IT Central Station
Unbiased reviews from the tech community

Case Study

Cisco Secure Email

reviewer1515012

Senior Infrastructure Engineer at a financial services firm with 51-200 employees

Review by a Real User
Verified by IT Central Station

What is our primary use case?

The big use case is filtering inbound messages for spam and malicious messages. Obviously, it's a huge issue for everyone to keep as much of that stuff out as possible.

How has it helped my organization?

Users are getting a lot fewer malicious and nuisance messages. When we moved to the cloud product, we added in a service for graymail unsubscribe which we didn't have before. That makes it very easy for people to safely unsubscribe from mailing lists, especially the sort that they have been added to without knowing what the company is. That has reduced the amount of time users waste going through that process and the amount of time IT has to spend responding to questions about what they can do about things like that. In general, it's enabled us to spend less time addressing user issues regarding junk mail. It has also been better about not blocking legitimate messages, which again comes down to saving time for both users and IT.

The migration from the on-prem email security to its cloud email security saved us money, versus where we would have been if we had kept the on-prem with them. Versus the Microsoft service, it was basically a wash. But compared to Cisco's on-prem service, the cost is the same, but you don't have to pay for the hardware and you don't have to maintain the system, as far as upgrades and hardware failures are concerned. It is cheaper to operate on their cloud service than it is to operate with their on-prem service. The hardware savings are from whatever level of hardware we ended up

not having to buy. If we had stayed on-prem with it, we would have needed to buy two new appliances that year, appliances which would have cost $10,000 or $12,000. I don't have a good figure on how much manpower we spent maintaining upgrades with the on-prem. It wasn't huge, but we probably save an hour a month, on average, on maintenance.

For maintenance, it depends on what's going on, but there may be a few hours a month for reviewing, reporting, and for addressing any user issues. User issues mainly revolve around things like, "Okay, the user hasn't gotten an email from so-and-so. Check and see whether or not they've got it." But as far as actually maintaining it, to ensure it keeps functioning, it's pretty minimal; maybe an hour a month. The people who handle the maintenance are from our infrastructure group, which is a combination of systems and network functions.

What is most valuable?

A few of the big features are ones that we found that we missed terribly when we moved over to Microsoft. One of them is simply the logging that they have in the reporting. For example, if I wanted to get logs about emails since last week, from a certain address, with native Office 365 I would have to submit the search requests and I would get an email a few hours later with the results. With Cisco, it's not only a lot more detailed information, but it's nearly instantaneous. So if you have to do any sort of research into an issue, whether it's security or something is missing, it makes that much less labor intensive.

The filtering is definitely better at catching both spam and malicious messages, and there's a lot of extremely granular ability for setting up rules. You can do it the way you want to. The Microsoft solution tends to be pretty limited in how it allows some of that to be done. It forces you into doing it a certain way, even if it's not good for your business process.

What needs improvement?

The interface is dated. It has looked pretty much the same for 15 years or so. It would be helpful to be able to do everything from one spot. The centralized quarantine and reporting are completely separate from policy administration.

For how long have I used the solution?

We used it consistently from 2007 to the beginning of 2020, and when we went off of it, it was about three months before we started back up with the cloud option.

What do I think about the stability of the solution?

We haven't had any stability issues with it. It seems to be good.

What do I think about the scalability of the solution?

I haven't seen any scalability issues. I'm not quite sure how scaling would be handled if we had a truly immense increase, but I haven't seen any challenges with it. We're on the small side so we may not be a good example.

We don't really intend to change our usage much. We use it for all of our inbound and outbound email.

How are customer service and technical support?

I haven't talked with their technical support much in the last few years. The only issue I've had was a support case for getting command-line access set up. That was fine, but there was virtually no contact about it.

Which solution did I use previously and why did I switch?

We have had two runs with Cisco Secure Email. We initially ran it on-prem and that started in 2007. It was the same year, or a little bit before, Cisco bought the old IronPort product. And last year, we initially ended up dropping the on-prem, when we were moving into Office 365. Although we were happy with it, the thought was, "Okay, if we move everything to Office 365, Microsoft can handle that. We have their full-blown mail filtering products." We thought it would probably save us some workload, not having an extra product to deal with.

The intent was that we were going to consolidate to a single product when we moved to the cloud for email, and we found out that it didn't work as well as we had expected. We didn't do a direct conversion from the on-prem to the cloud solution. There were a couple of months between it during which we tried the Microsoft option.

We then found out that they were not nearly as good as one would expect from a market leader in corporate email. I then contacted Cisco about what it would cost to do it in the cloud with their products. I was rather surprised to find out that they don't charge anything more to host it, than they do to have you run it on your own equipment. We ended up jumping back into it with their hosted solution, without really planning to. When the cost came back and was as attractive as it was, we decided, "Okay, this Microsoft filtering is not working out. Let's go back to Cisco." We went back to it and it's been working really well, better than it did when it was on-prem, because we don't have to maintain as much of it.

We had been using encryption on Cisco before, but we did end up leaving that with Microsoft, just because it integrates with their Outlook browser better. I'm at something of a toss-up on which one I prefer. Because the Microsoft solution integrates directly with the Outlook client, it is a bit easier for users to manage. But the encryption on it seems to work fairly

decently, although it has the same problem that all of them do. There are tons of standards for that. Everyone has their own. It would be great if there was some sort of multi-vendor standard for that but, without it, we moved it over to the Microsoft solution and that seemed that to be a little easier for users.

Because we had those few months in between, we didn't qualify for a license transfer. We had let the initial service lapse and then we brought on the cloud service.

How was the initial setup?

It ended up being a really easy setup for the Cisco cloud product. I was pleasantly surprised how much was already ready for you out-of-the-box.

I found the setup to be straightforward, as someone who was familiar with the management environments. If I had not had the experience with it, there would have been areas that could use more documentation to explain what different sections of the product do. But I had been using it for a long time, so that was not an issue. But I could see that is an area they could put more into. We also had a technical contact available to us for when getting started, to whom we could reach out. But it would be good to add in some more entry-level documentation.

As far as the policy setup goes, our equipment was end-of-life and we weren't at a version that we could migrate from. So we decided to do greenfield for the setup and we're actually happy we did because Cisco's default setup on its cloud product, when they brought up a new blank instance for us, had a really good framework for rules, et cetera. We copied in exception lists and the like from our existing setup and we were up and running in an afternoon.

When we went in, we initially did it as a trial, because they offered a 30- or 60-day trial. We did that to see if this was what we wanted to do. We ended up poking around in the environment a little bit first, because the whole thing was an unbudgeted change for us. When we moved over to Microsoft we found we were having all these issues. We put some resources into trying to resolve them but we saw there were deficiencies in Office 365, when it comes to the filtering of email. We started the trial with Cisco to see if going back to them and their cloud would solve things. We liked what we saw and decided to move everything over. The grass really was greener on that side.

The downtime involved in the migration from Cisco's on-prem solution to the cloud email security was minimal, about 15 minutes. The downtime aspect wasn't especially important since we did it after hours. It's emails, so it's not like anybody was going to notice that it was down for that amount of time.

The learning curve involved in migrating from the on-prem to the cloud email security was pretty easy. The environment really is very similar to manage in the cloud. If you look at the

management consoles that you're used to seeing on-prem, and you look at the ones in the cloud, about 99 percent is the same. There are some things that are unavailable because Cisco is handling the software upgrades, but almost all of it that you had on-prem is the same. There are a few extra steps to getting into the command line, they're a little bit weird, but all the policies are identical to the on-prem method. There's not much learning curve involved in switching.

Overall, the migration was massively easier than I expected it to be. We did it on a Sunday afternoon and it only took about three hours.

What about the implementation team?

We were in touch with the technical contact from Cisco for some basic stuff, for getting started.

Which other solutions did I evaluate?

We were just evaluating between Cisco and Microsoft's advanced threat protection.

We decided not to evaluate anyone else when we saw that Cisco was going to be less expensive than we thought it was going to be. My expectation going in was that the cloud service would cost more than the licensing for on-prem would, because they're hosting it. But that wasn't actually the case. It ended up costing about the same as what the on-prem cost, except that we didn't have to buy hardware anymore, which obviously saves some money.

What other advice do I have?

It's definitely worth looking at Cisco's cloud email security offering. It's surprisingly simple to get going with, and it really is easier to use than the on-prem because of everything they have built into it. It is surprisingly cost-effective.

It's integrated with their AMP product, although that's sold as a part of it. We haven't integrated it with other Cisco stuff at the moment. We've got third-party stuff that we have it integrated with.

Read 21 reviews of Cisco Secure Email

See All Reviews