Mantenha o controle com o IBM QRadar on Cloud

QRadar

IBM Security

Sumário

SIEM inteligente como serviço

Proteger dados e redes localmente e na nuvem é uma tarefa desafiadora para organizações de qualquer tamanho. Novas vulnerabilidades são descobertas quase todos os dias; novas espécies de malware são desenvolvidas assim que um script de detecção é criado para as antigas; e os cibercriminosos podem comprar kits de exploits pré-embalados na darknet com o apoio de equipes de suporte profissionais. Como analista de segurança, você precisa mais do que algumas soluções pontuais feitas para defender a borda da rede. Você precisa de visibilidade, perspectiva e uma percepção inata de quando as coisas simplesmente não parecem certas.

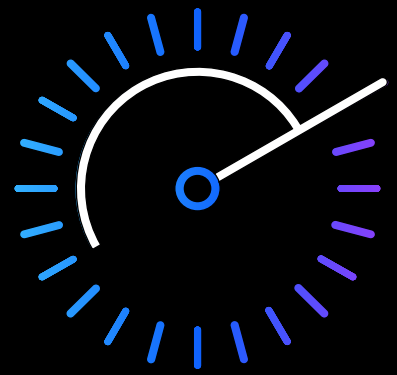
O IBM® QRadar® on Cloud é excelente para essas tarefas. Com recursos robustos de gerenciamento de eventos e informações de segurança (SIEM), a solução ajuda a proteger dados e redes com uma ampla gama de recursos que podem mostrar quem está fazendo o quê, onde e quando. Ele usa painéis e visualizações avançadas, compactando milhares ou milhões de incidentes distintos em indicações simples de suspeita de problema; além disso, preserva registros detalhados de atividades suspeitas para análise futura. Ao mesmo tempo, seus recursos avançados de criação de log e ferramentas de geração de relatórios ajudam você a cumprir rapidamente requisitos básicos, como obrigações de relatórios regulatórios.

Saiba mais sobre o IBM QRadar on Cloud →

O QRadar on Cloud é capaz de processar mais de

500.000

eventos por segundo.[1]



Principais benefícios do IBM QRadar on Cloud para os negócios

“Os CIOs precisam parar de perguntar ‘**A nuvem é segura?**’ e começar a perguntar ‘**Estou usando a nuvem de forma segura?**’”

Gartner
Gartner.com

Conheça os benefícios →

Atenda às demandas regulatórias e de segurança ao mesmo tempo

É provável que você tenha implementado medidas básicas de segurança no perímetro da rede para evitar ataques simples. No entanto, a maioria dos endpoints têm falhas de segurança e alguns usuários simplesmente não conseguem resistir a clicar em links mal-intencionados. Dispositivos e credenciais são comprometidos com muita frequência, abrindo caminho para perda de dados e possíveis interrupções nos negócios.

A implementação de um sistema de coleta de dados e relatórios de conformidade é relativamente fácil. Todavia, não é nada fácil deixar os auditores satisfeitos e proteger os dados críticos da sua organização. Quanto mais avançado o sistema, mais completamente ele prepara você para gerenciar atividades rotineiras e violações incomuns na rede, que exigem investigação e resposta a incidentes.

Obtenha mais insights sobre as ameaças empresariais atuais com a IBM X-Force Threat Intelligence® →

Assista e descubra mais sobre ameaças persistentes avançadas →

"O processamento e a correlação de dados desestruturados usando recursos cognitivos nos proporcionará mais contexto para recomendações ainda mais precisas e acionáveis. Também tornará a vida dos analistas de segurança mais fácil no dia a dia."

Christophe Bianco
sócio-gerente e Chief Technology Officer, Excellium Services

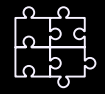
Leia o estudo de caso →

O que o QRadar on Cloud oferece:

Mudança do modelo CAPEX para OPEX

Preenche o deficit de competências

Alta visibilidade, conformidade e segurança



Mais de 500 integrações prontas para o uso

Insights orientados por dados usando inteligência artificial

Flexibilidade e escalabilidade

Obtenha insights profundos para proteger seus ativos críticos na nuvem

É importante detectar e erradicar malware, assim como estabelecer regras de firewall para proteger sub-redes. Você provavelmente investiu em segurança do perímetro por esse motivo. Entretanto, o software de análise de segurança baseia-se no conceito fundamental de que nenhum perímetro conectado à internet é realmente seguro e as organizações precisam ser capazes de detectar anomalias e alterações comportamentais.

Com o modelo de nuvem, sua organização pode implementar gateways de dados ricos em segurança e enviar seus dados de segurança para um ambiente em nuvem implementado e gerenciado de forma especializada, com taxas operacionais mensais previsíveis. O modelo de nuvem deixa você no controle. Além disso, permite que sua equipe passe a maior parte do tempo monitorando o ambiente, ajustando as regras de detecção de ameaças e personalizando relatórios regulatórios ou de gerenciamento, em vez de ficar aplicando correções de software e fazendo backups de dados.

Fique a par da conformidade e dos regulamentos →

Um tomador de decisões de TI passa quase

2 horas por dia procurando dados relevantes.[2]

69% das empresas

percebem que as obrigações de conformidade geram despesas.[3]

Prepare sua organização para a conformidade

A solução QRadar on Cloud exerce uma importante função orientada pelos negócios. Protegendo dados e preservando, em formato pronto para auditoria, um registro dos eventos e práticas de segurança que possibilitam a proteção, ela ajuda as organizações a cumprir os regulamentos do governo e do setor. Se ignoradas, essas obrigações podem resultar em penalidades para uma organização, da mesma maneira como um malware pode resultar em perda de dados.

Uma série de requisitos e padrões de melhores práticas, desenvolvidos para proteger as informações pessoais e financeiras do cliente e aumentar a transparência corporativa, determina como os dados organizacionais e dos clientes são reunidos, armazenados e protegidos. A Sarbanes-Oxley Act (SOX), o Payment Card Industry Data Security Standard (PCI DSS), a Health Insurance Portability and Accountability Act (HIPAA), o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e outros regulamentos significam que as empresas podem enfrentar penalidades civis ou criminais, proibições do uso de cartões de pagamento e outros riscos que podem incluir interrupções devastadoras nos negócios por práticas de falta de conformidade.

Confira a extensão de conteúdo do IBM QRadar para a GDPR →

As violações da HIPAA podem incorrer em penalidades criminais, assim como em multas de até US$ 50.000 por violação, com um máximo anual de

US$ 1,5 milhão.[4]

88% das empresas

gastaram mais de US$ 1 milhão para se preparar para a GDPR.[3]

Ajude a priorizar as ameaças

É possível abordar algumas ameaças de segurança de maneira tática, usando ferramentas especializadas que tratam de aspectos individuais da segurança. Essas ferramentas podem ser úteis para lidar com ameaças definidas e problemas conhecidos. Também podem gerar respostas simples, como bloqueio seletivo de portas de rede, remoção de uma instância de malware ou correção de um ativo vulnerável identificado.

No entanto, o software QRadar é muito mais valioso do que soluções pontuais porque coleta uma variedade maior de dados de segurança compartilhados em essencialmente todos os módulos de inteligência de segurança. Depois de observar e calcular limites para normas de fluxo de dados na sua rede, ele automaticamente detecta eventos que violam tais limites e alerta sua equipe de segurança. As regras de limite podem ajudar a detectar transferências de dados de saída excepcionalmente grandes, uso da largura de banda, alterações em aplicações ou um número estranhamente alto de tentativas de login de um endereço de Protocolo de Internet (IP) inesperado. O QRadar também observa eventos conectados, comparando, por exemplo, identidades de usuário, endereços IP de origem e destino e locais geográficos onde a atividade se originou. Ele examina esses eventos vinculados em busca de contexto para distinguir melhor ofensas verdadeiras e casos únicos de novos comportamentos.

Leia mais sobre as previsões de segurança da IBM X-Force para 2020 →

A segurança cibernética está se tornando mais complexa do que nunca. Em 2019, o tempo médio para identificar e conter uma violação foi de

279 dias

com o custo médio global da violação de dados estimado em

US$ 3,9 milhões.[5]

A assistência médica é o setor mais caro, com as violações de dados custando às organizações

US$ 429 por registro perdido ou roubado.[5]

Adote um novo modelo de despesas com um software de segurança baseado em nuvem

O software pode ser crítico para as operações empresariais e de TI. No entanto, para a maioria das organizações, manter o software de segurança internamente acrescenta uma carga de trabalho extra que, na realidade, pode atrapalhar as principais tarefas de segurança. Reduzir e simplificar a combinação de funções que os profissionais de segurança precisam exercer pode ser um motivo significativo para adotar uma alternativa com base em nuvem.

Conseguir uma melhor segurança sempre | exigirá algum nível de recursos humanos e técnicos. Entretanto, com uma solução hospedada com base em nuvem, o tempo e as despesas associadas que a equipe de segurança dedica a deveres de rotina podem ser realocados para análise e planejamento.

Leia este White Paper para saber mais sobre o QRadar on Cloud, uma solução de SaaS flexível e altamente escalável →

Comparação de custos

No local ou na nuvem

Custos iniciais	On local	SaaS
Customização	●	●
Hardware	●	
Implementação	●	●
Equipe de TI	●	
Gerenciamento de ciclo de vida	●	
Manutenção	●	
Licenças de software	●	
Treinamento	●	●
Custos recorrentes		
Custos contínuos de TI	●	
Manutenção contínua	●	
Patches e correções	●	
Upgrades	●	
Taxa de assinatura		●

“Em média, o custo total aumentou, mas não consideramos esses aumentos necessariamente ruins. Estamos investindo na proteção de dados para o longo prazo porque sabemos que as violações de dados não vão desaparecer.” [6]

Supervisor de TI/África do Sul/ Industrial no estudo Ponemon Cost of Data Breach Study de 2018

Leia o estudo →

Amplie o QRadar com outras ferramentas de segurança

O QRadar on Cloud herda mais de 500 integrações existentes desenvolvidas na última década, respondendo a solicitações de clientes locais e alinhando-se a soluções de terceiros que complementam a plataforma de inteligência de segurança. Os profissionais experientes que fazem sua implementação de nuvem raramente precisarão desenvolver novos módulos de suporte para começar a aceitar dados de seus ativos e aplicações. A maioria dos clientes começará a perceber o valor poucos dias após a conclusão do contrato.

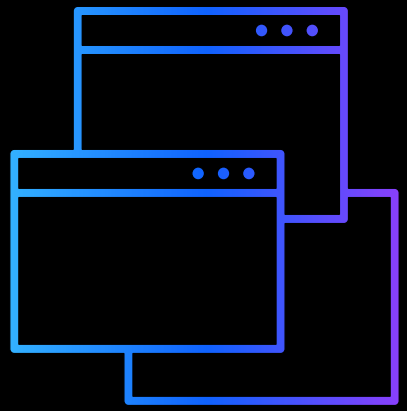
É possível baixar e instalar novas extensões ou aplicações do IBM Security App Exchange que aprimorarão seus recursos de monitoramento de rede. A equipe de manutenção da IBM CloudTM dará suporte à extensão de tecnologia. Já existem dezenas de extensões com suporte, incluindo novas visualizações, integrações, patches, regras personalizadas e aplicações novas completas, como o app IBM QRadar User Behavior Analytics. Todo o conteúdo no site é analisado pela IBM Security por meio do processo de validação Ready for IBM Security Intelligence.

Saiba mais sobre os plug-ins e extensões do QRadar no IBM Knowledge Center →

O QRadar pode coletar eventos de log e fluxos de rede de

mais de 500

aplicações e dispositivos.[7]



Preencha o deficit de competências com inteligência artificial

Nos últimos anos, houve um aumento acentuado no deficit de competências de segurança cibernética. O app IBM QRadar Watson Advisor foi desenvolvido para ajudar sua organização a detectar ameaças mais rapidamente.

O aplicativo usa inteligência artificial (IA) para auxiliar os usuários com análise, triagem e resposta a incidentes e riscos. Também permite que as equipes de operações de segurança façam mais com maior precisão. O resultado? Uma redução drástica no tempo usado para investigar incidentes, que diminui de dias e semanas para minutos ou horas.

Além disso, as equipes de segurança passarão menos tempo trabalhando em tarefas rotineiras do centro de operações de segurança (SOC) e mais tempo em outras prioridades estratégicas.

Veja como o QRadar Advisor with Watson pode ajudar sua equipe do SOC a fazer mais com maior precisão. Assista ao vídeo →

Descubra o QRadar Advisor with Watson versão 2.5.0 →

Os cargos não ocupados de segurança cibernética devem chegar a

1,8 milhão

até 2022.[8]

De acordo com um estudo recente, a força de trabalho de segurança cibernética global precisa

crescer 145%

para preencher o deficit de competências Nos EUA, precisa crescer 62%.[9]

"O Cargills Bank conseguiu superar essas limitações usando o IBM QRadar SIEM e o QRadar Advisor with Watson para receber alertas priorizados em tempo real. O excelente portfólio de segurança cognitiva da IBM nos ajudará a antecipar ameaças e mitigar riscos, contribuindo, assim, para nossa posição como banco digital líder."

Rohan Muttiah
Chief Operating Officer, Cargills Bank

Leia o estudo de caso →

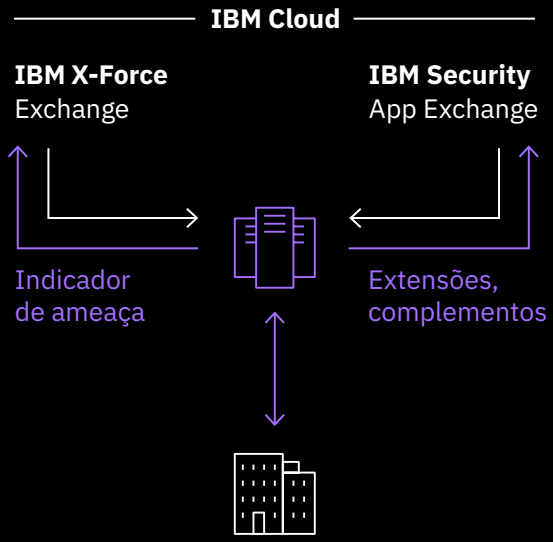
Alcance mais flexibilidade e escalabilidade

A compra de software como serviço (SaaS) oferece vantagens em escalabilidade e flexibilidade porque significa que as mudanças de capacidade não estão vinculadas à infraestrutura local e são muito menos dependentes da disponibilidade de profissionais internos. As empresas podem mudar muito rapidamente nesta economia. Sejam aumentos ocasionais no tráfego ou mudanças permanentes nas cargas de trabalho por causa de fusões e aquisições, com a solução QRadar on Cloud, elas podem ampliar o poder de computação conforme o necessário. Como a infraestrutura vive na nuvem e é desenvolvida pensando em mudanças de capacidade, não é preciso alterar o software localmente. A capacidade pode ser aumentada ou diminuída em curto prazo e com a mínima necessidade de envolvimento do cliente.

Destaques da oferta QRadar on Cloud

- Upgrades elásticos; rápido tempo de maturação
- DevOps dedicadas
- Monitoramento de integridade 24x7
- Gerenciamento de sistemas: upgrades, patches
- Suporte para mais de 450 integrações de segurança e TI
- Detecção avançada de ameaças
- Painéis configuráveis de SOC e gerenciamento
- Cobertura global de ponto de presença
- Suporte a modelo multilocatário para prestadores de serviços

IBM QRadar on Cloud



Ativos locais ou na nuvem do cliente

- Dispositivos de segurança
- Servidores e recursos de nuvem
- Atividade virtual e de rede
- Atividade de dados
- Atividade de aplicações
- Vulnerabilidades e ameaças
- Usuários e identidades

"Antes, sempre achávamos que estávamos atrasados no que se refere à segurança. Agora, porém, estamos muito mais proativos."

Michael Warrer
CIO, NRGi

Leia o estudo de caso →

Obtenha acesso a serviços gerenciados

Para organizações que precisam de ajuda além dos recursos que a equipe de segurança tem tempo ou conhecimento para fornecer, serviços de gerenciamento adicionais opcionais também estão disponíveis. O QRadar on Cloud oferece integração com os Serviços Gerenciados de Segurança da IBM, oferecendo serviços totalmente gerenciados com monitoramento e resposta a ameaças de segurança de forma contínua 24 horas por dia, sete dias por semana. Opcionalmente, as organizações podem terceirizar as operações de segurança para um parceiro Provedor de Serviços Gerenciados de Segurança (MSSP) externo da IBM. Os MSSPs oferecem soluções abrangentes de gerenciamento e monitoramento de segurança, bem como uma ampla gama de serviços complementares de monitoramento de ameaças para cobrir os casos de uso essenciais ou avançados.

A IBM foi novamente selecionada no Quadrante Mágico Gartner 2019 para Serviços Gerenciados de Segurança, Mundial.

Baixe o relatório →

A IBM oferece segurança gerenciada em escala global com capacidade de entrega local para ajudar a proteger seus ambientes em nuvem híbrida e multinuvem.

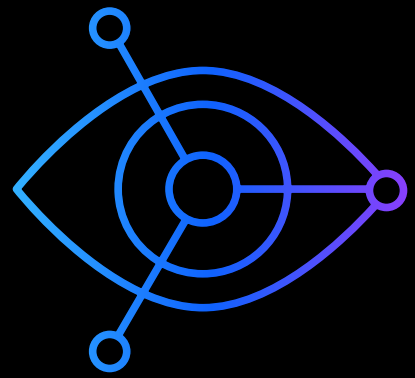
Saiba mais sobre os Serviços Gerenciados de Segurança da IBM →

A infraestrutura do QRadar on Cloud é

monitorada

24x7

por profissionais de confiança da IBM.[10]



Migre para um modelo de despesas operacionais otimizado para a nuvem

O IBM QRadar on Cloud aplica a experiência adquirida com milhares de implementações locais do QRadar para atender às necessidades do seu ambiente.

Não é necessário manter ou ajustar o software de segurança local. Com atualizações de software automáticas e escalabilidade sob demanda, o QRadar on Cloud ajuda a simplificar a vida da equipe de segurança de TI, mudando de um grande modelo de despesas de capital (CAPEX) para um modelo mais flexível baseado em despesas operacionais (OPEX).

O sistema é capaz de análise de nível empresarial, com recursos que incluem:

- Recursos de coleta de dados, correlação e relatório para alcançar a conformidade regulatória.
- Grandes máximas de evento por segundo (EPS), atendendo às necessidades de clientes com centenas de locais globais.
- Configuração de sistema altamente disponível com níveis de serviço confirmados e garantias de tempo de atividade.
- Aplicativos, complementos e extensões por meio do IBM Security App Exchange.
- Alertas enriquecidos com feed X-Force Threat Intelligence incluso.

Quais são os próximos passos?
Faça este test-drive de 14 dias da solução QRadar on Cloud e saiba mais sobre os sofisticados recursos de detecção.

Iniciar a avaliação gratuita →

Por que escolher a IBM?

A IBM Security oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança corporativa. O portfólio, apoiado pela pesquisa de renome mundial da X-Force, fornece inteligência de segurança para ajudar as organizações a proteger integralmente suas infraestruturas, seus dados e suas aplicações, oferecendo soluções para gerenciamento de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicações, gerenciamento de risco, gerenciamento de endpoint, segurança de rede e muito mais.

Essas soluções permitem que as organizações gerenciem efetivamente os riscos e implementem segurança integrada para dispositivos móveis, nuvem, redes sociais e outras arquiteturas empresariais de negócios. A IBM opera uma das maiores organizações de pesquisa e desenvolvimento e fornecimento de segurança do mundo, monitora 15 bilhões de eventos de segurança por dia em mais de 130 países e possui mais de 3.000 patentes de segurança.

Além disso, a IBM Global Financing oferece várias opções de pagamento para te ajudar a adquirir a tecnologia de que você precisa para expandir sua empresa. A IBM fornece gerenciamento completo do ciclo de vida de produtos e de serviços de TI, desde a aquisição até o descarte. Para obter mais informações, acesse ibm.com/financing.

Para saber mais sobre a IBM QRadar Security Intelligence Platform na nuvem, entre em contato com seu representante ou Parceiro de Negócios da IBM ou acesse ibm.com/software/products/en/qradar-on-cloud.

IBM Corporation
New Orchard
Road Armonk, NY 10504

Produzido nos Estados Unidos da América
Fevereiro de 2020

Este documento é considerado atual na data inicial da publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países em que a IBM atua.

Os dados de desempenho e os exemplos de clientes citados têm fins somente ilustrativos. Os resultados reais de desempenho poderão variar dependendo das configurações e das condições operacionais específicas. AS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO SÃO FORNECIDAS “NO ESTADO EM QUE SE ENCONTRAM”, SEM NENHUMA GARANTIA, EXPLÍCITA OU IMPLÍCITA, INCLUSIVE SEM NENHUMA GARANTIA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM FIM ESPECÍFICO E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO INFRAÇÃO. As garantias dos produtos IBM estão de acordo com os termos e as condições dos contratos segundo os quais foram fornecidos.

O cliente é responsável por assegurar o cumprimento das leis e dos regulamentos aplicáveis a ele. A IBM não oferece orientação jurídica nem declara ou garante que seus serviços ou produtos assegurarão o cumprimento de qualquer lei ou regulamento pelo cliente.

Declaração de boas práticas de segurança: A segurança de sistemas de TI envolve a proteção de sistemas e de informações por meio de prevenção, detecção e resposta ao acesso inadequado de dentro e de fora da sua empresa. O acesso inadequado pode resultar em alteração, destruição, emprego indevido ou uso incorreto de informações, ou pode causar danos ou uso indevido dos seus sistemas, inclusive para uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança pode ser completamente efetivo na prevenção do uso ou acesso inadequado. Os sistemas, produtos e serviços da IBM são desenvolvidos para fazer parte de uma abordagem de segurança legal e abrangente, o que implicará, necessariamente, em procedimentos operacionais adicionais e poderá exigir que outros sistemas, produtos ou serviços sejam mais eficazes. A IBM NÃO GARANTE QUE NENHUM SISTEMA, PRODUTO OU SERVIÇO ESTEJA IMUNE, OU TORNARÁ SUA EMPRESA IMUNE, À CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PARTE.

1 IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_siem_vrt_ap_ov.html

2 “Data management challenges are having a severe impact on profitability.” Help Net Security, 13 de março de 2019. https://www.helpnetsecurity.com/2019/03/13/data-management-challenges/

3 Josh Fruhlinger. “Top cybersecurity facts, figures and statistics for 2018.” CSO, 10 de outubro de 2018. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics. html

4 “HIPAA Violations and Enforcement, American Medical Association. Acessado em dezembro de 2019. https://www.ama-assn. org/practice-management/hipaa/hipaa-violations-enforcement

5 2019 Cost of a Data Breach Report: https://www.ibm.com/security/data-breach

6 2018 Cost of a Data Breach Study: Global Overview. Realizado pelo Ponemon Institute. https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf

7 QRadar On Cloud Overview. YouTube. https://www.youtube.com/watch?time_continue=53&v=dCTnR_hHToU&feature=emb_logo

8 Marten Mickos, “The Cybersecurity Skills Gap Won't Be Solved in a Classroom.” Forbes, junho de 2019. https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#353d37bd1c30

9 “Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap”, SECURITY, novembro de 2019, https://www.securitymagazine.com/articles/91224-cybersecurity-workforce-needs-to-grow-145-to-close-skills-gap

10 IBM Managed Services - https://www.ibm.com/security/services/managed-security-services

WGW03245-BRPT-02