IT Central Station
Unbiased reviews from the tech community

Case Study

Cisco Secure Email Cloud Mailbox

cisco

reviewer1378053

Systems Administrator at a university with 1,001-5,000 employees

✓ Review by a Real User
✓ Verified by IT Central Station

What is our primary use case?

We're using it to collect data. We haven't fully implemented any of the features to stop any attacks. At this point we're using it for informational purposes, until we get a better grasp on everything. It's gathering any spam messages or malicious email messages that come through.

It's in the cloud and hosted by Cisco.

How has it helped my organization?

I can't provide a detailed example of how the product has improved our organization but only because I don't want to give out too much information. In broad strokes, being able to go in there and see where stuff is coming from and who it's going to, and being able to see, hour-by-hour, where threats came in, we can help pinpoint when issues started, who an issue started with and who it's going to, to best remediate issues.

Because the user interface is very intuitive and doesn't require specialized training, less time is needed to dive in to get to the basics of it before a deep-dive ever happens.

What is most valuable?

The most valuable feature that I have found so far is that it actually works within our tenant. If we have anybody that we serve the email that it would go to, and someone else that we serve the email to, it will find that; it will go through that filter as well. And it will do it quickly and efficiently for us. It's not something that we need to push out to then have it circle back in so that our email filters or spam filters will catch things.

On ease of use, it rates very high. It's something that I was able to get into without really looking at any documentation. I wanted to see what it felt like before I started looking at any documentation on how to use it, and it was very easy to use. It works very smoothly. The user experience is very intuitive. They did an amazing job on that.

The solution also provides a diversity of intelligence, the way that we have it implemented. Since it's not taking anything out, it can bring stuff to our attention and we can remediate it if there is actually a threat. And it shows us the links, and all the information regarding why it caught something.

What needs improvement?

The search area has room for improvement. When you go to the next page, it remains at the bottom of the current page that you're on.

Also, under the reports section, it allows you to see any "convictions," but if you want to search for those convictions you have to remember when they all came in and go back and edit the search accordingly. You cannot click on the list of convictions to actually see if you had a spike at a certain time.

For how long have I used the solution?

We've been using it for at least four weeks.

What do I think about the stability of the solution?

So far, we haven't seen any issues with it. It seems very stable.

What do I think about the scalability of the solution?

It appears to be doing a very good job in terms of scalability. With the transition from one mailbox to all mailboxes, we really didn't see an impact on the time that it was processing information.

We have about 3,000 to 5,000 mailboxes covered under Cisco Secure Email Cloud Mailbox.

How are customer service and technical support?

We haven't used technical support yet.

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

We have used other Cisco items to accomplish some of the same tasks we're using Cisco

Secure Email Cloud Mailbox for, so we're beta-testing Cisco Secure Email Cloud Mailbox.

How was the initial setup?

Our initial deployment of the solution took well under an hour, and that includes the configuration because we had to go into Office 365 and set it up and then actually deploy it. That time, altogether, was very short and it was very smooth.

When it came to the deployment process for Cisco Secure Email Cloud Mailbox in our Office 365 environment, I had to read the document again because I couldn't believe that the initial setup was that easy. The concern that we have is the amount of rights that it needs. It doesn't seem like it should need that many rights to be able to do what it does. But overall, just implementing it was very smooth and very easy.

Our implementation strategy was that we did it on a single mailbox as a proof of concept, and from there we expanded it to our tenant.

In terms of staff involved in deployment and maintenance of this solution, two of us, as systems administrators, have been the focus on this, along with a security person, who is involved in security analysis.

What about the implementation team?

We did it ourselves.

Which other solutions did I evaluate?

We didn't evaluate any other products. Cisco reached out to us to have us test this.

What other advice do I have?

Lock down who has access to the product, for the purpose of being able to see all email coming in and out; seeing who it's to, who it's from, and the subject. To best protect data, you would want to limit who has access to that data.

In terms of the solution's ability to prevent phishing and business email compromise, it's kind of hard to evaluate because we haven't fully implemented it. It will show us what it catches, and the implementation will actually take it out of the user's mailbox. I feel like that would be good. It seems to still catch some stuff as spam that may not be spam, according to the user.

We're using Cisco AMP on our desktops and it seems to be doing fine as a virus scanner. The only issue I have seen is that on a few machines it spikes the CPU utilization for the whole time that it's scanning.

I would give the solution an eight out of 10, just because we haven't implemented everything yet. The parts that we have implemented have been very smooth and very easy to use. There are small portions that we haven't fully implemented yet.

Read 2 reviews of Cisco Secure Email Cloud Mailbox

See All Reviews