IT Central Station
Unbiased reviews from the tech community

# Case Study

## Cisco Secure Email

**Mark Rodrigue**

IT Admin / Manager at a retailer with 501-1,000 employees

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

## What is our primary use case?

All of our inbound and outbound emails flow through the CES environment and we leverage it for spam filtering, phishing filtering, malicious URL detection, attachment scanning, and data leak protection. It basically covers all of the security layers for email.

## How has it helped my organization?

It's cut down quite a bit on the amount of false-positive spam that we get. The spam engine that's utilized by CES, we found to be pretty effective. It's rare that things end up in a quarantine when they aren't supposed to be there, which is very beneficial. I believe that was one of the reasons that we moved from the previous hosted solution that we were utilizing to CES.

## What is most valuable?

The malicious URL scanning, as well as the anti-malware features, have been really useful for us in our environment. Specifically, the URL scanning has helped to knock down quite a few phishing attempts that come into the organization. The broader blanket automated attempts get knocked down pretty quickly since those URLs typically get flagged early on, and then the appliance just picks up on those URLs and knocks them down. It is the same with malicious attachments. The malware scanning that's done via AMP, which is deployed elsewhere in the organization as well, just grabs all of that before it hits the inboxes.

We have our email security feeding into the

SecureX solution and it's nice to have all of our security platform statistics in one place. We leverage quite a bit of the Cisco security stack and having all of that feed into the SecureX dashboard is great. The dashboard continues to evolve, but it is at least nice to be able to see everything at once.

Integrating this product with SecureX was pretty quick and easy. Both of the solutions are cloud-hosted and the SMA, which is the reporting module that feeds the data into SecureX, was done via the API. The documentation on the SecureX portal walks you through exactly how to add the various integrations.

We leverage the AMP functionality that exists in CES, and it also ties into threat response, which is the threat-hunting platform that Cisco has. The benefits of these integrations were pretty important in the decision to stay within the Cisco product family. The threat hunting and threat response are really nice because we're able to see if something malicious makes it into the environment. Once that happens, we are able to trace that back and find out if that was done via an email, and then grab the information for that specific message. This will tell us if there have been any other indications of compromise on any other hosts. When it comes to being able to do that, having it all in a uniform environment is pretty important.

## What needs improvement?

The UI is definitely one area of improvement because it doesn't match other interfaces and the navigation can be a little clunky. Generally speaking, it is just dated, and I know that they're working on enhancing it for later versions.

They should continue to develop their integration with Office 365 or Hosted Exchange since a lot of organizations, ours included, are moving primary Exchange services to the Microsoft Cloud. Being able to integrate tighter with that environment is important.

## For how long have I used the solution?

I have been using Cisco Secure Email since joining the company.

## What do I think about the stability of the solution?

We haven't had any issues at all with the stability of the platform.

## What do I think about the scalability of the solution?

With it being cloud-hosted, it can scale as wide as you need to.

We have roughly 1,000 employees and all of our inbound and outbound emails go through this system. This means that there are several tens of thousands of messages a day flowing through it. We haven't had any sort of performance issues at all with our environment.

## How are customer service and technical support?

Cisco's technical support is very good. We've just recently had a couple of tech cases that we needed help with. We were researching why some of our partner's messages weren't getting through intact. Because this is a hosted solution and they have quite a bit of visibility, it has always been great.

We've never had any issues with support on this platform.

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

In previous organizations, we've leveraged Postini, which was a cloud-based solution that was acquired by Google. I've also worked in environments that have leveraged Microsoft's Office 365 email spam filtering, and they've been good, but generally, usability is sometimes a problem. It goes back to the UI and then the accuracy.

The amount of spam that is stopped has not always been great. As such, I feel that CES has a pretty good balance in that regard.

## What about the implementation team?

As this solution is hosted on Cisco's cloud, we don't manage the underlying infrastructure.

We probably have about eight individuals who work with it. Some of them are within our support organization, there are messaging or Exchange admins, and there are network engineers.

## What was our ROI?

Return of investment is something that is difficult to measure because you're essentially trying to prove a negative. It is difficult to say what it has prevented or what has been stopped from happening. That said, I think the overall satisfaction, at least from the user perspective, is good.

When you consider the spam and anti-phishing components, in addition to the IT benefit of the anti-malware and antivirus, I think we definitely get an appropriate return. Nobody questions the expenditure on the solution as being ineffective.

## What's my experience with pricing, setup cost, and licensing?

With respect to transferring policies and licenses, Smart Licensing has really improved the overall licensing model for Cisco. We've been really happy with Smart Licensing.

There are additional fees for adding features. For example, things like AMP are additional licenses. Because it's all done via the Smart Licensing portal, when new licenses are acquired they're dropped in our bucket, so to speak, and then the solution just grabs those licenses. There is no back and forth required. The license ends up in the bucket and then the solution syncs with Smart Licensing and we're good to go.

## What other advice do I have?

For the future, we are looking at moving to newer versions that allow for additional advanced phishing protection. That's something that we're targeting. Also, we're trying to figure out how to streamline our mail flow with the majority of our inbound and outbound email that is now flowing through Office 365. Essentially, we're figuring out how we can tighten up that integration and lessen our dependence on on-premises Exchange for our mail flow.

With respect to versioning, it is controlled by Cisco. I believe that version 13.5 is when they introduced the advanced phishing protection. We're notified when new versions are released and we can ask for earlier versions, but we get adopted once those versions become generally available.

My advice for anybody who is implementing this product is to leverage the Cisco Validated Design (CVD) documents that exist. They're super helpful. Cisco has done a lot of work with Microsoft in figuring out integrations and documenting those. There is quite a bit of really good documentation, both within Microsoft and Cisco on building those integrations and configuring them.

We have also leveraged Cisco's adoption services around renewal times to make sure that we're using the platform to the fullest extent. They offer health checks for their hosted solutions, so on a yearly basis, you can sit down with an engineer and walk through and make sure you're on a good version of the code. You can make sure that you've again implemented from a high level, those feature sets correctly, and that you're leveraging things properly. Cisco does a lot of things to make sure that it's an easy renewal conversation to have, specifically with leadership.

The biggest lesson that I have learned from working with this product is to make sure that you're engaged with your Cisco teams to guarantee that you're getting the most benefit out of the platform. Again, you should be taking advantage of the health check services and adoption services because they're really unique.

In summary, this is a good solution but I think there's always room for improvement. I don't think that anything is perfect and they've definitely got some work to do on tightening up the UI and the configuration presentation. From a functionality perspective, the platform is great.

I would rate this solution an eight out of ten.

## Which deployment model are you using for this solution?

Public Cloud

Read 9 reviews of Cisco Secure Email

See All Reviews