delle funzionalità del prodotto per la disponibilità di funzionalità specifiche nel tipo di console prescelto.

## Visualizzazione Pro

Simile alla console Kaspersky Business Hub

## Visualizzazione Expert

Simile alla console Kaspersky Security Center

	Kaspersky Next EDR Optimum	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
Gestione tramite cloud <b>Visualizzazione Pro</b> Numero massimo di utenti = 2.500	✓	✓	-
Gestione tramite cloud <b>Visualizzazione Expert</b> Numero minimo di utenti = 300	✓*	✓	-
On premises. <b>Visualizzazione Expert</b>	✓	✓	✓

\* La visualizzazione Pro è consigliata per la maggior parte degli utenti di Kaspersky Next EDR Foundations, ma se avete più di 2.500 utenti o avete bisogno di un controllo granulare specifico non disponibile nella visualizzazione Pro, potete utilizzare la visualizzazione Expert

**In che modo  
Kaspersky può  
aiutarvi**



## Protezione dei dati

- **Normative**  
GDPR | LGPD | PIPL | PDPB | CCPA
- **Reputazione**
- **Phishing**

Le aziende ritengono che le questioni relative alla protezione dei dati siano le più impegnative<sup>1</sup>

55%



## Ransomware

- **Aziende Enterprise e SMB**
- **Costo del riscatto e del ripristino**
- **Doppia estorsione**

Aziende che hanno subito attacchi ransomware<sup>1</sup>

42%

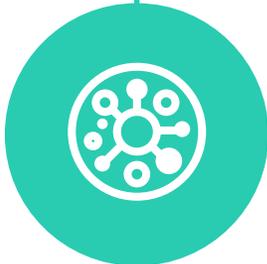


## APT\*

- **Danni elevati**
- **Dati non integrati**
- **Ci vuole troppo tempo per l'identificazione**

Aziende che hanno subito attacchi APT<sup>2</sup>

31%



## Complessità

- **Superficie di attacco in crescita**
- **Gap di competenze**
- **Limitazioni di budget**

Oggi le operazioni di sicurezza sono più complesse<sup>3</sup>

52%

\* Advanced Persistent Threat

1 Fonte: [IT Security Economics 2022, Kaspersky, 2022](#)  
2 Fonte: [Managed Detection and Response Report, Kaspersky, 2022](#)  
3 Fonte: [SOC Modernization and the Role of XDR, Enterprise Security Group, 2022](#)



## Normative

Sanzioni per la perdita di informazioni personali<sup>1</sup> in base alle normative sulla protezione dei dati. Può incidere anche sui costi assicurativi

## Reputazione

Gli autori degli attacchi amano pubblicizzare i loro successi

## Phishing

I dati rubati possono essere utilizzati in attacchi futuri

## Raccomandazioni

### Processi

Definite i dati sensibili, stabilite un criterio di sicurezza e un processo di reazione agli incidenti

### Controlli

Limitate l'accesso ai dati critici, monitorate le attività degli utenti

### Strumenti

Come IAM<sup>2</sup>, DLP<sup>3</sup> e software di backup specializzati, nonché strumenti di cybersecurity

Strumenti di cybersecurity consigliati

EPP

EDR

XDR

Threat intelligence

<sup>1</sup> Informazioni personali | <sup>2</sup> Gestione delle identità e degli accessi | <sup>3</sup> Prevenzione della perdita di dati



## Kaspersky Next EDR Foundations

### Motore anti-malware

Prevenite malware e crypto-locker tramite il machine learning

### HIPS<sup>1</sup>

Impedite l'accesso non autorizzato ai dati e alle risorse di sistema

### Cloud discovery

Individuate l'utilizzo di servizi cloud di terze parti



## Kaspersky Next EDR Optimum



### Gestione della crittografia

Cifrate file, unità rimovibili e l'intero disco

### Eliminazione dei dati

Eliminate remotamente i dati da un host

### Cloud Discovery e Cloud Blocking

Scoprite e bloccate l'utilizzo di servizi cloud di terze parti

### Data Discovery

Controllate i dati sensibili in SharePoint Online, OneDrive e Teams



## Kaspersky Next XDR Expert

### Advanced detection

Rilevate minacce complesse tramite più meccanismi, inclusi IoA proprietari<sup>2</sup>

### Threat hunting

Cercate in modo proattivo le minacce che potrebbero nascondersi nel vostro ambiente senza essere rilevate

### Molteplici fonti di dati

Automatizzate la correlazione dei dati provenienti da più fonti migliorando ulteriormente il rilevamento delle minacce complesse

### Playbook

Reazione rapida grazie all'automazione e all'orchestrazione

<sup>1</sup> Host Intrusion Prevention System

+ Funzionalità di Kaspersky Next EDR Foundations

+ Funzionalità di Kaspersky Next EDR Optimum



### Grandi imprese e PMI

Oltre il 40% di entrambi i tipi di aziende ha subito attacchi ransomware nel 2022

### Costi

Oltre ai costi diretti del riscatto, il ripristino può richiedere più di 20 giorni

### Doppia estorsione

I dati vengono spesso rubati prima della cifratura e utilizzati per ottenere un secondo riscatto

### Raccomandazioni

#### Aggiornamenti

Aggiornate il software su tutti i dispositivi utilizzati per correggere le vulnerabilità note

#### Backup

Impostate backup offline che gli attaccanti non possono manomettere

#### Monitoraggio dei dati

L' RDP non dovrebbe essere esposto su reti pubbliche. Monitorate il movimento laterale e l'esfiltrazione dei dati

### Strumenti di cybersecurity consigliati

EPP

EDR

XDR

Formazione

Threat intelligence



## Kaspersky Next EDR Foundations

### Motore anti-malware

Impedite l'ingresso del ransomware tramite il machine learning

### Anti-Cryptor

Impedite la cifratura malevola dei file presenti su cartelle di rete condivise sull'host

### Remediation engine

Eseguite il rollback delle azioni eseguite dal malware nel sistema operativo<sup>1</sup>

### Analisi della root cause

Analizzate gli eventi in modo visivo per trovare la causa principale della minaccia, la sua portata completa e le potenziali tracce lasciate nel sistema



## Kaspersky Next EDR Optimum



### Formazione

Imparate a riconoscere un attacco e a raccogliere dati

### Funzionalità EDR essenziali

- Ottenete visibilità sui rilevamenti
- Analizzate le minacce e trovate la causa principale
- Reagite rapidamente alle minacce su uno o più host
- Effettuate verifiche con indicazioni integrate per la reazione
- Scoprite minacce elusive su altri host utilizzando gli IoC<sup>2</sup>



## Kaspersky Next XDR Expert

### EDR

- Rilevamento avanzato con IoA<sup>3</sup>
- Mappatura MITRE ATT&CK
- Eseguite la ricerca delle minacce in base ai dati di telemetria raccolti
- Reagite alle minacce con opzioni automatizzate, semi-automatizzate e guidate

### XDR

- Rilevamento da più sorgenti di dati
- Correlate eventi da più fonti
- Esaminate più host in un singolo incidente

+ Funzionalità di Kaspersky Next EDR Foundations

+ Funzionalità di Kaspersky Next EDR Optimum



### Danni significativi

Le minacce APT sono per lo più associate all'esfiltrazione di dati e al ransomware, che possono comportare gravi interruzioni delle attività

### Dati non integrati

L'80% delle aziende utilizza più di 10 sorgenti di dati e desidera consolidare gli strumenti di cybersecurity<sup>1</sup>

### Troppo tempo per l'identificazione

Sono necessari competenze e strumenti significativi per il rilevamento e la neutralizzazione

### Raccomandazioni

#### Protezione efficace

Oltre il 25% degli incidenti di elevata gravità è collegato a malware<sup>2</sup>

#### Ricerca delle minacce

Gli attacchi mirati gestiti da esseri umani sono in aumento. La ricerca proattiva delle minacce, supportata dalla threat intelligence, è fondamentale

#### Risposta agli incidenti

Un'analisi e una reazione rapida e corretta sono fondamentali per affrontare un attacco mirato

### Strumenti di cybersecurity consigliati

EPP

EDR

XDR

Threat intelligence

Servizi di cybersecurity



## Kaspersky Next EDR Foundations

### Non applicabile

#### Nota:

Fermare gli attacchi APT richiede strumenti più specializzati e un approccio consolidato



## Kaspersky Next EDR Optimum

### Non applicabile

#### Nota:

Fermare gli attacchi APT richiede strumenti più specializzati e un approccio consolidato



## Kaspersky Next XDR Expert



### Advanced detection

Il rilevamento della correlazione degli eventi e gli IoA sono supportati da un motore antimalware basato su machine learning

### Correlazione tra risorse

Correlazione in tempo reale di eventi provenienti da diverse fonti

### Mappatura MITRE ATT&CK

Comprendete l'intera portata di un attacco, applicate la TI<sup>1</sup> e identificate le TTP<sup>2</sup>

### Threat hunting

Cercate in modo proattivo le minacce che potrebbero nascondersi senza essere rilevate nell'ambiente

### Grafico di indagine

Semplifica l'indagine e la risposta unendo dati provenienti da diversi sistemi

+ Funzionalità di Kaspersky Next EDR Foundations

+ Funzionalità di Kaspersky Next EDR Optimum



### Superficie di attacco in crescita

A causa del sempre più diffuso lavoro da remoto e dell'utilizzo dei servizi cloud

### Gap di competenze

È difficile imparare a utilizzare nuovi strumenti mentre si gestiscono le attività di routine

### Vincoli di budget

La complessità dell'infrastruttura è il primo fattore di spesa

### Raccomandazioni

#### Consolidamento

Riunire dati e strumenti diversi in una singola posizione aiuta a ridurre la superficie di attacco e la complessità

#### Automazione

Rende la sicurezza efficiente e riduce il burnout, facilitando al tempo stesso l'apprendimento sul lavoro

#### Focalizzazione sul TCO<sup>1</sup>

L'implementazione cloud e un unico ecosistema riduce il TCO

Strumenti di cybersecurity consigliati

EPP

EDR

XDR

MDR<sup>2</sup>

<sup>1</sup> Total Cost of Ownership (costo totale di proprietà) | <sup>2</sup> Managed Detection and Response



## Kaspersky Next EDR Foundations

### Massima automazione

La maggior parte delle attività è automatizzata e il prodotto opera in modalità "set and forget".

### Multipiattaforma

Supporta endpoint che eseguono diversi sistemi operativi, inclusi Windows, Linux, Mac, iOS e Android

### Vulnerability assessment

Panoramica rapida delle applicazioni installate e delle patch disponibili



## Kaspersky Next EDR Optimum

### Cloud security

Controllate la superficie di attacco estesa nel cloud

### Controllo adattivo delle anomalie

Regole di controllo basate sui ruoli per la riduzione della superficie di attacco

### Patch management

Gestite in remoto gli aggiornamenti e le patch delle applicazioni: un'attività cruciale per la cybersecurity semplificata

### Indicazioni per la reazione

Scoprite come utilizzare EDR e accelerate le attività con i suggerimenti integrati all'interno degli eventi



## Kaspersky Next XDR Expert



### Correlazione tra risorse

Esaminate gli incidenti relativi a più risorse in un'unica soluzione

### Gestione dei casi

Consolidate avvisi e dati e coordinate le risposte

### Playbook e indicazioni

Velocizzate le operazioni automatizzando la risposta agli incidenti

### Connettori di terze parti

Riunite diverse origini dati in una singola posizione

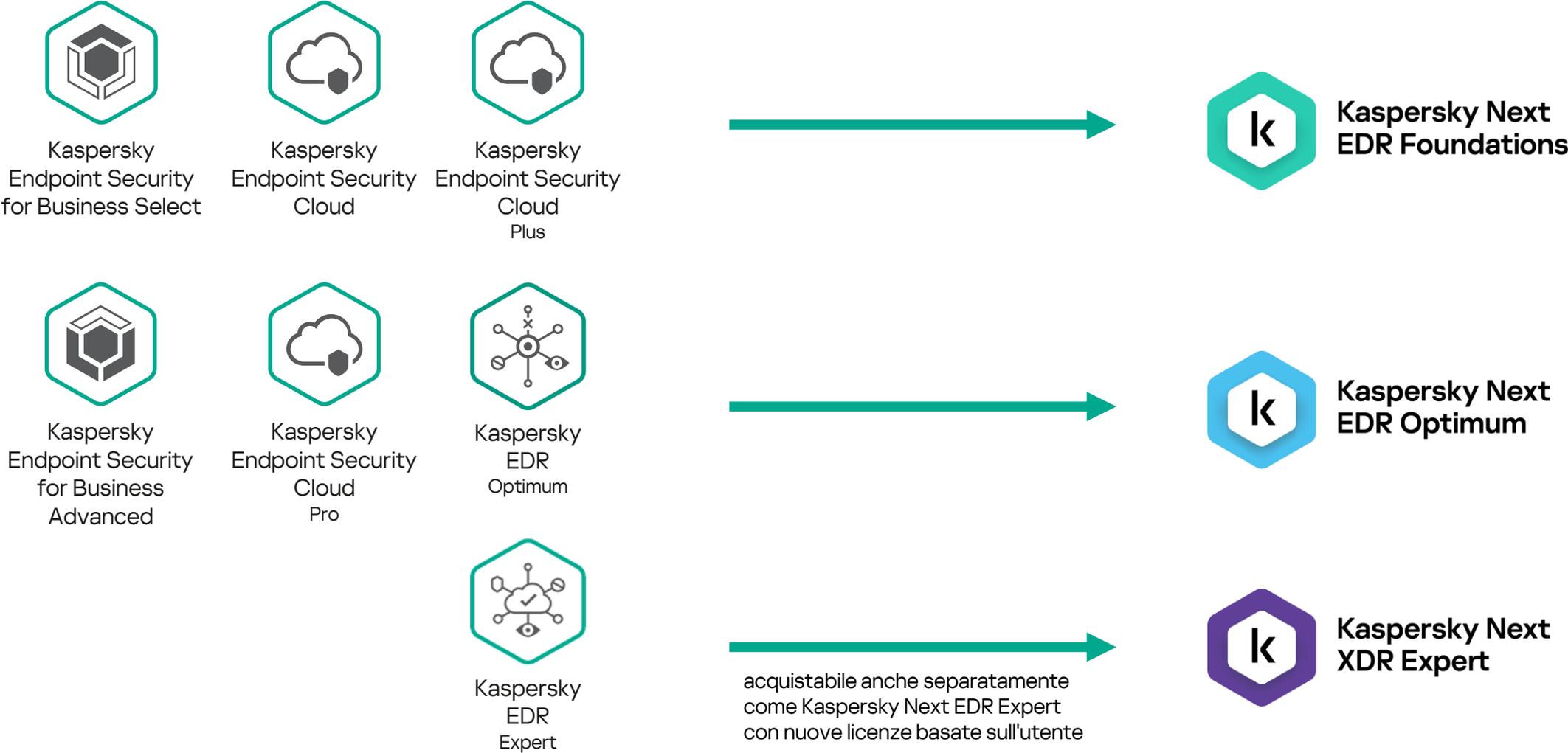
+ Funzionalità di Kaspersky Next EDR Foundations

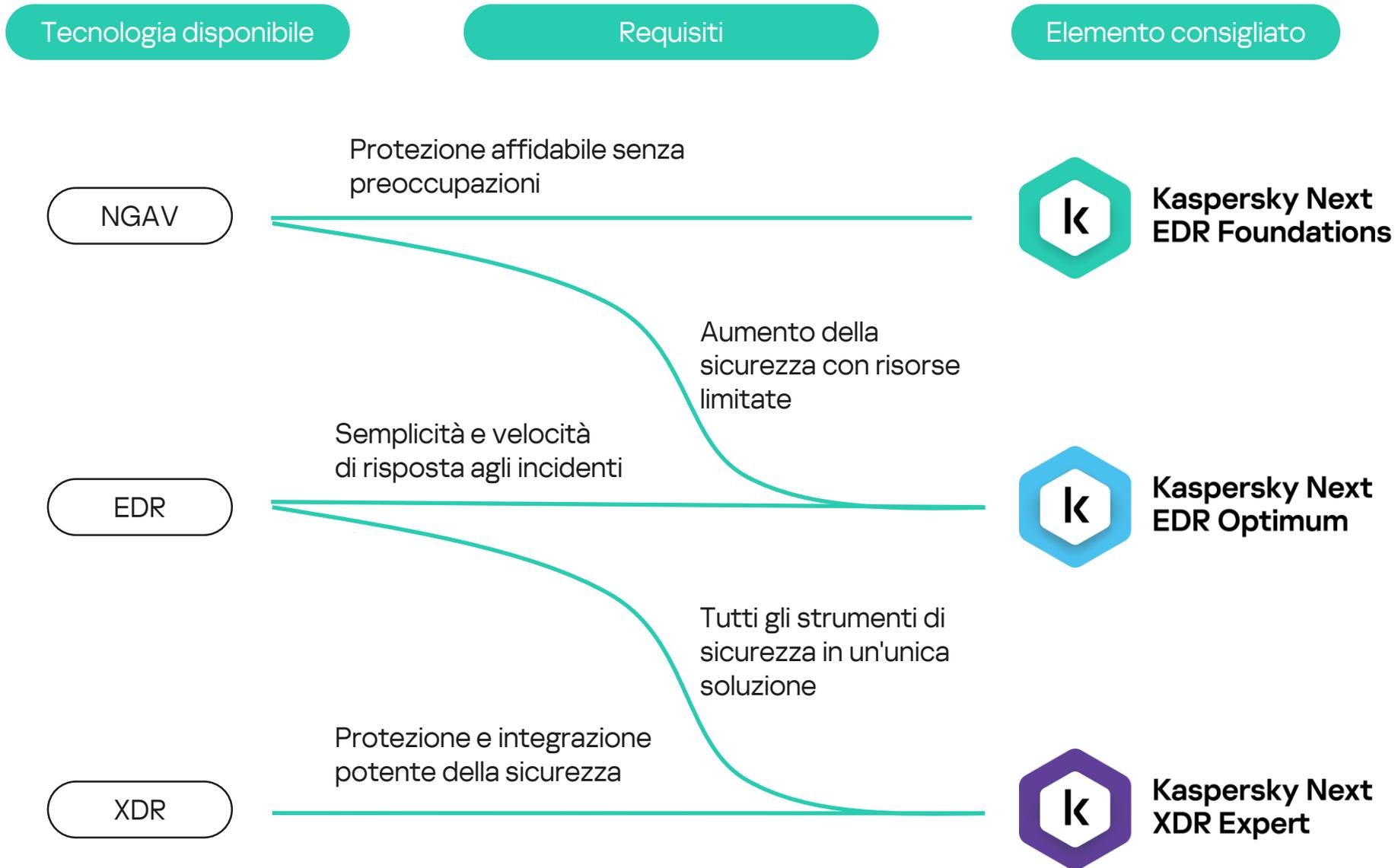
+ Funzionalità di Kaspersky Next EDR Optimum

# Migrazione



# Come effettuare l'upgrade





**Altri prodotti**

A decorative graphic element on the right side of the page, consisting of a teal-to-white gradient that forms a curved, abstract shape pointing towards the bottom center.



## Kaspersky Managed Detection and Response

è una soluzione completa che offre una **protezione avanzata 24 ore su 24** anche contro le minacce sconosciute e complesse.

[Ulteriori informazioni](#)

### Monitoraggio 24/7

per analizzare qualsiasi attività sospetta

### Protezione endpoint

con sistemi di sicurezza preventivi e risposte automatizzate alle minacce note

### Threat hunting

per le minacce sconosciute e indicazioni dettagliate con risposte agli incidenti da parte degli esperti SOC di Kaspersky



## Kaspersky Security Awareness

Soluzioni di formazione interattive per aiutare le organizzazioni a **ridurre il numero di incidenti legati a errori umani**, aumentando le competenze informatiche dei dipendenti e creando una cultura della cybersecurity a tutti i livelli

[Ulteriori informazioni](#)

### Valutazione del livello di conoscenza

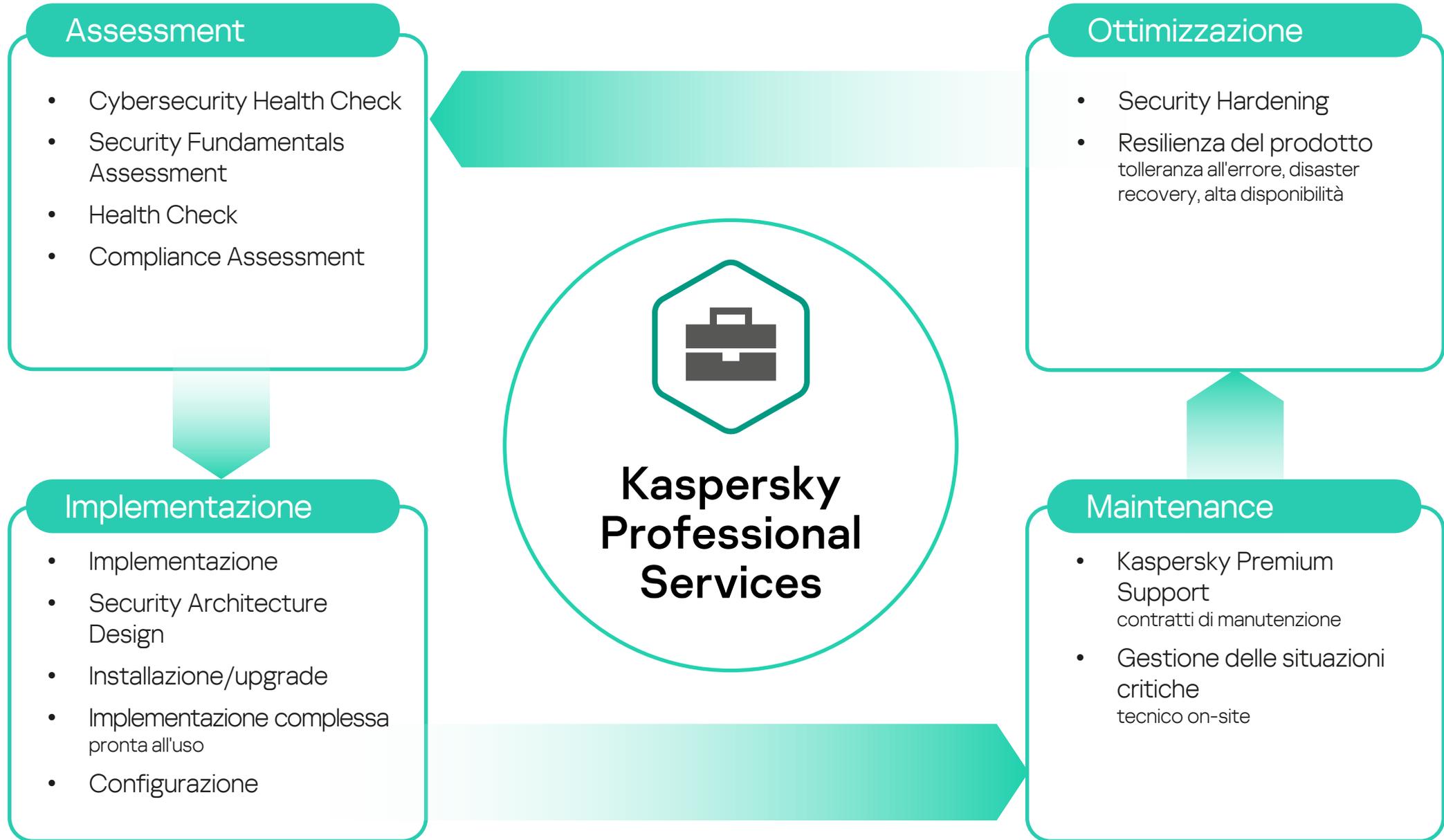
Scoprite il reale livello di cybersecurity awareness in azienda e motivate i dipendenti a saperne di più

### Coinvolgimento e motivazione

Aiutate il management a comprendere l'impatto della cybersecurity sulle attività di business e a trovare un linguaggio comune con gli specialisti IT e IS, attraverso la simulazione di diversi scenari di attacco.

### Acquisizione di competenze pratiche

- Oltre 350 competenze pratiche per sviluppare nuove abitudini di sicurezza informatica per tutti i dipendenti
- Moduli di apprendimento interattivi e attacchi di phishing simulati
- Aiuta il reparto IT a riconoscere i primi segnali d'attacco e a raccogliere dati sugli incidenti



# Migliorate ancora di più la cybersecurity

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
Kaspersky Security for Mail Server	Sicurezza perimetrale nello stesso ecosistema	Sicurezza perimetrale nello stesso ecosistema	Sorgenti di dati
Kaspersky Hybrid Cloud Security	Protezione di cloud pubblico e VM		Protezione di cloud pubblico e VM
Kaspersky MDR*	Protezione 24/7 che non richiede personale aggiuntivo	Protezione 24/7 che non richiede personale aggiuntivo	Threat hunting gestito
Kaspersky Next EDR Expert	<b>Upgrade**</b> alle funzionalità EDR avanzate		Sorgenti di dati, ricerca delle minacce, risposta
Kaspersky Anti-Targeted Attack	Rilevamento avanzato a livello di rete		



Incluso



Consigliato



Disponibile

Nota: la maggior parte di questi prodotti è disponibile solo on-premises e non può essere gestita dalla console cloud. Per le opzioni di integrazione e la disponibilità della console, consultate la documentazione del prodotto corrispondente

\*MDR è disponibile in **visualizzazione Expert** cloud o on-premises | \*\* Upgrade disponibile a Kaspersky Next EDR Expert con modello di licenza per utente

# Conclusioni





## Kaspersky Next



### Kaspersky Next EDR Foundations

#### Solida sicurezza per tutti

Proteggi tutti gli endpoint

#### Vantaggi della soluzione

- Solida protezione degli endpoint
- Controlli della sicurezza
- Analisi della root cause
- Cloud discovery
- Massima automazione



### Kaspersky Next EDR Optimum

#### Create le vostre difese

Aumentate la sicurezza con investigation e response essenziali

#### Vantaggi della soluzione

- Funzionalità EDR essenziali
- Blocco e monitoraggio cloud
- Controlli di livello Enterprise
- Formazione sulla cybersecurity



### Kaspersky Next XDR Expert

#### Equipaggiate i vostri esperti

Proteggete la vostra azienda dalle minacce più avanzate e complesse

#### Vantaggi della soluzione

- Rilevamento delle minacce avanzate
- Correlazione tra risorse
- Potenti strumenti di threat hunting
- Integrazione seamless



# **Kaspersky Next**

Sicurezza all'avanguardia

# Parliamone!



**Kaspersky  
Next**

Jane Doe

Responsabile delle vendite

[jane.doe@Kaspersky.com](mailto:jane.doe@Kaspersky.com)

**kaspersky**