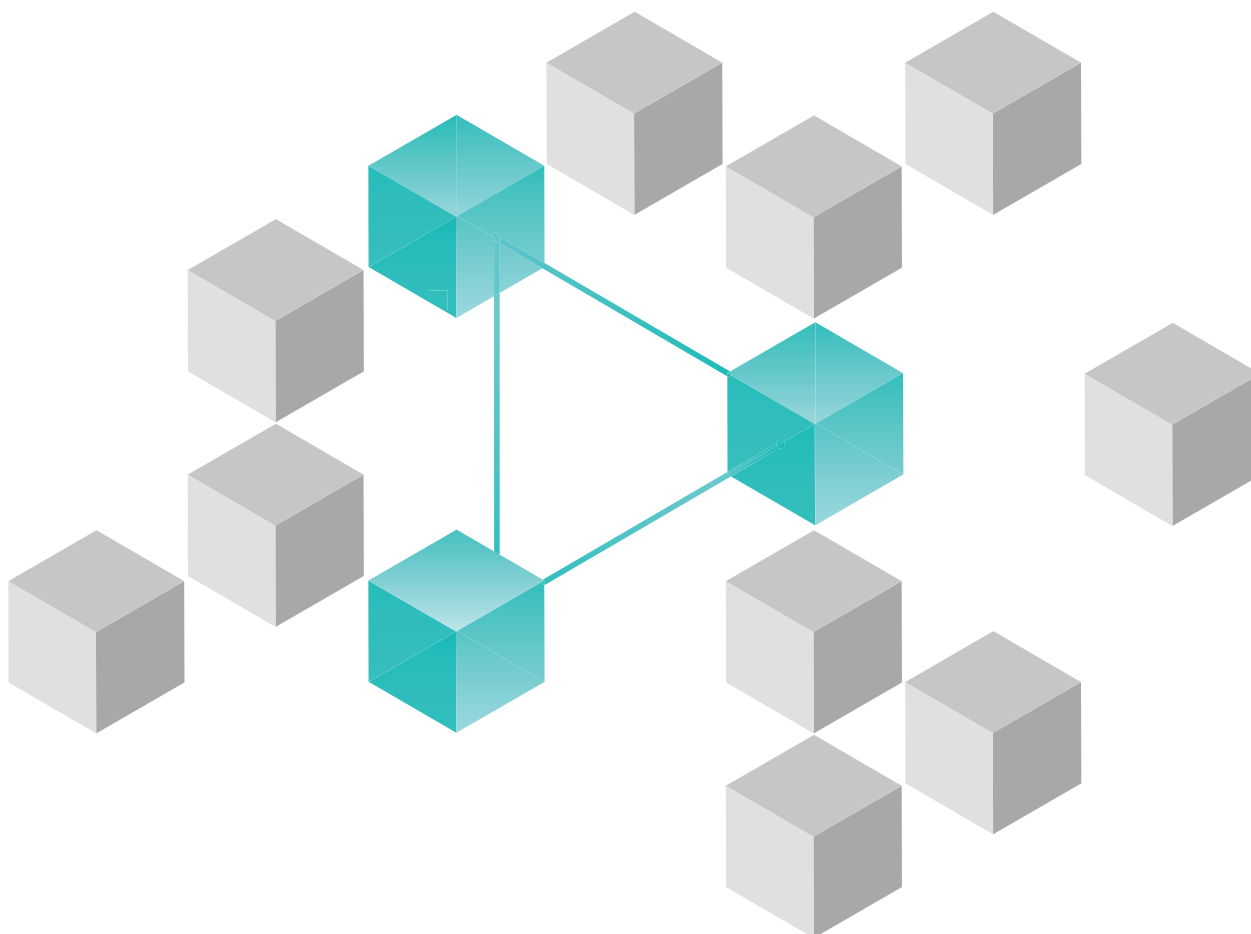


IBM Security ReaQta for MSSPs

Segurança como estratégia de
crescimento



Apresentando o IBM Security ReaQta for MSSPs

Projetada para que provedores de serviços de segurança gerenciados (MSSPs) gerenciem e protejam sem esforço mais endpoints de seus clientes, essa plataforma de segurança de endpoint aclamada pelo setor foi criada com recursos avançados e completos de detecção e resposta de endpoint (EDR) para gerenciamento simplificado.

A plataforma ReaQta simplifica o tratamento e o gerenciamento de ameaças para MSSPs ao incluir recursos avançados de automação e identificação de ameaças. Em uma única plataforma, os MSSPs têm recursos de monitoramento contínuo, resposta a incidentes e análise pós-violação.

Com inteligência artificial e aprendizado de máquina, o ReaQta tem níveis excepcionais de automação, além de design intuitivo para detectar e corrigir ameaças (novas ou desconhecidas) quase em tempo real.

Através de deep learning, a plataforma é aprimorada constantemente para definir o comportamento normal personalizado para cada empresa e cada endpoint, barrando qualquer comportamento anômalo. Com isso, os MSSPs têm segurança sem complexidade e sabem que os dados e ativos valiosos dos clientes estão protegidos contra as ameaças mais avançadas.

Principais vantagens para os MSSPs



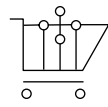
Aumento da produtividade

Com níveis excepcionais de inteligência artificial e aprendizado de máquina, a plataforma ReaQta detecta e corrige as ameaças mais sofisticadas quase em tempo real, e as equipes não precisam fazer análise manuais.



Mais eficiência

O ReaQta diminui o excesso de alertas para o MSSP porque emite alertas precisos, resumidos e em tempo real. Isso permite que os usuários tenham visibilidade dos processos e insights detalhados. Isso facilita a ação rápida para interromper as ameaças de forma ágil e eficaz.



Redução de custos

A plataforma simplifica as operações para os MSSPs com uma interface intuitiva, fácil de usar e com processos automatizados. Não é preciso ter mais pessoal ou funcionários altamente qualificados.



Três motivos para os MSSPs estarem mudando para o ReaQta

1. Tecnologia de nível internacional

Estamos reinventando a EDR. O ReaQta é totalmente automatizado e funciona de forma autônoma para detectar e corrigir as ameaças mais avançadas. Nossa maneira exclusiva de utilizar a IA e o aprendizado de máquina, combinada com nossa tecnologia proprietária NanoOS, foi criada para ser invisível para invasores e malware e para não ser alterada, desativada ou substituída.

Com a tecnologia NanoOS, os MSSPs têm visibilidade total dos processos e aplicações executados nos endpoints dos clientes. O NanoOS funciona na camada do hipervisor e protege o endpoint de fora do sistema operacional.

2. Melhor suporte do setor

Os clientes são nossa prioridade. Chega de esperar em filas de atendimento e falar com uma infinidade de pessoas para resolver seus problemas. Tenha acesso direto a uma equipe de suporte especializada amigável e dedicada, treinada e capacitada para resolver suas dúvidas do início ao fim.

3. Maior ROI

Gerencie e proteja mais endpoints. Aumente a produtividade e a eficiência da equipe com nossos alertas precisos e resumidos. Assim, os MSSPs têm visibilidade direta da atividade em todos os terminais e ameaças. Reduza custos com nossa interface do usuário intuitiva. Não é preciso ter funcionários adicionais ou altamente qualificados.

Criada para ser fácil de operar e de administrar

Mais fácil de operar

- Aproveite o alto nível de automação da plataforma ReaQta. Contenha qualquer situação em segundos com orientação de correção completa e automações de resposta por clique que fornecem aos analistas um único fluxo de trabalho fácil de usar.
- O design intuitivo da plataforma, junto com alertas resumidos de alta precisão, reduz o nível de qualificação necessário para responder a ameaças.
- Experimente a identificação simplificada de ameaças. As estratégias de detecção em um clique da plataforma ReaQta podem ser implementadas de forma eficaz em toda a base de clientes.
- O Cyber Assistant aprende com as ações dos analistas, reduzindo as tarefas repetitivas e liberando tempo para análises e remoções de ameaças mais complexas.
- Os MSSPs podem conectar facilmente o ReaQta a outros componentes do stack de soluções usando uma API flexível.

Gerenciamento simples

- Fácil de usar e multilocatária, a plataforma ReaQta ajuda os MSSPs a gerenciar clientes novos e atuais com apenas alguns cliques.
- O poderoso recurso de relatório da plataforma permite que os MSSPs reportem informações técnicas e de gerenciamento de maneira rápida e compatível para clientes individuais ou em geral.
- Opções de implementação flexível ajudam os MSSPs a seguir as políticas de dados dos clientes.

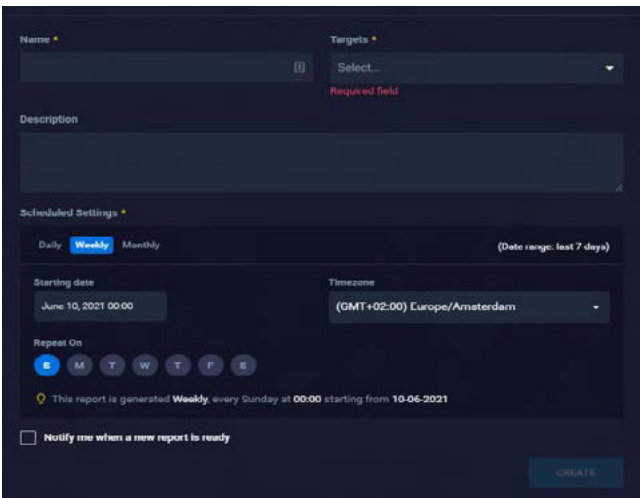
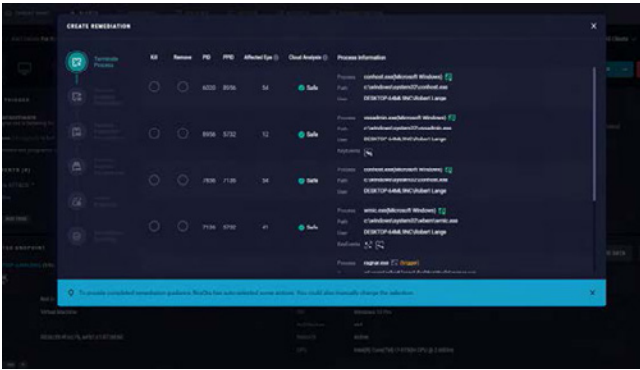
Veja o IBM Security ReaQta em ação

Veja mais informações em:

ibm.com/products/reaqta

Todas as ferramentas que você precisa, num só lugar

Beneficie-se de monitoramento contínuo, resposta a incidentes e análises pós-violação, tudo em uma única plataforma.



© Copyright ReaQta, IBM Company 2022

IBM Brasil Ltda

Rua Tutóia, 1157 CEP 04007-900
São Paulo – SP

Produzido nos Estados Unidos da América
Março de 2022

IBM, o logotipo da IBM, e ReaQta são marcas registradas da International Business Machines Corp., registrada em muitas jurisdições no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atual de marcas registradas da IBM está disponível na Web na seção “Copyright and trademark information” de ibm.com/legal/copytrade.shtml.

Este documento é atual na data de sua publicação inicial e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países onde a IBM opera.

AS INFORMAÇÕES NESTE DOCUMENTO SÃO FORNECIDAS “TAL COMO ESTÃO”, SEM GARANTIA EXPRESSA OU IMPLÍCITA DE, ENTRE OUTRAS, COMERCIALIZIDADE, ADEQUAÇÃO A UM DETERMINADO FIM OU DE NÃO INFRAÇÃO. Os produtos da IBM têm a garantia de acordo com os termos e condições dos acordos dentro dos quais são fornecidos.

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.