Migration from On-Prem Email to Symantec Email Security.cloud

Matthew R Lorenzen

Western Governors University

**Table of Contents**

[Summary 3](#_Toc441471473)

[Review of Other Work 3](#_Toc441471474)

[Changes to the Project Environment 3](#_Toc441471475)

[Methodology 3](#_Toc441471476)

[Project Goals and Objectives 3](#_Toc441471477)

[Project Timeline 4](#_Toc441471478)

[Unanticipated Requirements 4](#_Toc441471479)

[Conclusions 4](#_Toc441471480)

[Project Deliverables 4](#_Toc441471481)

[References 6](#_Toc441471482)

[Appendix A: 7](#_Toc441471483)

[Appendix B: 8](#_Toc441471484)

[Appendix C: 9](#_Toc441471485)

[Appendix D: 10](#_Toc441471486)

# Summary

Rogue IT has successfully completed the migration of the email infrastructure to the Symantec Email Security.cloud platform. During the migration process a full analysis of emails considered spam that had previously made it through prior filtering was performed. This analysis both categorized and risk rated each email to provide a better understanding of the immediate attack surface. This task was performed to create a base-line of email flow in order to better understand and quantify the improvements to Rogue IT security provided by the Symantec systems. Additionally, prior to beginning the deployment of the new service a review of current capacity was performed to determine a normalized traffic flow in hopes of reducing the current on-premise architecture.

The deployment of the Symantec Email Security.cloud services were successfully deployed to the production environment in under four hours without interruption. This goal was set by Rogue IT leadership to ensure zero downtime for the email infrastructure in order to minimize impact to the daily run-the-business activities. During the migration of the DNS records from Rogue IT to Symantec no email queuing was observed.

Post deployment Rogue IT has observed a 35% decrease in over-all spam getting through to the network. The insight provided by the Symantec portal dashboards has been an easy adaptation for the Rogue IT staff to monitor. The original goal when deploying the Symantec service was to reduces spam rates by 20%, the dashboards are providing real-time data reflecting the volume of spam blocked on the network. The Rogue IT teams continue to perform analysis and turning to ensure system stability. This process will continue, however, time spent tuning is already proving to be less than required by the previous system.

# Review of Other Work

In this section, provide an expanded review of the Review of Other Work section in task 2, including three additional third-party artifacts on the topic that supported the development of the project, and explain how the artifacts supported the implementation.

# Changes to the Project Environment

Rogue IT made minimal changes to the physical on-premise network during this migration; however, it was able to reduce the architecture by removing two of the Dell PowerEdge R250 servers from the rack. This reduction was justified as Rogue IT no longer needs the processing power after the migration to the Symantec Email Security.cloud service. The Dell PowerEdge servers will be wiped and reconfigured to host virtual machines for testing in another department.

The current environment is comprised of the Symantec Email Security.cloud platform with an entry point into Rogue IT via a BigIP i10000 series load balancer with a configured VIP of the DNS records for “rogue.it” that serves traffic to a pair of Palo Alto Networks PA-7000 series firewalls via DNS Round Robin. The Palo Alto devices are running in an active-active configuration and handle deep packet inspection. These firewalls serve the traffic to two clustered high-availability Dell PowerEdge R250 Rack Servers with the Intel Xeon E-2334 processors with 32GB of RAM running Microsoft Windows Server 2019.

# Methodology

The methodology used to on-board, configure, and deploy the Symantec Email Security.cloud platform will be the ADDIE method. Rogue IT has chosen to utilize this method during the deployment process for a variety of reasons including; the teams are already familiar with the ADDIE model, the ADDIE model provides a simple method to capture milestones during the deployment, the ability to step through the process systematically, while preserving the ability to roll back at any given time. This process will help to ensure email uptime during the deployment, and minimize impact to end users and clients, preventing lost emails in the process. During the initial discussions there was substantial debate between the Agile method and the ADDIE, however, the teams for Rogue IT decided that while the Agile method would in fact be appropriate, Agile would take a back seat due to the complexity and overhead of the project.

The five phases of the ADDIE model are: Analysis, Design, Development, Implementation, and Evaluation. The individual phases for the project are detailed below:

Analysis – Rogue IT will perform a full analysis of all spam that has made it past the filtering for the current on-premise Exchange environment. These emails will be categorized and rated on severity. Additionally, traffic for the current Exchange environment will be reviewed to determine if the need for four email servers will remain justifiable post completion of the Symantec Email Security.cloud deployment. During this phase all security policies for the current Exchange environment will be analyzed for efficacy.

Design – While the design phase for the Symantec Email Security.cloud deployment is minimal; the Rogue IT security staff will need to determine and design the infrastructure to ensure capacity is sufficient post the deployment of the Symantec service. This design phase will re-work any details provided during the analysis process.

Development – Rogue IT security engineers and IT staff will develop the steps to work toward implementation of the security service. During this phase the “Welcome Email” from Symantec will be reviewed and configuration on the Email Security.cloud service will be prepared. The teams will gather all information needed to migrate the user database from the Active Directory environment, ensure they have a clear outline of the anti-spam policies, link following, and quarantine guidelines.

Implementation – Rogue IT staff will deploy all configuration changes and other action items determined during the analysis, design, and development phases. The teams will provide a seven-day notice to all employees prior to implementation as per the standard maintenance window notification determined by the Change Approval Board. The teams will work to configure the platform and ensure all appropriate DNS records have been created and waiting for deployment. The Rogue IT user database will be uploaded through the admin panel with the use of the tools provided by Symantec. Teams will enable and configure the security measures determined during the analysis phase, including Skeptic and Heuristic analysis. During the phase the DNS records for SPF, DMARC, and DKIM will be updated for Rogue IT, along with the change to the MX records for Rogue IT. This will allow for email to begin to flow through the Symantec Email Security services.

Evaluation – Upon completion of deployment, a full analysis and comparison of the Rogue IT email flows will be performed. This evaluation will include an initial review including testing of both internal and external email flow to ensure there is no data loss. Additionally, teams will perform tests with sample emails provided by Eicar and Symantec to ensure protections are working and assist in providing feedback for additional configuration adjustments.

# Project Goals and Objectives

**Goals, Objectives, and Deliverables Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Goal | Supporting objectives | Deliverables enabling the project objectives | Met/Unmet |
| 1 | Reduce the volume of spam on the Rogue IT network while removing additional overhead. | 1.a. Unwanted emails categorized and rated by severity. | 1.a.i. Categorization of existing spam on the network. Average spam seen, daily, weekly, monthly, yearly. This will allow us to determine the total decrease in spam on the network post deployment. | Met |
| 1.a.ii. Provide a risk rating based upon the categories in 1.a.i and aid in determining the reduction of risk to the overall footprint for Rogue IT. Risk rated 1-5 to determine the likelihood of successful attack and potential risk associated. Providing data to for Rogue IT to prioritize during routine maintenance. | Met |
| 1.b. Determine capacity for new Exchange environment | 1.b.i. Projected capacity needed post implementation. This will assist in determining if Rogue IT can reduce the current infrastructure. | Met |
| 1.b.ii. Assist in providing insight into the potential downsizing of the on-premise Exchange environment. As the heavy lift of processing is handed off to the Symantec infrastructure. | Met |
| 2 | Successful deployment of Symantec Email Security.cloud without interruption to email flow. | 2.a. Successful cutover from mx.rogue.it to Symantec hosted MX records. | 2.a.i. Successfully migrate live email flows from Rogue IT to Symantec Email Security.cloud without interruption or incident. | Met |
| 2.a.ii. Zero downtime, network infrastructure migration without interruptions to business flows, seamless cut-overs without email queueing. | Met |
| 2.b. Migration scheduled for 4 hours | 2.b.i. A successful migration without incident in under 4 hours, this will be seen as a successful migration. | Met |
| 3 | Rogue IT anticipates a 20% decrease in spam getting through to the network. | 3.a. Post implementation a noticeable reduction in spam making it through filtering on the Rogue IT network. | 3.a.i. An assessment of spam on the email quarantine within Symantec Email Security.cloud, categorized, and determined false positive or true positive. | Met |
| 3.a.ii. 20% reduction on emails determined to be spam on a given sample email inbox. This will be an analysis taken from live sample accounts collecting a mirrored production email account. | Met |
| 3.b. 20% or greater overall increase in spam actively blocked by the Symantec Email Security.cloud platform. | 3.b.i. Dashboards on the Symantec Email Security.cloud platform reflects 20% increase of spam blocked when compared to the current dashboard on the Microsoft Exchange environment from the week prior. | Met |
| 3.b.ii. Week over week monitoring comparing the new security platform to the current exchange environment for the week prior. | Met |

Rogue IT’s migration to Symantec Email Security.cloud primary goal was to reduce the volume of spam that was not being captured by the previous infrastructure and to reduce any remaining on-premise overhead. Due the complexity and importance of the email workflows, this was achieved through a successful deployment of a new service to the production environment without incident. The implementation phase of the project was given a four-hour window to make the changes. This target time frame provided a minimal window for impact and aligned with standard DNS record time-to-live. The Symantec Email Security.cloud systems are help Rogue IT more efficiently manage the email workflows while providing a data driven reduction in spam on the network. This is captured via real-time monitoring via the Symantec Email Security.cloud portal.

* Objective 1.a. Unwanted emails were categorized and rated by severity. The first step of the project was to understand the types of emails were making it through the previous Exchange environment. This was crucial to being able to understand the reduction in impact with the email security services provided by Symantec.
* Objective 1.b. Determined capacity for the Exchange environment by estimating the bandwidth trade off with the increase processing capabilities provided by the Symantec infrastructure. This information was used to determine that Rogue IT can reduce the on-premise hardware configurations. Further reduction of the over-all threat landscapes for Rogue IT.
* Objective 2.a. Successfully cutover from mx.rogue.it to Symantec hosted MX records. This goal was set forth to express the importance of an incident free implementation. Rogue IT handles a large portion of their daily operations through these email work flows. Given that inbound email can be delivered at any given point in time during the day, zero down time becomes a warranted and targetable goal.
* Objective 2.b. Migration scheduled for 4 hours. This goal was developed to align with the time to live on the Rogue IT MX records and to reduce the overall impact window during the implementation. Adherence to this time frame was vital and check points for implantation were set for go/no-go and rollback to prevent down time.
* Objective 3.a. Post implementation a noticeable reduction in spam making it through filtering on the Rogue IT network. A measurable metric based on real-time data is assisting in ensuring a return on investment of the Symantec Email Security.cloud services. This was designed to be a data-driven metric that is produced on a week-over-week and month-over-month time frames.
* Objective 3.b. 20% or greater overall increase in spam actively blocked by the Symantec Email Security.cloud platform. The second targetable metric Rogue IT is capturing post implementation is being achieved through the Symantec portal. The portal provides real-time metrics for volume of emails blocked as spam and provides additional metadata including spam signatures to further investigate and improve detection.

# Project Timeline

In this section, compare the projected and actual timelines of the milestones or deliverables of the project and explain why the differences occurred. Explain the reasons for each deviation of the actual time frame from the estimated time frame.

Note: All timeline dates MUST be in the past as this document is an after-action report that should reflect a project that is completed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Milestone or deliverable | Duration  (hours or days) | Projected start date | Anticipated end date | Anticipated end date |
| Unwanted emails categorized and rated by severity | 2 days | 01/23/2023 | 01/25/2023 | 01/25/2023 |
| Determine capacity for new Exchange environment by estimated bandwidth trade off with the increase processing capabilities provided by the Symantec infrastructure. | 1 day | 01/23/2023 | 01/24/2023 | 01/24/2023 |
| Successful cutover from mx.rogue.it to Symantec hosted MX records. | 4 hours | 01/26/2023 | 01/26/2023 | 01/26/2023 |
| Post implementation a noticeable reduction in spam making it through filtering on the Rogue IT network. | 1 week | 01/26/2023 | 02/02/2023 | 02/02/2023 |
| 20% or greater overall increase in spam actively blocked by the Symantec Email Security.cloud platform. | 1 week | 01/26/2023 | 02/02/2023 | 02/02/2023 |

# Unanticipated Requirements

During the migration to the Symantec Email Security.cloud infrastructure the teams failed to notify customers of the maintenance window. While this had no direct impact on the project, the communication was vital to the transparency at Rogue IT. This failure to communicate the change generated contacts to the IT help desk upon completion of the migration, with reports of “strange links” being received in emails. Upon investigation it was determined that the “strange links” were in-fact the link re-writing functionality with in the Symantec Email Security.cloud services. A communication for all Rogue IT employees was crafted and distributed via multiple channels to quickly update the Rogue IT staff.

# Conclusions

The Rogue IT migration to the Symantec Email Security.cloud systems will decrease the volume of spam on the Rogue IT network and provide additional depth-in-defense to the threat landscape. The Rogue IT staff will experience an overall decrease in time spent tuning policies for anti-spam on the Microsoft Exchange environment, instead being able to place trust in the anti-spam, anti-malware, and Skeptic and Heuristic architecture of the Symantec Email Security.cloud systems. This will allow for the Rogue IT staff to focus on further hardening the network and supporting its customers base.

Rogue IT anticipates seeing an overall 20% or more reduction in spam making it through the filtering and into end user inboxes. Additionally, the dashboards provided with the Symantec portal will provide real-time insight into email flows, including metrics such as:

* Volume of spam per hour
* Volume of email per hour
* Email quarantine on a per user level
* Week-over-week and year-over-year metrics

The long-term benefits of migrating to the Symantec services are provided scalability and increase capacity on the fly without purchase of new hardware. The protection of an industry leading security company.

# Project Deliverables

Appendix A illustrates the logical network diagram post migration to the Symantec Email Security.cloud infrastructure. The diagram includes the architecture for the remaining Rogue IT infrastructure including the BigIP i10000 load-balancer, the Palo Alto firewalls, and the two remaining Dell PowerEdge R250 Rack Servers.

# References

# Appendix A

# Title of Appendix

Put any supporting material in these appendices. Add additional or delete superfluous appendices as needed.

# Appendix B

# Title of Appendix

Put any supporting material in these appendices. Add additional or delete superfluous appendices as needed.

# Appendix C

# Title of Appendix

Put any supporting material in these appendices. Add additional or delete superfluous appendices as needed.

# Appendix D

# Title of Appendix

Put any supporting material in these appendices. Add additional or delete superfluous appendices as needed.