Halo

UNLIMITED VISIBILITY

Endpoints' Raw Data Gathering & Enrichment

certego

Halo | Unlimited Visibility

Piena visibilità, massima sicurezza: il valore dei dati telemetrici degli endpoint

Gli endpoint rappresentano i punti più vulnerabili nei sistemi IT, rendendo necessarie soluzioni di rilevamento efficaci.

Con l'aumento delle informazioni di sicurezza e degli alert, disporre di un accesso completo alla telemetria degli endpoint diventa cruciale per garantire una protezione precisa e personalizzata.

Le piattaforme EDR tradizionali sono progettate per soddisfare esigenze standard dei reparti IT interni e spesso non offrono una visibilità completa sui dati raccolti. Questa limitazione può penalizzare i team di Security Operations più esperti, che necessitano di un accesso approfondito ai dati degli endpoint e della possibilità di creare rilevamenti personalizzati. Solo così possono eseguire analisi tempestive e perfezionare continuamente le difese dei clienti con strategie mirate e proattive.

Halo - Endpoints' Raw Data Gathering & Enrichment

Servizi MDR avanzati grazie alla massima visibilità

Certego offre servizi MDR basati su un approccio personalizzato e caratterizzato da una significativa riduzione dei falsi positivi.

Le piattaforme EDR tradizionali, a causa della visibilità limitata sugli eventi telemetrici e delle regole di detection predefinite e inaccessibili (black-box), possono ostacolare un approccio MDR avanzato.

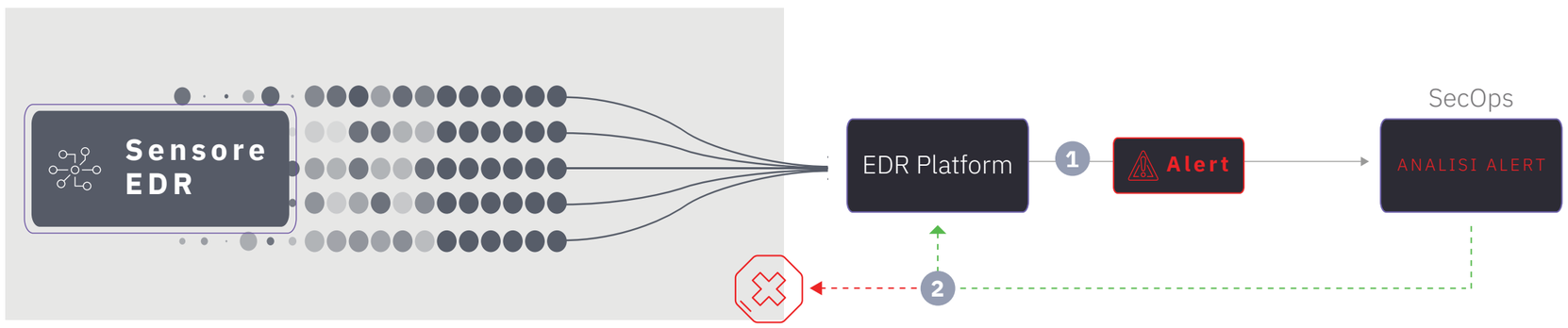
Per ottimizzare le prestazioni delle soluzioni EDR e fornire servizi MDR di livello avanzato, Certego ha sviluppato Halo, la piattaforma che si integra con gli EDR dei vendor per raccogliere, analizzare e arricchire l'intera telemetria degli endpoint.

Halo

- \+ Raccolta e correlazione avanzata degli eventi
- \+ Accelerazione dei tempi di risposta
- \+ Analisi avanzata
- \+ Significativa riduzione dei falsi positivi
- \+ Creazione di regole di detection personalizzate
- \+ Integrazione con Intelligence sulle minacce

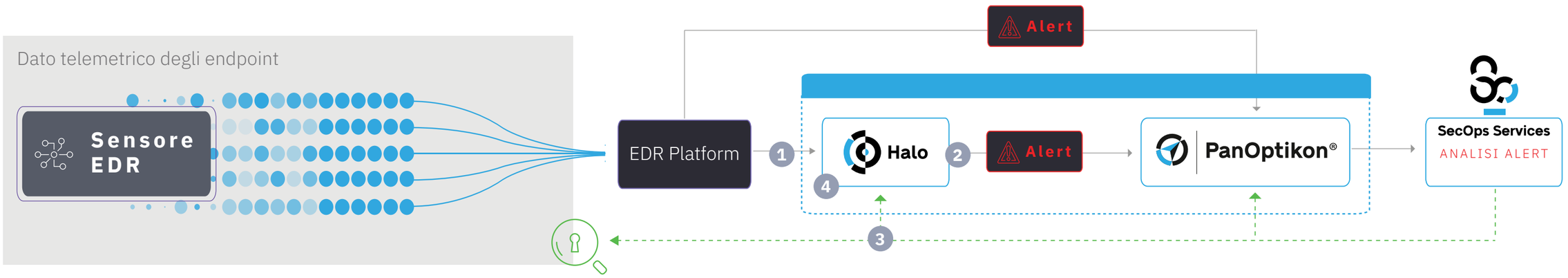
Halo | Unlimited Visibility

Caso 1 | EDR tradizionale | Limitata visibilità dei dati telemetrici degli Endpoint



1. Generazione Alert da parte della piattaforma EDR.
2. Gli strumenti di analisi della piattaforma EDR mostrano solo dati telemetrici parziali, offrono funzionalità di correlazione limitate e non consentono di esaminare le regole di detection che hanno generato un Alert.

Caso 2 | Certego Halo | Completa visibilità dei dati telemetrici degli Endpoint



1. La piattaforma EDR condivide con Halo tutti i dati telemetrici dei sensori Endpoint → Visibilità totale.
2. Halo correla eventi di telemetria multipli per creare un unico alert nella piattaforma PanOptikon® → Riduzione falsi positivi.
3. Attraverso Halo, gli analisti Certego possono esaminare i dati telemetrici degli Endpoint e le regole di detection che hanno generato un allarme in Halo → Analisi più dettagliate, maggiore velocità di risposta.
4. La piattaforma Halo consente di creare regole di detection personalizzate e importare un numero illimitato di IOC e BIOC → Personalizzazione e maggiore precisione di rilevamento.

Halo | Unlimited Visibility

SOLUZIONE SU MISURA

Personalizza e sfrutta al massimo le capacità delle soluzioni EDR

→ **Libertà operativa:** supera le restrizioni black-box dei tradizionali sistemi EDR.

→ **Regole ad hoc:** definisci e applica regole di detection adatte al tuo contesto operativo.

→ **Maggiore controllo:** accedi alle logiche di detection e ottimizza le strategie di risposta.

RIDUZIONE DEI FALSI POSITIVI

Ottimizza i carichi di lavoro

→ **Correlazione avanzata:** le query multi-evento aggregano molteplici segnali in un unico allarme.

→ **Detection sempre aggiornata:** adattamento costante delle regole di detection.

→ **Maggiore precisione:** ricevi solo alert realmente rilevanti, riducendo il rumore di fondo.

INTEGRAZIONI CON FONTI DI THREAT INTELLIGENCE

Applica IOC e BIOC da più fonti senza limiti di importazione

→ **Superamento delle restrizioni:** importa IOC e BIOC, senza i vincoli imposti dagli EDR tradizionali.

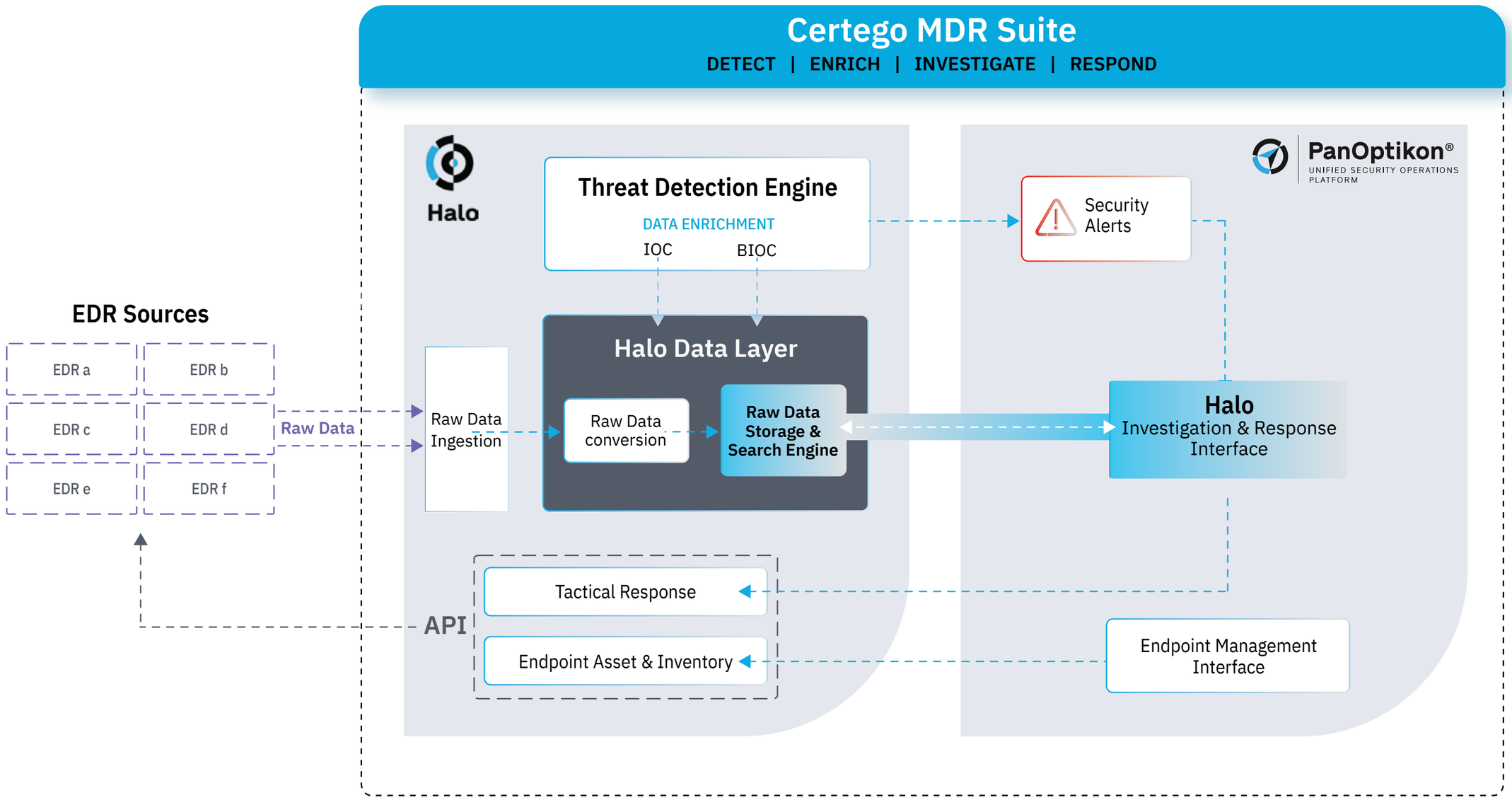
→ **Rilevamento potenziato:** identifica in tempo reale minacce di nuova generazione.

→ **Approccio proattivo:** implementa strategie proattive per anticiparei rischi emergenti.

Halo | Unlimited Visibility

Certego MDR Suite

Halo si integra nell'ecosistema applicativo Certego (MDR Suite), offrendo una soluzione avanzata che garantisce un servizio d'eccellenza in termini di rilevamento, investigazione e risposta alle minacce.



Halo | Unlimited Visibility

Endpoint Detection: EDR tradizionale VS EDR tradizionale + Halo

Halo si integra nell'ecosistema applicativo Certego (MDR Suite), offrendo una soluzione avanzata che garantisce un servizio d'eccellenza in termini di detection, investigazione e risposta alle minacce.

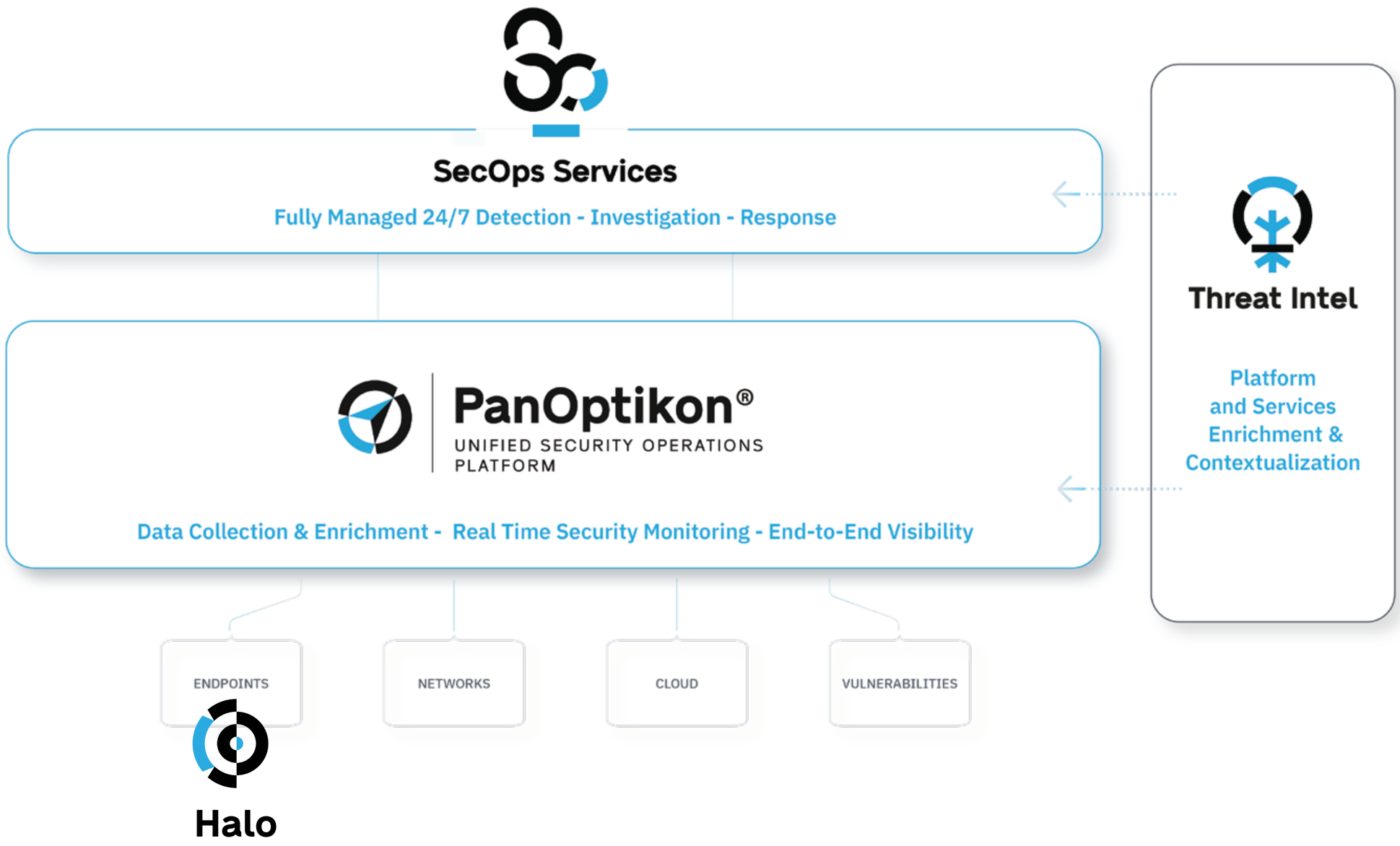
Endpoint Detection Module (Key features)	EDR TRADIZIONALE	Halo + EDR TRADIZIONALE
Devices: Windows, Linux, and Mac OS	✓	✓
Anti-malware & Behavioral analysis	✓	✓
Device control	✓	✓
File & Process Events Monitoring & Logging	✓	✓
Application and Endpoint Inventory	✓	✓
Automatic Remediation	✓	✓
Raw Telemetry Endpoint Visibility & Analysis	Limited Visibility	Full Visibility
24/7 MDR Services		✓
Enhanced Threat Detection Rules (BIOC)		✓
Italian-based Threat Intelligence Rules (IOC)		✓
Custom Threat Hunting		✓
Custom Playbooks		✓
Custom Reports		✓

Certego

Pure-play MDR provider con oltre 12 anni di esperienza nella lotta al cybercrime

L'offerta di Certego si basa su quattro pilastri che, quando integrati sinergicamente, costituiscono il fondamento della sua forza: la piattaforma unificata di Security Operations "**PanOptikon®**", la piattaforma **Halo** per una visibilità completa della telemetria degli endpoint, un team dedicato ai **Security Operations Services** e un'attività di ricerca avanzata in **Cyber Threat Intelligence**.

La forte interconnessione tra tecnologia avanzata, competenze altamente specializzate e analisi approfondita delle minacce posiziona Certego come un player di riferimento nei servizi di Managed Detection & Response (MDR).



50 **Specialisti di cybersecurity**

200+ **Clienti**

1.2M+ **Asset monitorati**

120K **Allarmi rilevati** (2024)

14K **Incidenti gestiti** (2024)

Via F. Lamborghini 81, 41121 Modena (MO)