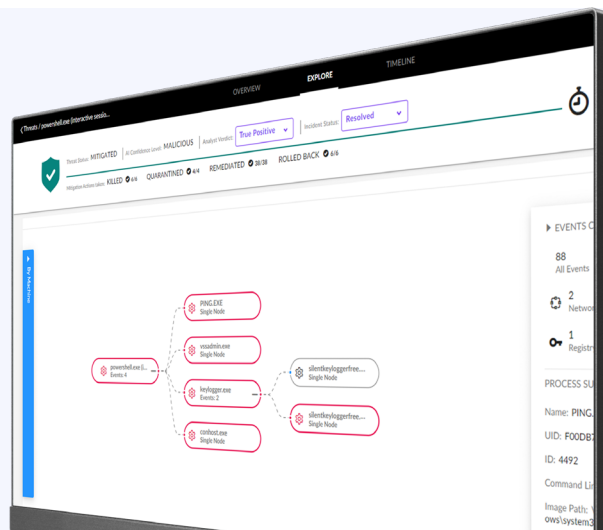


## Endpoint Detection and Response

Una soluzione standalone di N-able con tecnologia SentinelOne®

Con N-able™ Endpoint Detection and Response (EDR) MSP e reparti IT prevencono, rilevano e risolvono le minacce informatiche in continua evoluzione, grazie al rilevamento minacce basato su IA comportamentale, all'applicazione automatica di rimedi e al rollback. I professionisti della sicurezza hanno a disposizione l'implementazione intuitiva basata sui criteri di Automation Manager e la verifica dell'integrità EDR all'interno delle piattaforme di monitoraggio e gestione da remoto di N-able.



### Sfrutta diversi motori di rilevamento basati su IA

- Avvaliti dell'IA per analizzare i nuovi schemi delle minacce e il machine learning per migliorare le modalità di reazione
- Rileva le attività dannose, come lo sfruttamento della memoria, grazie all'intelligenza artificiale comportamentale
- Rileva il malware avanzato, basato su file e senza firme grazie all'IA statica

### Tieni alla larga gli attacchi informatici

- Proteggi i clienti dalle nuove minacce senza attendere le scansioni ricorrenti o gli aggiornamenti alle definizioni dei malware
- Applica una protezione basata su criteri e personalizzata per i clienti, bloccando o consentendo l'accesso alle unità USB e ai dispositivi

### Rispondi efficacemente grazie all'automazione

- Automatizza il rapido contenimento delle minacce oltre alle operazioni di eliminazione, messa in quarantena e applicazione di rimedi
- Ripristina l'integrità di endpoint e file compromessi precedente all'attacco in caso di ransomware (solo per sistemi operativi Windows)

### Accelera le indagini sulle minacce

- Utilizza l'intelligence sulle minacce immediatamente disponibile tramite feed leader di terze parti e fonti SentinelOne per completare tutte le indagini necessarie
- Visualizza l'attività delle minacce (la catena completa degli eventi che hanno portato a un attacco) per comprendere rapidamente il contesto, la causa scatenante e i lateral movement

### Tecnologia SentinelOne®,

**leader nella valutazione 2022 MITRE Engenuity™ ATT&CK®:**

- 100% protezione e rilevamento
- Elevata visibilità e copertura per analisi
- 100% in tempo reale. Zero ritardi nel rilevamento

## Collegati senza intoppi ai sistemi di terze parti

- Semplifica gli eventi syslog per il SIEM
- Sfrutta le notifiche granulari per assegnare la priorità e instradare i ticket tramite il sistema di gestione di ticket PSA
- Utilizza i servizi API

## Piattaforma Singularity™

- Pacchetti Singularity™ Control e Complete disponibili
- Include il controllo di dispositivi e firewall dell'endpoint, l'esecuzione di una shell remota, la quarantena di rete e sistemi antimanomissione

## Informazioni su N-able

N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e ad espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore.

[n-able.com/it](https://n-able.com/it)

© 2022 N-able Solutions ULC e N-able Technologies Ltd. Tutti i diritti riservati.

I marchi registrati, marchi di servizio e loghi 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.

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.