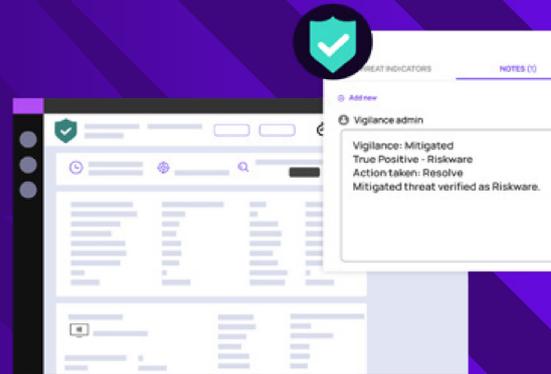


# Servizi gestiti di rilevamento e risposta 24x7x365

Con assegnazione ibrida delle priorità delle minacce basata su IA e risoluzione condotta da esperti, grazie al team di SentinelOne Vigilance

N-able Managed Endpoint Detection and Response (MEDR) amplia le funzionalità di N-able EDR, grazie alla tecnologia SentinelOne, con servizi gestiti di rilevamento e risposta sempre disponibili. Basato sul framework di rilevamento e risposta gestiti di Vigilance Respond, offre servizi esperti di monitoraggio, indagini e risoluzione delle minacce 24 ore al giorno, tutti i giorni, per aiutare i team addetti alla sicurezza a restare al passo con le minacce emergenti senza il carico operativo.



## La tua soluzione EDR avanzata

Per MSP o team IT e di sicurezza interni, N-able Managed Endpoint Detection and Response funge da estensione fluida delle operazioni di sicurezza. La soluzione, supportata da analisti esperti disponibili 24 ore al giorno, tutti i giorni, consente ai team di esternalizzare il monitoraggio delle minacce e l'implementazione di risposte, liberando tempo e risorse che potranno concentrarsi su iniziative strategiche e ad alto impatto.

### Vantaggi di rilevamento e risposta gestiti 24x7x365 condotti da esperti

- ▲ Approfitta della visibilità continua sulle minacce e dell'applicazione rapida di risposte per tutti gli endpoint
- ▲ Elimina la necessità di disporre di personale a ogni ora del giorno e riduci il carico operativo
- ▲ Affida il triage degli avvisi quotidiani ad analisti esperti
- ▲ Riduci lo stress da avvisi grazie alle informazioni sulle minacce basate su contesto e con priorità fornita dall'IA
- ▲ Accelera la risoluzione degli incidenti e riduci i tempi di attesa
- ▲ Supporta la conformità e preparati a eventuali audit grazie alla conservazione avanzata di dati e documentazione sugli incidenti
- ▲ Rafforza la tua posizione per sottoscrivere polizze assicurative per la sicurezza informatica tramite il monitoraggio continuo e l'implementazione di rimedi condotta da esperti

## Come funziona

1

### Rilevamento

I motori basati su IA di N-able EDR eseguono scansioni continue per individuare comportamenti anomali e schemi noti in tutti gli endpoint.

2

### Indagine

Gli analisti multilivello sfruttano IA e machine learning, l'intelligence delle minacce con dati completi e TTP MITRE per classificare e contestualizzare le diverse minacce, riducendo i falsi allarmi e individuando ciò che conta davvero.

3

### Analisi

Ogni incidente è associato a un contesto, inserito nella console e documentato con dati fruibili a supporto di processi decisionali rapidi.

4

### Risposta

Le minacce sono contenute e risolte da analisti esperti, con trasferimento proattivo al bisogno, il che assicura interruzioni minime e la massima efficienza.

## I vantaggi di N-able Managed EDR



### Monitoraggio continuo, classificazione e assegnazione delle priorità

- ▲ Monitoraggio continuo degli endpoint grazie ad analisti esperti che assicurano l'individuazione di ogni singola minaccia.
- ▲ Triage e assegnazione priorità basati su IA, personalizzati in base all'ambiente, che riducono i falsi allarmi e rilevano ciò che conta.
- ▲ L'approccio human-in-the-loop migliora l'accuratezza del rilevamento e riduce lo stress da avvisi.



### Coinvolgimento e reportistica continui

- ▲ Notifiche in tempo reale per la verifica di attività malevole o sospette.
- ▲ Report programmati di Vigilance Insights per la massima visibilità sulle tendenze per le minacce, gli interventi di mitigazione e i falsi positivi.
- ▲ I trasferimenti sono riservati agli eventi critici, così il tuo team può occuparsi di ciò che conta di più.



### Ricerca delle minacce emergenti

- ▲ Ricerca delle minacce avanzata con la licenza N-able EDR Complete.
- ▲ Ricerche proattive condotte dagli analisti per le tecniche di attacco, sfruttando l'intelligence globale sulle minacce.
- ▲ Bollettini e avvisi tempestivi sulle minacce per ricevere aggiornamenti circa le campagne pertinenti.



### Indagine, contenimento e risposta alle minacce

- ▲ Storico delle minacce basato sul contesto valutato e commentato direttamente nella console EDR.
- ▲ Contenimento e risoluzione rapidi grazie ad analisti esperti e supportati da SLA di risposta pari a quattro ore.
- ▲ La conservazione dati estesa supporta la conformità, ti prepara a eventuali audit e alla ricostruzione degli incidenti.



### Conformità e preparazione alla stipula di polizze assicurative

- ▲ Documentazione completa sugli incidenti e conservazione dei dati a lungo termine aiutano e rispettano i requisiti normativi.
- ▲ Monitoraggio continuo e implementazione di rimedi condotta da esperti rafforzano la tua posizione per la sottoscrizione di polizze assicurative.



In N-able, la nostra mission è proteggere le attività dalle minacce informatiche in evoluzione con una piattaforma unificata di resilienza informatica per gestione, messa in sicurezza e ripristino. La nostra infrastruttura tecnologica scalabile include funzionalità basate su IA, integrazioni di terze parti leader del settore e la flessibilità necessaria per utilizzare le tecnologie di preferenza al fine di trasformare i flussi di lavoro e di produrre risultati di sicurezza critici. Il nostro approccio incentrato sui partner combina prodotti, esperti, formazione ed eventi tenuti da colleghi che consentono ai nostri clienti di stare al sicuro, essere resilienti e avere successo. [n-able.com/it](https://n-able.com/it)

---

Il presente documento viene fornito per puro scopo informativo e i suoi contenuti non vanno considerati come una consulenza legale. N-able non rilascia alcuna garanzia, esplicita o implicita, né si assume alcuna responsabilità legale per le informazioni qui contenute, per l'accuratezza, la completezza o l'utilità dei dati qui inclusi.

I marchi registrati, i marchi di servizio e i loghi di N-able sono di esclusiva proprietà di N-able Solutions ULC e N-able Technologies Ltd. Tutti gli altri marchi registrati sono di proprietà dei rispettivi titolari.

© 2025 N-able Solutions ULC e N-able Technologies Ltd. Tutti i diritti riservati.