Securonix Security Analytics Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Securonix Security Analytics

Read 7 reviews of Securonix Security Analytics

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

IT Project Manager at a manufacturing company with 10,001+ employees

ITProjec55d8

WHAT IS OUR PRIMARY USE CASE?

We use the solution for protection of engineering intellectual property. We currently look at engineering data in two systems, one a commercial system and one which is a homegrown system.

HOW HAS IT HELPED MY ORGANIZATION?

We've seen a couple of circumstances where people accessed data, especially in our internal application, and we weren't sure how they did it, because they shouldn't have been authorized to access it. We actually found a backdoor on our side. Their access did not go through that backdoor intentionally, but they did find a backdoor way to get the data. We shut that one down as soon as we found it. The other thing we do, where it's been a big help, is that we people who, from a process standpoint, bring down a ton more data than they should. They aren't doing something malicious, but there are ways to bring down simplified data subsets. We've been able to educate the users to take down simplified sets. In essence, that saves them time and effort in having to bring all that data down and then call it up and use it. It's really tough to put hard numbers on that but we have certainly seen a reduction in the amount of these high-volume downloads and it's really been because of a process change on the part of the users.

WHAT IS MOST VALUABLE?

The most valuable feature is being able to look at users' behavioral profiles to see what they typically access. One of the key events that we monitor is people's downloading of objects, files from either the engineering or the homegrown application. It's very easy to see people's patterns, what they typically do. The system might identify somebody who is engaging in anomalous behavior. Especially with the product's rev 6, there are a lot of tools to go in and do investigations, even without talking to the person, to try to determine what were they doing. Is it a case that they normally don't do something but this looks like a legitimate action, or is it something we need to investigate? That is pretty neat.

Securonix Security Analytics

Read 7 reviews of Securonix Security Analytics

WHAT NEEDS IMPROVEMENT?

It's tough in some cases for the solution to do it, but we have a lot of users who, because they're engineers and they're bringing down product data - where, at times, a top-level product could be 10,000 or 15,000 objects - it's difficult for us to determine what should be a concern and what shouldn't be a concern. We work with the Securonix folks to try to come up with better ways to identify that. That's a difficult problem to solve because it's very application-driven and very user-driven, based on what the user's role is.

FOR HOW LONG HAVE I USED THE SOLUTION?

We started our implementation in October of 2016. We are currently on Revision 6.2 of Securonix (/products/securonix-security-analytics-reviews) using the SaaS cloud version.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

The stability has been pretty good. On rev 5, once we got it going, it was very stable. We didn't find very many issues. As we go from rev 5 to rev 6, the architecture's a little bit different and we have run into a couple of issues which they are in the process of fixing. Once those are fixed, we'll discontinue use of rev 5 and use rev 6 because we feel comfortable with what we're seeing in the data for rev 6. The stability issues I mentioned are definitely bug-related. We had a call with Securonix's development management last week and they gave me a very good technical explanation of what was going on. It made sense but it was complicated. It had to do with the sequence of what they were doing and the data sources and how it's different in the architecture. These are just things they didn't expect to run into. Once they understood it, they started fixing it and making sure that it not only fixes our instance but other customers' instances, where they might have run into something similar.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

It's certainly extremely scalable. They have a lot of connectors into different data sources. We haven't identified a data it seems we wouldn't be able to read in. We certainly have plans to increase usage. We started this as more of a pilot with engineering data access on these two systems. Currently, on our homegrown system, there are about 20,000 users a month. On the commercial system, which houses a lot of the engineering model data, there about 13,000 users. That's the number of people whose activities we're looking at. That's internal, customer employees, as well as contract-contingent workers, onsite and offsite.

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

We didn't have a previous solution. On our homegrown system, we made a little bit of a homegrown solution, but the only thing it did was that if somebody had a high number of downloads, it would send us a note. On the commercial system, we were trapping things in the log, but the logs are typically about 1.5 million rows a day, and that's really tough to analyze by hand. That is why I said, "I can't do this. I need an analytics tool to do this." This was really the first analytics tool that we deployed for this particular purpose.

HOW WAS THE INITIAL SETUP?

For me, the system setup, itself, was of medium complexity because, for both applications, there were standard connections into them. We had to write our own queries. We learned from that. Our homegrown system was fairly easy because we just look for objects downloaded. Our other application looks for more than just these download events. So it was more complicated to come up with the query and then for us to come up with use cases to have the system analyzed. We find that that process is ongoing. From when we started, we've never really stopped improving how we're trying to get results with the system. From my experience, you don't set it up and you're done. It's very much an evolutionary process. As you learn more, you can help feed that into the system. You can say, "Oh, I thought this was a problem. You're saying it shouldn't be. Okay, I'll take care of that now and I won't flag that. Or I'll make a different peer group to analyze data against." For us, it's very much a continuous process so that we can improve and hopefully minimize what we think are things that we need to investigate. In terms of how long our deployment

took, to me, it is still evolving. If I look at the initial one that we did on rev 5, the system was set up in October and just after Christmas we were, for both sources, doing pretty well. We were getting very usable results. The homegrown one was very easy to implement and we got that one going before Christmas. The other one is a little more complicated and took about three months. We've constantly refined ever since. The implementation strategy, initially, was to apply it to these two applications but we didn't necessarily know what we would find, what the typical behavior would be. So we really needed to understand what people are doing, with our various use cases. Our strategy has been to continue to improve, to reduce the amount of time we take to look at data to see if something is an issue. And then, we're looking at a reading in more engineering data sources. Currently, we're in the process of figuring out the best way to read in from a SharePoint Azure site, to get data from our SharePoint on what people are using for accessing documents. Then we're also looking at what we call data "exfiltration," which is: Did somebody take the data once they downloaded, did they send it to a printer, did they email it out? Did the data go somewhere off the computer of the user to somewhere else? Our strategy has included taking that to the next step. When we move from rev 5 to rev 6, there are new capabilities, new enhancements, and so it took a few months to get ready. The best way to describe the move to rev 6 is that it's a totally different system. It's a SaaS environment. The one we have now is on-premise. What you do is re-set up the use cases that you are currently using and your policies and then re-ingest data, but from a shorter timespan. Because of what we were doing, it is a little more work. But the Securonix folks helped us with the initial setup and the data ingest. From our standpoint, it was just a matter of validating on our internal system for rev 5, how the data was looking in rev 6. It certainly took some time.

WHAT ABOUT THE IMPLEMENTATION TEAM?

The consultants from Securonix are key, from our standpoint. I have almost daily calls with them to talk about what are we seeing, what are we doing, how can we improve things. We actually have a team call with some of the Securonix consultants and management every week. We generate a weekly report of what we have run into that we need help on, what our accomplishments have been, and if there are any issues, what their statuses are. We have excellent communication with the Securonix consultant folks. They're very good.

WHAT WAS OUR ROI?

For this kind of solution, unless you find somebody who physically took something and was going to sell it or try to, and you were able to recover it, it's really tough to put a monetary number on intellectual property loss. You would be making an assumption about what might have happened if the competition had it. Still, I would certainly say that that we have seen a return on investment. We haven't seen a return where we actually stopped our engineering IP from going out the door. Then we would definitely have an ROI because all it takes is stopping one person and you've paid for your investment over and over again. But what we've been able to do, if nothing else, is to let more people know that we are aware, that we're watching what's going on. We've had factory managers who are actually appreciative and feel more comfortable knowing that someone is watching this information. Again, we're back to these intangibles, but our company very much sees the value in this and, as we move forward, we'll see even more value. It might cost us a little bit more but we'll see more ROI if we find out what's going on with things like data exfiltration.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

I can't say anything from a numbers standpoint, but we went in on a three-year agreement which has an annual licensing fee, based upon the number of people that we're monitoring. There have not been any additional costs to the standard licensing fees.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We did evaluate other options. The main competitor was Exabeam. My manager was the one who did a lot of the investigation of the various tools. At the time, the competitor's system was extremely limited in the number of data sources it could read in, whereas Securonix had a lot of pre-made connectors. In our cases it had out-of-the-box connectors to the two data sources that we needed. We had to write our own query, but it could at least connect directly into the logs that we had. The other thing that Securonix had, and the other one didn't, is incident-management or case-management functionality. If someone were to download a high number and we decided we needed to investigate it, I could open a case right in the tool. It would be able to directly reference the data that they downloaded and we could open and shut the case directly in the tool, as well as report from it. Since it was all integrated, it was extremely helpful. That was one of the things that we liked. Also, at the time, Securonix was the most mature in the user and entity behavioral analytics, among the groups which offered that kind of functionality and software.

Securonix Security Analytics

Read 7 reviews of Securonix Security Analytics

WHAT OTHER ADVICE DO I HAVE?

The best advice is to make sure that you understand your use cases. For example, we said we want it to trap a high number of downloads, we want to see if people downloaded and then emailed out any of the objects. We came up with the use cases of what we wanted to check for even before we started our implementation. Then the Securonix people were able to better set up the individual threats that we were watching for. The other thing that we do is we categorize our data. We say a given type of intellectual property is high, medium, or low. That way we know what we really want to protect. Somebody taking a nut or a bolt isn't the same thing as somebody taking a turbocharged engine and trying to sell it to somebody. It took us a while to actually come up with a standard for categorizing and then to actually categorize, because there were millions and millions of objects or drawings that we needed to classify. That was a project in and of itself. We did that before we did any kind of analytics with Securonix. The first thing we did was classify our data. When I took this role, they said, "Hey, we want you to protect our high IP." So I smiled and said, "So how can I tell what the high IP is?" And they said, "Oh, well it's in this folder." I said, "What happens when it's out of the folder? How do I know?" I wanted it so that the data could always tell me it's IP level, regardless of what folder it was in or even if it was out on someone's desktop. That's why, to me, that's the first thing that you need to do. Because otherwise, it's just hearsay in terms what's important to protect. If it's important to protect, label it and then we'll understand. We look for ways for us, and for the system, to improve identifying things. For the majority, we've been happy for what's there. With typical software you run into software issues that might slow you down and you have to get them fixed. They've been very good about resolving issues when we find them, especially because we find stuff that is pretty unique because of what we're doing with application monitoring. It's so specific and it's really customized for how we've set this up. There are just a handful of users of the solution. I'm the main one who works with the consultants. Otherwise, it's a group of just under ten people who are even able to get into Securonix and look at the information. Like me, most are in IT. There's one person in insider-threat security who helps with coordinating investigations. There's also someone on the business side, even though he is, in a way, more IT-related. He works for the engineering standards group on the business side. In terms of deployment and maintenance of the product, we certainly rely on the Securonix folks. There was one main person we used for the deployment of Securonix. Sometimes that person had a second, and I was involved as well. Only three people, from our side, were involved in the actual deployment, although I needed people to write the query to ingest the data. But once that was done, I didn't need those people anymore. Maintenance is done by me and the Securonix consultant. Since it's a SaaS environment, I have no idea how many people they have on their side, making sure that the system's working fine. For what we're doing and what it can do, on a scale of one to ten, I would put it in the nine to ten range. The only reason I wouldn't say ten is that means it's always perfect. There are always issues. But I'd say it's at least a nine.

Learn more: Read 7 reviews of Securonix Security Analytics