IBM

IBM QRadar

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

IBM QRadar

Review by a Real User

Verified by IT Central Station

Security Manager at a pharma/biotech company with 1,001-5,000 employees

it_user631740

WHAT IS MOST VALUABLE?

The search capability (I've used other solutions) and data consolidation are some of the key features.

HOW HAS IT HELPED MY ORGANIZATION?

For this organization, it was the first log management solution. So, it definitely gave us the ability to search through the data when we had events. We could search based on the identity of the person, or the machine, or the IP address. We could do a lot of different searches. We could also do payload searches, and depending on how much capacity you have, you can do quite a lot with it.

WHAT NEEDS IMPROVEMENT?

I want to see a three-dimensional perspective of the data. I don't want to see just an event perspective of the data. I want to be able to identify a user, and within clicks, know all the activity of that user. I don't want to see it in events. I want to see it in relevant information. There needs a little bit more investment into enhancing the user interface. That is the main thing; making it represent an actual incident response state-of-mind, similar to how you would troubleshoot an incident. That is the main issue. It was a major position by IBM when they bought it. But we see a lot of things being done around the Cognitive side, around the Watson side. But what we're not seeing the growth in, is the actual tools interface and usability. And that's what we wanted to see. We wanted to be able to see seamless identification of log sources, seamless categorization and normalizing of log sources, seamless alerts. In all those things, for the solution to mature, it has to be able to take data and make sense of it by itself, without a lot of input. And those are the areas that they can really improve it.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's been stable. Stability hasn't been a problem, as long as you have enough capacity. It's all about sizing it right for the size of your environment. We do drop packets every day. So depending on how our log volume increases or reduces, you see the impact on the packets being dropped.

IBM QRadar

Read 47 reviews of IBM QRadar

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

We've used technical support and it hasn't been great. It didn't seem like we could get the answers we needed without having to use professional services. For a solution like this, little things like how to tune it, how to upgrade it; there are things that as a customer we don't feel the need to use professional services for. We want to be able to just find a document on how to upgrade, and that has been difficult to find.

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

We didn't have a previous solution. We kind of inherited it as part of another acquisition from IBM, and then we scaled it up to meet our capacity.

HOW WAS THE INITIAL SETUP?

We got the basic functionality working, which is not difficult. It's getting the full value out of the solution, which is harder.

WHAT OTHER ADVICE DO I HAVE?

From an analytics perspective, it's a good tool. But you have to have the resources to own it. It's not only about buying it. It's not only about capacity, but somebody has to care and feed it. It's not one of those things that you can put it in, walk away and just consume the data. If you don't take care of it and feed it, you won't get what you need out of it.

Learn more: Read 47 reviews of IBM QRadar