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

This section describes and details changes to the project environment made by the implementation of the project, after its completion. Analyze the systems and describe the status of the project environment after the implementation of the project.

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 BigIP i10000 series load-balancer continues to support the VIP as the configured entry point for the email workflow from Symantec.

# Methodology

This section describes and details the specific methodology. The methodology is the process that the project filled by being implemented. Explain how a standard methodology was applied for the implementation of the project.

# Project Goals and Objectives

In this section, provide a detailed explanation on how some goals and objectives were met and why some goals and objectives for the project were not accomplished. Identify the objectives that were met and explain how they were met, and then explain the reasons why some objectives were not accomplished.

**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 |

# 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

In this section, describe the requirements or components that were not anticipated at project initiation but emerged during implementation. Describe the problems encountered and the unanticipated requirements, and then explain how they were resolved or why they were not solved.

# Conclusions

In this section, provide an explanation of the actual results and potential effects of the completed project. Describe the actual project accomplishments and discuss the immediately observable effects and potential future impacts of the completed project on the project environment. Explain why the project is or is not considered successful using the evaluation framework from the Outcome section in the project proposal.

# Project Deliverables

In the Project Deliverables section, explain and detail the project key deliverables. The actual project development will be documented by the key deliverables. The project includes some sort of formal report. The deliverables should provide a detailed logical explanation of what the project provided to substantiate the work and completion of such. Describe the artifacts being used to show evidence of the project’s completion and use the appendices to include the actual artifacts. Actual project artifacts may include code samples or screen shots; flowcharts, UML, or other process diagrams; charts, tables, and graphs; network diagrams (before and after); training materials; and/or the technical IT product itself.

# References

List all the outside sources that the narrative refers to in-text. For in-text and reference list citations, please refer to the web link in or visit the WGU Writing Center.

Smyth, A. M., Parker, A. L., & Pease, D. L. (2002). A study of enjoyment of peas. Journal of Abnormal Eating, 8(3), 120-125. Retrieved from

http://www.articlehomepage.com/full/url/

Bernstein, M. (2002). 10 tips on writing the living Web. A List Apart: For People Who Make Websites, 149. Retrieved from http://www.alistapart.com/articles/writeliving

Bell, T., & Phillips, T. (2008, May 6). A solar flare. Science @ NASA Podcast. Podcast retrieved from http://science.nasa.gov/podcast.htm

OLPC Peru/Arahuay. (n.d.). Retrieved April 29, 2011 from the OLPC Wiki: http://wiki.laptop. org/go/OLPC\_Peru/Arahuay

Plath, S. (2000). The unabridged journals. K. V. Kukil (Ed.). New York, NY: Anchor.

# 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.