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

Matthew R Lorenzen

Western Governors University

**Table of Contents**

[Proposal Overview 3](#_Toc124548118)

[Problem Summary 3](#_Toc124548119)

[IT Solution 3](#_Toc124548120)

[Implementation Plan 3](#_Toc124548121)

[Review of Other Work 6](#_Toc124548122)

[Project Rationale 8](#_Toc124548123)

[Current Project Environment 9](#_Toc124548124)

[Methodology 10](#_Toc124548125)

[Project Goals, Objectives, and Deliverables 12](#_Toc124548126)

[Goals, Objectives, and Deliverables Table 12](#_Toc124548127)

[Goals, Objectives, and Deliverables Descriptions 13](#_Toc124548128)

[Project Timeline with Milestones 15](#_Toc124548129)

[Outcome 16](#_Toc124548130)

[References 18](#_Toc124548131)

# Proposal Overview

## Problem Summary

Currently Rogue IT manages an on-premise MS Exchange environment for their email purposes. Due to the increases seen in phishing attempts and multiple events including business email compromise it has been recommended that Rogue IT cease maintaining the existing on-prem environment security controls, instead migrating the security policies of the current email infrastructure to Symantec Email Security.cloud.

## IT Solution

The solution will be to standup Symantec Email Security.cloud as a service, at which point the existing on-prem security measures will depreciated. The Symantec Email Security.cloud service is well known to the information security world. The documentation for the product is robust, additionally, there forums are active with Enterprise corporations adding to the “best practices” for configuration. Symantec Email Security.cloud is AWS hosted by region, this provides additional high availability protections, as the service is geo-balanced globally. This will provide less overall maintenance, while increasing the security posture for Rogue IT’s email infrastructure.

## Implementation Plan

The first phase to implement Symantec Email Security.cloud will include reviewing the “Welcome email” from Symantec. The email contains general information for account setup and basic configuration methods. The email further provides details into the steps taken to configure the security service, add users, and configure security policies. The email provides a check list of steps to take to onboard the service and ensure the configuration is correct. This will prevent delays while setting up the service.

The next phase will be to log into the Symantec Email Security portal. Using the information provided in the “Welcome Email”, an administrator account will be created. This account is created to avoid any type of “lockout” in the event of an on-premise Active Directory or LDAP account failure.

The next step will be to configure the security service to synchronize the user database. Utilization of the Symantec Schemus tool provides a near real-time sync of Rogue IT’s users. During this configuration step a new user account will be created on the Symantec Email Security.cloud portal for Rogue IT. This account will require four specific roles to allow for the synchronization tool to perform correctly. The required roles for the account are as follows:

* Mail Platform – Edit Configuration
* LDAP User Groups – Edit Configuration
* Mail Platform – View Configuration
* LDAP User Groups – View Configuration

It is important here to note that this account should have a password that never expires, nor should the account be used to sign into the Symantec Email Security.cloud portal.

The next step will be to determine where the Schemus tool will reside on the network. It is recommended by Symantec to run the Schemus tool locally on an Active Directory server. Symantec offers two versions of the Schemus tool, one bundled with JRE and one without. Since the Rogue IT Active Directory service is already running a JRE later than 1.5 the either of the downloads will suffice. This tool will be configured as a running job on the Active Directory server to allow for synchronization, as a recommended setting it will be configured to run twice daily. This is done to ensure the user-base is updated in a timely fashion when on-boarding new employees, or while off-boarding employees upon departure. During the configuration of the tool the domain for Rogue IT will be provided along with the organization unit or hierarchy for the domain.

The next step will be to perform the required address registration. This step is performed to register all current known email addresses for Rogue IT. Address Registration is a security measure implemented by the service to prevent email address spoofing and aids in preventing dictionary attacks on the inbound route while also preventing unwanted emails from reaching the Rogue IT infrastructure.

The next step will be to configure Anti-Virus and Anti-Spam settings through the Symantec Email Security.cloud portal. During this step all current rules from the current on-premise Exchange environment will be evaluated for efficiency prior to migration to the Symantec Email Security.cloud environment. This will allow for removal of any duplicate in ineffective policies to be removed. Additionally, DMARC, SPF, and DKIM will be configured for the Rogue IT domain. These additional protections will initially be configured with a “soft failure” which will allow for logging however not aggressively block potentially valid emails from entering the Rogue IT domain.

The final phase will be to cut the email traffic over by changing the MX records for the Rogue IT infrastructure to point to the Symantec Email Security.cloud environment. During the process email a “send connector” will be created on the on-premise Exchange environment. This connector will provide the connectivity for outbound email from the Rogue IT domain. See Appendix A for the diagram and instructions for configuration. The MX record changes will take up to four hours of additional time to propagate the Symantec Email Security.cloud infrastructure. Upon completion of the MX record changes email will delivered via the new security system.

# Review of Other Work

As the threat to business security compromise through email phishing attacks grows, the importance for trusted email security increases. In 2014, 1 in 244 emails was a phishing email. (Symantec Internet Security Threat Report, n.d.) However, the threat to the company is not only malicious emails, but also includes data loss. The Symantec Email Security platform tightly integrates with the Symantec Data Loss Prevention software to prevent outbound emails from containing confidential data, including PCI and PII. This further adds to the security posture for Rogue IT and can quickly prevent intentional and unintentional disclosure of personal information. Not only does the service prevent this data type from being sent outbound from the network but can be quickly leveraged as an alerting system in the event of an insider threat.

The built in URL protection that comes with the out of the box configuration with Symantec Email Security Cloud will help protect Rogue IT further by preventing malicious URL redirects. The Internet Security Threat Report (ISTR) states cybercriminals are using increasingly sophisticated methods to disguise malicious URL links embedded in email messages. This includes randomly redirecting links to a sequence of different destinations around the world and adding programmed time delays. These new techniques are highly effective at disguising malicious links and fooling traditional link scanning tools. (Symantec Internet Security Threat Report, n.d.)

Further supporting the need for a dedicated email security client, the ISTR discusses the built-in functionality from Microsoft Office and Office 365, Google Apps, and other cloud-based email solutions simply aren’t enough. For example, link scanning technologies for Office 365 and some other cloud-based email security companies are limited to “blacklists” of known bad URLs. (Symantec Internet Security Threat Report, n.d.)

A review of Symantec Email Security.cloud Skeptic Whitepaper, provides a non-biased opinion of the email security service and outlines the technical approach used to deploy the service. All of the papers reviewed mention corporations migrating their security for email to a hosted cloud solution such as provided by Symantec, Cisco, and Proofpoint, however this whitepaper suggests it as the opening line, stressing the importance for solid email security as a foundation to a secure network. With the understanding that a vast number of breaches occur due to target phishing emails, this becomes an ever-growing demand. With the increase in demand the increase need for 100 percent uptime becomes crucial. Symantec provides this SLA to its customers underpinned with significant service credits in the event of downtime. The service credits provide the confidence to back the ability to deliver a robust email security service. (Tech Republic, n.d.)

The 100% uptime combine with a global infrastructure located in secure server storage facilities provides another layer of security for data traversing the web for Rogue IT. These facilities are configured geographically to provide support and help guarantee uptime, placing them in key locations within the US and Europe. This further provides a benefit to Rogue IT as it reduces the need for hands-on failovers or re-routes for MX records in the event of an outage. The globally distributed configuration can assist in reducing further overhead for Rogue IT.

Further research provides insight into the longevity of Symantec Email Security.cloud, providing a proven long running background of the service. As covered in “The Evolution of Email Security: Symantec Brightmail Integrated Email Security Appliance.” Brightmail being the original technology for the service known as “Message Labs”, which was the name of the Symantec Email Security.cloud service. This whitepaper provides depth into the evolution of the service including the migration of the service from on-premise to cloud hosted. The original device named the Symantec Mail Security 8100 series provided the ground work for the basis of today’s modern cloud service, including traffic shaping to limit an attacker’s ability to spam the network, to advance skeptic and heuristics to further proactively mitigate against new spam that doesn’t have a dedicate spam signature. This provides the assurance that choosing Symantec Email Security.cloud will provide a service Rogue IT long into the future, as Symantec has a proven track record for adapting to new technologies. (Yumpu.com, n.d.)

A review of further work provides confirmation that Symantec takes email security seriously, and has long recognized that email is one of the most important threat vectors. (*Confidently Secure Your Email with Symantec*, n.d.) Symantec as a company was recently purchased by Broadcom. The writer Sunil Choudrie expresses an in-depth understanding of email security as a foundation to a protected infrastructure. Further assuring Rogue IT that choosing to migrate the email infrastructure security to Symantec is the correct decision.

# Project Rationale

While Rogue IT currently manages an on-premise MS Exchange environment for their email purposes. An ever-growing volume seen in phishing attempts and multiple events including business email compromise it has been recommended that Rogue IT cease maintaining the existing on-prem environment security controls, instead migrating the security policies of the current email infrastructure to Symantec Email Security.cloud. On a daily average there are roughly 283 million spam emails sent the need for Rogue IT to migrate to a dedicated, cloud-based security service is increasing. (Statista, 2022)

The recent business email compromises experienced by Rogue IT are further indication that the current on-premise solution is no longer sustainable as a security measure. By migrating the email traffic to the Symantec Email Security.cloud platform Rogue IT is creating layers of depth the security for the email infrastructure. This added defense in layers will not only act to prevent real time attacks against the email environment but also act as a deterrent.

# Current Project Environment

The current environment is comprised of a BigIP i10000 series load balancer with a configured VIP of the DNS MX records for “mx.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 four clustered high-availability Dell PowerEdge R250 Rack Servers with the Intel Xeon E-2334 processors with 32GB of RAM running Microsoft Windows Server 2019.

The BigIP i10000 has all recent security patches and is patched every third Thursday of the month to ensure minimal downtime. The BigIP device is also configured with an SSL certificate for secure connectivity. The Palo Alto firewalls are patches on the same frequency as the BigIP load balancer. The Palo Alto firewalls are considered Next Generation Firewalls (NGFW), these devices provide layers of security such as machine learning (ML) for traffic shaping, behavioral analysis to detect devices and recommend security policies. (BasuMallick, 2022)

The Dell PowerEdge R250’s host the Microsoft Exchange environment for Rogue IT. The environment has been configured as best possible to prevent unwanted email traffic such as spam, newsletters, and phishing attempts, however, recent the Rogue IT Exchange environment has been subject to a variety of attacks. While this environment has performed well for Rogue IT, it has become increasingly difficult to maintain. Due the complexity of attacks the Exchange environment has experienced an increase in downtime and an up-tick in phishing attacks hitting end user email inboxes. The teams at Rogue IT are spending more and more time tuning the environment or searching for better methods to reduce the attack surface. Ultimately, it has been agreed that migrating the primary security load to Symantec Email Security.cloud is the best solution. Providing depth in defense, a single pane of glass view for blocked spam, phishing, and various other unwanted email types, along with quarantine capabilities in the event a false positive is captured.

# 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, Objectives, and Deliverables

## Goals, Objectives, and Deliverables Table

|  |  |  |  |
| --- | --- | --- | --- |
|  | Goal | Supporting objectives | Deliverables enabling the project objectives |
| 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. |
| 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. |
|  |
| 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. |
| 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. |
|  |
|  | … |
| … |
|  |
| 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. |
| 2.a.ii. Zero downtime, network infrastructure migration without interruptions to business flows, seamless cut-overs without email queueing. |
|  |
| 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. |
|  |
|  |
|  |  |
|  |
|  |
| 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. |
| 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. |
|  |
| 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. |
| 3.b.ii. Week over week monitoring comparing the new security platform to the current exchange environment for the week prior. |
|  |
| … |  |
|  |
|  |

## Goals, Objectives, and Deliverables Descriptions

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

* Objective 1.a. Unwanted emails categorized and rated by severity. The first step of the project is to understand what types of emails are making it through the current Exchange environment. This is crucial to being able to understand the reduction in impact with the email security the Symantec systems.
* Objective 1.b. Determine capacity for new Exchange environment by estimated bandwidth trade off with the increase processing capabilities provided by the Symantec infrastructure. This information will be used to determine if Rogue IT can reduce the on-premise hardware configurations. Further reducing the over-all threat landscapes for Rogue IT.
* Objective 2.a. Successful cutover from mx.rogue.it to Symantec hosted MX records. This goal is 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 the this time frame is vital, check points for implantation have been 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 will assist in ensuring a return on investment of the Symantec Email Security.cloud services. This is designed to be a data-driven metric that can be produced on a week-over-week or month-over-month time frame.
* 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 will capture post implementation will be 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 with Milestones

|  |  |  |  |
| --- | --- | --- | --- |
| Milestone or deliverable | Duration  (hours or days) | Projected start date | Anticipated end date |
| Unwanted emails categorized and rated by severity | 2 days | 01/23/2023 | 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 |
| Successful cutover from mx.rogue.it to Symantec hosted MX records. | 4 hours | 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 |
| 20% or greater overall increase in spam actively blocked by the Symantec Email Security.cloud platform. | 1 week | 01/26/2023 | 02/02/2023 |

# Outcome

In this section, describe the anticipated project outcomes and explain how the success of the project will be measured once completed. Explain the expected project outcomes and describe the evaluation framework to be used once the project is completed to assess the project’s success and effectiveness.

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.

# References

Symantec Internet Security Threat Report. (n.d.). *Finding Email Security in the Cloud*. Media Zones. <https://media.zones.com/images/pdf/symantec-whitepaper-finding-email-security-in-the-cloud.pdf>

*Confidently Secure Your Email With Symantec*. (n.d.). Symantec Enterprise Blogs. <https://symantec-enterprise-blogs.security.com/blogs/product-insights/confidently-secure-your-email-symantec>

Yumpu.com. (n.d.). *WHITE PAPER The Evolution of Email Security: Symantec . . .* yumpu.com. <https://www.yumpu.com/en/document/read/35927739/white-paper-the-evolution-of-email-security-symantec->

Tech Republic. (n.d.). *SymantecTM Email Security.cloud - SkepticTM Whitepaper*. Tech Republic. <https://lg-static.techrepublic.com/direct/whitepapers/b-symc-email-security-cloud-technical-overview-WP.en-us.pdf>

Statista. (2022, April 28). *Daily spam volume worldwide 2020-2021*. <https://www.statista.com/statistics/1270424/daily-spam-volume-global/>

BasuMallick, C. (2022, June 10). *Top 10 Firewall Hardware Devices in 2022*. <https://www.spiceworks.com/it-security/network-security/articles/top-10-firewall-hardware-devices/>