

Soluzioni di rilevamento e risposta per gli endpoint

# Come dimostrare il ritorno sull'investimento

**e-guide**



## Introduzione

La pandemia ha stravolto il modo di condurre le nostre attività quotidiane. Passiamo più tempo online a lavorare, fare shopping, partecipare a eventi virtuali e persino a consultare medici. Tutto questo impone alle aziende di accelerare la transizione al cloud. Se aggiungiamo l'uso di dispositivi personali e il lavoro da casa a questo quadro, avremo una maggiore connettività e superfici di attacco più ampie per individui e imprese.

È responsabilità degli MSP gestire e proteggere asset IT, dati e procedure aziendali dei clienti, pertanto queste figure spesso hanno un ampio accesso ai sistemi dei clienti. Questo fa di MSP e dei relativi strumenti un interessante vettore di attacco. Secondo un recente [report di N-able](#)<sup>1</sup>, gli MSP stanno rapidamente diventando obiettivi primari per gli attacchi informatici, con il 90% di loro che registra un aumento degli attacchi da inizio pandemia. E non ci sono segnali che questa tendenza rallenti.

Nel corso degli ultimi anni, abbiamo assistito a una rapida adozione dei sistemi di rilevamento e risposta per gli endpoint nel settore degli MSP. Un numero sempre maggiore di provider di servizi sta scegliendo di [abbandonare le soluzioni antivirus tradizionali](#)<sup>2</sup> a favore degli strumenti di rilevamento e risposta per gli endpoint. Tuttavia, alcuni incontrano resistenze da parte dei clienti e viene loro chiesto di dimostrare il ritorno sull'investimento di questa scelta.

In questa e-guide, illustreremo le best practice per risolvere questa sfida e discutere in modo proattivo delle soluzioni di rilevamento e risposta con le parti interessate.

## Best practice per dimostrare il ROI di una soluzione di rilevamento e risposta per gli endpoint

Dimostrare il ritorno sull'investimento può risultare un'operazione impegnativa. Tuttavia, con un approccio ben concepito e strutturato, è più semplice.

1. Istruisci i clienti sul panorama di minacce informatiche
2. Comprendi le esigenze e le prospettive aziendali
3. Svela i costi reali di un attacco
4. Delinea la tua soluzione e i piani futuri per la sicurezza
5. Poni opportuni limiti se i clienti continuano a rifiutarsi

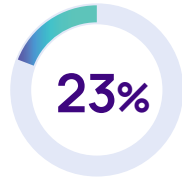
**Vediamo alcuni argomenti chiave per conversazioni per ciascun punto.**

## 1 Istruisci i clienti sul panorama di minacce informatiche

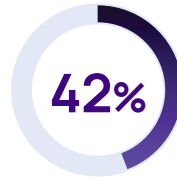
Usa le statistiche per illustrare un quadro rilevante. E se non sono sufficienti, puoi citare le ultime notizie circa le violazioni, ad esempio:

**105%**

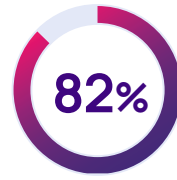
Il ransomware ha battuto nuovi record nel 2021, con un aumento del **105% rispetto al 2020**<sup>4</sup>



Il **23% delle violazioni dati** è causata dall'errore umano<sup>5</sup>



Il **42% degli attacchi registrati più di frequente** dagli MSP è dovuto a ransomware<sup>6</sup>



L'**82% dei clienti degli MSP ha registrato** l'aumento dei tentativi di attacco informatico<sup>7</sup>

Il tuo obiettivo non è quello di spaventare, ma piuttosto di aiutare i clienti a capire che tutte le aziende, di qualsiasi dimensione, rappresentano obiettivi appetibili e che le soluzioni legacy non riescono a stare al passo con i rapidi progressi delle minacce di sicurezza informatiche.

## 2 Comprendi le esigenze e le prospettive aziendali

Assicurati di comprendere al meglio esigenze e attività dei tuoi clienti. Per scoprire cosa davvero conta per loro e proporre una soluzione adeguata, chiedi ai clienti quali sono gli obiettivi aziendali e i presupposti. Ecco alcune domande per iniziare:

- L'azienda è mai stata colpita da ransomware o altro malware?
- Si sono verificati tempi di inattività nelle procedure operative aziendali? Qual è stato il loro effetto?
- L'impatto dei tempi di inattività sull'azienda è fonte di preoccupazioni?
- Quale sarebbe il costo orario dei tempi di inattività?
- Esiste un piano di emergenza in caso di indisponibilità dei sistemi o dei dati?
- L'azienda può continuare a lavorare in caso di indisponibilità temporanea dei sistemi? Per quanto tempo?
- La situazione attuale è fonte di preoccupazione?
- Quali responsabilità legali sarebbero previste se i servizi diventassero improvvisamente non disponibili?
- Realisticamente, per quanto tempo sarebbe possibile andare avanti senza accedere ai dati?
- Quale sarebbe l'impatto sulla reputazione dell'azienda se i clienti restassero senza assistenza per un giorno?
- Le polizze assicurative informatiche e per la protezione dei dati sono state riviste? L'azienda è a rischio di mancata copertura se non vengono impiegate le più recenti tecnologie di sicurezza?

Di solito le obiezioni che vengono mosse agli MSP dai relativi clienti durante queste conversazioni riguardano l'aumento dei prezzi per una soluzione avanzata (ad esempio quelle di rilevamento e risposta per gli endpoint) e il dubbio che l'attività del cliente sia troppo piccola e poco appetibile per i criminali informatici. Niente di più falso.

Ecco alcune delle obiezioni più comuni mosse agli MSP e come contrastarle:

### “Ho già una soluzione antivirus. Non ho bisogno di uno strumento di rilevamento e risposta per gli endpoint”

Il paragone non regge perché i clienti non prendono in considerazione i diversi livelli di protezione offerti da ciascuna delle due soluzioni e sottovalutano il componente personale/lavoro. Spiega loro le differenze tra le due soluzioni, soprattutto per quanto riguarda i diversi livelli di protezione e il lavoro che implica la gestione della sicurezza con ciascuna delle due soluzioni.

**Le soluzioni di rilevamento e risposta per gli endpoint offrono un'ampia gamma di funzionalità molto più avanzate rispetto alla semplice protezione con antivirus. Ecco un rapido riepilogo delle differenze tra le due soluzioni:**

#### ANTIVIRUS

- Proteggono da malware e virus. Generalmente necessitano di un file da scansionare.
- Normalmente si basano sulle firme dei virus. Ciò significa che il fornitore dell'antivirus deve avere individuato il software dannoso, inviato l'aggiornamento delle firme alla base utenti e l'utente finale deve avere aggiornato le firme dei virus.
- L'amministratore deve eseguire delle scansioni regolarmente.

#### Soluzioni di rilevamento e risposta per gli endpoint

- Proteggono da diversi vettori di attacco (tra cui attacchi senza file, documenti dannosi e script pericolosi avviati al di fuori di una finestra di scansione) utilizzando l'intelligenza artificiale per valutare il comportamento.
- Cercano attivamente potenziali minacce, invece che affidarsi a una scansione. Se rilevano attività sospette, avvisano quasi in tempo reale (se l'avviso è giustificato).
- Rispondono automaticamente alle potenziali minacce. Alcune soluzioni di rilevamento e risposta per gli endpoint, come N-able EDR, permettono persino di eseguire il rollback degli endpoint basati su Windows a uno stato sicuro noto subito dopo un attacco ransomware, il che consente di annullare i danni subiti.

Secondo alcuni [sondaggi di settore](#)<sup>8</sup> e in base all'esperienza dei nostri esperti di sicurezza, il tempo mediano impiegato per l'applicazione manuale di rimedi dopo che una soluzione antivirus ha rilevato una minaccia corrisponde a circa 3,5 ore. Per contro, la qualità dei dati analitici e telemetrici registrati da una soluzione di rilevamento e risposta per gli endpoint, insieme all'applicazione automatica di rimedi (incluso il rollback) e alle funzionalità aggiuntive, può ridurre le tempistiche di risoluzione a meno di 30 minuti e spesso ad appena cinque minuti.

### “I costi sono troppo elevati”

Concentrandoti sul valore dei tuoi servizi, è più facile che tu riesca a placare i dubbi delle parti interessate. Fai comprendere ai clienti a quali altri costi potrebbero andare incontro se non passano a un programma di sicurezza avanzato.

### “Correrò il rischio, pagherò il riscatto e procederò con la richiesta di indennizzo assicurativo”

Le compagnie assicurative generalmente faranno di tutto per dimostrare la negligenza dell'assicurato. Basta poco perché respingano la richiesta di risarcimento.

### “La mia azienda è troppo piccola: a me non succederà”

Chiunque è vulnerabile a un attacco. Il cliente potrebbe non essere l'obiettivo previsto, ma fungere da varco di ingresso. Aiuta i clienti a evitare di diventare l'anello debole della catena.

### “A me non succederà: chi dovrebbe volere i miei dati?”

I tuoi dati potrebbero non interessare ai criminali informatici, ma questi potrebbero comunque volerli tenere in ostaggio perché tu ne hai bisogno e la tua attività potrebbe essere a rischio se li perdi. I criminali vogliono metterti in condizione di pagare il riscatto.

## 3 Svela i costi reali di un attacco

Quando si sostiene la “causa” di una nuova soluzione di sicurezza, occorre utilizzare un termine chiaro per qualsiasi dirigente di azienda: denaro.

Sono due gli aspetti che rapidamente giustificano l'acquisto di una soluzione di rilevamento e risposta per gli endpoint: il costo dei tempi di inattività (che si traduce in perdite economiche a seguito della perdita di opportunità commerciali) e i tempi necessari per tornare operativi, che si traducono in lavoro e impegno per i dipendenti.

Per rendere tutto più concreto, chiedi alle parti interessate di immaginare uno scenario in cui i sistemi sono completamente fuori uso a causa di un attacco ransomware. Poi, fai il calcolo dei costi. A confronto, una soluzione di rilevamento e risposta per gli endpoint sembrerà un vero affare.

Il costo giornaliero dell'inattività può essere calcolato in questo modo: produttività persa + perdita di ricavi + costo del ripristino + costi immateriali, vale a dire i seguenti, in base ai diversi casi:

- Pagamento del riscatto
- Sanzioni e penali normative
- Costi legali
- Premi assicurativi più alti
- Consulenze e formazione dei dipendenti
- Danni collaterali
- Perdita di opportunità commerciali o di clienti
- Danni reputazionali

## Ecco un esempio a cui ricorrere a supporto della conversazione:

### Presupposti:

Un'azienda di contabilità con 40 dipendenti viene colpita da un attacco ransomware che causa l'indisponibilità dei sistemi per 24 giorni. Considerando una giornata lavorativa di otto ore, il numero di ore di inattività sarà pari a 192.

In termini di produttività persa per queste 192 ore e supponendo che tutti i dipendenti siano interessati e che il costo orario per dipendente corrisponda a 50 \$, ecco il calcolo dei costi della mancata produttività:

Le best practice relative al ritorno sull'investimento di una soluzione di rilevamento e risposta per gli endpoint condivise in questa guida sono state fornite dall'Head Nerd di N-able Stefanie Hammond.

Segui il [team di Head Nerd di N-able](#) per conoscere altre best practice concepite per la crescita delle attività di MSP, [gli eventi per la sicurezza](#) e i corsi di formazione.

#### COSTO DEI TEMPI DI INATTIVITÀ (192 ORE)

##### 1. Costi della produttività dei dipendenti

Reparti interessati dall'inattività:

TUTTI

N. di dipendenti in azienda

40

N. di dipendenti dei reparti interessati

40

% media della mancata produttività

100%

Costo medio dei dipendenti per ora

50 \$

N. totale di ore di inattività

192

Costi della produttività dei dipendenti

384.000 \$

In termini di costi legati ai mancati ricavi, supponendo che i ricavi lordi annuali siano pari a 1 milione di dollari, con un numero di giorni lavorativi pari a 240 (cinque giorni a settimana x 48 settimane in un anno), e che l'intera somma dei ricavi persi sia irrecuperabile, ecco il calcolo della mancata produttività:

## COSTO DEI TEMPI DI INATTIVITÀ

### 2. Costi legati alla perdita di ricavi

Fatturato lordo annuale	1.000.000 \$
N. di giorni lavorativi all'anno per l'azienda	240
N. di ore lavorative al giorno	8
% del giro d'affari irrecuperabile	100%
Ricavi persi al giorno	4.166,67 \$
Ricavi persi all'ora	520,83 \$
Ricavi persi per la durata dell'inattività	100.000 \$

Per quanto riguarda i costi legati all'applicazione di opportuni rimedi, se consideriamo la tariffa media di lavoro per un tecnico di sicurezza IT come pari a 150 \$ all'ora, ecco il calcolo dei costi di applicazione di opportuni rimedi:

## COSTO DEI TEMPI DI INATTIVITÀ (192 ORE)

### 3. Costi legati all'applicazione degli opportuni rimedi

N. totale di ore di lavoro necessarie per il ripristino totale	192
Tariffa oraria di lavoro per l'applicazione degli opportuni rimedi	150 \$
Costi totali per il ripristino del sistema (costi legati all'applicazione dei rimedi)	28.800 \$

Quindi, i costi nascosti legati all'inattività potrebbero essere pari ai costi della produttività dei dipendenti + i mancati ricavi per il periodo di inattività + i costi dell'applicazione dei rimedi:

**Costo totale dell'inattività** **512.800 \$**

**Costo totale dell'inattività/ora** **2.670,83 \$**

Aggiungendo i costi immateriali, in base a quanto considerato in precedenza, il costo totale di un attacco ransomware è significativamente più alto. Ad esempio, considerando il riscatto medio di 925.000 \$, in base a quanto dichiarato da Palo Alto, i costi nascosti potrebbero superare il milione di dollari.

Per stimare l'impatto complessivo, l'azienda deve valutare gli altri costi immateriali che valgono per le diverse imprese oltre che considerare domande quali:

- Che succederebbe se l'azienda non fosse in grado di consegnare i progetti previsti a causa dell'attacco?
- Che succederebbe se l'azienda perdesse i clienti?
- Qual è l'impatto del passaparola?

In altre parole, quale sarebbe l'impatto dell'evento sulle attività, sulla reputazione e quindi sulla bottom line dell'azienda? L'impatto complessivo si tramuta in costi nascosti più i costi associati alla reputazione danneggiata, alla perdita dei clienti e ad altri danni imprevedibili.

Se confrontiamo i costi illustrati nell'esempio precedente con il costo reale dell'implementazione di una soluzione di rilevamento e risposta per gli endpoint per contrastare gli effetti catastrofici di un attacco ransomware, i risparmi annuali potrebbero stupirci.

## 4 Delinea la tua soluzione e i piani futuri per la sicurezza

Il tuo approccio globale per la sicurezza è robusto quanto il tuo anello più debole. Se permetti ai clienti di determinare la validità della suite di sicurezza e delle misure di protezione in base a un budget arbitrario e preconcorso, un attacco a un cliente può servire da backdoor anche nella tua attività di MSP.

### **Secondo le best practice, dovresti:**

- Implementare un programma di protezione di base e applicarlo a tutti i clienti. Via via che il panorama di sicurezza informatica diventa sempre più sofisticato, le soluzioni proattive, come quelle di rilevamento e risposta per gli endpoint, potrebbero aiutare a proteggerti dalle minacce informatiche di nuova generazione, sia note sia sconosciute e vanno viste come una protezione di base.
- Dimostrare lungimiranza ed esperienza in merito alla sicurezza spiegando il tuo programma ai clienti e obbligarli ad adottarlo.

## 5 Poni opportuni limiti se i clienti continuano a rifiutarsi

Sei tu ad avere esperienza circa la sicurezza per i tuoi clienti. Quando succede un disastro, è te che chiameranno per risolvere il problema. Se non vogliono adottare il programma di protezione che hai sviluppato, dovranno assumersi la responsabilità delle conseguenze della mancata implementazione dei tuoi suggerimenti.

Devi inoltre avere un piano per evitare che i clienti non rappresentino un rischio per la tua azienda. Questo piano potrebbe prevedere un nuovo accordo quadro per l'erogazione dei servizi con una responsabilità limitata o una clausola liberatoria, una lettera di accettazione dei rischi e nuovi obiettivi per il livello di servizi che applichino tariffe diverse in caso di inattività, laddove non siano implementate le misure appropriate.

### Conclusioni

Dimostrare il ritorno sull'investimento durante le conversazioni finalizzate alla vendita è come fare un disegno per raccontare una storia a tema sicurezza informatica. Le strategie illustrate in precedenza dovrebbero aiutarti a fare chiarezza durante le conversazioni con i clienti. Puoi ulteriormente perorare la tua causa condividendo recensioni positive e storie di successo che dimostrino quanto altri clienti abbiano beneficiato dei tuoi servizi, mostrando report e articoli di settore che raccontino le richieste esorbitanti degli hacker nei recenti attacchi ransomware o le statistiche che spiegano i costi legati a questo tipo di violazioni per un'azienda che non abbia implementato un adeguato piano di protezione. Qualsiasi esempio concreto citato durante la conversazione finalizzata alla vendita metterà in luce la serietà della questione e darà credibilità alla tua azienda.

Per sfruttare al meglio i consigli forniti nella presente guida, sarà necessario offrire a tutti gli interessati un'eccellente soluzione di protezione degli endpoint.

Scopri di più

Per ulteriori informazioni, visita la pagina

<https://www.n-able.com/it/products/endpoint-detection-and-response>.

## Risorse

<sup>1</sup><https://www.n-able.com/it/resources/state-of-the-market-the-new-threat-landscape>

<sup>2</sup><https://www.n-able.com/it/press/press-releases/n-able-partners-worldwide-say-goodbye-to-legacy-av-solutions-in-favor-of-sentinelone-edr-to-protect-over-1-million-customer-endpoints>

<sup>3</sup> <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2022-97-million-records-breached>

<sup>4</sup><https://www.sonicwall.com/2022-cyber-threat-report/>

<sup>5</sup><https://www.ibm.com/security/data-breach>

<sup>6</sup>Situazione del mercato | Il nuovo panorama delle minacce | Il futuro della sicurezza degli MSP, report di N-able, marzo 2022: <https://www.n-able.com/it/resources/state-of-the-market-the-new-threat-landscape>

<sup>7</sup>Situazione del mercato | Il nuovo panorama delle minacce | Il futuro della sicurezza degli MSP, report di N-able, marzo 2022: <https://www.n-able.com/it/resources/state-of-the-market-the-new-threat-landscape>

<sup>8</sup><https://blog.barracuda.com/2019/09/26/threat-spotlight-inefficient-incident-response/#:~:text=Inefficient%20incident%20response%20%E2%80%94%20Suspicious%20emails,click%20on%20a%20malicious%20link.>

<sup>9</sup>In media i giorni di inattività sono pari a 24, secondo un report del 2022 di Coveware: <https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022>

<sup>10</sup><https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/#:~:text=The%20numbers%20are%20startling%3A%20The,rose%2071%25%20from%20last%20year>

## 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 a 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://www.n-able.com/it)

N-ABLE, N-CENTRAL e gli altri marchi e loghi di N-able sono di esclusiva proprietà di N-able Solutions ULC e N-able Technologies Ltd. e potrebbero essere marchi di common law, marchi registrati o in attesa di registrazione presso l'Ufficio marchi e brevetti degli Stati Uniti e di altri paesi. Tutti gli altri marchi menzionati qui sono utilizzati esclusivamente a scopi identificativi e sono marchi (o potrebbero essere marchi registrati) delle rispettive aziende.

Il presente documento viene fornito per puro scopo informativo. Le informazioni e i punti di vista qui espressi potrebbero cambiare e/o potrebbero non essere applicabili al singolo caso. N-able non rilascia alcuna garanzia, esplicita o implicita, né si assume alcuna responsabilità legale per quanto riguarda l'accuratezza, la completezza o l'utilità delle informazioni qui contenute.