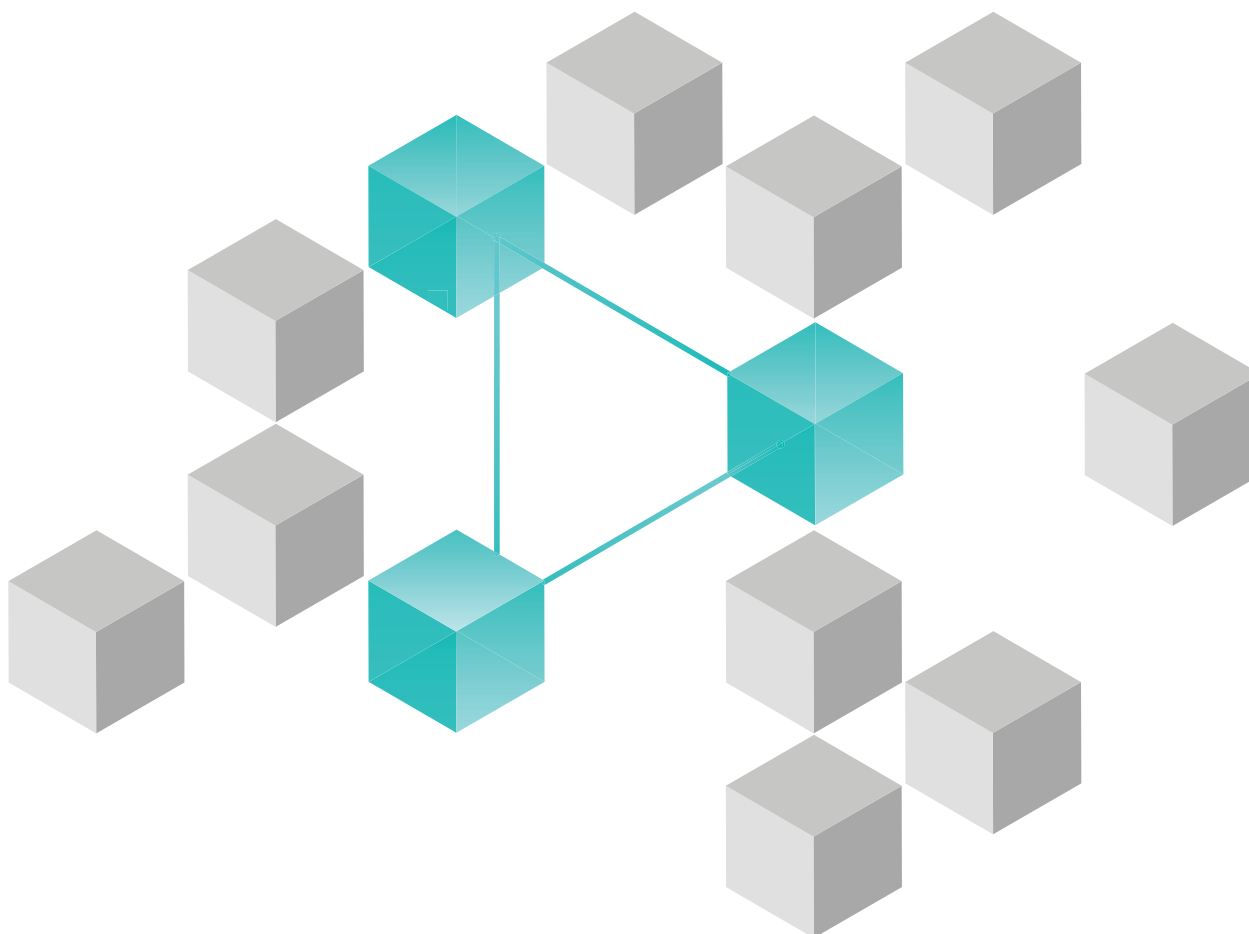


# IBM Security ReaQta pour les MSSP

La sécurité en tant que stratégie  
de croissance



# Présentation d'IBM Security ReaQta pour les MSSP

Cette plateforme de sécurité des terminaux est conçue pour aider les fournisseurs de services de sécurité gérés (MSSP) à contrôler et à sécuriser facilement un nombre plus élevé de terminaux des clients. Plébiscitée par la profession, elle est dotée de capacités puissantes et complètes de détection et de réponse des terminaux (EDR) pour une gestion simplifiée.

La plateforme ReaQta simplifie le traitement et la gestion des menaces pour les MSSP en dotant ces derniers de puissantes capacités de traque des menaces et d'automatisation. Les MSSP bénéficient d'un suivi en continu, d'une réponse aux incidents et d'une analyse après intrusion, le tout sur une seule et même plateforme.

ReaQta s'appuie sur l'IA et le machine learning, pour associer des niveaux d'automatisation exceptionnels à une interface intuitive. Elle est ainsi capable de détecter et de corriger de manière autonome les menaces, connues ou non, en temps quasi réel.

La plateforme utilise le deep learning pour améliorer en permanence sa capacité à identifier les comportements normaux de chaque entreprise sur chaque terminal afin de bloquer tout comportement anormal. Les MSSP bénéficient ainsi d'une sécurité sans complexité et savent que les données et actifs précieux de leurs clients sont protégés contre les menaces les plus évoluées.

## Principaux avantages pour les MSSP



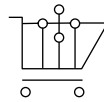
### Une productivité accrue

Grâce à des capacités d'IA et de machine learning exceptionnelles, la plateforme ReaQta détecte et neutralise de manière autonome les menaces les plus sophistiquées en temps quasi réel, ce qui évite aux équipes d'effectuer des analyses manuelles.



### Une efficacité renforcée

ReaQta réduit la désensibilisation aux alertes des MSSP en fournissant en temps réel des alertes hautement fidèles et condensées qui offrent une visibilité immédiate et une compréhension approfondie des processus. Il est ainsi possible d'agir rapidement pour enrayer efficacement les menaces.



### Une réduction des coûts

La plateforme simplifie les opérations des MSSP grâce à une interface intuitive et à des processus automatisés. Aucun personnel spécialisé ou effectif supplémentaire n'est nécessaire.



## Trois raisons pour les MSSP de choisir ReaQta

### 1. Une technologie d'envergure internationale

Nous réinventons l'EDR. ReaQta est entièrement automatisée et fonctionne de manière autonome pour détecter et neutraliser les menaces les plus avancées. Nous utilisons l'IA et le machine learning de manière unique en l'associant à notre technologie exclusive NanoOS pour nous rendre invisibles pour les attaquants et les logiciels malveillants et prévenir tout changement, modification ou interruption.

Grâce à la technologie NanoOS, les MSSP bénéficient d'une visibilité parfaite sur les processus et les applications exécutés sur les terminaux de leurs clients. NanoOS se positionne au niveau de la couche de l'hyperviseur et protège le terminal depuis l'extérieur du système d'exploitation.

### 2. Une assistance inégalée

Nous donnons la priorité à nos clients. Plus de files d'attente pour obtenir le support client ou d'interlocuteurs multiples pour obtenir une réponse. Accédez directement à une équipe d'assistance accueillante et expérimentée, capable de répondre à vos questions du début à la fin.

### 3. Un ROI optimal

Gérez et sécurisez davantage de terminaux. Augmentez l'efficacité de vos équipes et améliorez votre productivité grâce à nos alertes condensées et hautement précises qui procurent aux MSSP une visibilité directe sur l'ensemble de l'activité des terminaux et des menaces. Réduisez vos coûts grâce à notre interface utilisateur intuitive sans recourir à des effectifs supplémentaires ou à du personnel spécialisé.

# Conception privilégiant la simplicité d'utilisation et de gestion

## Fonctionnement simplifié

- Profitez du haut niveau d'automatisation de la plateforme ReaQta. Maîtrisez n'importe quelle situation en quelques secondes grâce à des instructions de résolution détaillées et à des réponses automatisées expliquées en quelques clics qui offrent aux analystes un processus unique et facile à utiliser.
- L'architecture intuitive de la plateforme, associée à des alertes condensées hautement fidèles, allège le niveau de compétence requis pour répondre aux menaces.
- Détectez les menaces en toute simplicité. Les stratégies de détection en un clic de la plateforme ReaQta peuvent être déployées efficacement auprès de l'ensemble des clients.
- Le Cyber Assistant tire des enseignements des interventions des analystes, ce qui réduit les tâches répétitives et libère du temps pour des analyses de plus haut niveau et la traque des menaces.
- Les MSSP peuvent facilement relier ReaQta à d'autres composants de leur stack de solutions en utilisant une interface de programmation d'applications (API) flexible.

## Simplicité de gestion

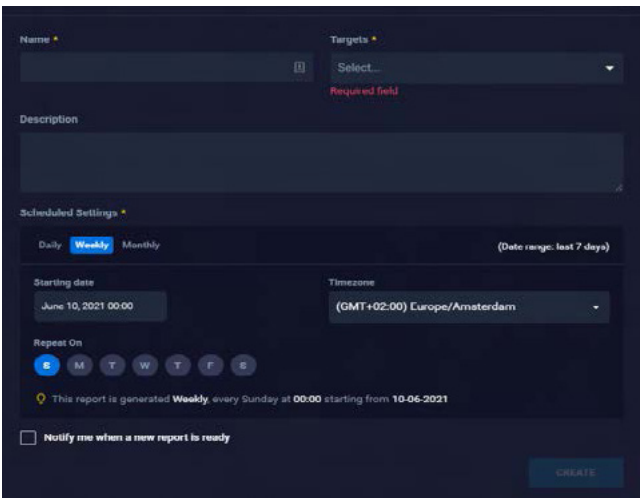
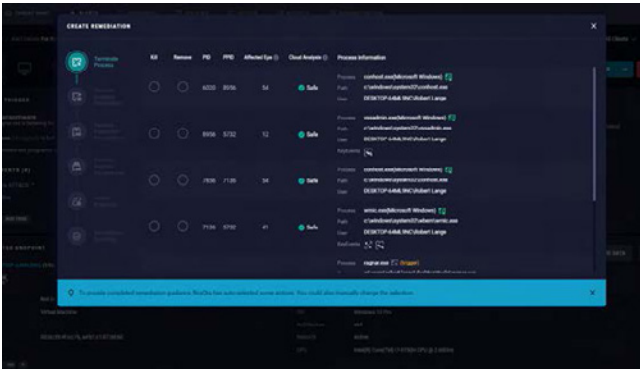
- Adaptée aux MSSP et multi-locataires, la plateforme ReaQta vous permet de gérer vos clients actuels et futurs en quelques clics.
- La puissante fonction de création de rapports de la plateforme permet aux MSSP de générer des rapports techniques et de gestion, rapidement et en toute conformité, pour un client donné ou pour l'ensemble des clients.
- Des options de déploiement flexibles aident les MSSP à respecter les politiques des clients en matière de données.

## Voir IBM Security ReaQta en action

Pour en savoir plus, rendez-vous sur :

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

**Tous les outils dont vous avez besoin, au même endroit**  
Profitez d'un suivi en continu, d'une réponse aux incidents et d'une analyse après intrusion sur une seule et même plateforme.



© Copyright ReaQta, une société IBM 2022

**Compagnie IBM France**

17 avenue de l'Europe  
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique  
Mars 2022

IBM, le logo IBM et ReaQta sont des marques commerciales d'International Business Machines Corp. déposées dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web « Copyright and trademark information » à l'adresse suivante : [ibm.com/trademark](http://ibm.com/trademark).

L'information contenue dans ce document était à jour à la date de sa publication initiale et peut être modifiée sans préavis par IBM. Les offres mentionnées dans le présent document ne sont pas toutes disponibles dans tous les pays où la société IBM est présente.

LES INFORMATIONS CONTENUES DANS LE PRÉSENT DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE À CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE À L'EXÉCUTION D'UN TRAVAIL DONNÉ. Les produits IBM sont garantis conformément aux dispositions des contrats qui régissent leur utilisation.

Énoncé des bonnes pratiques de sécurité : La sécurité du système informatique implique la protection des systèmes et des informations par la prévention, la détection et la réponse à un accès inapproprié à l'intérieur et à l'extérieur de votre entreprise. Un accès inadapté peut entraîner la modification, la destruction, l'appropriation illicite ou l'utilisation abusive des informations ou peut entraîner des dommages ou une mauvaise utilisation de vos systèmes, y compris pour des attaques sur des tiers. Aucun système ou produit informatique ne doit être considéré comme totalement sécurisé et aucun produit, service ou mesure de sécurité ne peut être totalement efficace pour empêcher une utilisation ou un accès inapproprié. Les systèmes, produits et services d'IBM sont conçus pour faire partie d'une approche de sécurité légale et complète, qui impliquera nécessairement des procédures opérationnelles supplémentaires, et peuvent exiger que d'autres systèmes, produits ou services soient plus efficaces. IBM NE GARANTIT PAS QUE LES SYSTÈMES, LES PRODUITS OU LES SERVICES SONT À L'ABRI DE, OU IMMUNISERONT VOTRE ENTREPRISE CONTRE, LA CONDUITE MALVEILLANTE OU ILLÉGALE D'UNE PARTIE QUELLE QU'ELLE SOIT.