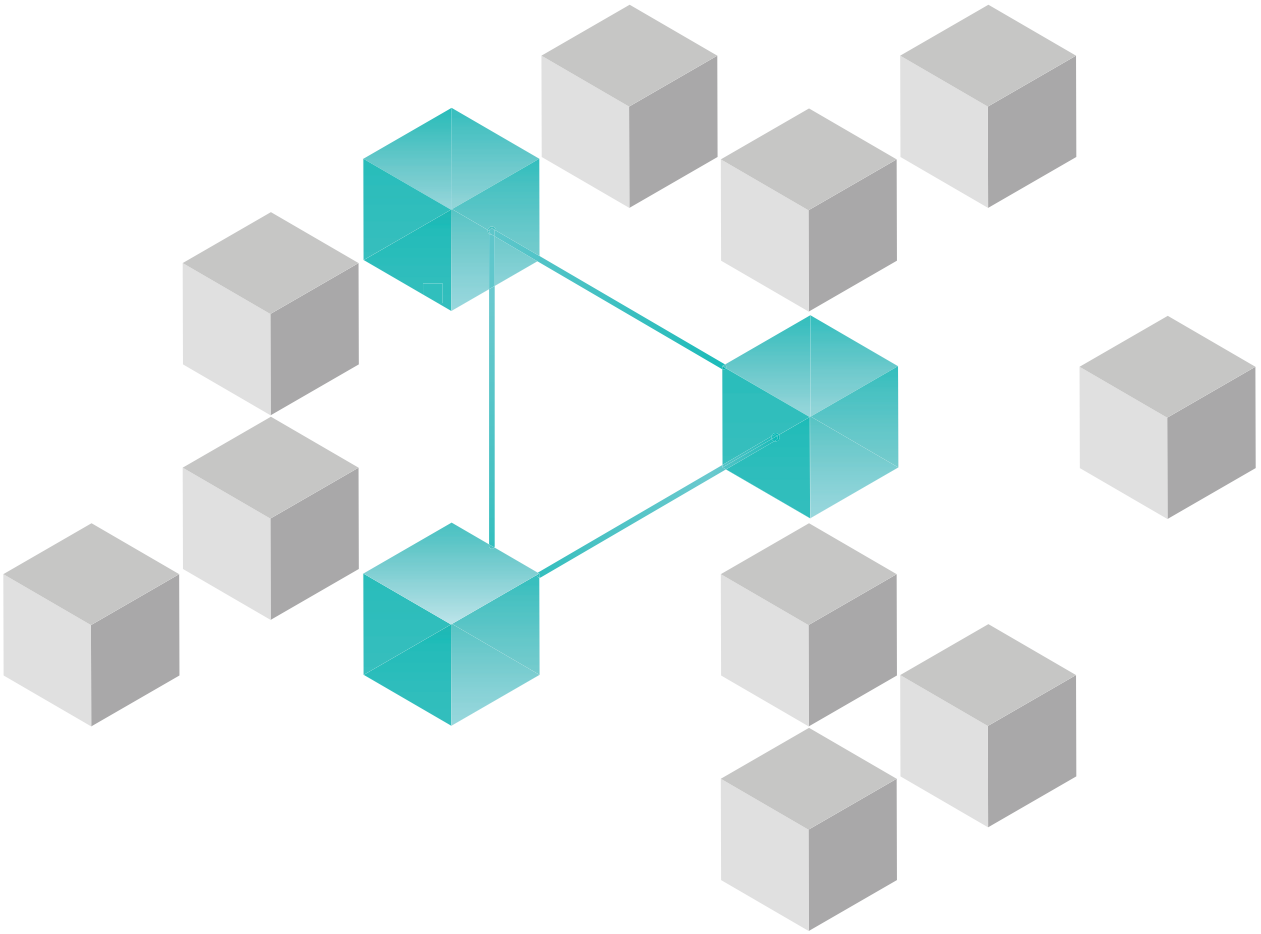
REAQTA
an IBM Company

IBM

IBM Security ReaQta für MSSPs

Sicherheit als Wachstumsstrategie



Überblick: IBM Security ReaQta für MSSPs

Diese branchenweit renommierte Plattform für Endpunktsicherheit wurde für Managed Security Service Providers (MSSPs) entwickelt, die mühelos mehr Endpunkte ihrer Kunden verwalten und schützen möchten. Sie verfügt über eine leistungsfähige, umfassende Funktionalität für die Endpoint Detection and Response (EDR) und rationalisiert so Ihre täglichen Aufgaben.

Die ReaQta Plattform vereinfacht die Handhabung und Verwaltung von Sicherheitsbedrohungen für MSSPs und gibt ihnen zugleich mächtige Funktionen zum Suchen nach Bedrohungen an die Hand. MSSPs profitieren von der kontinuierlichen Überwachung und Reaktion auf Vorfälle sowie von Analysen erfolgter Verstöße – alles über eine einzige Plattform.

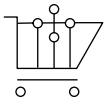
Mittels KI und maschinellem Lernen kombiniert ReaQta einen außergewöhnlichen Automatisierungsgrad mit einem intuitiven Design zur autonomen Entdeckung und Korrektur von bekannten wie unbekannten Bedrohungen nahezu in Echtzeit.

Durch Deep Learning verbessert die Plattform ihre Definition des normalen Verhaltens immer weiter, individuell zugeschnitten auf das jeweilige Unternehmen an jedem einzelnen Endpunkt, und blockiert jede Unregelmäßigkeit. So erleben MSSPs Sicherheit ohne Komplexität und profitieren von der beruhigenden Gewissheit, dass die geschäftskritischen Daten und Assets ihrer Kunden selbst gegen komplexeste Bedrohungen sicher geschützt sind.

Die wichtigsten Vorteile für MSSPs

Höhere Produktivität
Durch das außergewöhnliche Niveau an KI und maschinellem Lernen der ReaQta Plattform werden selbst die höchst entwickelten Bedrohungen nahezu in Echtzeit entdeckt und autonom korrigiert. Dies entlastet Teams von manuellen Analysen.

Mehr Effizienz
ReaQta reduziert die Alarmmüdigkeit auf Seiten der MSSPs durch Bereitstellung genauer, komprimierter Alarme in Echtzeit, die unmittelbare Transparenz und aussagekräftige Informationen in die Prozesse bringen. Dies erleichtert flexible Maßnahmen zur schnellen, effektiven Beendigung von Bedrohungen.



Geringere Kosten
Die Plattform vereinfacht den operativen Betrieb für MSSPs durch eine benutzerfreundliche, intuitive Schnittstelle und automatisierte Prozesse. Es sind weder zusätzliches qualifiziertes Personal noch größere Teams erforderlich.

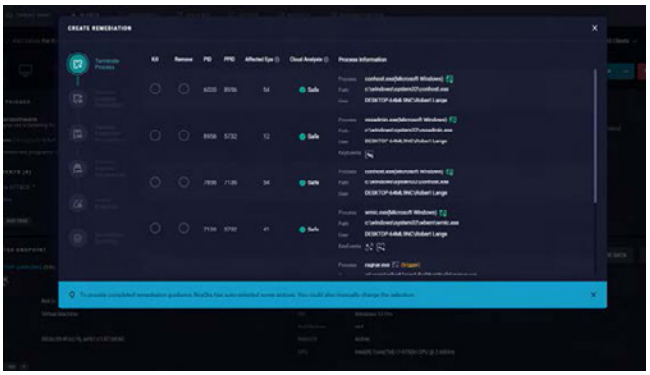
Drei Gründe, warum MSSPs zu ReaQta wechseln

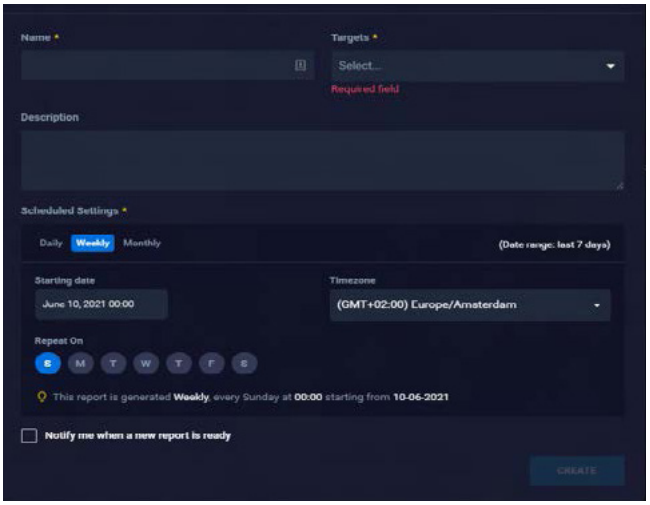
1. **Erstklassige Technologie**
   Wir erfinden EDR neu. ReaQta ist vollständig automatisiert. Es entdeckt und korrigiert autonom selbst komplexeste Bedrohungen. Unsere einzigartige Nutzung von KI und maschinellem Lernen, in Kombination mit unserer proprietären NanoOS Technologie, ist darauf ausgelegt, dass die Anwendung für Angreifer und Malware unsichtbar ist und nicht verfälscht, abgeschaltet oder ausgetauscht werden kann.

   Durch die NanoOS-Technologie gewinnen MSSPs umfassende Transparenz über die auf den Endpunkten ihrer Kunden ausgeführten Prozesse und Anwendungen. NanoOS wird in der Hypervisor-Schicht ausgeführt und schützt den Endpunkt außerhalb des Betriebssystems.

2. **Erstklassiger Support**
   Kundenorientierung ist für uns eine Frage der Überzeugung. Warten Sie nie wieder in Warteschlangen des Kundensupports, um mit unzähligen verschiedenen Menschen zu sprechen, die Ihre Frage beantworten sollen. Erhalten Sie stattdessen direkten Zugang zu freundlichen, fest zugeordneten Experten des Support-Teams, die geschult und autorisiert sind, Ihre Fragen von Anfang bis Ende zu lösen.

3. **Überragender ROI**
   Verwalten und schützen Sie mehr Endpunkte. Steigern Sie die Effizienz und Produktivität Ihres Teams mit unseren komprimierten, genauen Alarmen, durch die MSSPs unmittelbare Transparenz über sämtliche Endpunkte und Bedrohungsaktivitäten erhalten. Reduzieren Sie Ihre Kosten dank unserer intuitiven Oberfläche – keine zusätzlichen Beschäftigen oder hochqualifiziertes Personal erforderlich.





Einfacher Betrieb, unkompliziertes Management

Einfacherer Betrieb

- Profitieren Sie vom hohen Automatisierungsgrad der ReaQta-Plattform. Dämmen Sie jede Situation innerhalb von Sekunden ein – mit umfassender Anleitung für die Korrekturmaßnahmen sowie Antwortaktionen mit einfachster Benutzerführung, die Ihren Analytikern einen einfachen, benutzerfreundlichen Workflow an die Hand geben.
- Durch das intuitive Design der Plattform, gepaart mit den komprimierten, genauen Alarmen, sinken die Anforderungen an Beschäftigte bzgl. der Reaktion auf Bedrohungen.
- Erleben Sie, wie einfach die Bedrohungssuche sein kann. Die Entdeckungsstrategien der ReaQta-Plattform per einfachem Mausklick lassen sich effizient für Ihren gesamten Kundenstamm bereitstellen.
- Der Cyber-Assistent lernt von allen Aktionen der Analytiker, senkt die Belastung durch monotone Arbeit und räumt Zeit frei für höherwertige Analysen und die Bedrohungssuche.
- Über eine flexible API können MSSPs ReaQta leicht an weitere Komponenten ihres Lösungs-Stacks anbinden.

Einfaches Management

- Die MSSP-freundliche, mandantenfähige ReaQta-Plattform ermöglicht Ihnen die Verwaltung bestehender und neuer Kunden mit nur wenigen Klicks.
- Durch die leistungsstarke Berichtsfunktion der Plattform können MSSPs technische und verwaltungstechnische Informationen schnell und gesetzeskonform für einzelne Kunden oder global in Berichte fassen.
- Flexible Implementierungsoptionen helfen den MSSPs bei der Einhaltung der jeweiligen Datenrichtlinien ihrer Kunden.

Erleben Sie IBM Security ReaQta in der Praxis

Weitere Informationen finden Sie unter:
ibm.com/de-de/products/reaqta

Sämtliche Werkzeuge, die Sie benötigen, an einem Ort
Profitieren Sie von kontinuierlicher Überwachung und Reaktion auf Vorfälle sowie von Analysen erfolgter Verstöße – alles über eine einzige Plattform.

© Copyright ReaQta, ein IBM Unternehmen 2022

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen

Hergestellt in den Vereinigten Staaten von Amerika
März 2022

IBM, das IBM Logo und ReaQta sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter: ibm.com/trademark.

Das vorliegende Dokument ist mit Stand vom Datum der ersten Veröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GARANTIE ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN. Die Garantie für Produkte von IBM richtet sich nach den Bestimmungen und Bedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.