



SecaaS Implementation Guidance

Category 4 // Email Security

September 2012

© 2012 Cloud Security Alliance

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance Security as a Service Implementation Guidance at <http://www.cloudsecurityalliance.org>, subject to the following: (a) the Guidance may be used solely for your personal, informational, non-commercial use; (b) the Guidance may not be modified or altered in any way; (c) the Guidance may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Guidance as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Security as a Service Implementation Guidance Version 1.0 (2012).

Contents

Foreword	5
Letter from the Co-Chairs	6
Acknowledgments	7
1.0 Introduction	8
1.1 Intended Audience	8
1.2 Scope	9
2.0 Requirements Addressed	10
2.1 Business Value	10
2.1.1 Leveraging Message Aggregation	10
2.1.2 Rapid Response	11
2.1.3 On Demand Provisioning	11
2.1.4 Advanced Skillset	11
2.2 Key Challenges in Migration of E-Mail to the Cloud	11
2.2.1 Data Security and Protection	11
2.2.2 Regulatory Compliance	12
2.2.3 Data Residency	12
2.2.4 Unauthorized Disclosure	12
2.3 Solutions Roadmap	12
2.3.1 Standards-Based	13
2.3.2 Malware and Spam Protection	13
2.3.3 Identity and Encryption	13
2.3.4 Secure Access	14
2.3.5 Integration with Data Asset Protection Systems	14
2.3.6 Records Retention/Data Destruction	14
2.3.7 System Management and Logging	14
3.0 Implementation Considerations and Concerns	15
3.1 Considerations	15
3.1.1 Multi-Tenancy	15
3.1.2 Portability	15

3.1.3 Programmatic Access	15
3.1.4 Self-Service	15
3.1.5 Client Controls	16
3.1.6 Management and Monitoring	16
3.1.7 Integration	16
3.2 Concerns	16
3.2.1 Data Security	16
3.2.2 Regulatory Compliance.....	17
3.2.3 Data Disclosure	17
3.2.4 Data Residency	17
3.2.5 Identity	18
3.2.6 Logging.....	18
3.2.7 Communications.....	18
4.0 Architecture and Implementation Steps	19
4.1 Architecture Overview.....	19
4.1.1 Fully Outsourced Email Implementation.....	20
4.1.2 Email Security Cloud Augmentation to Premise Enterprise Implementations	20
4.2 Guidance and Implementation Steps	22
4.2.1 Client Security.....	22
4.2.2 Administration.....	23
4.2.3 Submission End-Point, the Mail Submission Agent.....	23
4.2.4 Mail Delivery Agent	23
4.2.5 Mail Transfer Agent	24
4.2.6 Mail Storage.....	24

Foreword

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. We are reaching the point where computing functions as a utility, promising innovations yet unimagined. The major roadblock to full adoption of Cloud Computing has been concern regarding the security and privacy of information.

Much work has been done regarding the security of the cloud and data within it, but until now, there have been no best practices to follow when developing or assessing security services in an elastic cloud model—a model that scales as client requirements change.

One mission of the Cloud Security Alliance is to provide education on the uses of Cloud Computing to help secure all other forms of computing. To aid both cloud customers and cloud providers, the CSA SecaaS Working Group is providing Implementation Guidance for each category of Security as a Service, as delineated in the CSA's SecaaS [Defined Categories of Service](#). Security as a Service was added, as Domain 14, to version 3 of the [CSA Guidance](#).

Cloud Security Alliance SecaaS Implementation Guidance documents are available at <https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/>.

We encourage you to download and review all of our flagship research at <http://www.cloudsecurityalliance.org>.

Best regards,

Jerry Archer

Alan Boehme

Dave Cullinane

Nils Puhlmann

Paul Kurtz

Jim Reavis

The Cloud Security Alliance Board of Directors

Letter from the Co-Chairs

Security as a Service is a specialized area categorized two years ago as growing rapidly and in unbound patterns. Vendors were struggling. Consumers were struggling. Each offering had its own path. We felt it was urgent to address the needs and concerns common to the implementation of Security as a Service in its many forms.

The [Defined Categories of Service](#) helped clarify the functionalities expected from each Category. In this series, we hope to better define best practices in the design, development, assessment and implementation of today's offerings.

We want to thank all of the many contributors worldwide who have worked so hard to produce these papers providing guidance for best practices in Cloud Computing Security. Many have been with the Security as a Service Working Group since the beginning; many others joined in this effort. Each has spent countless hours considering, clarifying, writing and/or editing these papers. We hope they help move forward toward those unimagined innovations.

Sincerely,

Kevin Fielder and Cameron Smith
SecaaS Working Group Co-Chairs

Acknowledgments

Chair

Mark Hahn, TCB Technologies, Inc.

Contributors

Marcelo Carvalho, FATEC-SP

Yael Nishry, Vaultive

Yogesh Paliwal, Cisco

Paul Pottorff, Faster Motion

Adam Swidler, Google

Peer Reviewers

Varun Badhwar, CipherCloud

Dennis Dayman, Eloqua

Tim O'Brien, Tata Steel Group

Ron Poserina, Symantec

CSA Global Staff

Luciano JR Santos, Research Director

John Yeoh, Research Analyst

Aaron Alva, Research Intern

Vicki Hahn, Technical Writer/Editor

Kendall Scoboria, Graphic Designer

Evan Scoboria, Webmaster

1.0 Introduction

Electronic mail now plays a vital role in business interactions among customers, partners and internal staff. It allows data and messages to be transferred easily between senders and receivers over the Internet or internal networks, allowing messages to be received, responded to, stored, forwarded and broadcast among recipients. These extensive capabilities have caused email to be widely adopted as the official communications method for many organizations. Also common for personal use, electronic mail is available thru a diverse number of compatible software clients, and also via web-browser.

Due to its ubiquitous use, electronic mail is both the prime target of, and primary vehicle for, attacks, and must be protected on both ends: sending and receiving. Email service is a well-defined utility in the enterprise, and securing email in the cloud is similar to securing email in the enterprise. Email Security as a Service (SecaaS) has a few unique aspects, but most responses entail differences of degree, rather than instituting new methods of security.

Email security services conform to one of two service models: fully outsourced and enterprise augmentation. The first service model outsources the entire mailbox and user interface to a cloud provider (either in a single-tenant or multi-tenant model). The second service model adds security processing to an existing enterprise email implementation. In a fully outsourced model, the service provider is responsible for monitoring all threats using email as a channel (spam, phishing, malware propagation, etc.), and for providing an email user interface (UI) and possibly assistance to an organization's end users. In the enterprise augmentation model, an existing on-premise email deployment is augmented by additional cloud-based services and functionalities.

This paper explores both common forms of usage and additional extended services (such as identity federation and data loss prevention), and describing best practices for evaluating, developing, installing and using cloud-based email security services.

1.1 Intended Audience

Email security services are viewed from two perspectives: the providers of these services and the consumers or purchasers of email security services. Both sides need to be aware of and plan for key service features and how these features are used to mitigate threats to email security.

Section 2 provides an executive level overview of email security services and delivery methodologies, and shows how security threats are mitigated in a cloud-based service versus a traditional self-hosted solution. Section 3 presents considerations and concerns that should be part of any conversation regarding the use of Email Security as a Service. Section 4 is a technical discussion of typical architectures and the implementation of Email SecaaS using current best practices as defined by the industry. Section 5 provides lists of both references and useful links to supplement this information

1.2 Scope

This paper discusses the use of SecaaS services to mitigate email threats arising from viruses, phishing, spam, denial of service and operational disruptions. Features covered are email digital signatures, encryption, email archival services, threat detection and prevention services and data loss prevention (DLP). One best practice around email services in the cloud is the use of a federated identity system to ensure proper authenticity of messages and service users.

The scope of this document includes secure implementation of electronic mail services on cloud architectures, including:

- Common electronic mail components
- Electronic mail architecture protection
- Common electronic mail threats
- Peer authentication
- Electronic mail message standards
- Electronic mail encryption and digital signature
- Electronic mail content inspection and filtering
- Securing mail clients
- Electronic mail data protection and availability assurance techniques

2.0 Requirements Addressed

Email is a primary mechanism by which information is created and exchanged within and between organizations. Email services and email protection services are largely commoditized so all solutions, cloud-based or non-cloud-based, follow a similar model.

Cloud-based vendors may be able to provide organizations with compelling value propositions for fully outsourced email, or for security augmentation services for in house enterprise email implementations. One major advantage to cloud-based security is that large vendors can view the aggregated traffic from many organizations, and thereby have early indications and insights into new types of malware and spam floods. This benefit is not available to a single tenant outsourced or single enterprise implementation, which will have to respond after being affected, or await alerts from other sources.

2.1 Business Value

Cloud-based vendors offer organizations many methods of securing email services using specialized skills and tools. Organizations utilizing Email SecaaS offerings can:

- Obtain early response to new forms of malware or spam floods, because their vendor's multi-tenant model allows them access to message traffic across multiple organizations.
- Receive rapid deployment of new configurations and updated filtering algorithms because the vendor is able to deploy changes which apply to all clients.
- Utilize on-demand provisioning for increasing or decreasing usage, thereby eliminating the need for excess capacity for seasonal or unusual events.
- Utilize the specialized skills and techniques that vendors have developed without investing training and expense in a non-core competency.

2.1.1 Leveraging Message Aggregation

When considering cloud-based services, it is often a concern that the multi-tenant model presents risks to data protection. However, with email traffic filtering, this multi-tenant model increases the power of the solution. A cloud Email Security as a Service provider is able to correlate message traffic trends and data across multiple sources for many organizations. This provides the cloud service provider with tremendous insight into current threats and intelligence about changing threat models.

This capability is simply not available to an organization that operates an enterprise email system in a single tenant manner. A single tenant or completely in house enterprise email system will never be as effective unless it is augmented with services utilizing a multi-tenant model.

2.1.2 Rapid Response

The email threat landscape changes rapidly as malware writers and spam operators change tactics to evade filter systems. This arms race results in a need to rapidly deploy new techniques and configurations. Cloud-based vendors provide rapid response because they only have to deploy changes once to their infrastructure to provide improvements for many clients. In this way, an organization can take advantage of a cloud-based vendor's ability to test and deploy new solutions versus having to investigate, test and deploy the changes individually. This removes the latency many email systems experience in response to changes in threats.

2.1.3 On Demand Provisioning

Email is a key organizational asset and must be available quickly for new users. This usually means an organization must build in excess capacity in anticipation of future demands. There always is a significant amount of underutilized capacity at any one time, which increases costs. Further, a failure to properly predict future demand will leave an organization with an unstable email system which limits the effectiveness of a key business asset.

Because cloud-based vendors' growth is the aggregated demand across many organizations, their growth predictions can be more precise and capacity can be reliably added in advance of demand. Organizations whose needs decrease can easily deprovision services and reduce costs. In this way, costs for a cloud-based solution more accurately track the usage curve, making them easier to manage financially.

2.1.4 Advanced Skillset

For most organizations, the implementation and operation of an email system is a business need but not a core competency. For cloud-based email and email security vendors, the email system is their core competency and therefore they are able to hire experts in the field and dedicate full time, trained staff to the function.

In order to have the best trained engineers working on highly efficient email security solutions, an organization may need to turn to a specialized vendor. These vendors likely will be offering a cloud-based, multi-tenant model for their service offerings. SecaaS vendors may offer the most effective solutions to address the email needs of an organization.

2.2 Key Challenges in Migration of E-Mail to the Cloud

2.2.1 Data Security and Protection

The cloud introduces a broad range of security threats, including the possibility of the cloud provider being hacked, the potential for malicious actions by a rogue employee of the cloud provider, and the intermingling of data in a compromised multi-tenant environment.

2.2.2 Regulatory Compliance

Enterprises are subject to an array of regulatory requirements including: US federal laws with both domestic and international applications, such as Sarbanes-Oxley (SOX) or The Patriot Act; varying national data protection measures; international requirements like the European Union Data Protection Directive; and industry-specific regulations (e.g., HIPAA, GLBA and PCI DSS). There also are a number of good practices and standards (e.g., COSO, COBIT, NIST, ISO, etc.) that enterprises adhere to in order to best protect data.

2.2.3 Data Residency

Businesses that have an international presence are faced with the daunting task of complying with the multitude of growing privacy and data residency regulations. To comply, enterprises often pay cloud computing providers a premium to add costly infrastructure in each jurisdiction.

2.2.4 Unauthorized Disclosure

Cloud providers may be required to comply with legal processes seeking access to private emails and account information, such as search warrants, national security letters or subpoenas. Under many circumstances, organizations may not even be notified of this disclosure of their key business correspondence.

2.3 Solutions Roadmap

Email security addresses an organization's needs to provide secure messaging systems for the exchange of information between personnel. Email SecaaS addresses many requirements for information security. These requirements include:

- The ability to send and receive email in standard formats and protocols
- Prevention of malware infections via email
- Removal of unwanted spam messages
- Strong identification of email users
- Securing clients and securing remote access to email
- Integration with Data Loss Prevention tools
- Retention of email records
- Encryption of emails at-rest in cloud providers' environments with secure key management
- Mail management and logging
- Sender authentication frameworks

Email Security as a Service is provided either as a fully outsourced email service or as specific solutions which augment an existing enterprise email implementation. In a fully outsourced implementation, the vendor provides both the email service and the security features in a single solution. In the enterprise add-on solution, an organization augments an in-house email implementation with security services from cloud-based security vendors.

Using a cloud provider, an organization should be able to add or remove features or services in small increments on demand, using a single vendor or multiple vendors. This greatly increases flexibility and responsiveness to changing environments and demands.

2.3.1 Standards-Based

In any implementation, the security vendor should use industry standard formats and protocols for messaging and message transmission. In particular, all industry standard email protocols have TLS/SSL (Transport Layer Security / Secure Sockets Layer) versions that allow the use of strong encryption to protect all traffic (mailbox passwords as well as message bodies). Vendors should use the encrypted forms of all email protocols for access to, and transmission of, email messages. These protocols should be configured with options which disallow known weak encryption algorithms (DES, MD5 hashes) and options for strong user authentication.

Vendors should adopt operational methods which adhere to industry standards and best practices. Infrastructure should be deployed and built to pass strong physical security standards such as SSAE 16 (or the older SAS 70) so that the service foundations can be trusted. Further, guidance should be followed for the proper maintenance of services. This guidance can take the form of the COBIT, COSO, ISO 27000, CSA Guidance, or industry regulations such as HIPAA, Sarbanes-Oxley and others.

2.3.2 Malware and Spam Protection

Malware and spam protection are the primary threats to the operation of an email system. Vendors provide a variety of solutions to mitigate these threats. Use of an in house or single tenant hosted email system limits the effectiveness of any solution. In a multi-tenant cloud-based solution, the cloud-based security provider is able to correlate message traffic across multiple organizations to get richer data regarding malware and spam floods, which in turn provides earlier detection with greater accuracy.

As Email Security as a Service vendors gain intelligence from multiple streams of message traffic and the resulting larger data sets, they are able to rapidly deploy responses and algorithm changes to many organizations at once. This quick response is of benefit to all organizations using that vendor.

2.3.3 Identity and Encryption

The security of the overall email system, whether fully outsourced or enterprise hosted and augmented with security services, is driven first by securing the individual components to industry standards and organizational policy.

Cloud vendors should provide methods which allow the integration into the organization's identity management systems. This integration is described in the SecaaS Category 1 // Identity and Access Management Implementation Guidance. In the fully outsourced model, cloud vendors should also provide native strong authentication mechanisms, such as two-factor authentication.

2.3.4 Secure Access

Cloud-based vendors must provide a strong infrastructure and allow access to email systems using only secured (encrypted) protocols. As mentioned before, the SSAE 16 standard provides a report on the controls a vendor uses to manage their operations.

Users access email from a variety of devices, and vendors must provide controls which allow the users convenient but secure access. Use of encrypted protocols including HTTPS and IMAPS should be required for all access from all devices whether it is a PC, a laptop or a mobile device.

2.3.5 Integration with Data Asset Protection Systems

Email messages are a convenient method for moving data inside an organization and to an organization's partners. However, this convenience also creates difficulties for controlling the distribution of confidential information. Email vendors should allow the integration of encryption at-rest and data loss prevention tools to protect the organization from unauthorized leakage or transfer of sensitive data.

The use of Data Loss Protection tools is described in SecaaS Category 2 // Data Loss Prevention Implementation Guidance.

2.3.6 Records Retention/Data Destruction

Email messages often are critical business documents that need to be protected and retained for specific periods. Many of these documents relate to critical business decisions and discuss matters that are covered by regulations, laws and the organization's by-laws. An email system should provide methods to specify the records retention policy, and also completely remove digital copies of documents as desired or required.

Vendors should ensure that media on which email messages are stored are indeed erased and overwritten, rather than just returned to "free space." This requirement is especially critical for vendors using a multi-tenant model, because of the potential for data leakage events due to the re-use of storage that was not properly erased, or other factors.

2.3.7 System Management and Logging

Vendors must provide management tools for provisioning, configuration and operations management. Tools availability should be included in the Service Level Agreement (SLA) so an organization can properly manage their services. It is important that logging be provided so that unusual events can be properly investigated as the need arises. Cloud-based Email Security as a Service vendors will differentiate themselves by providing easy to use tools with powerful features for management, reporting and incident investigation.

3.0 Implementation Considerations and Concerns

Email security is a relatively mature field, but due to the ubiquitous nature of email, it is a common attack vector for malware and scams. Security as a Service vendors can use cloud scale and on-demand resources to analyze incoming email for malware and respond to fluctuations in mail message loads.

When evaluating cloud-based services for email security it is important to give due care and research into a number of different aspects of the service model, as described below.

3.1 Considerations

3.1.1 Multi-Tenancy

As with many cloud services, consideration should be given to how customer data is segregated in a multi-tenant environment. Cloud service providers should implement processes and technologies which prevent the interaction of customer environments. Vendors should implement controls which satisfy the requirements of an SSAE 16 audit. These audits provide customers with assurance that their data is properly safeguarded.

3.1.2 Portability

When choosing a vendor, the vendor's migration tools should be evaluated to ensure they provide the necessary capabilities. It is important that the vendor offer manageable methods to switch to the provider, switch between vendors, or switch back to an in-house service.

3.1.3 Programmatic Access

Vendors should provide a methodology for programmatic access to the email security system. Possibly, by leveraging a provider's Application Programming Interface (API), an organization can create tools which integrate the email and email security systems into existing workflows and monitoring capabilities. Programmatic access allows an organization great flexibility and enables very responsive on-demand features such as a fully automated workflow for provisioning and deprovisioning of users or services.

3.1.4 Self-Service

As much as possible, the services provided should encompass end-user self-service tools as well as administration tools. On-demand workloads enabled by cloud services work best when all users have the ability to create and extend the services. Such tools might be the creation of email lists or automatic forwarding of emails. Management controls should allow each organization to choose which features are offered to users, as different organizations may have different policies surrounding various capabilities.

3.1.5 Client Controls

Many vendors allow for centralized control of system features, particularly those features relating to security. For example, many smartphone email clients allow the email server to control the user's choices for screen lock passwords and remote data removal. It may be the policy of an organization that a user enable screen lock on their phone before receiving mail, or allow the email system to remove data ("remote wipe") from a phone that has been lost. These sorts of controls should be included features in an email security service offering.

3.1.6 Management and Monitoring

An email security service should provide features for management and operations. Management features include the ability to increase or decrease services, monitor loads and perform configuration changes, among others. The management toolset should allow the monitoring of traffic, current levels of malware and spam being detected and user patterns.

3.1.7 Integration

The cloud service vendor should integrate and allow integration of various subsystems. Subsystems include malware detection, spam protection, data loss prevention, content filtering, email encryption, monitoring and reporting. The ability to integrate other services into the email handling pipeline allows an organization to build a best of breed solution with the most effective tools available.

3.2 Concerns

There are a number of concerns or challenges to be solved when implementing email security. An organization's policies or regulatory environment may give rise to different choices to resolving the concerns below.

3.2.1 Data Security

Data should be secured at all times by the email service. Encryption should be used for data at rest, data in transit and data in use. Encryption keys should be retained by the organization and not the cloud provider. Protection of the data in only some stages of the data lifecycle does not adequately secure the data and leaves it vulnerable to attack.

3.2.1.1 Data at Rest

Encryption should be used to protect Data at Rest, i.e., data while stored in the email system or extended archival systems.

3.2.1.2 Data in Transit

Data in Transit includes data transiting from an end user endpoint computer (e.g., laptop) on the Internet to a web-facing email service provider in the cloud or amount various email system components (i.e. between the Mail Transfer Agent and an Email Anti-Virus filtering system provided by a Cloud-Based provider).

3.2.1.3 Data in Use

Data in Use refers to the actual processing of data in computer memory, in addition to on-screen display and presentation of data. It is common for systems that use encryption when storing or transmitting data to decrypt data for processing (e.g., searching or indexing). It is best practice to use algorithms and tools which limit the amount of data needing decryption for searching and indexing. These tools use tokenization or decrypt only key fields which increase the safeguards on the email data. Research algorithms for full searching of encrypted data offer more safeguards; fully homomorphic encryption remains in the future.

3.2.2 Regulatory Compliance

An organization which is covered by specific regulatory guidelines (such as a financial institution or a government agency) will need to ensure that the vendor's infrastructure and operational policies meet the imposed regulatory guidelines. This may eliminate certain vendors, or specific offerings from other vendors.

Of special note should be data retention requirements. If using a cloud service provider for email storage, the costs for archived data should be properly calculated. If costs become prohibitive or if the vendor has storage limits that prevent long term retention, a separate archiving solution must be considered which will change the economics of the cloud-based solution.

3.2.3 Data Disclosure

Ideally, there is a segregation of duties between the customer, which owns the data, and the Email Cloud Service Provider, which hosts and processes the data. For encrypted data, at any stage of the data lifecycle, the customer should retain control of the encryption keys. This principle of segregation, which renders the data hosted by the provider as useless cypher text, enables the customer to be involved in all cases in which the data is subpoenaed, as the keys to decrypting the data are held exclusively by the customer.

3.2.4 Data Residency

Regulatory Compliance leads to further challenges regarding Data Residency controls. When dealing with data that is covered by country or region specific regulations, the vendor may need to provide controls surrounding where data is stored or processed. In some cases, such as the European Union Data Protection Directive, the ability to access the data is considered processing. A vendor may have a data center in the European Union (EU), but if its administrators are located outside the EU, the vendor may still be in breach of the regulations.

In most cases, email messages should not be used by an organization as critical control points, such as formal sign-off for general ledger postings, etc. However, sensitive data may find their way into email messages (e.g., identified patient information). In this case, the possibility may require an organization to have greater control over data residency than a vendor is able to provide. This concern must be paramount when choosing an email security service vendor.

3.2.5 Identity

Identity services are a key concern when deploying an email system. Email systems typically have weak controls over the initiation of email messages, even though stronger protocols have been developed and are available. An organization should insist that all user facing features implement strong identity controls through the use of federated identity systems that integrate with the organization's primary identity policy.

3.2.6 Logging

Logging of system actions and errors is key to the proper operation of a system. When services are outsourced, operations logs typically are maintained by the vendor, which may make tracking down problems more difficult. Vendors should provide tools, where appropriate, to allow customers to search their usage logs. A good working relationship with the vendor and usage of cloud security gateways should help mitigate this concern.

3.2.7 Communications

The responsiveness of the security service is largely dependent on the speed of the organization's network connection and the latency of transmission to the vendor's infrastructure. When choosing a vendor, due diligence should be given to the need for adequate network connections to mitigate this concern.

4.0 Architecture and Implementation Steps

4.1 Architecture Overview

The architecture of an email system includes features for sending, receiving and storing email, as shown in figure 1. Users interact with a Mail User Agent (MUA) which is either a web User Interface (UI) or a Remote Client program provided by the mail hosting service. The MUA allows the reading and sending of email messages.

When the user sends an email message from the MUA, it goes to the Mail Submission Agent (MSA) which is provided by the mail hosting service. The MSA performs user authentication and message filtering actions. The filtering action might include data leak protection, malware protection and adding legal footers or disclaimers. The MSA then passes the email to the Mail Delivery Agent (MDA) which will route the email to recipients using Mail Exchange (MX) records from the Domain Name System (DNS). MX records provide information the MSA uses to send the message to the recipient's Mail Transfer Agent (MTA). Messages sent from other sources are sent to the mail hosting service MTA.

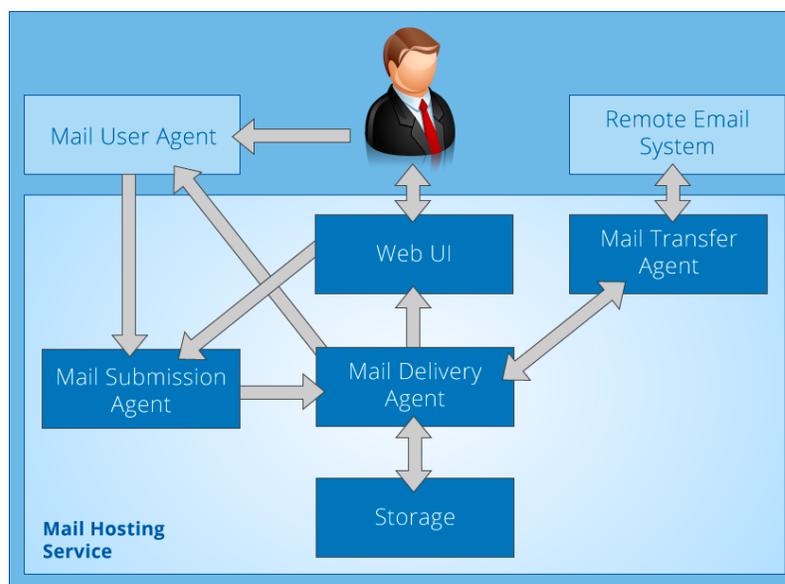


Figure 1: Email System

These components are used in common for any email system, whether cloud-based or traditional implementations.

A traditional email hosting provider typically provides service using an inelastic single tenant system which delivers services in large increments. A cloud service provider will offer a more elastic service using a multi-tenant system that allows for small increments of growth (and usage decrease).

In a fully outsourced solution, the cloud email security provider is responsible for everything inside the Mail Hosting Service. When the cloud email security provider delivers additional processing to an enterprise hosted email platform, there are integration details that require attention to ensure the security of the system.

4.1.1 Fully Outsourced Email Implementation

There are two types of cloud deployment models for fully outsourced email deployments: single-tenant/private cloud and multi-tenant.

Single-tenant systems provide the organization with its own database and its own instance of the software application. Placed on an individual server, or segregated via extensive security controls to create its own virtual server, organizations using single-tenant systems possibly enjoy the benefits of more product configurability and less risk to data mingling. However the single tenet system loose the benefits of cloud elasticity (as the vendor provisions for only one client and must have excess capacity allocate to meet future demands) and in the case of spam, malware and phishing protection, they lose the expanded insight a cloud vendor gains from the analysis and correlation across the traffic of many organizations.

Multi-tenant solutions perform the same functions for multiple companies on the same server at the same time, generally separating them from each other via a simple partition that prevents data from migrating from one company to another. Because they are running the same solution software, each of the companies is running the same application, with the common functionality and the same configuration capabilities.

In both of the fully outsourced cloud email security models, the email provider is responsible for end-to-end security of all components except for enterprise or end-user managed devices.

The email security provider should be responsible for the following key features:

- Identity management or integration to a Federated Identity solution
- Login security
- Anti-Malware prevention in incoming and outgoing email
- Spam filtering in incoming email
- Email archiving and preservation
- Continuity and disaster recovery

4.1.2 Email Security Cloud Augmentation to Premise Enterprise Implementations

Organizations which continue to maintain their email servers on premises can still recognize the benefits of the cloud by electing to utilize additional security features and functionalities supplied by third parties in the cloud. When using email security services to supplement an existing enterprise hosted implementation, the service might be built as shown in Figure 2.

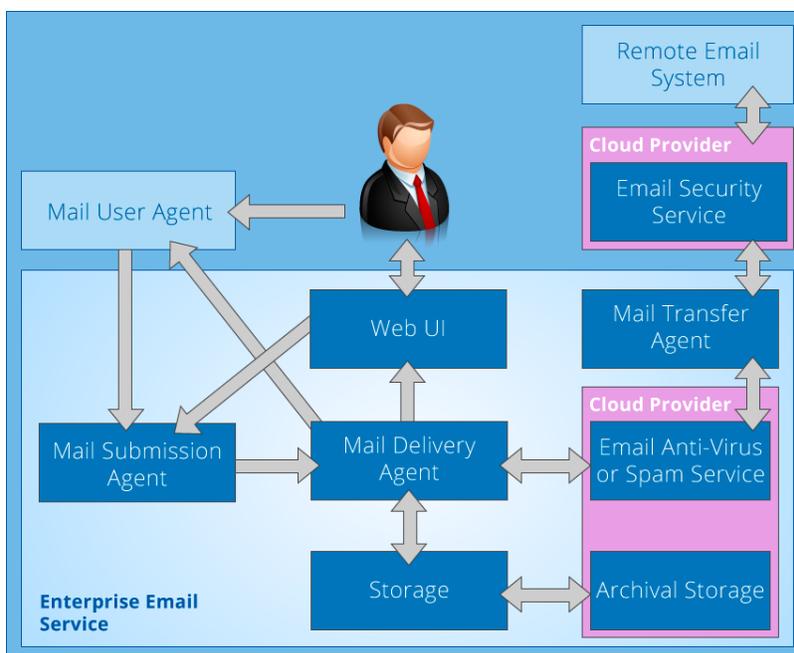


Figure 2: Enterprise Implementation Supplemented with Email Security Service

In this implementation, the services provided internally are depicted inside the blue box. The enterprise then supplements their service by interfacing with Email Security Service vendor systems which are shown as surrounded by the pink boxes.

Examples of such features include:

- **Anti-Malware Prevention** – Programs used to prevent, detect and remove malware, such as computer viruses, adware, backdoors, malicious BHOs, dialers, fraud tools, hijackers, key loggers, malicious LSPs, rootkits, spyware, Trojan horses and worms. This service may be applied to both incoming and outgoing email.
- **Identity Management** – Management of individual identities, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.
- **Login Security** – Individual access to a computer system controlled by identifying and authenticating the user by referring to credentials presented by the user.
- **Spam Filtering** - Inbound email filtering involving scanning messages from the Internet addressed to users protected by the filtering system. Outbound spam filtering to protect against compromised computers on the customer network, as well as the customer domain getting blacklisted by other spam filters.
- **Content Filtering** – Allowing the customer to create custom rules based on who sends what to whom. Allows an organization to provide greater controls over the balance of email not identified as malicious or unwanted.

- **Reporting** – Allows the customer to have visibility into their mail flow. Also provides the tools needed by customer administrators to trace or search for email messages as part of their support workflow.
- **Encryption** – The process of transforming information (plaintext) using an algorithm (cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Solutions exist for encryption of data at-rest, in-use and in-transit of all email messages & attachments. Encryption keys should be retained by the organization and not the cloud provider.
- **Archiving and Preservation** – A systematic approach to saving and protecting the data contained in email messages so it can be accessed quickly at a later date.
- **Business Continuity and Disaster Recovery** – Services that enhance an organization's ability to recover from a disaster and/or unexpected event, and resume or continue operations.

4.2 Guidance and Implementation Steps

The security of the overall email system, whether fully outsourced or enterprise hosted and augmented with security services, is driven first by securing the individual components to industry standards and organizational policy.

4.2.1 Client Security

In order to provide appropriate security measures, a cloud-based provider should offer, at a minimum, the following security mechanisms:

- **End-point Encryption** – Starting with the general user interface or access, ensure the end point delivery is secured via encryption protocols.
- **Security Protocols** – Mail clients use industry standard protocols to access email such as POP3 and IMAP. Encrypted versions of these protocols (POP3S and IMAPS) use Transport Layer Security (TLS, also call SSL3) which allows for session negotiation of encryption algorithm and length of key. Negotiation options can be limited on the server side and should be configured to prevent use of weak keys or older algorithms.
- **Encrypted Protocols** – When using a web-based UI, it is important that HTTP traffic use TLS (i.e., HTTPS).
- **Encrypted API Protocol** – An Ajax style web UI may access server APIs, so APIs must be accessed using HTTPS as well.
- **Session Timeouts** – User sessions should have session timeouts that limit access to data.
- **Usage Policies** – Users should be advised against the use of email on public computers such as airport kiosks or public libraries, as message text or login information may be cached on such machines. Recommend users avoid these computers altogether, or not open or download sensitive emails. As a minimal requirement, they should log out when finished.

4.2.1.1 Mobile Devices

Mobile devices such as tablets and smart cell phones have other security problems. While they are very convenient and allow 24/7 access to email, their design presents difficulties for the email administrator. Because they are carried on a person, there are physical security issues. The user's password is saved on the

device permanently. This provides quick, easy access to email, but offers significant security challenges. Since such devices are easily lost, stolen or left unattended, end point security easily can be compromised.

To mitigate security concerns, phones should be secured with a PIN to unlock. Some devices offer a central administrator the option to require certain security options before mail will be delivered to the device. Common options are “require PIN for unlock” and “allow remote wipe commands.”

When the client is displaying email, the UI should be able to identify mail that has originating security features, such as valid Domain Key Identified Email (DKIM) or questionable email that has been marked as suspicious or does not meet Sender Policy Framework (SPF) inspection. Indicators that mail has DKIM or other attributes should be easily visible in the UI, whether the UI is on a smart phone, personal computer, tablet or other user interface.

4.2.2 Administration

In an enterprise hosted environment, features for central administration are inherent in the products chosen by the organization’s mail administrator. In cloud-hosted scenarios, these administration features are a critical differentiator among cloud-based vendors. Vendors should strive to provide a suite of effective tools for use by mail administrators.

4.2.3 Submission End-Point, the Mail Submission Agent

The Mail Submission Agent is the portion of the system that accepts email messages from users and prepares them to send, either within the organization or outside. Upon initial receipt of email from an internal user, the identity of that user should be verified using the extended SMTP protocol, ESMTP. Key to the secure use of ESMTP is use of options for both encryption with TLS and for sender authentication. TLS options, when well chosen, should prevent the use of weak keys and older algorithms.

The mail submission agent should require strong user authentication to prevent abuse of the mail system. User authentication can be configured to require a username and password, or use the exchange of credential tokens from a service such as Kerberos.

The use of a mail submission agent can also implement restriction of email according to a sender policy framework and by requiring user authentication prior to accepting messages for transmission.

The configuration system should allow for the creation of organization wide automatic compliance message footers which are added to the bottom of each message so outbound messages adhere to corporate notification policies.

4.2.4 Mail Delivery Agent

The mail delivery agent is used for email that either is originating in the email system or incoming email destined for this email system. The bulk of security is usually provided by this module. It can be configured to interact

with a variety of other services to support different types of security functions, such as filtering or message encryption.

A key filtering sub-module is an antivirus filter. A common form of malware propagation is via email, so an antivirus filter is one of the first items to configure in the Mail Delivery Agent. When using a cloud-based filtering service, there are a number of key considerations.

- Incoming mail should be transmitted to the service provider with a secure protocol such as TLS. The provider system will return results to the email system for it to act upon. Performance of the filtering service will be affected by the speed of the connection, the connection latency and the capacity of the service provider.
- The use of a spam filter is similar to the antivirus filter. Limiting spam is an excellent way to increase workplace efficiency by reducing the amount of useless email arriving in the organization's mailboxes. In addition, spam often will attempt to direct users to websites with malware.
- Use of a cloud-based service provider is effective in reducing spam because the provider will see email from multiple organizations and correlate spam messages across them in real time. The more often a spam filtering service sees a given set of spam emails, the more effective their heuristic algorithms will become, often in real-time as the spam propagation ramps-up.
- Message and results traffic to the provider should be encrypted using TLS.
- Performance will be affected by the speed of the connection, the connection latency and capacity of the service provider.

4.2.5 Mail Transfer Agent

The mail transfer agent is the mail system's interface to the outside world. Receipt of external email uses MX records in the organization's DNS configuration. Organizations typically will point their MX records to a service provider system when either using a fully outsourced implementation or when using a service provider to protect against denial of service (DoS) attacks. Cloud-based vendors can add capacity and filtering capability on-demand to react to changes in the threat landscape.

It is common for enterprise hosted platforms to configure a vendor's systems for spam and malware filtering as their Mail Transfer Agent in front of their internal mail system. In this case, the MX records for the organization will refer to the vendor's system. The service provider then receives all messages directly from outside parties and can respond on-demand to increased spam, malware and DoS events with minimal effect on the internal mail system. Message that pass the filtering criteria are then passed onto the organization's existing enterprise email system.

4.2.6 Mail Storage

Email messages may be or include key business correspondence and documentation. Proper care needs to be given to their proper management. Email represents "data at rest" and needs to be properly protected. When using a cloud email storage provider, this data at rest should be stored in encrypted form. The storage provider will typically use a "multi-tenant" storage model, where data from multiple organizations are co-mingled on

storage devices. This makes encryption of the each organization's data much more critical. The encryption keys for the stored email should be held only by the customer, or by an escrow agent which is not the cloud storage provider.

Traditionally, when data was stored in encrypted form, common features such as searching and indexing were limited or impossible. With the traditional method, the need for decryption or transfer of data could increase the time needed for processing, and add to data transfer costs.

Technologies such as tokenization and Format Preserving Encryption (FPE) enable the capability to perform basic server side operations over encrypted text. These technologies have been brought to the market in recent years, and are commercially available for adoption. As a best practice, organizations should adopt those technologies that allow sorting and searching, while reducing the amount of data needing to be decrypted. In recent years, homomorphic encryption algorithms have been developed which allow for basic operations on encrypted data. Full commercialization of homomorphic encryption remains in the future.

Email, as with all business documents, have a limited lifetime which should be defined by the organization. After the documents have reached their intended lifetime, they should be destroyed. A cloud service provider should provide guarantees that deleted data is truly overwritten and destroyed. When data is stored in encrypted format, mere destruction of the encryption keys are not enough, as algorithms weaken over time and data that was once "un-decryptable" may later fall within the reach of more computation power or a discovered failure in the algorithm or implementation.