Webinar

24-03-2022

channelcity

kaspersky

Complessità e compliance mettono in crisi la difesa dai cyberattacchi? Ecco la bussola per mettere al sicuro ripartenza e imprese

#Difendile

#Difendile

Diego Magni
Senior Pre-Sales Manager
Kaspersky

Marco Maria Lorusso
Giornalista
G11 Media

kaspersky

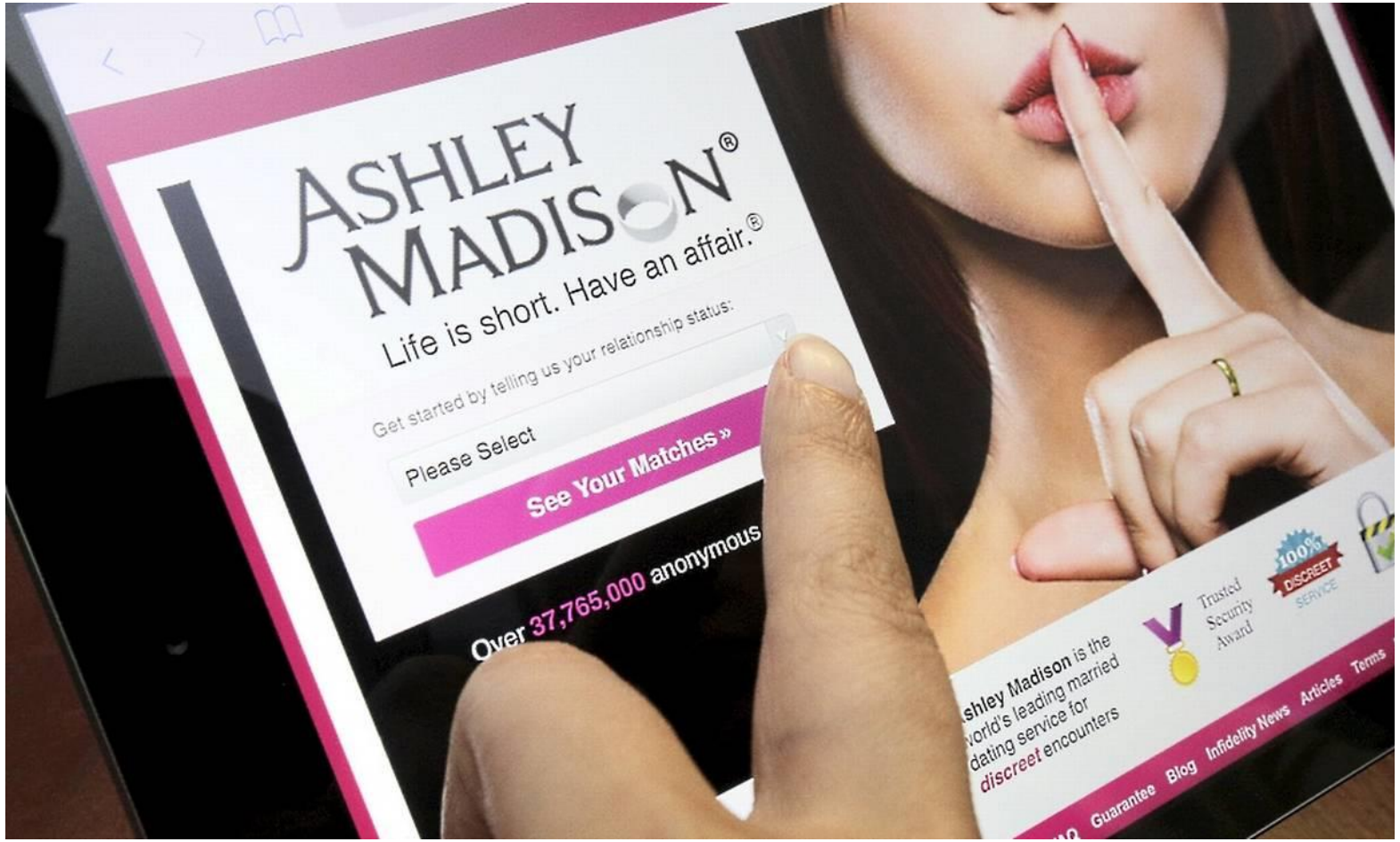

Webinar
#Difendile
Complessità e compliance mettono in crisi la difesa dai cyberattacchi? Ecco la bussola per mettere al sicuro ripartenza e imprese
kaspersky
24 marzo 2022
Dalle ore 11:00 alle ore 12:00

Tutto è cominciato, quasi sempre così, dal molto piccolo…

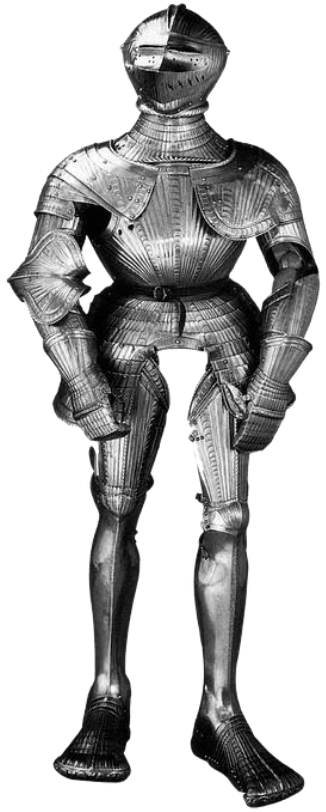
Poi ci si è messa una certa ansia da prestazione…

#DIFENDILE

IN PIÙ… AVEVAMO, GIÀ, UNA STORIA E UN DNA PRECISI…



#DIFENDILE



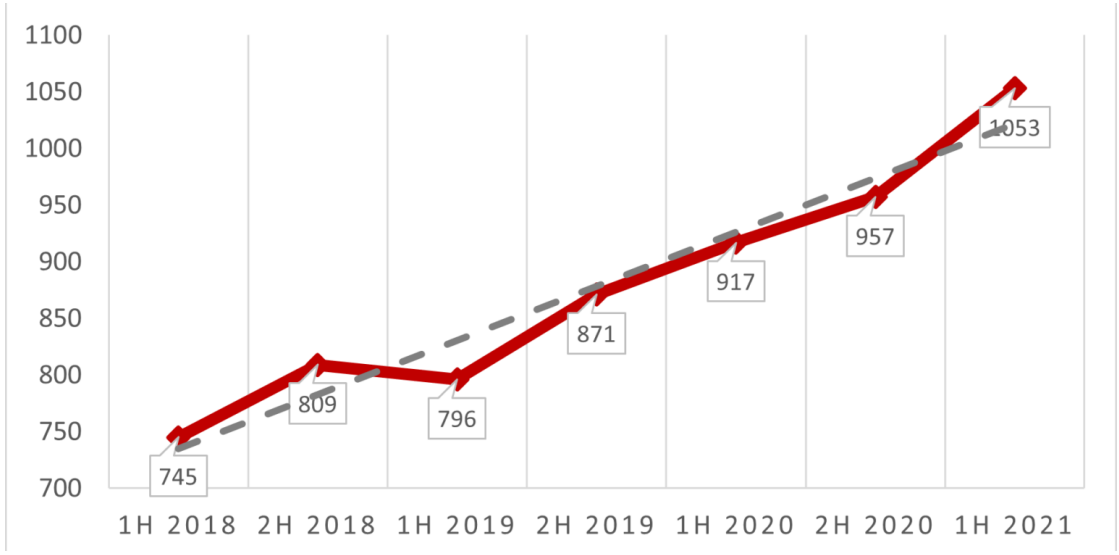

ABBIAMO SCELTO LA STRADA DELL’EMOTIVITÀ… QUELLA PIÙ SEMPLICE

Trend attacchi informatici 2021

- **Trasporti e Logistica: +108,7%**
- **Professional, Scientific: +85,2%**
- **News & Multimedia: +65,2%**
- **Retail: +61,3%**
- **Manufacturing: +46,9%**
- **Energia / Utilities: +46,2%**
- **Governativo / Difesa: (+39,2%)**
- **Arte e Divertimento: +36,8%**
- **Sanità: +18,8%**

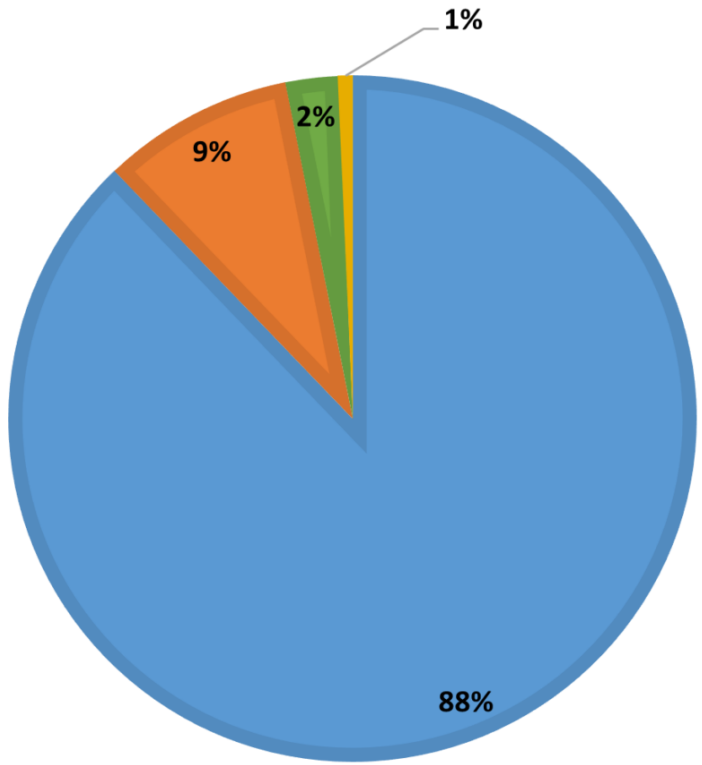
#DIFENDILE

Trend attacchi nel primo semestre



#DIFENDILE

TIPOLOGIA E DISTRIBUZIONE ATTACCANTI 1H 2021



Cybercrime EspionageSabotage InformationWarfare Hacktivism

© Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2021

Principali tecniche di attacco

- Malware (Ransomware): 41%
- Data Breach: 21%
- Sfruttamento delle vulnerabilità sistemi: 16%
- Phishing / Social Engineering: 10%
- Attacchi a tecnica multipla: 5%
- Furto di idntità e credenziali di accesso: 4%

Potrebbe essere peggio? Yes…

DATA PROTECTION

Gdpr: Italia seconda in Europa con 75 multe per 84,5 milioni. Le sanzioni più pesanti alle telco

Home > Privacy > GDPR

Condividi questo articolo

La Spagna ci supera con 273 provvedimenti. Ad Amazon multa da 746 milioni dal Lussemburgo, è la più colpita delle big tech. E a Google sanzione da 50 milioni in Francia

02 Nov 2021


THAT'S THE CHICAGO WAY
made on imgur

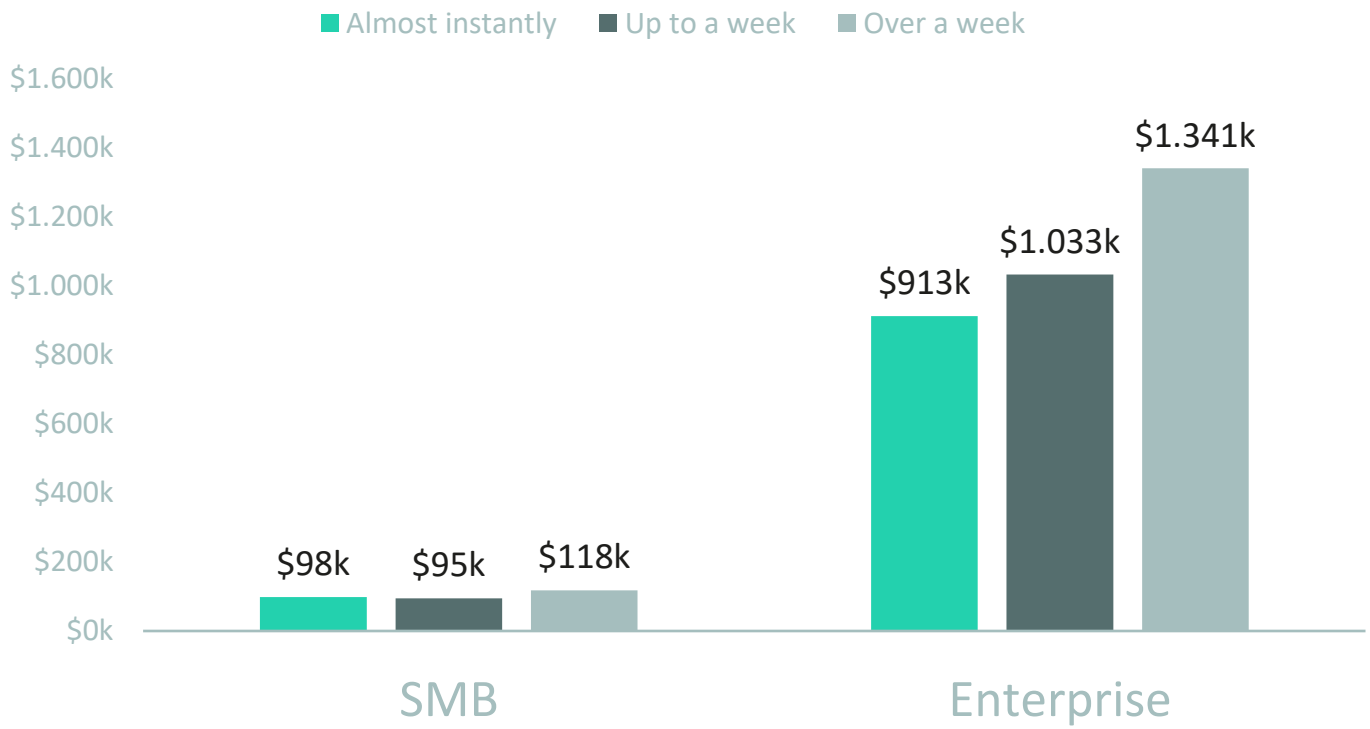
Vi siete mai chiesti…

- Sono sotto attacco in questo momento?
- Cosa farebbero al mio posto degli esperti?
- Cosa è riuscito a fare quel malware?
- Perché quell’utente non sapeva che non doveva aprire quel PDF??

IL CONTRASTO AGLI ATTACCHI COMPLESSI PARTE DALLA VELOCITÀ DI REAZIONE

Una risposta più rapida significa meno perdite o il poterle prevenire del tutto

Costo medio delle violazioni dei dati a seconda di quando sono state scoperte



32%

Anche in caso di attacchi riusciti, le perdite finanziarie erano inferiori del 32% se si rispondeva a una violazione in meno di una settimana

Source: Incident response analyst report, Kaspersky, 2020

Lo sviluppo di capacità di rilevamento e risposta diventa essenziale

No visibililità

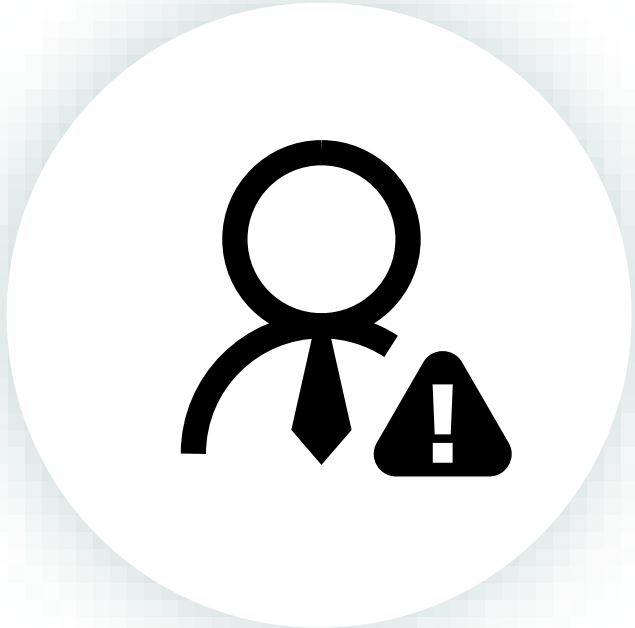
Cosa è successo?

Troppo complicato

Come posso analizzarlo?

Troppo lento

Come posso rispondere velocemente?



No confidence

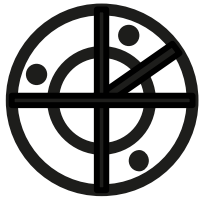
Cosa sono le minacce evasive e perché sono pericolose?

Evasive threats

- Malware
- Ransomware
- Financial spyware
- etc.

Facili da ottenere

Strumenti e metodi per creare attacchi evasivi sono facilmente disponibili per i criminali informatici



Difficili da rilevare

Strumenti legittimi e altre tecniche di evasione vengono utilizzate per ottenere l'accesso e aggiungere persistenza

Più pericolosi

Rimanere nascosti dà alle minacce più tempo per causare più danni

Cosa hanno in comune gli attacchi evasivi

Penetrazione

- Phishing
- Exploit
- Bruteforce

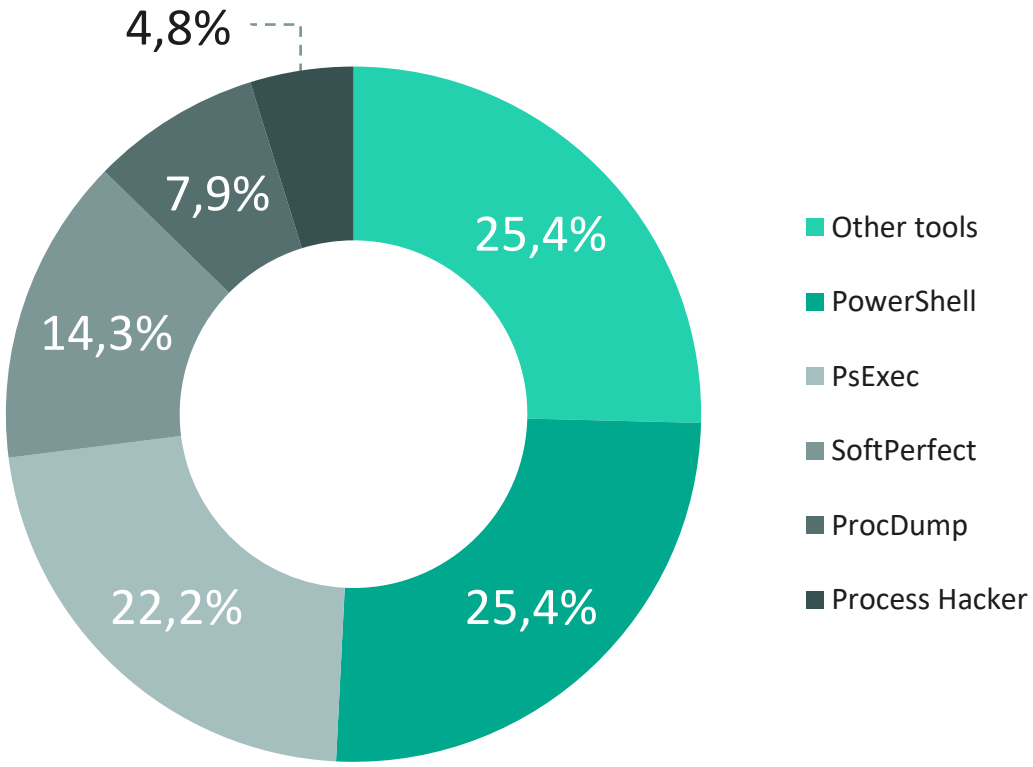
Strumenti legittimi

Il 30% degli attacchi utilizza strumenti legittimi, il che rende difficile il rilevamento automatico

Persistenza

Da veloci attacchi ransomware al furto di dati di lunga durata: le minacce evasive rimangono invisibili, causando danni più profondi

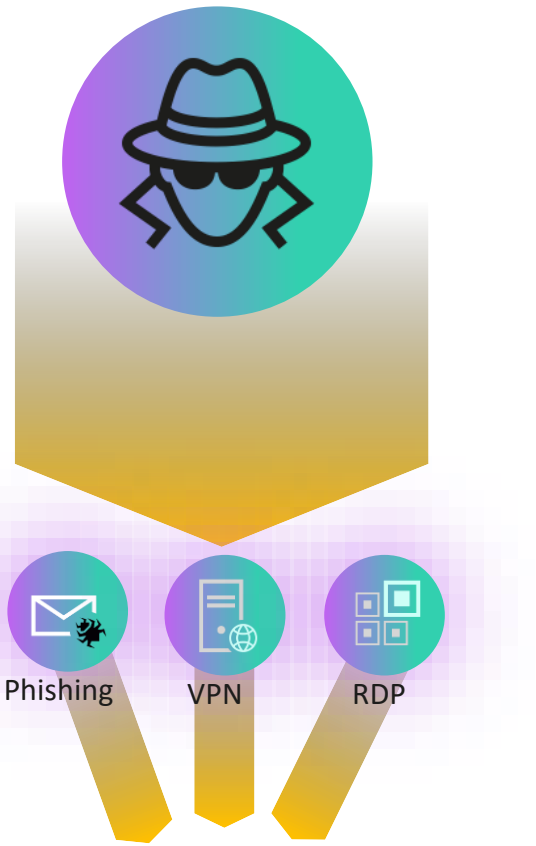
Strumenti legittimi utilizzati negli attacchi andati a segno



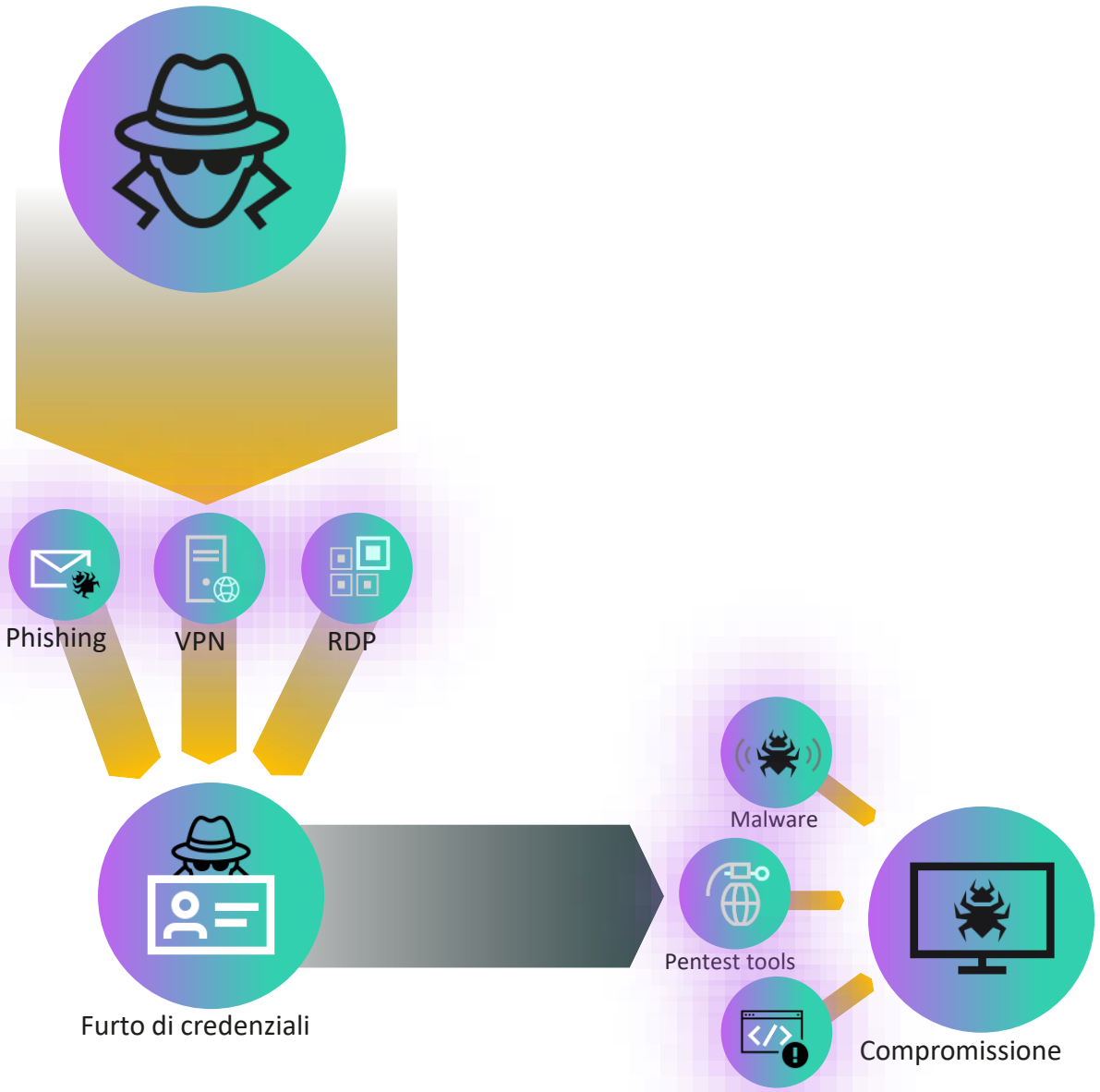
Source: Incident response analyst report, Kaspersky, 2020

Il meccanismo della doppio estorsione

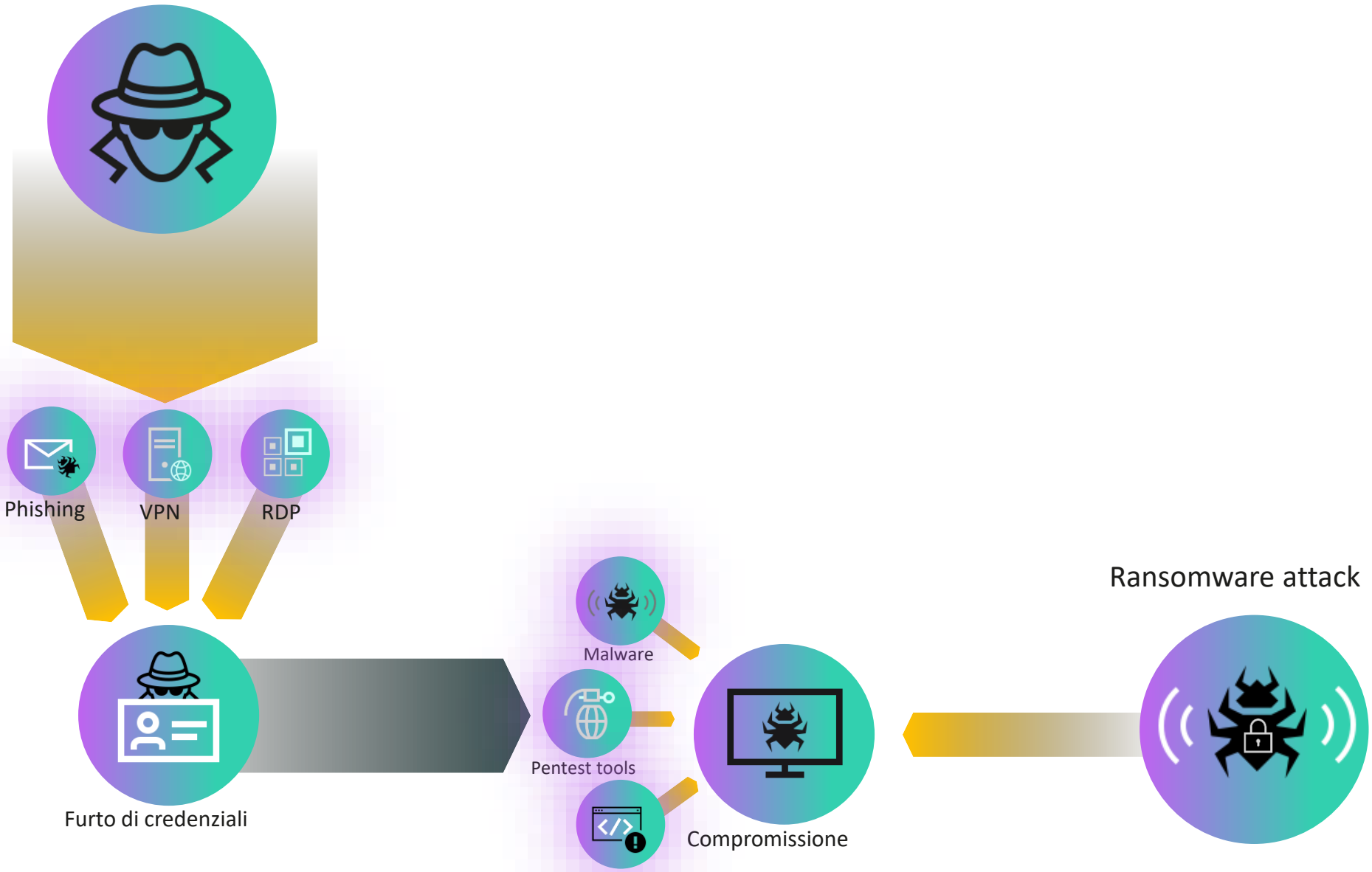
Il meccanismo della doppio estorsione



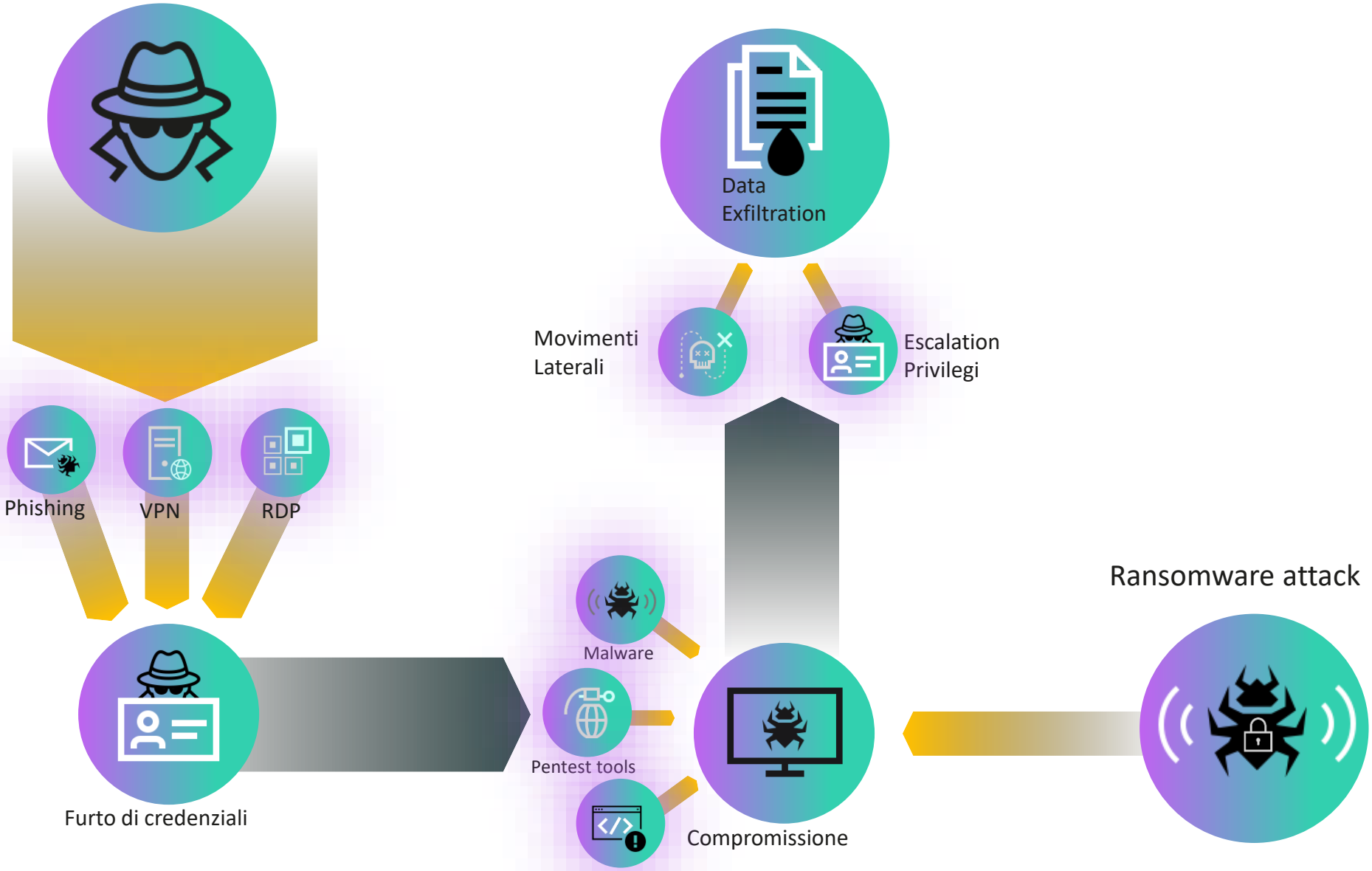
Il meccanismo della doppio estorsione



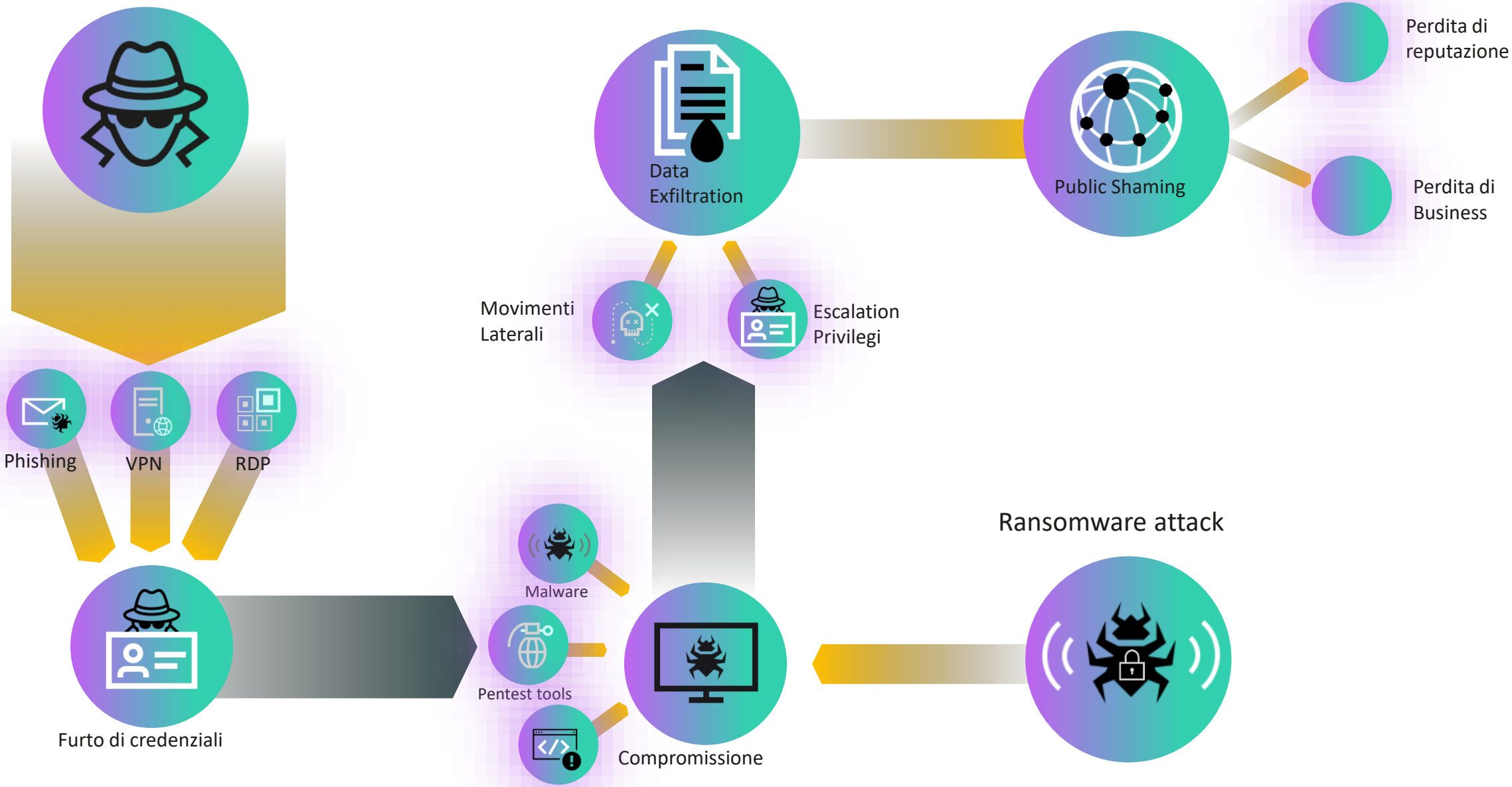
Il meccanismo della doppio estorsione



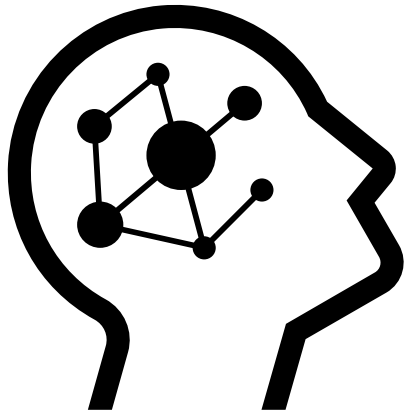
Il meccanismo della doppio estorsione



Il meccanismo della doppio estorsione



Tornando alle domande iniziali…



- Sono sotto attacco in questo momento?
- Cosa farebbero al mio posto degli esperti?
- Cosa è riuscito a fare quel malware?
- Perché quell’utente non sapeva che non doveva aprire quel PDF??

La risposta a queste domande sta nel rilevamento e nella risposta

Rilevare

Utilizzo del rilevamento avanzato per identificare le minacce evasive

Analizzare

Capire da dove proveniva la minaccia e cosa è successo

Rispondere

Avere la propria capacità di risposta

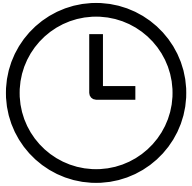
Formare

Aiutare gli utenti a fare meno errori aumentando la loro consapevolezza

I principali ostacoli all’evoluzione della sicurezza informatica nelle aziende

Budget limitato

Hardware, manodopera e denaro



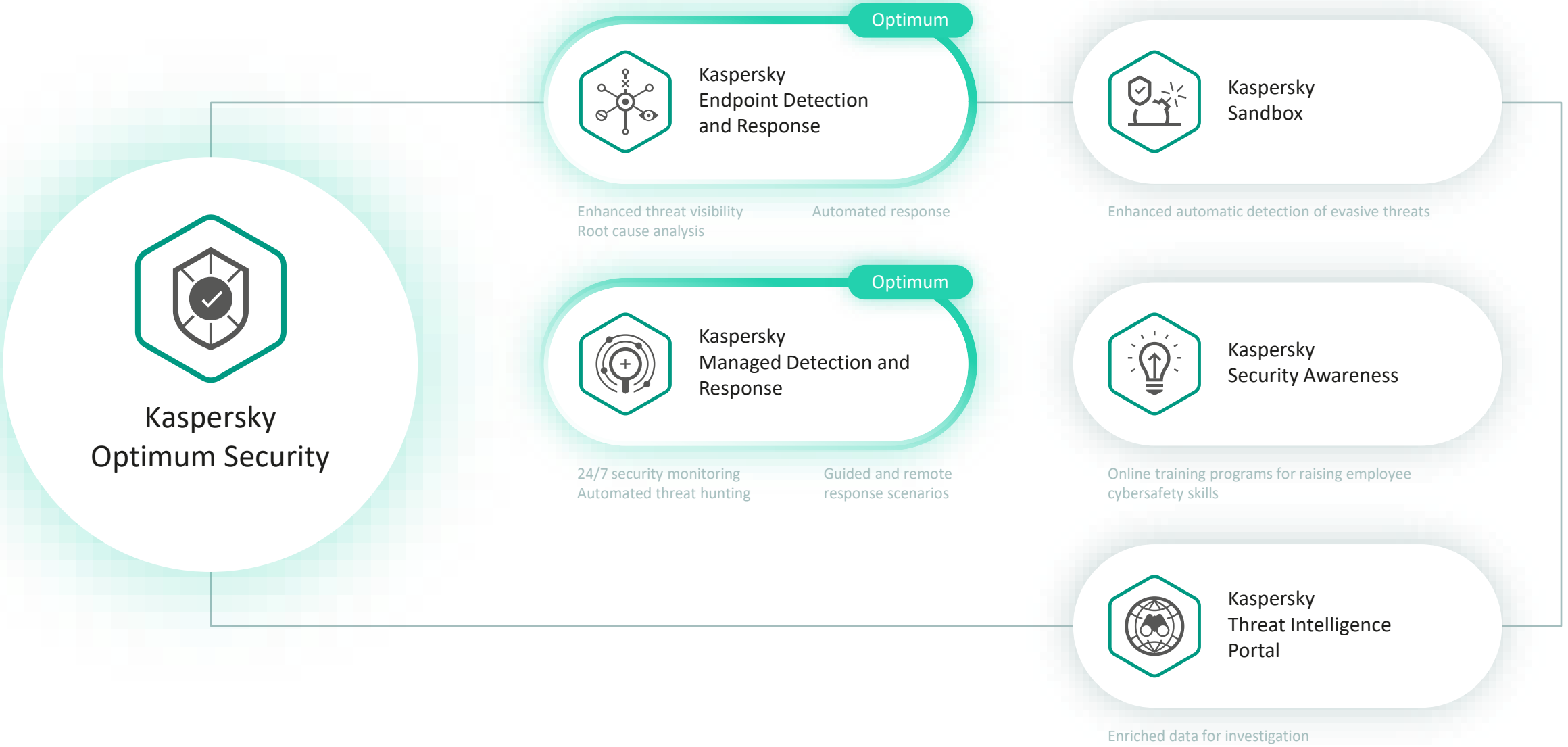
Tempo

Non è possibile dedicare molto tempo per rispondere agli incidenti

Complessità IT

Non è possibile integrare altri strumenti o utilizzare ulteriori strumenti di gestione

Kaspersky Optimum Security per consolidare la sicurezza informatica



Advanced Threat Detection

Gli esperti del SOC Kaspersky sono in grado di rilevare i più sofisticati attacchi mirati tramite centinaia di regole di threat hunting frutto della nostra Threat Intelligence e di più di 20 anni di esperienza nella cybersecurity.

Efficienza

Gli esperti del SOC Kaspersky monitorano gli eventi della vostra azienda **24x7**.

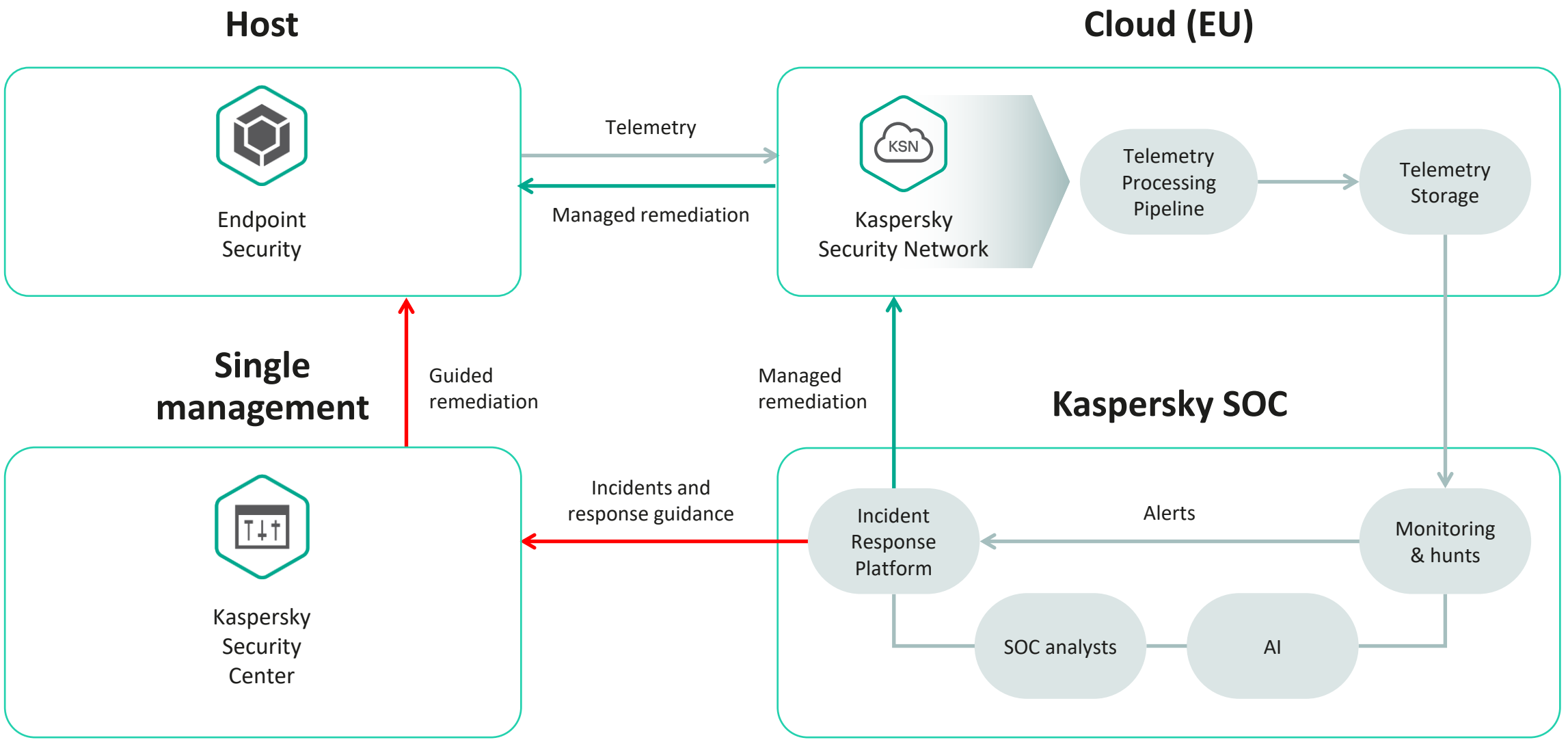
Analizziamo tutte le azioni sospette e segnaliamo solo gli incidenti reali, evitando i possibili falsi positivi.

Response and Remediation

Le segnalazioni degli incidenti sono affiancate dai suggerimenti su come rispondere ai threat rilevati.

È supportata anche la funzionalità di risposta preapprovata controllata da remoto.

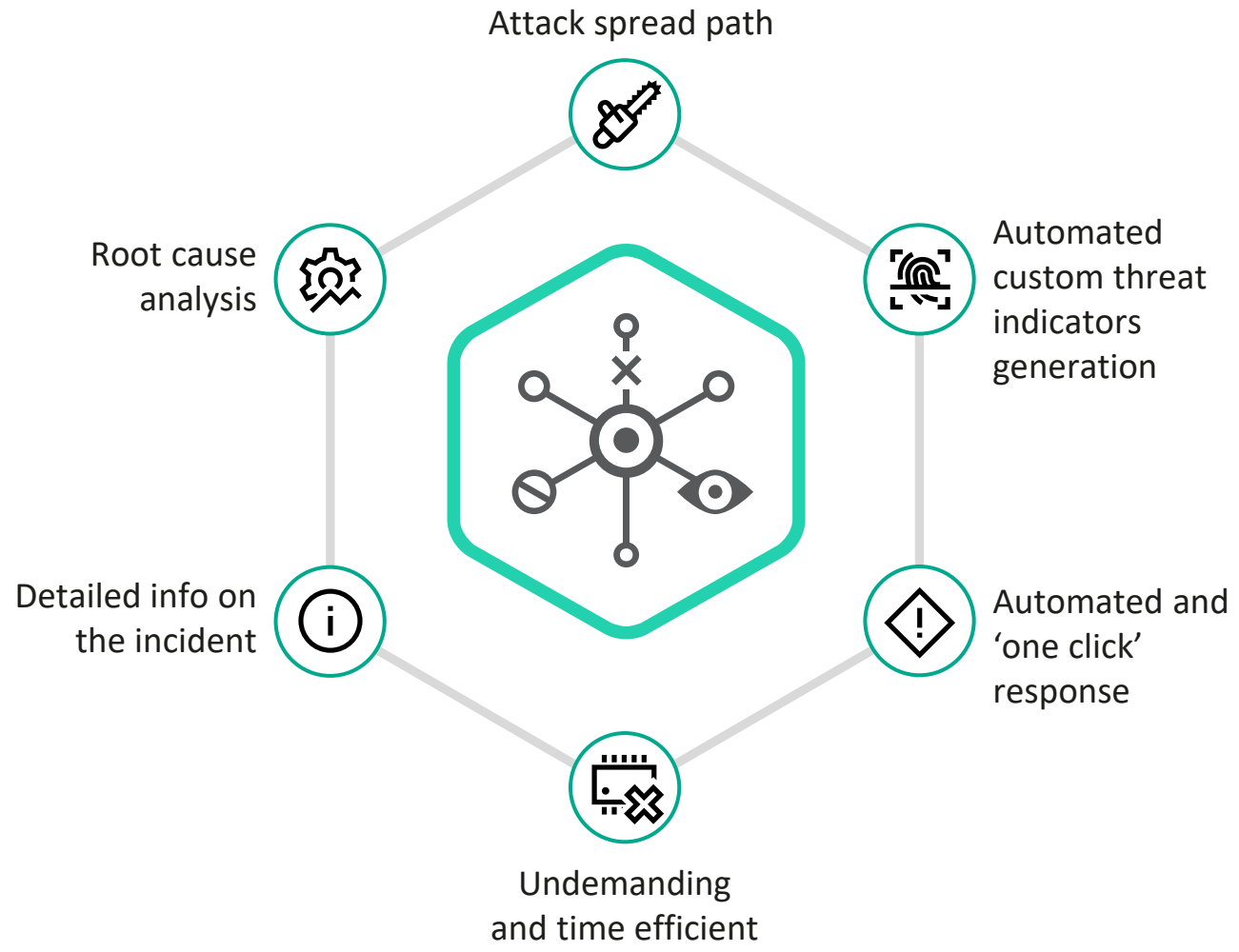
Architettura del servizio di alto livello



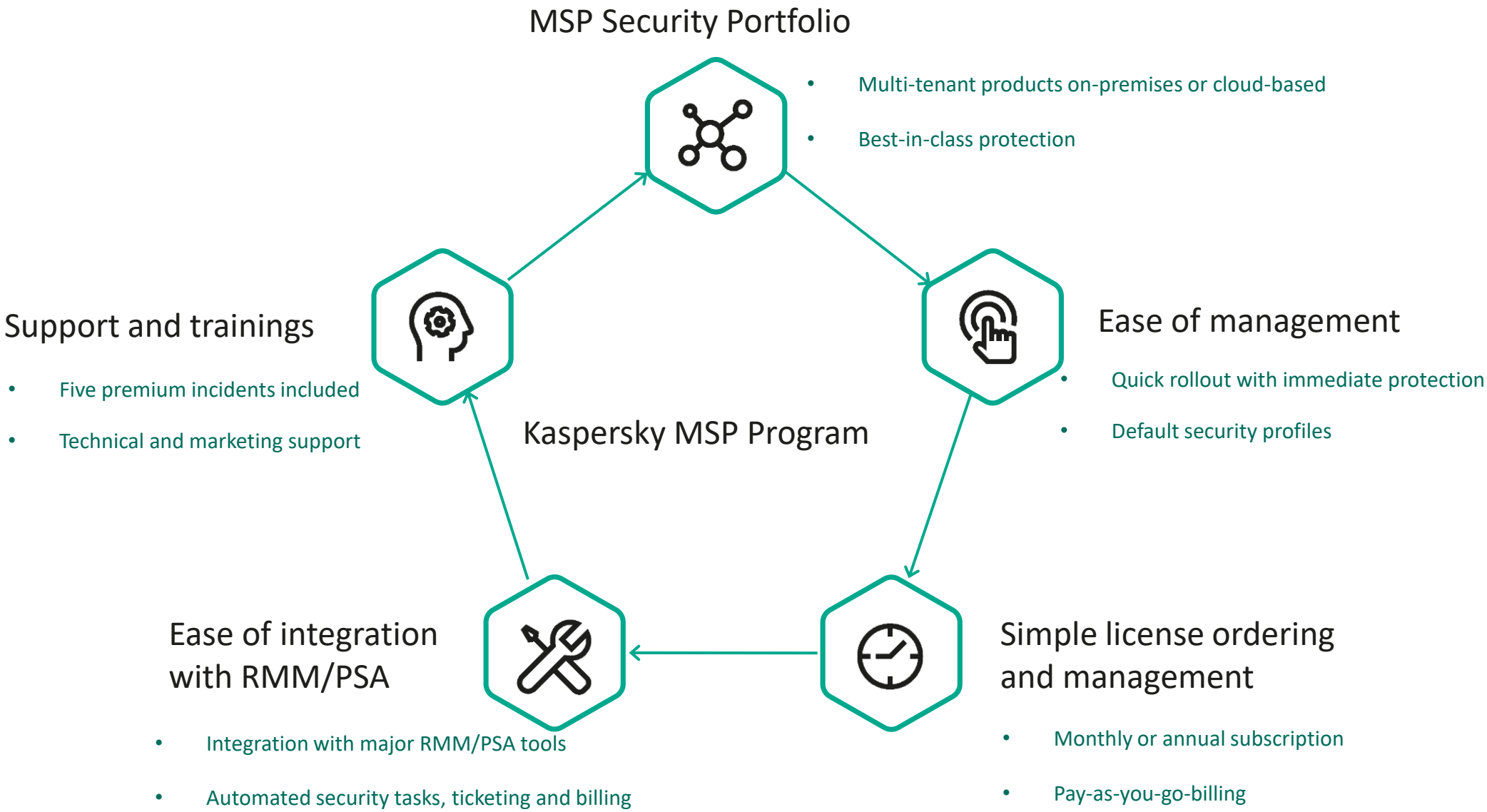
Kaspersky EDR Optimum

Obiettivi principali:

- Fornire piena visibilità sull'incidente
- Riduzione dei costi generali relativi all'implementazione della soluzione
- Fornire un semplice strumento di indagine
- Risposta rapida a minacce complesse ed evasive prima che si possano verificare ulteriori danni



Kaspersky MSP Vision



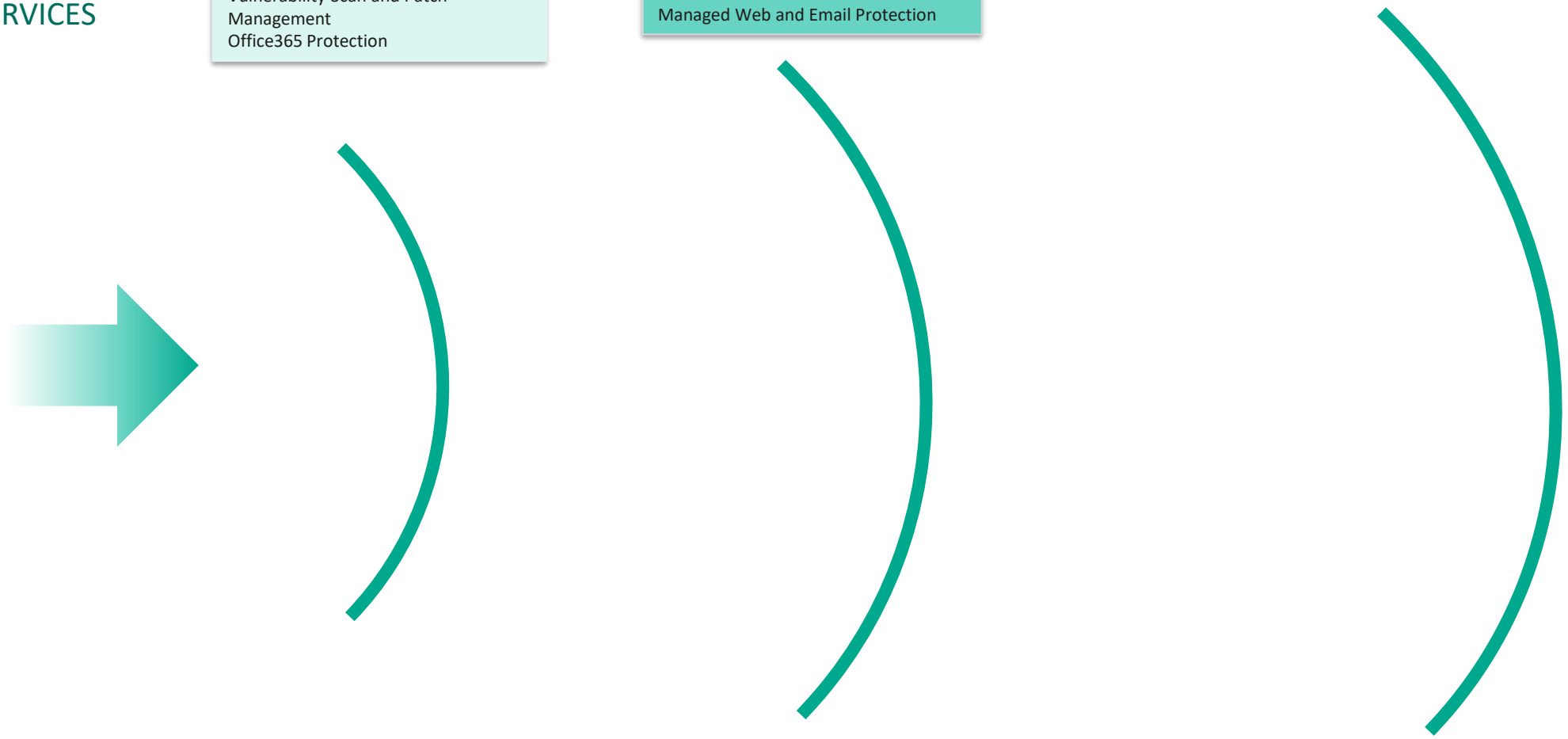
Managed Services with Kaspersky

BUILD SERVICES

Security Foundation
Endpoint Protection
Vulnerability Scan and Patch Management
Office365 Protection

Optimum Security
Incident Response
Security Awareness Trainings
Private and Public Cloud Protection
Managed Web and Email Protection

Expert Security
Security monitoring
Managed Detection and Response
Proactive Threat Hunting



Managed Services with Kaspersky

BUILD SERVICES

Security Foundation
Endpoint Protection
Vulnerability Scan and Patch Management
Office365 Protection

Optimum Security
Incident Response
Security Awareness Trainings
Private and Public Cloud Protection
Managed Web and Email Protection

Expert Security
Security monitoring
Managed Detection and Response
Proactive Threat Hunting

MSP

Kaspersky Endpoint Security for Business

Kaspersky Endpoint Security Cloud

Kaspersky Security for Microsoft Office 365

Managed Services with Kaspersky

BUILD SERVICES

Security Foundation
Endpoint Protection
Vulnerability Scan and Patch Management
Office365 Protection

Optimum Security
Incident Response
Security Awareness Trainings
Private and Public Cloud Protection
Managed Web and Email Protection

Expert Security
Security monitoring
Managed Detection and Response
Proactive Threat Hunting

MSP

- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365
- Kaspersky EDR Optimum
- Kaspersky Hybrid Cloud Security
- Kaspersky Sandbox
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security for Mail Server
- Kaspersky Security for Web Gateway

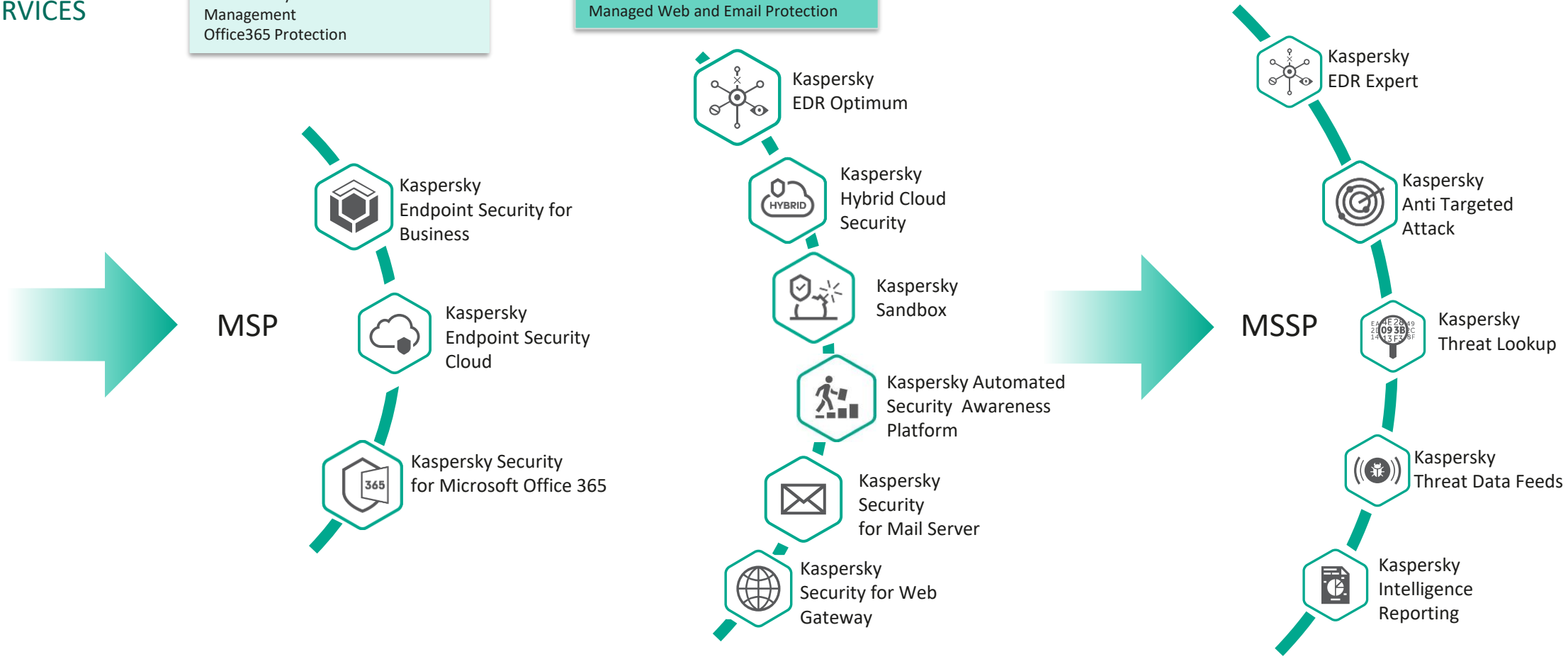
Managed Services with Kaspersky

BUILD SERVICES

Security Foundation
Endpoint Protection
Vulnerability Scan and Patch Management
Office365 Protection

Optimum Security
Incident Response
Security Awareness Trainings
Private and Public Cloud Protection
Managed Web and Email Protection

Expert Security
Security monitoring
Managed Detection and Response
Proactive Threat Hunting



Managed Services with Kaspersky

BUILD SERVICES

Security Foundation
Endpoint Protection
Vulnerability Scan and Patch Management
Office365 Protection

Optimum Security
Incident Response
Security Awareness Trainings
Private and Public Cloud Protection
Managed Web and Email Protection

Expert Security
Security monitoring
Managed Detection and Response
Proactive Threat Hunting

MSP

- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365

- Kaspersky EDR Optimum
- Kaspersky Hybrid Cloud Security
- Kaspersky Sandbox
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security for Mail Server
- Kaspersky Security for Web Gateway

MSSP

- Kaspersky EDR Expert
- Kaspersky Anti Targeted Attack
- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky Intelligence Reporting

KASPERSKY INTELLIGENSE AND EXPERTISE

- Kaspersky Security Network
- RMM and PSA Integrations
- Premium Support and Professional Services
- Cybersecurity Training
- Managed Detection and Response
- Expert Services

GRAZIE

kaspersky


Webinar
#Difendile
Complessità e compliance mettono in crisi la difesa dai cyberattacchi? Ecco la bussola per mettere al sicuro ripartenza e imprese
kaspersky
24 marzo 2022
Dalle ore 11:00 alle ore 12:00

channelcity

undici media