IT Central Station
Unbiased reviews from the tech community

Case Study

Cisco Secure Email Cloud Mailbox

Mike Bulyk

Director IT Security at a wellness & fitness company with 5,001-10,000 employees

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

What is our primary use case?

Our primary use case is the ability to see email activity in the east-west traffic. It does internal email tracking as well as leveraging it as another layer of email defense. We utilize Microsoft 365 (enterprise service) and its Advanced Threat Protection solution, which networks inline with Cisco Secure Email Cloud Mailbox. Then, Cisco Secure Email Cloud Mailbox does an additional layer of detection and protection against malicious email.

Business email compromise is the internal user use case, then phishing and malware delivery are certainly others. They are pretty common and definitely answered by Cisco Secure Email Cloud Mailbox.

After several months of use, Cisco Secure Email Cloud Mailbox has provided additional capabilities (and value) which enables much faster mal-email remediation times.

How has it helped my organization?

Having Cisco's solution gives us a fast way to track and identify. We haven't seen any specific events yet, but certainly having another layer that's able to give us visibility and detect malicious email from an insider is definitely useful. Insiders are typically the hardest to detect, including in an email environment.

So far, we haven't had any detections, which is a good thing. This just means that our traditional use cases of egress-ingress type monitoring work pretty well. However, we have seen some spam being detected. Even internal email forwarding, where an internal enterprise account will forward a spam message to another internal

account. This speaks to the system's ability to detect these and fairly quickly categorize them as spam, which is good. Luckily, it wasn't malware. Cisco Secure Email Cloud Mailbox seems to be working well.

Our administrative overhead costs are low, both for time and dedicating human resources. We set the solution, then check it daily. Because we haven't had any detections, which is a good thing, we don't really need to dedicate any additional resources in terms of generating an incident response process.

What is most valuable?

The ability to see east-west traffic is its most valuable feature. Traditionally, email defense focuses on north-south, inbound-outbound, egress-ingress traffic. With Cisco Secure Email Cloud Mailbox, it's able to quickly identify, track, tag, and categorize emails that are internal. That can typically give us visibility into if there's an internal compromised account (for example). Someone can then use that internal compromised account to email additional accounts with either malicious software or links, but internal within that Office tenant. Effectively, that email message never leaves the tenant. Any of the mail gateways really do not have any method or way of seeing this traffic since it's not leaving the environment.

The solution is very easy to use. It's just a single pane of glass, single screen web page that you access. Then, there are a small number of clicks necessary to get at the information you need. Reporting is easily generated. Likewise, the search capability is easily accessed and usable as well as provides the first initial information that you need about messages identified, categorized, and total volumes. All that information is easily identifiable and quickly accessible as soon as you log in. It is an easy to use, single web page, SaaS application.

Cisco Secure Email Cloud Mailbox's user interface is intuitive. We didn't need any training. There was a quick deployment document that you skim through, and it's fairly easy to both deploy as well as start using.

Threat Grid is a capability which allows for running or executing software in a special sandbox environment where it's not affecting your enterprise or corporate systems. For that particular use case, Threat Grid works really well. It also ties in with various threat intelligence sources, e.g., detonating/testing our particular software or file in the sandbox can immediately identify indicators of compromise and share them with other clients that leverage Threat Grid. Likewise, the software that I uploaded for sandboxing is immediately validated and checked against all other client submissions as well as open source and Cisco Talos Threat Intelligence Sources. I find that really valuable. While there are other sandboxing solutions out there, I use Threat Grid quite a bit and I find it to be extremely useful and very usable.

Threat Grid also gives us a sense of safety because I don't have to test it or build out

custom virtual machines to do the testing. I don't have to test it on enterprise systems. From that perspective, Threat Grid is definitely a very good solution. Its ability to integrate with other Cisco portfolio tools is helpful because then you can tie in and quickly view what malicious files might've been found in your environment regardless of what Cisco security solution you are using, whether it's AMP, Email Security, Cisco Secure Email Cloud Mailbox, or anything else.

AMP for Endpoints is something that I've used extensively. We have also used AMP for Network and Email. Collectively, it seems to be doing a pretty good job, especially when combined with Threat Grid because it's quickly able to identify files by hashing them and figuring out within the databases that Cisco owns, as well as open source threat intelligence databases, whether that particular hash is found in those databases. If it is, then it is malicious. It takes corresponding action pretty quickly.

If it's an unknown hash (after it identifies the file by hash value), and if it's unknown and not found in the databases, then it automatically uploads that file to Threat Grid for sandboxing and analysis. That layered approach with respect to treating the files as they come in works well, whether via email, network, or found on an endpoint, especially as an ecosystem solution that integrates with other Cisco components and security tooling that one may have in the enterprise. This works well because the information found on a single endpoint, for example, can then immediately take action on an email by blocking that identified malicious file. Likewise, if there is a file that's coming in via email and it's found to be malicious by AMP or Threat Grid, then the information about that file is immediately known by the endpoints. The endpoint solution can then take action on that malicious file. As an ecosystem, it works really well.

What needs improvement?

If Cisco could continue to develop integrations, whether it's internal tooling, Threat Grid, or AMP reporting which could be accessible via a single web page, that would be helpful. This would essentially add additional context on messages as well as files or links being detected. Potentially adding additional context on why certain messages are tagged as spam or malware. In our case, malware hasn't been detected yet, but spam certainly has been. Knowing what engines or which components of the message make it identifiable as spam, that could be useful. Additional context and reporting accessibly via the main dashboard would be great.

There is still room for improvement in terms of integrations with other Cisco tools and non-Cisco tools. There is also some room for improvement needed in terms of the reporting.

For how long have I used the solution?

6 months.

What do I think about the stability of the solution?

The solution is set and forget in our experience. It seems to be working pretty well. In our experience, we don't require any dedicate resources for maintenance.

So far, we have had no issues with stability. I could see how if there was an issue with Microsoft 365 tenant, then Cisco Secure Email Cloud Mailbox would not work, but so far we have had zero issues.

What do I think about the scalability of the solution?

We are a fairly large company who sees a sizable number of email messages daily. Cisco Secure Email Cloud Mailbox is able to keep up with the messages and message classifications, along with capturing and sending files to Threat Grid. The solution has the potential to be scalable to extremely large organizations as well as serve small to medium-sized businesses as well.

We have two individuals who are both members of the security team: one is a senior security analyst and the other is a security director.

How are customer service and technical support?

We did experience a false positive match where an email exhibiting spam behavior was actually legitimate. I had to escalate this issue with technical support to make sure to get it whitelisted or the engine tuning changed.

Our experience has been pretty good so far.

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

We previously used Microsoft native ATP, which is a built-in Microsoft email protection solution. We added added Cloud Mail Defense because it gives us another layer of protection for east-west traffic.

How was the initial setup?

The ease of the deployment process of Cisco Secure Email Cloud Mailbox is extremely simple. The methodology that Cisco uses to scan email is extremely usable and very simple. Likewise, to set it up, the only requirement is to have administrative level privileges for the Microsoft 365 tenant. Having those rights and permissions, that's really all an organization will need to add Cisco Secure Email Cloud Mailbox into its tenant.

The deployment took us five minutes or less.

What about the implementation team?

There was no effect on our administrative costs at all. In terms of configuration, we didn't have to do anything. The system comes preconfigured by Cisco, so we didn't have to do any configuration or setup. It's a set and forget kind of thing.

What was our ROI?

In our case, downtime certainly arrives from a detection of malicious software, like malware being delivered via email or identifying internal compromised users. Given the extra visibility that we have with this tool, it has the potential to prevent downtime. In our case, that hasn't been proven out yet.

In terms of spam detection, we have seen where Microsoft misses spam and is not quarantining it (taking any action against it), whereas Cisco Secure Email Cloud Mailbox is identifying it as spam. We have seen some success from that perspective.

What other advice do I have?

The files being captured by Cisco Secure Email Cloud Mailbox are pushed into Threat Grid for analysis. We do have a Threat Grid license, so that integration works for us. It was easy for us to integrate these two solutions.

If someone is only relying on Microsoft 365 Advanced Threat Protection (ATP), or even without the ATP solution as an add-on, then having Cisco Secure Email Cloud Mailbox would definitely introduce diversity and provide another view of emails coming through or being generated inside the tenant. Because Cisco Talos is unique and different from Microsoft's information, Microsoft will do its own analysis as well as introduce its own threat intelligence and machine learning logic to detect threats. However, as a company, it's resources don't cover everything. Layering it with Talos and Cisco's resources is definitely a good idea.

Overall, it's certainly a very good idea to integrate another layer on top of Microsoft Advanced Threat Protection. Cisco Secure Email Cloud Mailbox being a player in this market is definitely a good option. Cisco Secure Email Cloud Mailbox is competitive, and it seems to be working pretty well for us. Personally, it gives me peace of mind as well as flexibility in terms of locating internal email traffic. I also know that if Microsoft misses something that there is a chance that Cisco will detect it.

Read 2 reviews of Cisco Secure Email Cloud Mailbox

See All Reviews