National College of Ireland

Migrating an Email Filtering Solution from on Premise to Cloud

MSc Internship Project
MSc Cyber Security

Gearóid Kelly
Student ID: X20197365

School of Computing
National College of Ireland

Supervisor: Mark Monaghan
Industry Supervisor: Declan Byrne

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Gearóid Kelly
Student ID:	X20197365
Programme:	MSc CyberSecurity **Year:** 2022
Module:	MSc Interinship
Supervisor:	Mark Monaghan
Submission Due Date:	15th August 2022
Project Title:	Migrating an Email Filtering Solution from on Premise to Cloud
Word Count:	6823 **Page Count19**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: *Gearoid Kelly*

Date: 12/08/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Project – Migrating an Email Filtering Solution from on Premise to Cloud

Gearóid Kelly
X20197365

Abstract

Email filtering is one of the critical gateways to protecting an organisation from cyber-attacks. With 91% of cyberattacks originating from external emails, email filtering toolkits are crucial to protecting an organisation from cyber-attacks. After completing the post graduate diploma in Cyber Security and working within a cyber-based role, I elected to complete a project-based industry placement. The main brief of the project is to migrate the mail filtering toolset from on-premise to cloud. The current on-premise application can block anywhere from 70% -90% of inbound emails due to their content, with Cloud also expected to stop the same and more. The paper provides an insight into the overall project from fruition to deployment. It gives the rationale for decisions made alongside areas for future improvement and lessons learnt.

1 Introduction

Overview – 91% of cyber-attacks begin with an email [1]. In addition, cybercriminals are targeting multiple organisations across the globe every 44 seconds [2]. These statistics provide an insight into how organisations can remain vulnerable to attack. Working within the critical network infrastructure, the upkeep of mail filtering tools provides one defence barrier to an organisation. While it is not the only defence mechanism used by organisations, it is one of the entry barriers that potential cyber criminals can use to infiltrate an organisation's security controls.

The ESB (Electricity Supply Board) was established in 1927 and tasked with delivering a national electricity system. It has transformed over the years to having multiple subsidiaries across the globe. ESB has 7000 employees across its various divisions: Retail, Generation, Trading, Networks and Consultancy.

Having completed the post graduate diploma in cyber security I elected to complete the industry based internship and work on the delivery of a cyber themed project. The project brief focuses on upgrading the existing on-premise email filtering solution. As mentioned, 91% of cyber-attacks begin with a fraudulent email sent. Email is considered as a business critical application, I have been allowed to lead this implementation and migration. Furthermore, completing an industry Internship over a research-based one will enable me to utilise the theoretical knowledge gained and apply this knowledge within a corporate environment.

2 Related Work

All organisations now rely on email as a primary means of communication. Statistics show that 333.2 billion emails will be sent daily in 2022, with statistics showing that 45% of mail traffic sent in December was spam. The number of emails being sent is ever-increasing. In 2020 an average of 306.4 billion emails were sent and received daily, with this number said to rise to 376.4 billion emails by 2025. The importance of spam filtering is crucial to protecting a company's assets. The implications of neglecting the filtering of emails can have detrimental impacts on an organisation. One of Ireland's most recent high-profile attacks was where the HSE fell victim to a cyber-attack due to an employee opening an infected Excel file. The published report outlined the initial infection started by an employee interacting with a malicious Excel File attached to an email. [3]

Organisations are faced with ever-challenging operation conditions. The global pandemic followed by the unrest in eastern Europe and the global rise in inflation has undoubtedly added uncertainty across all organisations. [4]

The NIS Description of Cloud is as follows, "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources.*"
This description is a broad blanket description of generic systems. [5]

Anti-spam tool kits are software that detects and block potentially dangerous emails from user inboxes. Anti-spam protocols determine what an unsolicited and unwanted message (spam) is; in many cases, spam has advertised a product which may be legitimate (though still unwanted) or malicious. [6]

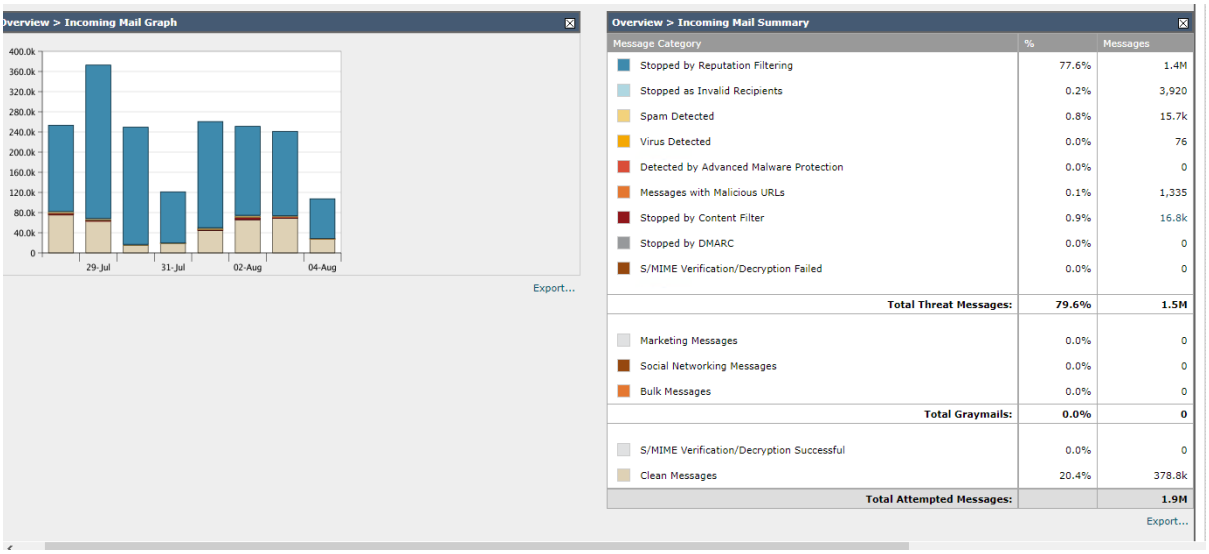
The argument of Cloud vs on-premise [7] can be discussed across the landscape of operating systems. It does not necessarily need to focus on implementing the Email Filtering Software. It is part of an organisation's overall strategic objectives and plans. Multiple organisations want to go with "Cloud First" over on-premise implementations. [8] While many organisations can migrate to the Cloud with relative ease and a lower level of risk. [9] ESB are a provider of Critical National Infrastructure. They maintain the electricity network and generate electricity for the national grid. Given our end users of systems have access to systems that integrate with these environments, there is additional governance and adherence to EU Directives [10]

A Salesforce article outlines the 12 Benefits of Cloud Computing [11]. Cloud migrations may not reduce or make processes redundant. From an operational perspective, the daily task will likely remain as is but a reduction in application maintenance may be reduced.

By choosing to migrate to the Cloud, an organisation is then handing off a level of control vs hosting the on-premise solution. Where on-premise existed, the organisation was in possession of upgrades and application maintenance. It also allowed for aspects of customisation to be implemented whereby processes were tailored for the organisation. However, when cloud migration occurs, organisations are now faced with having little control over system upgrades. This can be both positive and negative. For example, while the

organisation will be updated regarding security, they are also facing ad lib changes with new features or retirement of old features, which can impact operations.

Focusing on the overall Spam Filtering toolset and protecting the organisation from infiltration – It is also important to note that these applications will provide an organisation with a certain level of protection. Human error can count for 7%+ clicking on malicious links [12]. Even given the phishing simulations and tests, we are still seeing a high level of users clicking on what can be potentially malicious links within emails.



Source (Inbound Mail Graph ESB)

2.1 Interviews -

The following section features interviews with external and internal experts within the Cyber Security Landscape. The topic of the interviews was primarily around Cloud-Based Deployments and Email Security.

Matthew Conlon – CEO Cytidel – Matthew has multiple years of experience working in Cyber Security – He has experience working as a consultant for financial institutions alongside working within government bodies.

Paul Clarke – Incident Response Lead – ESB. Paul Clarke is the incident response lead for ESB. Paul is responsible for managing cyber-based incidents that occur within the ESB landscape.

Interview with Matthew Conlon, CEO of Cytidel. Cytidel is a cyber security start-up helping organisations reduce the risk of breaches, manage vulnerabilities and stay secure.

What are your views on On-premise Solutions vs Cloud Based Solutions?

"With security front and centre for many cloud solution providers, significant investment is made in ensuring their tools remain secure and backed up. This gives organisations peace of mind and reduces the operational overhead on internal IT teams who are already stretched

and struggling to balance the ever-growing workload. Moving to Clouds offering businesses a cost-effective means to have access to great toolsets; however, it's important to conduct a full review of each cloud provider you and evaluate the security practices they have in place to ensure they meet the requirements of your organisation and security policies."

While adoption rates in cloud technologies are up, we're still a long way from full adoption as mission-critical organisations continue to prefer the on-premise model to ensure strict control and access to data. This isn't something that will change overnight and will likely continue for many years to come"

Do you feel organisations are becoming vulnerable in moving to Cloud-based applications?
"In certain respects, yes. Organisations are offloading their data to cloud solution providers without always conducting appropriate due diligence and assuming they're handing over responsibility. In reality, it doesn't matter if it's the cloud provider's fault your data is breached. It's still your reputation on the line!"

We have seen how vulnerable the HSE were in the wake of the recent cyber-attack where a user has clicked a link in an email – Do you feel Staff in organisations realise the severity of the likely hood of clicking on a malicious link?

"Staff are becoming more aware of their responsibilities in maintaining data security and being conscious of potentially insecure activities. In addition, regular staff training helps improve staff awareness and understanding of the impact they can have on improving the organisations' overall security.

For companies without a staff training policy, this is one of the single biggest security improvements which can be made as many security breaches involve a threat actor tricking an employee to carry out an action such as clicking a malicious link in an email."

We are investing in technologies and toolsets to prevent the organisations being compromised. What do you feel is the biggest threat to organisations

"Cytidel are helping organisations to improve their vulnerability management capability, and predict cyber breaches before they happen. The company was started because we found this to be the area organisations were struggling the most to get right. Poor vulnerability management leaves the organisation as a prime target for a data breach, and more needs to be done to improve the efficiencies in this area. Simply running vulnerability scans is not enough. Organisations need robust processes underpinning them to ensure the ever-growing list of vulnerabilities is effectively managed and they have the ability to distinguish genuine threats from the noise."

Email Filtering and its importance in protecting organisations – The statistic of 91% of cyber-attacks can involve email – In your experience, do you feel there are positives and negatives in organisations choosing Clouds on-prem for email filtering and or do you feel that there is little difference and it is how the application is configured in ensuring that mail content is filtered correctly.

"Cloud email solutions have improved significantly over the past 5 years, with small companies having access to the latest security technologies at minimal cost. Cloud-based solutions also update their known threat lists on a regular basis, which on-premise tools often struggle to

keep up with. Ultimately, it's all in the configuration. A misconfigured email security solution will ultimately lead to a security incident, therefore focus should be on getting this correct".

Interview with Paul Clarke, Incident Response Lead ESB.

What are your views in On-premise Solutions vs Cloud Based Solutions?
"Both have their advantages and disadvantages. However, once configured securely, I believe Cloud-based solutions offer great advantages such as enhanced features, faster and easier updates and the support and expertise of the cloud provider. However, detailed consideration and risk assessment should be carried out before moving business-critical assets to the Cloud Is the increased risk worth the reward of the Cloud-based solution"

Do you feel organisations are becoming vulnerable in moving to Cloud-based applications?
"Yes, while moving to the Cloud gives some great features and support options, I believe moving away from on-premise makes the cloud solution more likely to be attacked. That coupled with often poor or misunderstood Configuration can lead to increased risk."

We have seen how vulnerable the HSE were in the wake of the recent cyber-attack where a user has clicked a link in an email – Do you feel ESB Staff realise the severity of the likely hood of clicking on a malicious link.
"No, I don't think that most users understand that the major cyber-attacks we see on the news regularly begin with a phishing email. Phishing is so common now in our personal lives I think users see it as someone trying to steal your bank details or con you for money and don't realise it could be someone trying to compromise the ESB.
I also don't think users realise that giving up your credentials in a phishing email lead to someone actively trying to log into your account (I'm still surprised how often we have incidents where passwords are compromised, and MFA is the saving factor."

We are investing in technologies and toolsets to prevent the organisations being compromised. What do you feel is the biggest threat to organisations?
"I think the biggest threat to the organisation currently is a human-operated ransomware attack similar to the HSE. This has the ability to affect all ESB business units, including electricity supply and generation. The technologies and toolsets we have in place, including email filtering, will hopefully allow us to detect these threats at the early stages so we can respond and eradicate the threat before the ransomware is deployed."

As Incident Response lead, what are your views on Email Filtering and its importance in protecting organisations?
"Email filtering is crucial in fighting all manner of cyber incidents from small fraud to major ransomware attacks. It can also be used as a preventative tool during zero-day vulnerabilities and stopping specific attacks. It is the gateway into your organisation for many malicious activities, so a well-configured and up-to-date email filtering tool is a must.
Even purely for spam/junk, if we did not have email filtering in place, the amount of spam and junk email that would reach ESB user's mailboxes would have an impact on all ESB business units productivity"

3 Research Methodology

The research procedure used here is more of a practical approach. This is due to it being a live system upgrade. However, the decision to move to Cloud can be based on the following –

The organisation's strategic objectives are to work with a cloud-first approach regarding systems and processes. ESB is an organisation with legacy systems and legacy processes where systems are now coming end of life – The organisation is committing to Net Zero Strategy by 2040. This company-wide strategy also encapsulates the update of systems and processes to achieve this [13].

Migrating from on-premise to Cloud will offer the organisation various benefits. Published articles will call out the benefits as

- Cost Optimisation,
- Automatic Software Updates
- Data Security
- Flexibility & Scalability
- Security*

These are just a few benefits organisations may face when moving their processes and applications to cloud vendors. However, while the overall cloud approach is most beneficial, there are additional aspects that organisations need to consider, such as Data Security and Storage. In addition, we are mandated to ensure that we comply with GDPR. This can often be highlighted around whereby the cloud locations are based and if they are located within the EEA.

Security – Given the Cloud is a shared service model, both of us within the ESB & Cloud vendors have a high level of responsibility in ensuring that the organisations are compliant and are not posing a risk to any other customers within the cloud tenant.

Access to regular software updates can also cause issues in the organisation. With the on-premise solution, we can maintain control of our versioning. However, with the cloud-based approach, we no longer have this level of control with it being a shared service model. This can sometimes mean we are upgrading with little control over version updates.

The focus of this project is migrating an on-premise email filtering solution to a cloud-based solution. Specific criteria define the methodology of applying a system upgrade, and having previous experience in completing complex system upgrades in a multi-integrated environment plays a pivotal part.

A DevOps approach was used to deliver the project criteria, and the SDLC Model was Adapted.

SLDC -Software Development Lifecycle.

Planning –
This is the first step in completing the research and defining the overall project scope and brief. The organisational requirements drive the project scope and brief. For example, in the planning stage, the statement “Migrate our Email Filtering” from on-premise to Clouds. Still, it does not allow us to create a definitive plan without completing a deeper dive into how the plan can be created.

Analysis –
The analysis stage was one of the critical areas. It complements the planning phase and provides a significant part of formulating the plan. The analysis stage is whereby stakeholder engagement takes place. It involved taking a holistic overview of the entire application. The inputs and outputs of the current set-up and transitioning these to the Cloud Completing the helicopter view allows one to identify the dependencies, criteria, scope, limitations, and constraints encountered within the project.

Design –
The concept of SAAS – Software as a Service is that a vendor provides an off-the-shelf solution. The benefits of SAAS are that there is often little opportunity for customisation. The design brief will be relatively rigid. However, it allows for the expectation of what will be delivered to be shared with all users. The design of this solution was to deliver the existing Configuration and feature set on-premise to the Cloud. Multiple additional features could have been implemented, available, and factored into the design brief. Choosing to work within the organisation's constraints and risk appetite was one of the critical principles of the design brief. As this application is now internet-facing, we did look at what options are available to ensure the maximum security of the application.

Implementation –
It should be noted here that this implementation is a multi-phased approach. Therefore, the implementation does not necessarily mean that we are fully operational with the complete migration of all mail domains. Instead, it is broken down into stage gates. The plan on a Page highlighted within the configuration document provides a high-level overview of the stages complete.

Testing and Integration –
Testing and Integration are the critical points for determining the success and full Integration of the project. Creating a test plan and testing objectives determines that we are ready to begin integrating fully and transitioning each mail domain from existing on-prem to cloud. Identifying critical tests to be carried out ensure due diligence. In addition, should any necessary path tests fail, one should not proceed past the said point without raising a defect and implementing a solution. It should only be that once all testing has been complete that we can move to production deployments.

Maintenance –
Again, this is another multi-phased process. The benefit of cloud-based systems means that the vendor partially covers application maintenance. This is only in terms of the operating systems versioning the security compliance and vulnerability management. Configurations and upkeep of the overall environment configs remain the responsibility of our cyber teams. They are migrating from on-premise to Cloud does not provide absolution from completing tasks.

There is no correct answer in determining the best deployment model for organisations. The deployment models are Agile, Waterfall, Lean, Iterative, Spiral & DevOps. It's fair to say each organisation will have a set deployment model adapted and tailored for their organisation and internal processes. Having completed previous releases in a different business unit, I felt that refining and utilising a skillset whereby we completed releases in a multi-tiered stack with more complexities would lend itself to completing this project.

When tasked with completing the upgrade, I looked at the following

- What is the objective
- What are the inputs and outputs?
- What is the current process?
- Who is impacted?
- Who needs to be involved?
- What needs to be tested
- What is the go-live Plan?
- What is the fall-back plan?

4 Design Specification

The project brief is to migrate our existing mail filtering appliance from an on-premise solution to a cloud-based application.
The organisation's requirements drive the design specification. The project's scope revolves around migrating the email filtering solution for a semi-state energy company responsible for hosting Irelands' critical national infrastructure. Taking a risk-averse approach in this project is crucial in minimising the organisation to any level of security risk

With an existing enduring solution already in place, some additional aspects can be considered in delivering this project.

- The benefits of migrating to a cloud network
- The additional feature sets available
- Review of the existing application
- Consideration of other marketplace options

Albeit unable to choose and analyse different systems, there are still rigorous aspects of design specifics that must be considered for the selected application, and specific requirements were identified.

- The new solution should have MFA (Multi-Factor Authentication) / SSO Single Sign On.
- IP Log-in Restriction – Users can only log into the application within the corporate network.
- Deliver the solution without exposing the organisations to any level of risk – This is an important one whereby we will not utilise all feature sets currently available – The organisation wishes to only migrate to the Cloud with our existing features on-prem. Any enhancements will be delivered at a future date.

The following needs to be considered, and a plan created to reach the end goal of the ESA Migration to Cloud

- Creation of an As is and To be Plan
- Stakeholder Identification
- Security Architecture Overview
- Governance and controls
- Project Timeline

Decomposing these items further allows for further information on the creation of our design specifics-

As is and To Be –
While migration to Cloud can mean additional feature sets are available, the focus is to implement a working solution that allows for the same email filtering level as in our on-premise environment. Therefore, the Crawl – Walk – Run method can be invoked to allow for a stable deployment of the solution. This allows for confidence and mitigates potential defects

when proceeding with the migration. In addition, allowing for stability means that future enhancements can be implemented and delivered with minimal risk.

In addition, having an As is and To Be Plan allows for a full review of both environments. It provides oversight into detailed configurations.

In an “As Is and To Be” plan, one completes a walk-through of the current process and details what the future process will entail. It allows one to take a holistic overview of the entire process, creating a process map of what the new solution must cover.

Stakeholder Identification – The identification of stakeholders is one of the most crucial aspects of the success or failure of a project. Additionally, utilising stakeholder engagement provides additional input into the design-specific plan and can be used to identify other areas that require attention or missed points.

Security Architecture Overview –
Ensures the proposed solution is being implemented and conforms to best practice standards.

To implement and migrate, the following was required –

Application Overview –
The existing application was on an older version where support was coming to the end of life. Given the importance of the application, we need to ensure that we migrate with all the current feature sets. A vendor-sanctioned health check was completed on the on-prem environment. The benefit of the health check was to identify areas of improvement and/or misconfigurations that may already be in the current environment. There is also a rationale for completing the health check on the existing system.

1. Provides a current state overview of the environment
2. Highlights areas of attention
3. Provides the foundation for the new system.

The cloud-based platform is a newer version of the current application. One of the tasks with this migration is that our existing Configuration is exported from the on-premise solution and ingested into the cloud-based application. It was coincidental that the health check was taking place alongside a proposed migration and had the options presented –

- Migrate to Cloud & Complete Health Check on Cloud Application
- Complete Health Check-in on-prem solution and implement changes on Cloud Platform
- Complete Health Check and disregard the results
- Complete Health check on the on-prem solution and implement changes in the on-prem solution.

My rationale was to complete the health check on the on-prem solution and implement changes in the on-prem solution. It may seem strange that one would go with this approach as the organisation was moving to a new appliance; however, the reasoning behind it is –

1. Health check was overdue in the on-prem solution with changes that required addressing.
2. Our on-prem config is the foundation for the cloud-based application
3. Health check results are addressed and implemented in the on-prem solution. If there is an outfall, they can be identified and decoupled from the migration to the Cloud
4. We are moving to the Cloud with the best configs, and there will be a clean period whereby no changes can be made during the migration period.

The outcome of the health check identified specific areas for improvement and allowed for the following

- Optimisation of Email Filtering.
- Enhancing Configuration to ensure system integrity.
- Adhering to vendors' standards and guidelines.

Integrations with other applications/ New Features

Additional Feature Sets

One of the design specifications was to look at the overall security of the application and how robust the existing solution was vs what the new solution could deliver. It is also one of the first steps within the project plan. There are various options available to organisations and how they can secure applications, and the CISA Article provides an overview of the importance of MFA.

Local User Account –
Allowing for the set-up of local user accounts can be utilised; however, it may present certain risks. These are highlighted when removing users' accounts within a movers/ leavers and joiners process. It can also mean that the same restrictions are not applied, and a user can access without specific provisions. They can accept ss without the benefits of Active Directory Feature Sets

SSO – Single Sign On –
Microsoft's definition of single sign-on is An Authentication method that allows users to sign in using one set of credentials to multiple independent software systems [14]. The additional pre-requests that single sign-on offers provide more peace of mind than using local user accounts. However, the Single Sign On method requires other steps. The users must be in the company domain, assigned to the relative active directory group and provided with the relevant feature set within the application. The benefits are that when a user's account is terminated, all other access associated with the user is terminated.

MFA Multi-Factor Authentication –
Multifactor authentication (MFA) [15] adds a layer of protection to the sign-in process. Users provide additional identity verification when accessing accounts or apps, such as scanning a fingerprint or entering a code received by phone.
Further securing the application can mean implementing an additional feature such as MFA. MFA will mean that the user needs to not only have the "Something you know" feature it also ensures there is an additional item such as "Something you Have". The different request is that a token is issued to a user's mobile device/ application to authenticate the request.

Some options are available to secure the domain; however, some additional features can be utilised. The factor to consider is that the cloud environment is more functional than an on-prem solution hence looking at these other feature sets.

IP Restriction –
The IP Address is the unique identifier for computers communicating over the internet and other networks. Exploring the option of implementing IP restrictions further ensures an organisation's robust security feature sets. Restricting access ensures that those only logged into the corporate network can access the defined links to the domain. Allowing for these feature sets does require some additional considerations. Given this is a cloud environment and a vendor-supported application, there needs to be consideration around implementing the restrictions and potential blocking of access to legitimate users outside our cloud domain.

To proceed with IP Restrictions, there are also additional considerations on how to implement this –

- Firewall level Configuration
- AD Policy Configuration
- Vendor Policy configuration

All the above allow for restricting access to the environment. The preferred approach may be to complete it from a company level as it gives us control over environment configurations.

SIEM Integration.
Security Information & Event Management (SIEM) [16] Integration captures event logs across the landscape within our security applications. It provides insight into threats and highlights any malicious activity within the system. There is existing SIEM Integration on our current solution. However, given that our configurations will be redundant, a newly architected solution integrating with the cloud application is required.

Vendor SIEM -
The vendor provides an application that issues security logs for their software products. As ESB are a user of the vendors' multiple software solutions, it could be considered to integrate this solution. While this will provide sufficient information in terms of security logs, there is an issue with compatibility with other platforms. It is, however, a proposed option that will be explored further.

Configure with the Same Configuration as on-prem –
This option is not viable because the integrations are speaking with an on-premise solution.

Site to Site VPN –
Transporting the logs via a site-to-site VPN from the cloud solution to our end solution allows for a direct connection without exposing full internet access. This ensures that there is a direct link between the two systems. However, it still does not allow for a barrier to intercept the traffic before it is ingested within the SIEM.
The preferred option is to implement the Site-to-Site VPN Connectivity with additional controls of where the Logs are ingested into a DMZ. While using the Site-to-Site VPN ensures that traffic is secured, the other feature allowing the traffic to be intercepted and securely checked before ingestion allows for controls.

The above information provides an overview of the design and rationale for the specifics chosen. These specifics are then transitioned from a design to an implementation stage. It is essential to state that each is subject to governance and control and advice from security architects and SMEs from a vendor perspective and an internal team. The design conforms to the best standards, ensuring that we mitigate any level of risk for the organisation.

5 Implementation

Implementing a solution provided by a vendor will require specific criteria from a relevant organisation. In this project, the requirement was to deliver the mail filtering solution for an energy company. Email filtering criteria will be universal to all organisations to protect them from attacks. When migrating to Cloud, organisations work based on a shared service model. This means that the vendor and business unit has a level of responsibility to ensure that they comply with and implement best practices. Implementing Email Filtering requires much more than a plug-and-play – There is a level of due diligence and a holistic view of the application. As the ESB are also a provider of essential services in the state, deploying or upgrading any systems must conform to standards as directed by the NCSC.

The implementation task began in May 2022 –

A pragmatic and phased approach to the implementation is required – The staged implementation ensures that due diligence is completed before a full production migration takes place. It is a staged process with certain items unable to take place until a critical path milestone has been reached – The steps are also completed in line with the criteria discussed in the design brief.

- *Risk Assessment completion and sign-off.*
- *Domain Provision by Vendor*
- *Securing the application*
- *Configuring the application*
- *Testing the application*
- *Review of the application*
- *Live Email Migration*
- *Project Review & Lessons Learnt*

Risk Assessments –
These assessments are mandatory for any new application deployed on the landscape and cover all aspects from Vendor Security, Data Storage Location, Company Policies and or ISO Certifications. This requires a large amount of input from the vendor as it ensures all aspects of their application do not pose a risk to the ESB Software Landscape.

Domain & Environment Provision by the Vendor –
This is where the vendor completes the build of the Email Filtering Appliance. First, it is the typical standing up of the application with the basic configurations.

Securing the Application –
This was one of the main feature requirements of moving to the Cloud and an essential requirement. We decided to use Single Sign-on, MFA Multi-Factor Authentication & IP Restrictions. The implementation of this has given a robust security architecture. Working to achieve this means we engaged with our cloud team and network teams.

Configuring the Application –
This is the crucial and possibly one of the most essential parts of the migration. It configures our email filtering solution to block any malicious emails entering the ESB Landscape. We must also ensure that the new appliance has the same configuration level as our existing solution. We could migrate the Configuration from our on-premise solution to the cloud-based application. This then formed the base level configuration with a manual sense check.

Testing the application –
A test plan was drawn up. The point of testing is to ensure that the application is working as expected and there are no bugs or glitches in the process.

Testing is broken down into multiple parts –

1. We implemented no significant feature changes. The main ones are SSO/ MFA and IP Restrictions. Signing onto the application was completed, and all aspects of SSO and MFA/ IP Restrictions were carried out to ensure it worked.
2. Scenario-based testing. This involves replicating the production scenarios and formulating the strategic approach of slow and steady rather than a big bang approach. The scenario-based tests mimic what would happen with live accounts but in a controlled manner. It assures that there are no risks when we move to live email accounts. – Here is where I differentiate between live domains and test domains. Live domains are all email users who use their mails for day-to-day work processes. Test domains allow us to control and limit exposure to the application while still replicating a live process.

Review of the Application/ Project –
Once testing has been completed and signed off, a review of the plan takes place with all stakeholders. It can also be considered Governance and Controls – Formulating governance and controls ensures that best practice is followed. We must adhere to internal and external protocols when delivering system upgrades. Adhering to the processes and having the governance and control allows for a well-documented and formulated project delivered with minimal risk.

An exit report is formulated outlining all that was captured and tested. Issues encountered and areas for future improvement.

Change Control –
After reviewing the project plan and work, it is submitted to the Change Control Board. As mail is one of the critical applications used within the organisation, all the above require completion before migrating live domains. Change control will ensure that all aspects, such as testing and planning, have been carried out.

Live Email Migration –
This is one of the final steps within the migration. Again, we work this on a phased approach and complete it with the smallest mail domain first and then increase the email domain migrations as we have confidence that there are no issues with the new platform. The live email migration is the last step and is completed in line with hyper care and roll-back methods if required.

Project review and Lessons Learnt.
Upon completing the migration, we explored the areas that were not covered. As a result, different aspects, such as the new feature sets, can now be implemented. This step takes place post hyper care and assures that implementing new features was not caused during the initial migration process.

6 Evaluation

This project has provided an overview and step through of completing a migration of an on-premise solution to a cloud-based mail filtering solution.

Environment Health Check.
Having completed a health check on the on-premise solution has highlighted areas whereby improvement was required. This was typically the enhancing of content filters and advances in processing within the application by streamlining configurations. Following the health check, baseline configurations were imported into the new cloud application.

Securing the Environment
The key directive was to implement SSO/ MFA & IP Restrictions. – The robust security controls retire the need for local user accounts. SSO & MFA – These are linked with the users' AD Accounts. This feature set also means that when access is being revoked, it is done globally and no longer required locally when removing users' access.

IP Restrictions –
As we have now moved to a cloud-based architecture and publicly available links, we need to ensure that access to these domains is limited. That means restricting the IP addresses of the application to specific users. The criteria checklist is that a user must be within a certain network before logging into the settings application. This is done both locally at an ESB Level and additionally at a vendor level.

As is to As is Migration –
Completing the as is to as is means we have migrated to the Cloud without enabling any additional feature sets. Instead, we have directly uploaded the configurations meaning there is an exact match between our on-premise and cloud-based applications. Even with completing the As is to As is Configuration, issues were still encountered, such as Mismatches and discrepancies. This mainly occurred due to the newer version of the cloud-based application. Items such as certain special characters were no longer supported within certain configuration items.

Stakeholder Overview –
The description of a stakeholder is those with a vested interest. This is a broad description, and while this change impacts all employees, there is no need to have all involved in the discussion and project. Identifying key stakeholders and SMEs (Subject Matter Experts) allowed me to identify a complete holistic overview of the migration. This ensures that no aspects of the migration are missed and minimises risk for business applications.

Lessons Learnt –
Working on this project has provided an insight into how we can deploy our email filtering application from an on-premise to a cloud application. There were some significant lessons learnt with the migration of the application. Some of the main points are

- Missing Configurations.
- Defects encountered.
- Configuration of On-Premise and Cloud Environments and knowledge gaps based on Configuration.

One of the main aspects of completing the change from on-premise to Cloud is the interdependencies of outbound mail from internal applications. Although applications are hosted within the DMZ (Demilitarised Zone), it's a buffer point between our organisation's network and, typically, the internet. Migrating to the Cloud now means rearchitecting these applications and potentially exposing them to direct internet because it is now a cloud-based solution.

Premise environment behaviour –
The on-premise environment behaviour highlighted several areas which required additional review. While these were not highlighted in the environment health check, they were highlighted within the application testing. In addition, there are some immediate areas of concern which require addressing. I would have addressed these immediately; however, as the project brief was to only work with our existing configurations, these areas will be added to an immediate application improvement plan to ensure that the environment is secure and utilised to its maximum potential.

7 Conclusion and Future Work

With email being a business-critical application, it is necessary to ensure stability and uptime on the delivery of mails. On a given day, the range of inbound emails blocked by email filtration can range anywhere from 70% - 90%.

The purpose of this project was to deliver the upgrade of our on-Premise mail filtering solution and migrate it to Cloud. The additional feature set of “Security” was the additional prime focus and was requested by the organisation's CISO.
We have successfully implemented the feature set of Single Sign on with MFA – Multi-Factor Authentication, IP Address restrictions and enhanced RBAC feature sets.

The cloud-based application also runs with the latest software versions with additional features and functionalities.

The project was also faced with restrictions on what we delivered. The cloud-based platform contains multiple features that we currently do not enable due to constraints within the organisation. We are a risk-averse organisation which is often slow to adapt to change. Therefore, a pragmatic approach was used for this project. The principle we worked with is the mindset used to deliver what we know works and then work on enhancing the additional features later.

There are plenty of avenues for future work within this application. We can look at implementing some of the product's additional features. This will occur at a future date once we know that our new as-is process is stable and working as expected. Working on a phased approach will allow for any new features to be delivered with minimal disruption.

Further to adding new features, certain mailbox domains could not be migrated as part of the project. This is due to the inter-complexity of system integrations. The overall change is minimal from the Email Filtration side, but the work required on the connected system caused a constraint for the project.

Another point to make here is that the implication of this project is to filter the inbound mail traffic into the organisation. Any malicious software/ links and content are required to be blocked by this solution. The criticality of successfully deploying this application without issue is of priority for the organisation. There would be a significant risk of not completing this task successfully. The risks of exposing the organisation to attack could have crippling consequences and potentially create a similar issue to the HSE Encountered.

It is fair to say there is a limited value add in choosing to migrate the entire application from on-premise to the Cloud. The key benefits of this application are around how it is configured in terms of content filters, i.e., “Blocking the bad stuff” The primary focus of the mail filter application is to block malicious links or applications entering the organisation. It is the main gateway and barrier to protecting the organisation. Yet, it will not entirely protect an organisation from human error or human threat actors clicking on malicious links.

8 References

[1] Deloitte Malaysia. 2022. *91% of all cyber-attacks begin with a phishing email to an unexpected victim | Deloitte Malaysia | Risk Advisory | Press releases*. [online] Available at: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

[2] Deloitte Malaysia. 2022. *91% of all cyber-attacks begin with a phishing email to an unexpected victim | Deloitte Malaysia | Risk Advisory | Press releases*. [online] Available at: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

[3] Hse. i.e. 2022. [online] Available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[4] Brooks, C., 2022. *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*. [online] Forbes. Available at: https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=594100d17864

[5] Mell, P. and Grance, T. (2011) *The NIST definition of cloud computing*. doi: 10.6028/NIST.SP.800-145.https://csrc.nist.gov/publications/detail/sp/800-145/final

[6] Mimecast. 2022. *What is Anti-Spam? | Anti-Spam Software | Mimecast*. [online] Available at: https://www.mimecast.com/content/anti-spam-software/

[7] Watson, L.A., Mishler CMA, CIA, CISA, C., 2014. From On-Premise Applications to the Cloud. Strategic Finance 96, 80–81. https://www.mendeley.com/catalog ue/63a7fb31-abb1-3bbf-9111-5964027a47d4/

[8] Nicholson, D. (2018). Cloud first – tackling the security challenges. *Computer Fraud & Security*, 2018(1), pp.8–11. doi:10.1016/s1361-3723(18)30005-8. https://www.sciencedirect.com/science/article/pii/S1361372318300058

[9] Researchonline.ljmu.ac.uk. 2022. [online] Available at: https://researchonline.ljmu.ac.uk/id/eprint/6934/1/X%20MACDERMOTT%20edit.pdf

[10] Enisa.europa.eu. 2022. [online] Available at: https://www.enisa.europa.eu/topics/nis-directive

[11] Salesforce.com. 2022. *12 Benefits of Cloud Computing and Its Advantages*. [online] Available at: https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/

[12] Ieeexplore.ieee.org. 2022. *Phishing Attack Simulation: Measuring Susceptibility among Undergraduate Students*. [online] Available at: https://ieeexplore.ieee.org/document/9243426

[13] ESB Corporate. 2022. *Understanding ESB's Net Zero by 2040 Strategy*. [online] Available at: https://esb.ie/media-centre-news/blog/article/esb/2022/04/13/understanding-esb-s-net-zero-by-2040-strategy

[14] Docs.microsoft.com. 2022. *What is single sign-on? - Microsoft Entra*. [online] Available at: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on

[15] Microsoft.com. 2022. *Multifactor Authentication | MFA | Microsoft Security*. [online] Available at: https://www.microsoft.com/en-gb/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication

[16] Ibm.com. 2022. *What is Security Information and Event Management (SIEM)? | IBM*. [online] Available at: https://www.ibm.com/topics/siem

9 Appendix

SSO	Single Sign On
MFA	Multi-Factor Authentication
VPN	Virtual Private Network
SIEM	Security Information Event Management
On-Prem	An Inhouse Solution where resources are deployed internally
ESB	Electricity Supply Board
ISO	Internal Office for Standardisation
IP	Internet Protocol
CISO	Chief Information Security Officer
RBAC	Role-Based Access Controls
HSE	Health Service Executive
GDPR	General Data Protection Regulation