Cisco Secure Email

Reviews, Tips, and Advice From Real Users

December 2020

IT Central Station
Unbiased reviews from the tech community

Get a custom version of this report...personalized for you!

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

Get your personalized report here.

Contents

Advice From Real Users

Cisco Secure Email

PROS

Andrew Fisher

"Cisco Secure Email Cloud Gateway has allowed our users to be able to concentrate on the emails that they do receive." "Previously, our users had to deal with nine million additional emails across the organization, which is nearly 1,000 emails per user to have to deal with a month." "That's a massive amount for our staff to deal with and probably several hours of their time." "We have a lot of clinical staff, being a hospital." "We want to make our staff as productive as possible." "By removing a lot of that spam and phishing type emails, this allow... [Full Review]

Phillip Collins

"It does a great job of preventing spam, malware, and ransomware." "I can only go by what people have told me and what I've seen, but I have not seen spam in a year and a half to two years in my own company mailbox." "And there are not a lot of catches where it's catching something that should have gotten through, either." [Full Review]

Enrique Diaz Jolly

"The most valuable features are Advanced Malware Protection, URL filtering, and of course Reputation Filtering." [Full Review]

Syed A. Raheem

"Anti-Spam and Advanced Malware Protection are the most valuable features..." "and we also have the option to block Zero-day attacks." [Full Review]

Security Officer

"Initially, the most valuable feature for us was the SenderBase Reputation, because that reduced the number of emails that were even considered by the system by a huge number..." [Full Review]

HeadOfSe948f

"We like the in-built features, like the email filtering based on the IP and domain." "Cisco has its own blacklisted domains and IPs, which is very good." "This filters around 70 percent of emails from spam, and we are seeing fewer false positives with this." [Full Review]

Muhammad Qureshi

"The most valuable feature is the different content filters we are using, such as DKIM." [Full Review]

Advice From Real Users

Cisco Secure Email

CONS

Andrew Fisher

"I would like more functionality and how to use it for Level 2 type staff." "The biggest issue is it needs to be easier to use and navigate." [Full Review]

Phillip Collins

"Typically, in a phishing email, they try to use a name everybody's going to recognize, like the CEO's name or the CFO's name..." "With this appliance, the way it's designed at the moment, for us to really stop that with any level of confidence, we have to build a dictionary of all the names of the people we want it to check, and all the ways they could be spelled." "My name would be in there as Phillip Collins, Phillip D." "Collins, Phillip Dean Collins, Phil Collins, Phil D." "Collins." "There could be eight or 10 variations of my name that we'd h... [Full Review]

Enrique Diaz Jolly

"The reporting functionality needs to be improved." [Full Review]

Syed A. Raheem

"The configuration UI should be made more intuitive." "Currently, it takes a while to understand how to do the basic configurations." [Full Review]

Security Officer

"We have occasionally had hardware problems because we are using an appliance-based solution, but that might change." "We may consider going to virtual systems." [Full Review]

HeadOfSe948f

"The solution needs to improve its advanced phishing filters." "It is very good at filtering things which have bad reputations." "However, when phishing or malicious emails are new or coming from a legitimate source, we don't feel that the solution is working." [Full Review]

Muhammad Qureshi

"We would like to see more options for the customization of content filters." [Full Review]

Advice From Real Users

Cisco Secure Email

PRICING AND LICENSING ADVICE

Andrew Fisher

"In my previous organization, avoiding four instances of CryptoLocker within an estimated six month period is approximately $600,000 in lost time and effort." "Our five year cost was about a million dollars, and the four outages that we had equated to 65 percent of that five year cost." [Full Review]

Phillip Collins

"You're going to get what you pay for." "If you're not willing to pay the price of Cisco, you're not going to get a product that's as good as Cisco." "I don't think Cisco is overpriced, because for the last two years I've been comparing it to Microsoft and Cisco has been cheaper and given us more features." [Full Review]

HeadOfSe948f

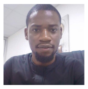
"It is not that costly." "We pay for the solution through a contractor and pay an annual fee." [Full Review]

Informate83d

"We were using Proofpoint and then we switched to Cisco..." "reportability was one of the main reasons we switched, but the biggest one was cost." "If you can get an equivalent functionality for a better price it's wise to do so." "That's what our primary decision came down to: We could get equivalent functionality at a lower price point." [Full Review]

MichaelLawrence

"There were no other costs in addition to the standard licensing fees." [Full Review]



John Agunbiade

"The license was not per user, the license model was per feature." "You could choose anti-virus, anti-spam, etc." "It was feature-based and charged yearly." [Full Review]

Ed Dallal

"Licensing costs depend on how many users there are." "It could range between $5 and $7 per month, per user." [Full Review]

Cisco Secure Email

See 17 reviews >>

Overview

Customers of all sizes face the same daunting challenge: email is simultaneously the most important business communication tool and the leading attack vector for security breaches. Cisco Email Security enables users to communicate securely and helps organizations combat Business Email Compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multilayered approach to security.

SAMPLE CUSTOMERS

SUNY Old Westbury, CoxHealth, City of Fullerton, Indra

TOP COMPARISONS

Proofpoint Email Protection vs. Cisco Secure Email ... Compared 22% of the time [See comparison]
Fortinet FortiMail vs. Cisco Secure Email ... Compared 18% of the time [See comparison]
Forcepoint Secure Web Gateway vs. Cisco Secure Email ... Compared 11% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Energy/Utilities Company ... 25%
Healthcare Company ... 13%
Manufacturing Company ... 13%
Consumer Goods Company ... 6%

COMPANY SIZE

1-200 Employees ... 29%
201-1000 Employees ... 24%
1001+ Employees ... 48%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Comms Service Provider ... 35%
Computer Software Company ... 20%
Energy/Utilities Company ... 7%
Government ... 5%

COMPANY SIZE

1-200 Employees ... 4%
201-1000 Employees ... 54%
1001+ Employees ... 42%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Cisco Secure Email

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Phillip Collins

Their trajectory feature is the most valuable. What I mean is that it has the ability to tell us, after an email has been delivered, where else it went, once it got inside. Maybe it's something we wanted it to stop and it didn't stop it, but it notified us later that it was something that it should have stopped. It can give us a trajectory of all the other places that it went internally and it can tell us what files were transferred as well. It does a great job of preventing spam, malware, and ransomware. I can only go by what people have told me an... [Full Review]

Andrew Fisher

The bulk of the email stopped would be marketing. Spam-related email tends to be our biggest issue. The most dangerous contain malicious content, and those tend to be the worst. The biggest issues are the social engineering and phishing. A lot of the spammers are actually quite good at spear phishing attacks and social engineering our emails. We obviously do checks. We run some simulations for our staff, where we try and train them so they are aware of what not to click on. Also, we have installed Umbrella and had it for a long time as well. Therefo... [Full Review]

Informate83d

One of the nicest things is that parts of it are highly intuitive. For instance, black-listing, white-listing, and things of that nature are very easy to do and they're very intuitive. You wouldn't even need any training to be able to perform those actions straight out-of-the-box. Even though it's not perfect, it has the IMS engine, Intelligent Multi-Scan engine, and it does a good job, right out-of-the-box, of blocking the vast majority of things that should be blocked. Again, it's not 100 percent, but out-of-the-box I didn't have to touch it, I di... [Full Review]

Security Officer

Initially, the most valuable feature for us was the SenderBase Reputation, because that reduced the number of emails that were even considered by the system by a huge number, before we ended up processing them to get through the spam, the marketing, and the virus-attached emails. Since then, customized filtering has been very effective and useful for us. In addition, Cisco has developed the product with its Talos product. They've developed the Cisco Secure Email Gateway systems so that instead of just specifically stopping known spam sources and usi... [Full Review]

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Phillip Collins

When it comes to phishing, I would not give this appliance a perfect score by any means. It's hard to get a perfect score on phishing with any solution. But typically, in a phishing email, they try to use a name everybody's going to recognize, like the CEO's name or the CFO's name. They might spell it wrong, but they will try to get your attention so that you'll do something. With this appliance, the way it's designed at the moment, for us to really stop that with any level of confidence, we have to build a dictionary of all the names of the people ... [Full Review]

Andrew Fisher

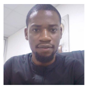
I would like more functionality and how to use it for Level 2 type staff. The biggest issue is it needs to be easier to use and navigate. I know there are a lot more documents in the later versions about how to do things. This is a great improvement from a few years ago when you would have to call a tech to get them to assist you, which they're more than happy to do, but now there are a lot more how-to guides. If they could continue to do that, then it would make the product even more usable. Also, it needs more detail/documentation around what diff... [Full Review]

Informate83d

We find bugs, just like anyone else. We bring them to Cisco's attention. If there was one area I would like to see improved it might be having someone who can help us when Cisco comes out with a new product. Let's say I'm going to be purchasing and utilizing version two of this product. They assign me an account specialist and a technical specialist to help with the bring-up. It would be nice if the specialist would be able to help foresee some of the issues we might run into, specific to the version we're implementing. I know that's a bit of a load... [Full Review]

Cisco Secure Email

Continued from previous page



John Agunbiade

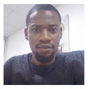
There were a couple of access issues. Also, they need to keep their intelligence top-notch. I remember a particular phishing email that came through to my then-CEO. So they could improve on their intelligence. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Phillip Collins

You're going to get what you pay for. If you're not willing to pay the price of Cisco, you're not going to get a product that's as good as Cisco. I don't think Cisco is overpriced, because for the last two years I've been comparing it to Microsoft and Cisco has been cheaper and given us more features. It really comes down to analyzing what you are actually getting. You might find something at half the price, but what are they not giving you that Cisco's giving you, and do you think that that matters to your company or not? It's an individual thing, ... [Full Review]



John Agunbiade

The licensing was not per user, the licensing model was per feature. You could choose anti-virus, anti-spam, etc. It was feature-based and charged yearly. Aside from the standard licensing fees, you have to pay for support. [Full Review]

Ed Dallal

Licensing costs depend on how many users there are. It could range between $5 and $7 per month, per user. There are no costs other than the standard licensing fees. [Full Review]

Keith Kroslow

We do annual licensing for Cisco Secure Email Gateway and SMA together, and possibly SmartNet support. Packaged together, the cost is just under $38,000. [Full Review]

Cisco Secure Email review by a real user

Stops the vast majority of email from getting in, across our multiple email domains

Sr Infrastructure Engineer at Delta Plastics of the South

Phillip Collins

WHAT IS OUR PRIMARY USE CASE?

The main use case is simply as a point of contact for all the emails to go through first, before they ever get into the Office 365 environment, so they can be scanned and checked for malware and spam, all before Office 365 even sees it.

We're currently on version 12. Our instance is in the cloud and we don't actually upgrade it, they do it for us. It should be upgraded to 13 in the next month or two.

HOW HAS IT HELPED MY ORGANIZATION?

The last time I checked, which was about a month ago, when I looked at all the emails sent to any of our domains — because we have about 10 email domains, and they all go through the appliance — by looking at a report the solution has, I saw that 84 percent of the email sent to those domains never got to our Office 365, because it was spam, malware, phishing, or there was something wrong with it. So it stopped 84 percent which was bad email. Based on my experience and talking to users, 99.8 or 99.9 percent of those emails that were stopped were spam or malware. There might've been 0.1 percent that was caught by the mistake. But that's 84 percent of email not even getting into our systems.

It has prevented downtime. The simple fact that 84 percent of them were stopped keeps people from having to look at those in their mailbox. If you take 1,000, out of that number 840 didn't even come through. That's less wasted time going through your mailbox and reviewing your messages. It also frees up the users, when they do see something that's not anywhere near normal, to clue in that there might be something wrong. We have had emails get through, phishing emails and things like that — it has happened — but I would say we probably get one through about twice a month, at most. The users will immediately shoot it right to the help desk. "Is this real? Is this spam? Is this something I should do?" There's no way to really put a number on it, because I've never really looked into it, but if nothing is coming through that you didn't want to see, then there's no downtime.

Only in a couple of cases have we had a user actually do something they shouldn't have done before they notified us, but that's training. You never have a perfect solution. Two a month is our average, over the last year, of emails that got through that we wished hadn't gotten through, but no harm came of it because the user notified us, and we just told them, "Delete it." We make sure everything is working right and that there was no malware involved and we let it go.

Also, as far as the IT department goes, it's made our lives a lot easier. We get emails if anything does happen. We've chosen to see any event. We only get notified of exceptions that we want to investigate or we want to look into. That makes things easier because we're not out looking all the time. We can wait for the email to come in.

We can look at the updates and the different changes Cisco makes to the system to see if any of those things is going to help us. We think about whether we want to invest any time in configuring those? And once it's configured, you're done. The most difficult part of that is remembering what you did. So we've learned to do our documentation that much better because we need to be able to go back and read what we did before, what we configured.

Our company might buy another company, so we have another domain to add our list of domains for email. In less than an hour we have all that set up and the whole system working, with emails going through the appliance. It's saved us a tremendous amount of time daily, just in terms of keeping track of things.

WHAT IS MOST VALUABLE?

Their trajectory feature is the most valuable. What I mean is that it has the ability to tell us, after an email has been delivered, where else it went, once it got inside. Maybe it's something we wanted it to stop and it didn't stop it, but it notified us later that it was something that it should have stopped. It can give us a trajectory of all the other places that it went internally and it can tell us what files were transferred as well.

It does a great job of preventing spam, malware, and ransomware. I can only go by what people have told me and what I've seen, but I have not seen spam in a year and a half to two years in my own company mailbox. And there are not a lot of catches where it's catching something that should have gotten through, either. We have an email going out daily of everything it puts into quarantine for a user, so the user can release it if it was caught accidentally. In the last six months, I have probably have had to release six or seven emails. It's not catching them. It's doing a good job of striking a good balance.

That is partly due to how you configure it, but we used the standard, best practices when we configured it. We do go back to Cisco, when they offer a free evaluation to review our configuration every nine to 12 months. That helps us make sure that it's set up right and, if there are any new features, that we're aware of them. We do take them up on that every time they offer it.

WHAT NEEDS IMPROVEMENT?

When it comes to phishing, I would not give this appliance a perfect score by any means. It's hard to get a perfect score on phishing with any solution. But typically, in a phishing email, they try to use a name everybody's going to recognize, like the CEO's name or the CFO's name. They might spell it wrong, but they will try to get your attention so that you'll do something.

With this appliance, the way it's designed at the moment, for us to really stop that with any level of confidence, we have to build a dictionary of all the names of the people we want it to check, and all the ways they could be spelled. My name would be in there as Phillip Collins, Phillip D. Collins, Phillip Dean Collins, Phil Collins, Phil D. Collins. There could be eight or 10 variations of my name that we'd have to put in the dictionary. There's no artificial intelligence to say "Phil Collins" could be all these other things, and to stop phishing from coming through in that way. It is stopping a lot of phishing when we do use that dictionary. We essentially let the email come in, but we put a header at the top, in red, telling the user to be very careful, this may not be a real email, and let the user decide at that point, because it's looking at whether or not it came from a domain outside our domains.

If I have to send myself an email from my personal domain at home, it has my name in it, Phillip Collins. We want it to notice that Phillip Collins is a name that's in the company directory, but it's not coming from one of our domains. We want the user to understand that that is how they get around it. Phishing emails will come from the attacker's own email address, but they will set the display name, what you'll see, as something familiar. That's why I wouldn't give it anywhere near a perfect score, because the artificial intelligence just isn't there yet. You have to manually put these things. As you have people come and go in your organizations, you have to decide if you want these people in that dictionary or not. If they leave then you've got to take them out. There's a lot of work to doing that with this solution at the moment.

Another minor thing is the interface that you work with as an administrator. It is not as intuitive as I would like it to be. It's all there, if you understand what you're doing; what email is doing and how you detect certain things. It is not difficult at all to work with, but it could be more intuitive for somebody starting out.

Finally, they separate the email security appliance from the reporting appliance. It's the Cisco Secure Email Gateway and the SMA; they are two separate appliances. The reporting appliance just gets information from the email security appliance and helps you formulate reports. To me, that should all be one. It doesn't bother me that it's not, but sometimes I have to think, "Do I need to go to this appliance or this appliance to get that information?" It should all be in one place, but those are minor things.

FOR HOW LONG HAVE I USED THE SOLUTION?

I have been using Cisco Email Security for two-and-a-half years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's extremely stable. It hasn't gone down on us since we've had it. They made a major move, moving their appliances out of the AWS cloud into Cisco's cloud. They notified us they were moving and we talked about it. We really didn't have to do much of anything, and there was no downtime at all when that happened.

We do have two security appliances in the cloud, so if one went down, the other would pick up. There is redundancy at the hardware level, but we've never gone down.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

It's extremely scalable, especially with it being a cloud appliance, because you're not bound by the hardware like you might be if you bought from an on-prem installation. If we need to go from 500 to 1,000 users, they can just tweak the hardware settings on their end and we're ready to go. I don't think scalability is an issue at all with it being in the cloud.

There are approximately 425 email accounts that it's monitoring and when I last looked at the report about a month ago, there were 25,000 emails a day, on average, that it was analyzing for those 425 users. We're about to add another 50 to 60 new users from a company we just bought. We'll go up to nearly 500 in the next month or two, but I don't see any issues with that . We'll be adding their domain to our system and then adding the users.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

I've worked with Cisco support two or three times in the two-and-a-half years we've had it and it's been wonderful. Most of what I've done is through email because it hasn't been an issue where the system is down. It was just that I wanted to understand something better or I wanted to implement something and needed to know if it was included. And if it was included, how would I work with it and could they send me the documentation? Always, within two or three hours, I've gotten a response, which is very acceptable to me considering we're not down. They've always gotten back rather quickly, and resolved almost everything within one or two emails.

Continued from previous page

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

Before this, we really didn't have a comprehensive email solution. We were simply using the antivirus on the machines. We didn't have anything to stop it from ever getting in, in the first place. Comparing it to other products I used before I came to this company, just about four years ago, it's done much better than any other product I've ever used.

I don't have any way to compare it to anything my current company had before because it didn't have much of anything before. When I came in, that was one of the tasks I was given —securing the email — along with moving us to Office 365. The company had been hit with ransomware before I got here. It had that experience of being attacked and being caught with ransomware, and it didn't have an IT department before I got there. I was the IT department for the first year. We've grown tremendously since then.

HOW WAS THE INITIAL SETUP?

On a scale of one to 10, with 10 being complex, the initial setup is about a four. It's not that complex. But that's what I meant about the interface. You've got to jump around from place to place to do it. It does have some good menus, but a quick wizard is something that would be nice, where you could just walk through it, and not have to jump between different sections of the menu.

The original deployment took about half a day, if that long. There were probably another eight hours' worth of work on my part going into it, getting familiar with it, and finishing some things here and there.

When they went through it with us, we hit the high points and the main things. I did most of the connecting it to Office 365. Once you do the main things, you always need to go back and you look for those little things that might help you. A little tweak here, a little tweak there — sensitivity settings. So I spent about another eight hours going back and reviewing everything and making myself feel comfortable that it was actually doing what it was supposed to do. There were probably another eight hours over the next couple of months after that, watching the reports and spending enough time with the reports to make sure that it was operating the way we wanted it to.

In terms of our staff involved in deploying and maintaining CES, it's me and there's a junior infrastructure engineer who works with me.

WHAT WAS OUR ROI?

The simple fact that users don't get trashed by email means we're working a fraction of the time that we used to work on emails and dealing with the results. It's paid for itself twice over, in my opinion. It has to have done so, based on the time we were spending on it.

Continued from previous page

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

You're going to get what you pay for. If you're not willing to pay the price of Cisco, you're not going to get a product that's as good as Cisco. I don't think Cisco is overpriced, because for the last two years I've been comparing it to Microsoft and Cisco has been cheaper and given us more features.

It really comes down to analyzing what you are actually getting. You might find something at half the price, but what are they not giving you that Cisco's giving you, and do you think that that matters to your company or not? It's an individual thing, but that was what we looked at. Does that make a difference to Revolution as a company or is it something we can do without? Cisco gave us the best overall package.

WHICH OTHER SOLUTIONS DID I EVALUATE?

The only other vendor we really looked at seriously at the time was going with a Microsoft solution and Office 365. Even back then they had something, not that it was very good. But it's simply that we were a Cisco shop, in the sense that we've had Cisco firewalls and Cisco switches for the infrastructure. At that point we had already committed to their Firepower option on the firewalls that collected the information. We had been doing that for about a year. I went to one of their events in Little Rock and that's where they talked about it. I was intrigued and did some more research on my own and determined that this was something we couldn't pass up.

We were a Cisco AMP shop for our antivirus already, which is part of Firepower in a sense. Everything was going to Talos already. The email just made sense because they would all talk to each other and they would get all the information from all the different angles, even across to web access through their Umbrella system. We used that for about a year. When we got our new SD-WAN, it had a lot of the same features the Umbrella system had and we dropped it at that point.

You can put all your eggs in one basket and that can be bad, but in this case it wasn't. It actually worked out well for us.

Everything goes through Cisco so we don't really see anything happening in Office 365. We do have the basic settings for this or for that set in Office 365, but we haven't gone in and fine tuned it the way we did Cisco, because Cisco's the main point of blocking things. When we chose the Cisco solution, there was no way Microsoft's Office 365 solution could have done what we needed it to do. There was no way it would have had any of these major capabilities we needed. It wouldn't have blocked a fraction of the email that the Cisco appliance does. I try to keep up on this and it could be that Microsoft's new ATP might be a game-changer. What I've read sounds a lot like the Cisco appliance. But Microsoft has thrown a kicker in there by adding artificial intelligence. With Microsoft, I wouldn't have had to put in all the name combinations because it would interpret all the names I need it to interpret, even with characters and symbols. I haven't tried it, and I don't have plans at the moment to do so, but from what I've read, Microsoft is catching up.

There are some issues with Microsoft with their integration, simply because you pretty much have to go all-in with Intune, Autopilot — all those features and tools they have to get Microsoft ATP to work. And then you've got to buy the Microsoft 365 E5 license to get all of those security features.

If things are similar, it all comes down to cost and we look at that every year when we renew. What are we paying Microsoft in subscription fees and what is Cisco costing us? So far, Cisco's been cheaper than upgrading Microsoft to the license level we need. Our contract renews in November, so we'll look at it again. That's when we really delve into Microsoft's capabilities. We would want to make sure it would do everything Cisco is doing, before we would make a change, if Microsoft were price-competitive.

Continued from previous page

WHAT OTHER ADVICE DO I HAVE?

Take Cisco up on the offer to walk you through the implementation. It's not that it's a necessity, but it certainly gives you a good feeling, when you're done, that you've covered all your bases. It gave me a good feeling that we covered this and we covered that and they showed me where things were. They give you a copy of the recording where you were on with them and went through everything. You can go back and watch it again later to review it. The same thing is true with their reviews every nine to 12 months. They record them and send you a copy of the recording so you can go back and look at it.

Take them up on that and be willing to sit there and just ask pertinent questions and make sure you understand as you go through it.

As far as the threat assessment analysis goes, what they analyze is what that the appliance decides to send them. That is part of the way it works. When it thinks it has found something and it's not certain, it sends that to Talos first. We don't even know it happened. They get a chance to review it and make a decision of yes or no: this should be stopped or we should go ahead and let it through. We have not leveraged anything other than that from the Talos threat management. We lean on them to help us make sure the right things come through. There have been several times that I have gotten an email as an administrator — you get these emails about statuses — that says, "This has been quarantined in the cloud until we can make a decision," and it will hold it. And once they make the decision, it either stops it or lets it go.

Something else that we're going to begin this year is a training solution to help our users understand what to look for.

I would give Cisco Email Security a nine out of ten. I would give it a 10 if it had a more intuitive interface and the artificial intelligence so we didn't have to do some of that manual stuff.

Cisco Secure Email review by a real user

The amount of traffic that it stops is massive

Andrew Fisher

Digital Program Manager at a healthcare company with 10,001+ employees

WHAT IS OUR PRIMARY USE CASE?

It is used as the primary perimeter gateway for our organization before you can access our environment. Being hosted with Cisco, it goes through Cisco Secure Email Cloud Gateway. Spam, marketing, malicious or virus-enabled emails are not delivered to us 90 to 91 percent of the time because they are stopped external to the organization. That is a massive win for us. We don't have to worry about having to deal with all those emails going through our email servers.

HOW HAS IT HELPED MY ORGANIZATION?

Cisco Secure Email Cloud Gateway has allowed our users to be able to concentrate on the emails that they do receive. Previously, our users had to deal with nine million additional emails across the organization, which is nearly 1,000 emails per user to have to deal with a month. That's a massive amount for our staff to deal with and probably several hours of their time. We have a lot of clinical staff, being a hospital. We want to make our staff as productive as possible. By removing a lot of that spam and phishing type emails, this allows them to do their job. A lot of our staff who are our cleaners don't necessarily use email as often as some of our clinical staff. Therefore, the numbers are worse with our clinical staff who probably end up getting double the amount of these emails.

From a user's point of view, if we're stopping them getting spam, they're happy.

The threat intelligence that we receive from Cisco Talos is good. We don't have the staff or SecOps to do it ourselves. We have one cybersecurity analyst who complements the rest of our IT support for communications, network, and server infrastructure. Things like Talos give us the ability to leverage what Cisco is doing without having to invest the money, infrastructure, and people.

Without it, we tend to be in our little bubble/ecosystem. We're not seeing the number of attacks. Whereas, with Talos being connected to so many organizations around the world, it gives us early warning that we wouldn't have normally had. Because we don't have many applications externally available to the organization, it's good that there's something out there looking out for our best interests. We're able to easily apply that to our infrastructure and without any effort. A lot of it's automated, so it's just applied.

It is a great benefit that we're able to run 24/7. With the help of Cisco and Talos, it helps keep our organization safe. We are very much on top of any sort of zero-day events that we hopefully don't see ourselves. So, we're able to leverage the misfortune of other organizations who have experienced events, in some instances, to our benefit.

Continued from previous page

WHAT IS MOST VALUABLE?

The bulk of the email stopped would be marketing. Spam-related email tends to be our biggest issue. The most dangerous contain malicious content, and those tend to be the worst.

The biggest issues are the social engineering and phishing. A lot of the spammers are actually quite good at spear phishing attacks and social engineering our emails. We obviously do checks. We run some simulations for our staff, where we try and train them so they are aware of what not to click on. Also, we have installed Umbrella and had it for a long time as well. Therefore, if something was malicious, and one of our users had clicked on it, Umbrella would usually stop anything outgoing. The combination of the two solutions has really helped secure our organization.

WHAT NEEDS IMPROVEMENT?

I would like more functionality and how to use it for Level 2 type staff. The biggest issue is it needs to be easier to use and navigate. I know there are a lot more documents in the later versions about how to do things. This is a great improvement from a few years ago when you would have to call a tech to get them to assist you, which they're more than happy to do, but now there are a lot more how-to guides. If they could continue to do that, then it would make the product even more usable. Also, it needs more detail/documentation around what different features do. That would be valuable for the product. That way, when you do have lower level staff who are using it, they will actually know what it can do, e.g., having help icons for each section, and even each setting, does make it easier for the users. As they can click on the question mark for that setting, then they can then see what it does or have it take them to a how-to page on what it does.

The reporting could be improved, especially at a senior management level. The reporting side of things is a big component of what people, especially executives, want to see. In that way, it can justify its use ongoing. The executives want to know the volume of traffic that it's stopping. While users have to deal with the potential loss of income and hours. With reporting, it becomes a no-brainer. It's one of those things on an IT budget that you need to have.

FOR HOW LONG HAVE I USED THE SOLUTION?

Probably five years.

Continued from previous page

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

We really haven't seen any issues on the stability side of it being cloud-based. We also have three virtual hosts that run in our environment. in the event that we lose one, there are two others. We have never seen any issues with the environment, which Cisco proactively monitors. They'll come back to us and indicate if there are any hardware performance issues and schedule appropriate restarts to appliances, if required. This happens occasionally.

Given a lot of people target hospitals, we tend to be attacked more than other corporations because there are health records, health information, financial information, and research information. Cisco Secure Email Cloud Gateway and some other products have definitely allowed us not to have the downtime that we may have had if our previous products and solutions were in place. As far as I'm aware, we haven't had any downtime since we put in Cisco Secure Email Cloud Gateway and Umbrella several years ago, which has been fantastic.

We have our security analyst who gets feeds out of Cisco Secure Email Cloud Gateway into our other products. We also get feeds into AMP for Endpoints, so we see what happens because we have our Cisco Secure Email Cloud Gateway integrated with AMP for Endpoints. That goes into our Threat Grid and Threat Response.

Our server team might get queries about messages that might have been quarantined or someone having trouble receiving external emails. That's usually where a domain might be rated above our parameters and gets blocked. With something like 3,000 mailboxes, we spend at most an hour a day checking on the Cisco Secure Email Cloud Gateway environment.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

Our environment is scalable, and we monitor that with Cisco. When we do our periodic Health Checks, we look at the performance of the appliances and how they're doing. They're handling the 10 to 12 million emails that we do receive through Cisco Secure Email Cloud Gateway a month. There are about 90 percent which are not even forwarded onto us. Therefore, it's handling the capacity that we have at the moment. At this stage, there's no need for any increase in our hardware.

It's an invisible service where every piece of email going in and out of the organization goes through CES.

We are doing more integrations with other security products, like Threat Grid, Threat Response, and AMP, along with SecureX. Getting the Cisco Secure Email Cloud Gateway feed into that and have one pane of glass to see the threats of the organization through both emails, firewalls, routers and VPN is fantastic.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

We have a team of resources at Cisco that we can call on, if we need things escalated. Having great customer-centered service and support is one of the reasons why going with Cisco has been such a fantastic decision for both organizations that I've been at.

Continued from previous page

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

Prior to using Cisco Secure Email Cloud Gateway and my being at the organization, they had a Qbot massive issue. I don't know a lot of the detail, but at the time, we had a lot of machines that had to run certain versions of software. Because of it being older software, legacy-type applications, they were more susceptible to issues. Qbot just went through the organization and took out a lot of that equipment/machines. Cisco actually came in and assisted to get rid of all the issues that we saw with Qbot, etc. It took several weeks spent by Cisco and other organizations trying to resolve our issues with Qbot to get things operational and back to normal. That was really the catalyst to get Cisco Email Secuity into the organization.

We were previously using McAfee for both their Endpoint Protection as well as for Email Servers. The difference was the volume of emails hitting our email servers. The servers had to deal with 10 million emails a month. Having to process those additional emails and pushing them onto users took a massive amount of infrastructure and resources at a server level. Whereas, at the moment, our servers are not having to deal with that because we have Cisco Secure Email Cloud Gateway right outside of our perimeter.

One of the reasons that we switched away from McAfee is that we moved to an enterprise agreement with Cisco. Under that, we get the Cisco Advanced Malware Protection (AMP) for Endpoints. Once we went down that path and install it, there was no point in having McAfee as well when the AMP for Endpoints already has some of the different engines. Plus, there was a duplication of costs and applications, such as the support costs as well as to maintain multiple antivirus and endpoint protection software.

At my previous organization, we were using the standard Office 365 controls and Email Gateway before we put in CES. The amount of email and spam that we got, even malicious emails, through Microsoft was horrendous. We ended up having four different massive outages because of getting some viruses in the organization and some of our file servers along with encrypted user hard drives. We had four instances of major outages where we were down for probably 24 hours each time, and that was only because we had the backups. We also had some other measures where as soon as we saw any change in the root directory (as that data encrypts our file shares), we'd automatically shut the services down. However, this was an inconvenience for the users. You would end up getting the initial malware, then also having to do remediation to get it back to normal. When you have potentially hundreds of staff who are offline for 24 hours, it's a very big cost to the organization when you don't have your systems up and running.

When the malware got through Office 365 on four different instances, that was directly attributable to the difference between Office 365 and CES. Our users still had to get their email through our on-prem server, but we did not let staff get their emails directly from the Microsoft 365 Server.

Once we put in CES, these issues disappeared altogether, and we were thankful that the volume of spam emails decreased considerably. Office 365 is a good second check to CES, but there's nothing that I've ever seen which has gotten through Cisco Secure Email Cloud Gateway that Office 365 has picked up.

HOW WAS THE INITIAL SETUP?

The initial setup is straightforward. Cisco does a very good job of onboarding customers and setting it up so it's very much ready to go based on some fairly standard settings from Cisco's point of view.

The deployment took only a few hours. Even at my previous organization, it was very quick. Once it was done, we changed our MX records to go to Cisco Secure Email Cloud Gateway instead of Office 365. From there, email went from Cisco Secure Email Cloud Gateway to Office 365. It was pretty simple. We had control of our DNS so it was very quick and easy for us to change the records and get our email flowing through Cisco Secure Email Cloud Gateway. We could see the benefits straightaway. We could see just how much volume was coming in, e.g., in my previous organization, we had something like a million emails per month, of which eight percent would be delivered to our end users.

In terms of switching from one solution to another, it's seamless for the user. They are not seeing the downtime because they're connected to the local Exchange Server. Therefore, they're not seeing the upstream components. There might be a slight delay in terms of the MX records globally, but that is, at worst, 24 hours. So, there might be some delayed emails, but that's probably the only thing. Once we had switched over, we received positive feedback saying, "Hey, what have you done? It's been fantastic. You've reduced the amount of spam messages we used to get."

WHAT ABOUT THE IMPLEMENTATION TEAM?

It was easy enough to do the implementation with Cisco and their support because we had adopted an enterprise agreement with them. Therefore, we had the support of Cisco implementing both Cisco Secure Email Cloud Gateway and Umbrella into our organization. They were very good at helping getting up and running.

There was one of my other staff who assisted me in setting up Cisco Secure Email Cloud Gateway with Cisco. It was relatively simple and easy.

Doing Health Checks with Cisco have been fantastic. Being able to do those every few months and going through what other options that we might want to lock down or change gives us an opportunity to ask them questions, see what we could be doing better, or what new measures/features have been deployed, furthering securing our organization. The Health Checks are an invaluable service that Cisco provides to CES.

WHAT WAS OUR ROI?

In my previous organization, avoiding four instances of CryptoLocker within an estimated six month period is approximately $600,000 in lost time and effort. Our five year cost was about a million dollars, and the four outages that we had equated to 65 percent of that five year cost. It ended up being a very simple decision to go with the security enterprise agreement with Cisco, which included Cisco Secure Email Cloud Gateway and all their other cybersecurity products.

WHICH OTHER SOLUTIONS DID I EVALUATE?

Office 365’s native security controls to protect your organization compared to this solution are terrible. With Office 365, unless you actually pay for the advanced options with email security, they're actually quite useless. You've no control over the standard offering.

My previous organization did look at the Symantec Cloud solution. At both organizations, it didn't really make any economical sense to look at other vendors. If we had an enterprise agreement with Cisco, then you get the support from Cisco that's second to none, where you get somebody on the phone straightaway to work through your issue until it's resolved. My previous dealings with Symantec and McAfee are that they're not as customer-focused in terms of their support. Cisco has been.

Continued from previous page

WHAT OTHER ADVICE DO I HAVE?

Don't have an organization that doesn't have this sort of protection in place. If I was to be in another organization, and they didn't have this sort of protection, I would definitely be advocating that they get something in very quickly.

Don't hesitate: The benefits are there. It can be seen as being a large cost. However, if you've ever had any instances where you've been affected by malware or CryptoLocker, there are a number of things that you should be doing as an organization: perimeter email security, DNS protection, and removing USB access on devices. These are probably the top three things that I'd be advising people to do.

We don't use Office 365 (which is now Microsoft 365) at the moment, but it's something that we are looking at. Being a large hospital, we're looking at aligning ourselves with our Department of Health so Office 365 is something that we will be using that to a certain extent. However, we would still be using Cisco Secure Email Cloud Gateway if we did move to that. We would deliver emails from Cisco Secure Email Cloud Gateway into Office 365. That way, we would still have the security. That's how I've set it up at previous organizations: Going from Cisco Secure Email Cloud Gateway into Office 365, delivering to our on-prem Exchange Server, and then onto our users.

The amount of traffic that it stops is massive. I would rate it a 10 out of 10.

WHICH DEPLOYMENT MODEL ARE YOU USING FOR THIS SOLUTION?

On-premises

IF PUBLIC CLOUD, PRIVATE CLOUD, OR HYBRID CLOUD, WHICH CLOUD PROVIDER DO YOU USE?

Other

Answers from the Community

What do you like most about Cisco Email Security?

Hi Everyone, What do you like most about Cisco Email Security? Thanks for sharing your thoughts with the community!

[See all 15 answers >>]

Answers from the Community

What needs improvement with Cisco Email Security?

Please share with the community what you think needs improvement with Cisco Email Security. What are its weaknesses? What would you like to see changed in a future version?

See all 15 answers >>

Answers from the Community

What is your primary use case for Cisco Email Security?

How do you or your organization use this solution? Please share with us so that your peers can learn from your experiences. Thank you!

See all 15 answers >>

Top Email Security Vendors

Over professionals have used IT Central Station research. Here are the top vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key

● **Views**	● **Comparisons**	● **Reviews**	● **Words/Review**	● **Average Rating**
Number of views	Number of times compared to another product	Total number of reviews on IT Central Station	Average words per review on IT Central Station	Average rating based on reviews

Bar length

The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows:

For each of **Reviews**, **Views**, and **Comparisons**, the product with the highest count in each area gets a maximum 18 points.
Every other product gets assigned points based on its total in proportion to the #1 product in that area.
For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's points for reviews would be 18 * 80% = 14.4.

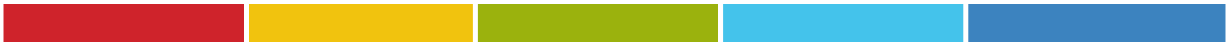
Both **Rating** and **Words/Review** are awarded on a fixed linear scale.
For Rating, the maximum score is 28 points awarded linearly between 6-10 (e.g. 6 or below=0 points; 7.5=10.5 points; 9.0=21 points; 10=28 points).

For Words/Review, the maximum score is 18 points awarded linearly between 0-900 words (e.g. 600 words = 12 points; 750 words = 15 points; 900 or more words = 18 points).
If a product has fewer than ten reviews, the point contribution for Rating and Words/Review is reduced:
1/3 reduction in points for products with 5-9 reviews, two-thirds reduction for products with fewer than five reviews.

Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

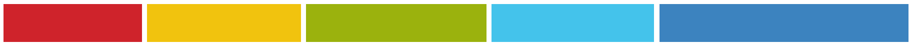
All products with 50+ points are designated as a Leader in their category.

1 Cisco Secure Email



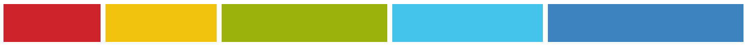
9,590 views **5,927** comparisons **16** reviews **1,121** words/review **8.8** average rating

2 Fortinet FortiMail



5,519 views **4,082** comparisons **12** reviews **609** words/review **8.7** average rating

3 Barracuda Email Security Gateway



3,871 views **2,934** comparisons **11** reviews **564** words/review **8.1** average rating

4 Proofpoint Email Protection

8,127 views 6,367 comparisons 4 reviews 311 words/review 9.0 average rating

5 Fortinet FortiMail Cloud

1,636 views 940 comparisons 10 reviews 610 words/review 8.2 average rating

6 Forcepoint Email Security

2,117 views 1,380 comparisons 5 reviews 475 words/review 7.4 average rating

7 Symantec Messaging Gateway

2,045 views 1,645 comparisons 4 reviews 594 words/review 8.3 average rating

8 Agari

3,070 views 1,830 comparisons 1 reviews 338 words/review 9.0 average rating

9 FireEye Email Security

1,646 views 1,410 comparisons 1 reviews 260 words/review 8.0 average rating

10 Check Point Anti-Spam and Email Security Software Blade

551 views 371 comparisons 2 reviews 765 words/review 8.0 average rating

Top 5 Solutions by Ranking Factor

● Views

		VIEWS
1	Cisco Secure Email	9,590
2	Proofpoint Email Protection	8,127
3	Fortinet FortiMail	5,519
4	Barracuda Email Security Gateway	3,871
5	Agari	3,070

● Reviews

		REVIEWS
1	Cisco Secure Email	16
2	Fortinet FortiMail	12
3	Barracuda Email Security Gateway	11
4	Fortinet FortiMail Cloud	10
5	Forcepoint Email Security	5

● Words / Review

		WORDS / REVIEW
1	Cisco Cloud Mailbox Defense	1,505
2	Cisco Secure Email	1,121
3	Check Point Anti-Spam and Email Security Software Blade	765
4	Area 1 Horizon	637
5	Fortinet FortiMail Cloud	610

About this report

This report is comprised of a list of enterprise level vendors. We have also included several real user reviews posted on ITCentralStation.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About IT Central Station

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created IT Central Station to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

IT Central Station helps tech professionals by providing:

- A list of enterprise level vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use IT Central Station to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

IT Central Station
244 5th Avenue, Suite R-230 • New York, NY 10001
www.ITCentralStation.com
reports@ITCentralStation.com
+1 646.328.1944