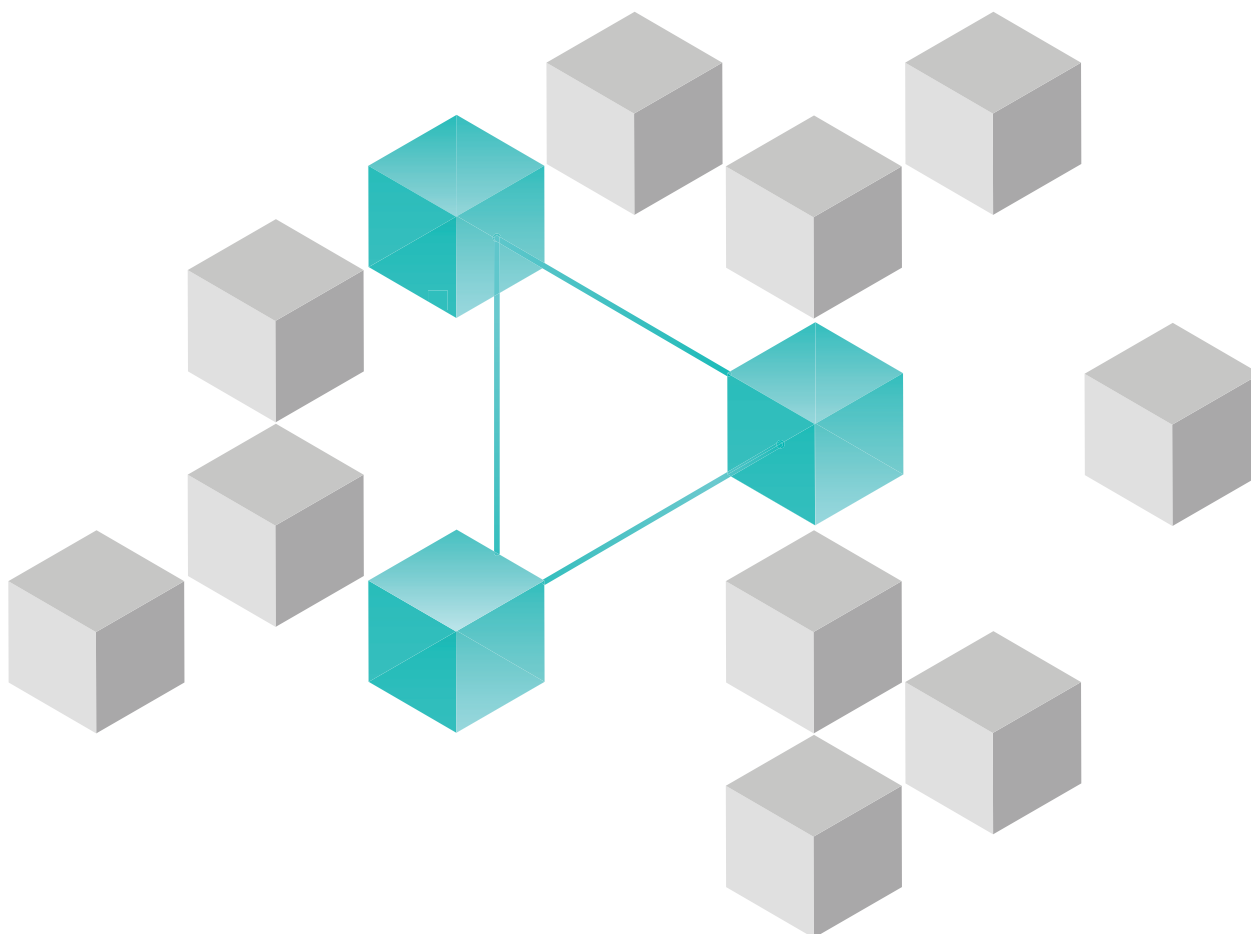


# IBM Security ReaQta per MSSP

La sicurezza come strategia di crescita



# Introduzione a IBM Security ReaQta per MSSP

Progettata per consentire agli MSSP (Managed Security Service Providers, Fornitori di servizi di sicurezza gestiti) di gestire e proteggere facilmente un numero più elevato di endpoint per i propri clienti, questa elogiata piattaforma di sicurezza degli endpoint semplifica la gestione grazie a potenti e complete funzionalità EDR (Endpoint Detection and Response) di rilevamento e risposta degli endpoint.

La piattaforma ReaQta facilita agli MSSP il trattamento e la gestione delle minacce, dotandoli al contempo di potenti funzionalità di threat hunting e automazione. In questo modo, gli MSSP possono sfruttare funzioni come il monitoraggio continuo e la risposta agli incidenti o l'analisi post-violazione su un'unica piattaforma.

Sfruttando l'intelligenza artificiale e l'apprendimento automatico, ReaQta combina livelli eccezionali di automazione a un design intuitivo per rilevare e correggere in modo autonomo le minacce conosciute o sconosciute, quasi in tempo reale.

Attraverso il deep learning, la piattaforma si migliora costantemente nella definizione del comportamento normale personalizzandolo su ogni singola azienda e su ogni endpoint e bloccando qualsiasi comportamento anomalo. Di conseguenza, grazie agli MSSP si ottengono sicurezza senza complessità e la tranquillità di sapere che i dati e le risorse preziosi dei propri clienti sono protetti in modo sicuro dalle minacce più avanzate.

## Principali vantaggi per gli MSSP



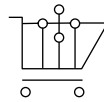
### Aumento della produttività

I livelli eccezionali di intelligenza artificiale e apprendimento automatico della piattaforma ReaQta rilevano e correggono in modo autonomo anche le minacce più sofisticate e lo fanno quasi in tempo reale, liberando il personale dal peso delle analisi manuali.



### Miglioramento dell'efficienza

ReaQta riduce la stanchezza dovuta ai continui allarmi degli MSSP fornendo in tempo reale avvisi condensati ad alta fedeltà che consentono una visibilità diretta e una comprensione approfondita dei processi. Ciò aiuta ad agire rapidamente per fermare le minacce in modo veloce ed efficace.



### Riduzione dei costi

La piattaforma semplifica le operazioni agli MSSP, grazie a un'interfaccia intuitiva e di facile utilizzo e a processi automatizzati. Non richiede l'impiego di personale altamente qualificato o aggiuntivo.



# Tre motivi per cui gli MSSP stanno passando a ReaQta

## 1. Tecnologia di livello mondiale

Stiamo reinventando l'EDR. ReaQta è una piattaforma completamente automatizzata, che rileva e corregge in modo autonomo le minacce più avanzate. Il nostro utilizzo unico dell'intelligenza artificiale e dell'apprendimento automatico, in combinazione con la nostra tecnologia proprietaria NanoOS, è progettato per essere invisibile agli aggressori e ai malware. Inoltre, non può essere manomesso, disattivato o sostituito.

Grazie alla tecnologia NanoOS, gli MSSP ottengono una visibilità completa sui processi e le applicazioni in esecuzione sugli endpoint dei propri clienti. NanoOS si trova al livello dell'hypervisor e protegge l'endpoint restando al di fuori del sistema operativo.

## 2. Miglior supporto del settore

Crediamo fermamente che i clienti debbano sempre avere la priorità. Ottenere una risposta a una domanda non deve comportare lunghe attese nelle code del supporto clienti e interazioni con una miriade di persone diverse. Accedi direttamente a personale di supporto esperto, cordiale e dedicato, nonché formato e autorizzato a gestire la tua domanda dal primo contatto alla risoluzione.

## 3. ROI maggiore

Gestisci e proteggi più endpoint. Aumenta l'efficienza del tuo team e incrementa la produttività grazie ad avvisi accuratamente sintetizzati e di alta precisione, che offrono agli MSSP una visibilità diretta su tutte le attività degli endpoint e delle minacce. La nostra intuitiva interfaccia utente riduce anche i costi, poiché non richiede personale aggiuntivo o altamente qualificato.

# Progettata per un facile utilizzo e una gestione semplificata

## Più facile da utilizzare

- Sfrutta l'elevato livello di automazione della piattaforma ReaQta. Contrasta qualsiasi situazione in pochi secondi grazie a un'assistenza completa fino alla correzione dei problemi e ad automazioni di risposta clickthrough che forniscono agli analisti un flusso di lavoro unico e facile da usare.
- Il design intuitivo della piattaforma, insieme agli avvisi strutturati e di grande precisione, riduce il livello di abilità richieste per rispondere alle minacce.
- Scopri il threat hunting semplificato. Le strategie di rilevamento mediante un solo clic della piattaforma ReaQta possono essere implementate in modo efficiente per tutta la base clienti.
- Cyber Assistant apprende dalle azioni degli analisti, riducendo il peso del lavoro ripetitivo e liberando tempo che è possibile dedicare alle analisi di livello superiore e al threat hunting.
- Gli MSSP possono collegare facilmente ReaQta ad altri componenti dello stack di soluzioni grazie a un'API flessibile di programmazione delle applicazioni.

## Semplice da gestire

- La piattaforma ReaQta è multi-tenant e pensata per gli MSSP e consente di gestire con pochi clic i clienti sia esistenti che nuovi.
- La potente funzione di reporting della piattaforma permette agli MSSP di condividere informazioni tecniche e di gestione in modo veloce e conforme per singoli clienti o in generale.
- Le flessibili opzioni di implementazione aiutano gli MSSP a rispettare le politiche di gestione dei dati dei clienti.

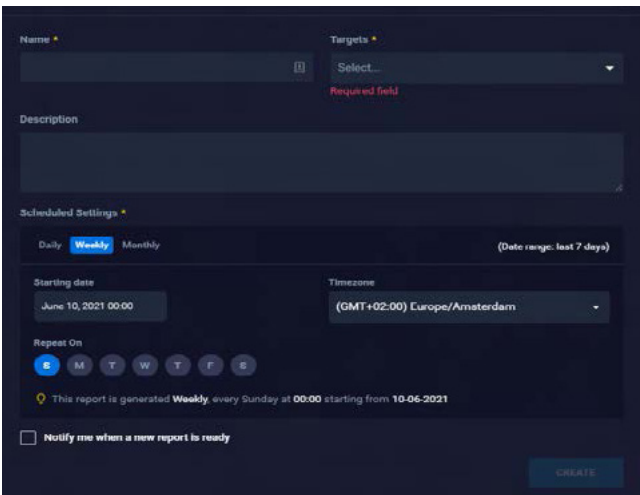
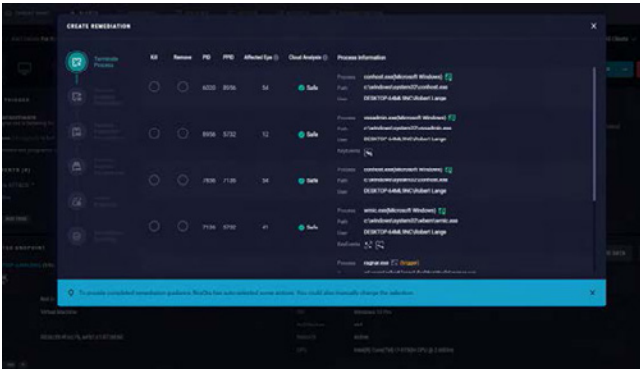
## Guarda IBM Security ReaQta in azione

Per ulteriori informazioni, visita:

[ibm.com/it-it/products/reaqta](https://ibm.com/it-it/products/reaqta)

**Tutti gli strumenti di cui hai bisogno, in un solo posto**

Sfrutta il monitoraggio continuo, la risposta agli incidenti e l'analisi post-violazione, il tutto su un'unica piattaforma.



© Copyright ReaQta, an IBM Company 2022

**IBM Italia S.p.A.**

Circonvallazione Idroscalo  
20054 Segrate (Milano)  
Italia

Prodotto negli Stati Uniti d'America  
Marzo 2022

IBM, il logo IBM e ibm.com sono marchi o marchi registrati di International Business Machines Corp., registrati in diversi Paesi del mondo. Altri nomi di prodotti e servizi potrebbero essere marchi di proprietà di IBM o di altre società. Un elenco aggiornato di marchi IBM è disponibile sul Web in "Copyright and trademark information" all'indirizzo [ibm.com/trademark](http://ibm.com/trademark).

Le informazioni contenute nel documento sono aggiornate alla data della prima pubblicazione e potrebbero essere modificate da IBM senza alcun preavviso. Non tutte le offerte sono disponibili in tutti i Paesi in cui IBM opera.

LE INFORMAZIONI FORNITE NEL PRESENTE DOCUMENTO SONO DA CONSIDERARSI "NELLO STATO IN CUI SI TROVANO", SENZA GARANZIE, ESPLICITE O IMPLICITE, IVI INCLUSE GARANZIE DI COMMERCIALIZZABILITÀ, DI IDONEITÀ PER UN PARTICOLARE SCOPO E GARANZIE O CONDIZIONI DI NON VIOLAZIONE. I prodotti IBM sono coperti da garanzia in accordo con termini e condizioni dei contratti sulla base dei quali vengono forniti.

Dichiarazione di conformità alle procedure di sicurezza: la sicurezza dei sistemi IT implica la protezione di sistemi e dati mediante prevenzione, rilevamento e risposta ad accessi impropri all'interno e all'esterno dell'azienda. L'accesso improprio può causare l'alterazione, la distruzione, l'appropriazione indebita o l'uso improprio delle informazioni; può inoltre provocare danni e uso improprio dei sistemi, che possono essere utilizzati per attaccare altri sistemi. Nessun prodotto o sistema IT può essere considerato completamente sicuro e nessun prodotto, servizio o misura di sicurezza è del tutto efficace nel prevenire l'uso o l'accesso improprio. Sistemi, prodotti e servizi IBM sono progettati come elementi di un approccio di sicurezza completo, nel rispetto delle normative, che richiederà necessariamente procedure operative aggiuntive e il probabile impiego di altri sistemi, prodotti o servizi per raggiungere la massima efficienza. IBM NON GARANTISCE CHE SISTEMI, PRODOTTI O SERVIZI SIANO ESENTI DA O RENDERANNO L'AZIENDA ESENTA DA, CONDOTTI DA, O ILLEGALE DI UNA QUALSIASI TERZA PARTE.