EMAIL SECURITY HEALTH CHECK REPORT

MicroAge®

The Digital Transformation Experts®

Email Security Health Check Report

TABLE OF CONTENTS

OVERVIEW AND CONTACTS.....3

1. EXECUTIVE SUMMARY DASHBOARD 4
2. ACCOUNT REVIEW 5
3. SERVICES REVIEW..... 10
4. DIRECTORIES REVIEW 10
5. GATEWAY REVIEW 14
6. ACCOUNT ASSESSMENT OVERVIEW..... 16
7. SECURE EMAIL GATEWAY..... 18
8. URL PROTECT 26
9. ATTACHMENT PROTECT..... 29
10. IMPERSONATION PROTECT 34
11. UNUSED OR DISABLED FEATURES SUMMARY.... 37
12. ADDITIONAL INFORMATION..... 38
13. MANAGEWISE EXPRESS OVERVIEW 43
14. END OF DOCUMENT 45

MicroAge® The Digital Transformation Experts® | cStor®

OVERVIEW AND CONTACTS

The following is an Email Security Health Check Report for the month of August, prepared for CLIENT on 8/26/22.

CLIENT has enlisted MicroAge for a Mimecast ManageWise Silver Service. See the Mimecast ManageWise Overview for Service details.

Contact Information (*Contact Information Redacted for Privacy*)

CLIENT
STREET
CITY, STATE ZIP
United States

Main Office PHONE NUMBER

CLIENT Contact
IT Manager: CLIENT NAME
Phone: PHONE NUMBER
Email: EMAIL ADDRESS

MicroAge Contacts
Account Manager: NAME
Solutions Architect: NAME
Project Coordinator: NAME
Engineer: NAME
Engineer: NAME

1. EXECUTIVE SUMMARY DASHBOARD

Please see below for Mimecast environment details based upon your ManageWise Silver **Discovery, Assessment, and Health Check** service engagement.

Account and Support Details

Customer Details

Customer Name	REDACTED
Mimecast ID	
Account Code	
Database Code	

Support Details

Support Information	Click here for support contact details and best practice information
Support Package	Advanced

Product Details

Main Product	2017 Mimecast M3RA
Retention	Perpetual
Retention Validated	Yes
Licensed Users	843
Renewal Date	30 Mar 2023

Key Contacts

Reseller/Partner/MSP	REDACTED
Customer Success Manager	
Customer Development Manager	
Phone	

2. ACCOUNT REVIEW

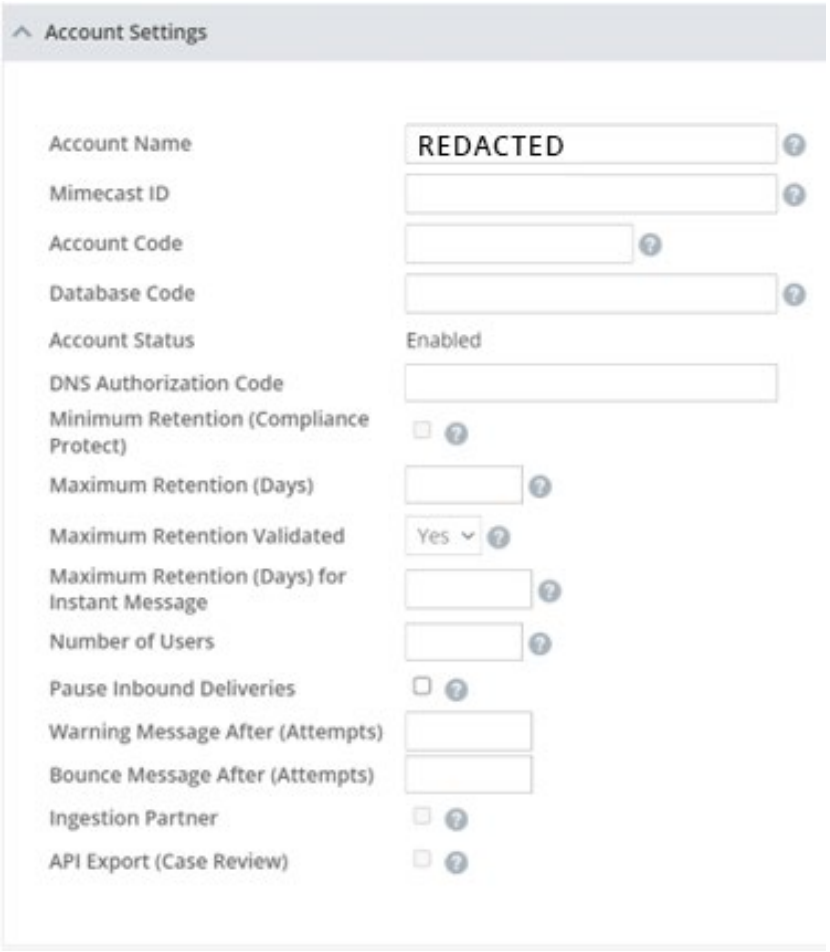
An **Account Review** has yielded the following Observations and Recommendations located in this section.

The Account Review is focused around the following areas:

- **Account Settings**
- **User Access and Permissions**
- **Password Complexity and Expiration**
- **Roles**

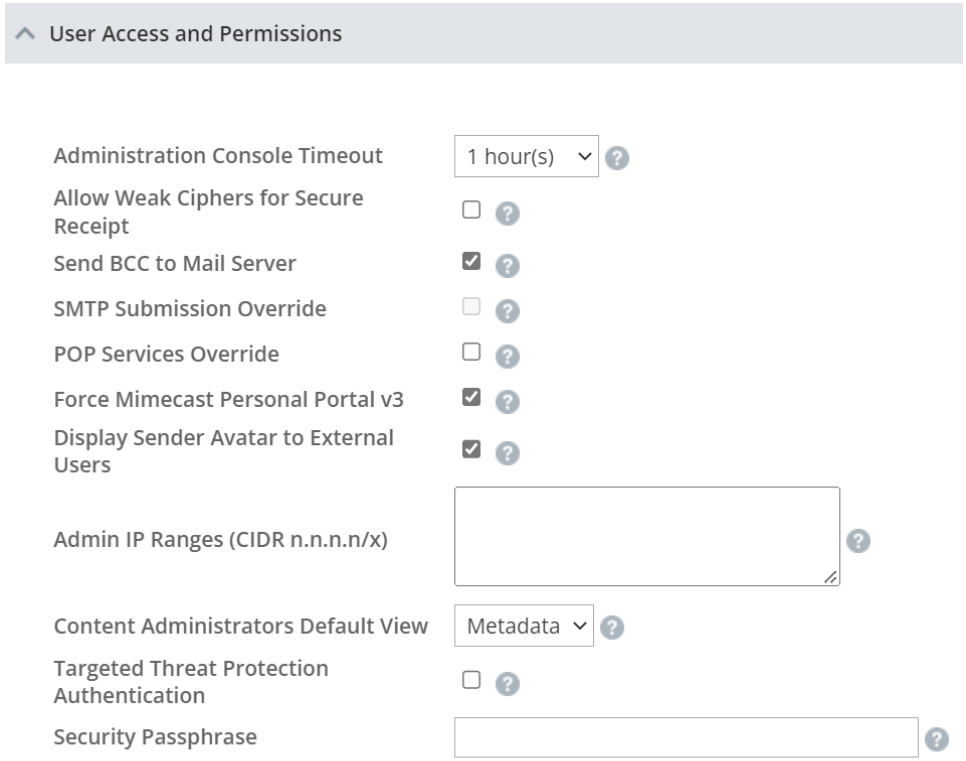
Account Settings > Account Settings
FINDINGS:

RECOMMENDATIONS: None



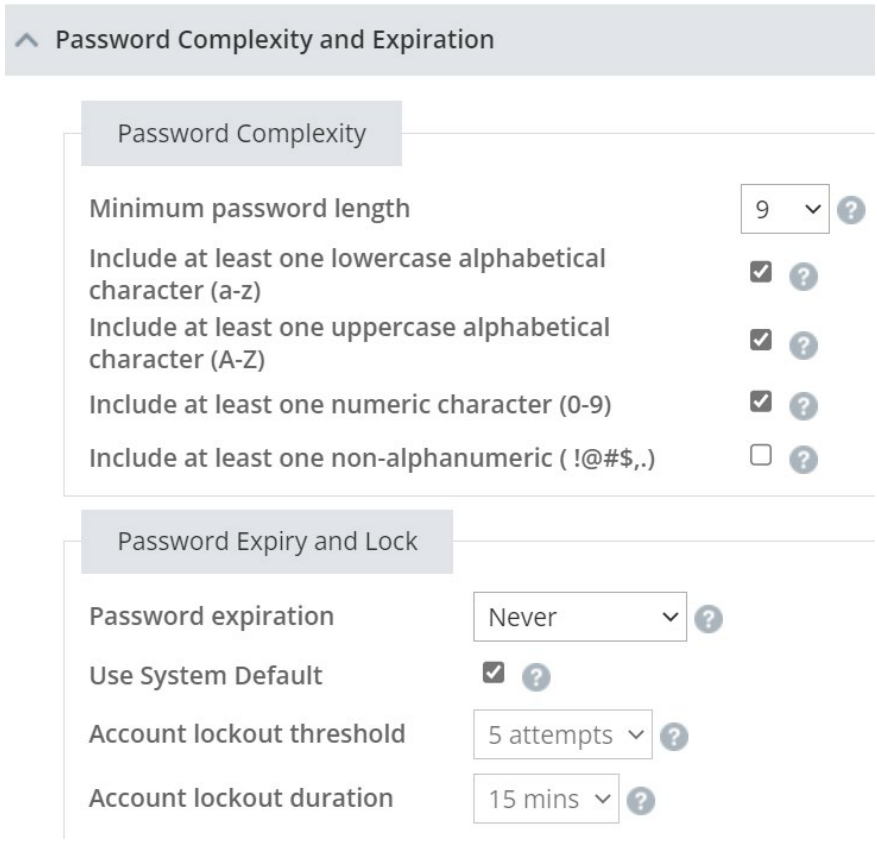
Account Settings > User Access and Permissions
FINDINGS:

RECOMMENDATION 1 (Optional): Client has MFA configured for Admins as a compensating control, best practice is to restrict admin access to IP Ranges to secure access to admin portal per business policy.
RECOMMENDATION 2 (Optional): Add Security Passphrase for added layer of security.
RECOMMENDATION 2 (LOW): Enable TTP Authentication and set timeout period of 30 days.



Account Settings > Password Complexity and Expiration
FINDINGS:

RECOMMENDATION (LOW): Add the option to include at least one non-alphanumeric character to password.



3. SERVICES REVIEW

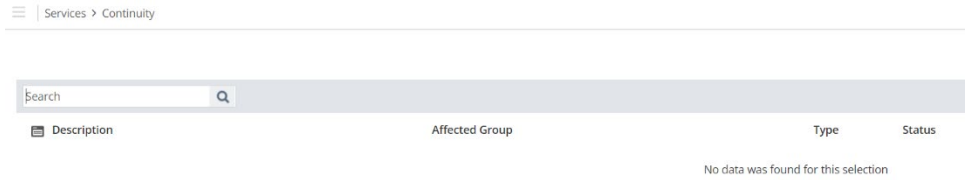
A **Services Review** has yielded the following Observations and Recommendations located in this section. The Services section covers the connectors to Mimecast and features enabled along with usage.

The Services Review is focused around the following areas:

- **Continuity**
- **Exchange Sync & Recover**

Services > Continuity
FINDINGS: Continuity not setup

RECOMMENDATION (Med): Setup Continuity to ensure High Availability



Services > Exchange Sync & Recover

FINDINGS: o365 sync & recover PHX OU > 8 Mailboxes have sync errors

o365 sync & recover TUS OU > 1 Mailbox has sync error

RECOMMENDATION (low): Resolve Sync errors

Server Connection	Task Name	Group	Status
O365 Sync and Recover	O365 Sync and Recover PHX OU	PHX	Enabled with errors
O365 Sync and Recover	O365 Sync and Recover TUS OU	TUC	Enabled with errors

4. DIRECTORIES REVIEW

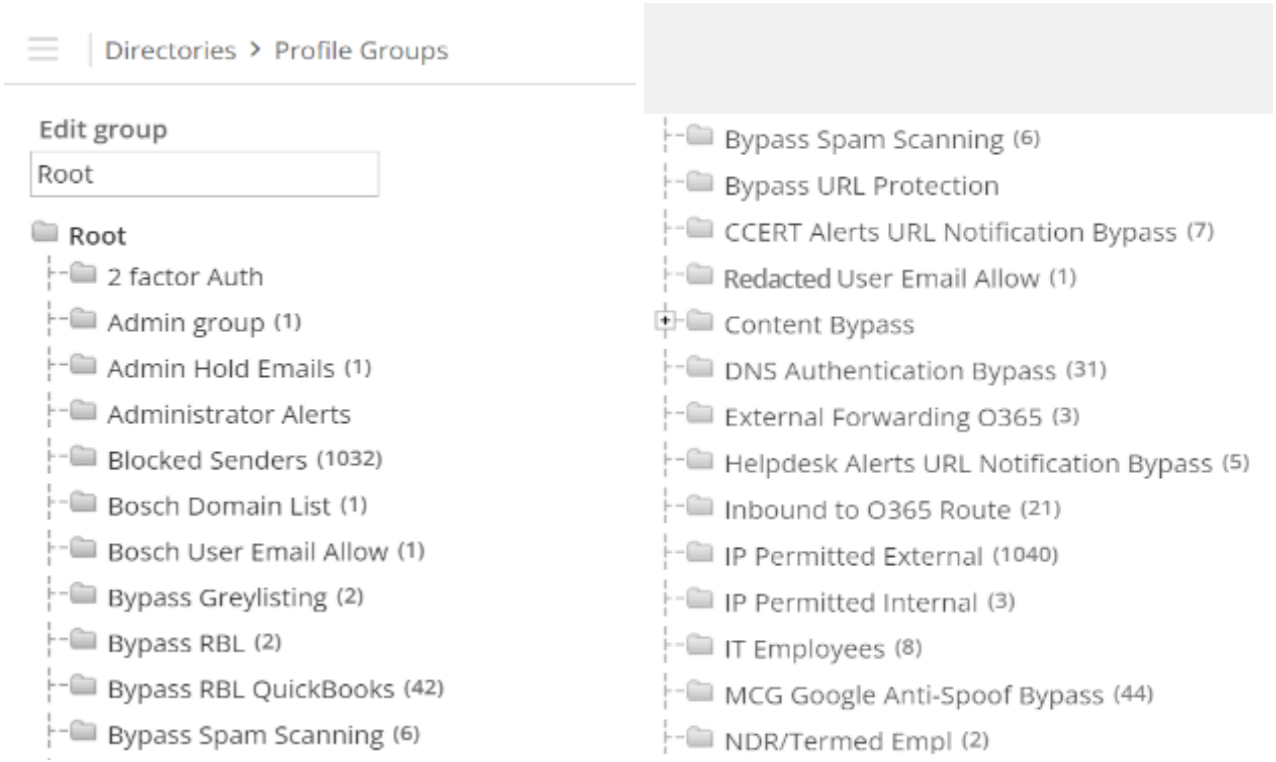
A **Directories Review** has yielded the following Observations and Recommendations located in this section. The Directories section covers both local and connected users and groups used in Mimecast for administration and policies

The Directories Review is focused around the following areas:

- **Profile Groups**

Directories > Profile Groups
FINDINGS: Reviewed all groups

RECOMMENDATION (LOW): Utilize folder for easier use with policies, expanded information in policy section.



5. GATEWAY REVIEW

A **Gateway Review** has yielded the following Observations and Recommendations located in this section. The Gateway section manages all security policies for Mimecast through authorized and unauthorized users and policies.

The Gateway Review is focused around the following areas:

- **Policies**

Policies

Gateway > Policies > all
FINDINGS: Verify IP's, Domains and review disabled policies
RECOMMENDATION: Review 139 Policies (Low Priority)

For all policies, please review the supporting documentation (CLIENTPolicies.xlsx)

6. ACCOUNT ASSESSMENT OVERVIEW

An **Account Assessment** was conducted based on available Mimecast data from August 1, 2022, to August 31, 2022.

The Mimecast Account Assessment is focused around the following areas:

- **Headline Statistics**
- **Secure Email Gateway**
- **URL Protection**
- **Attachment Protect**
- **Impersonation Protect**
- **Web Security**

At a Glance

Headline Statistics

mimecast

7. SECURE EMAIL GATEWAY

Mimecast Secure Email Gateway protects organizations and employees from spear-phishing, malware, spam, and zero-day attacks by combining innovative applications and policies with multiple detection engines and intelligence feeds to keep sophisticated attackers out.

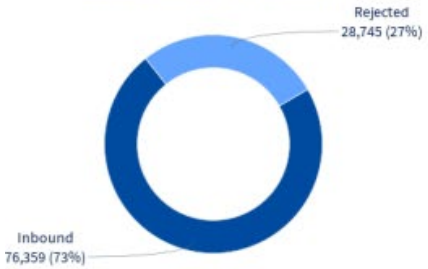
Secure Email Gateway Highlights

Inbound SMTP Overview

Secure Email Gateway

mimecast

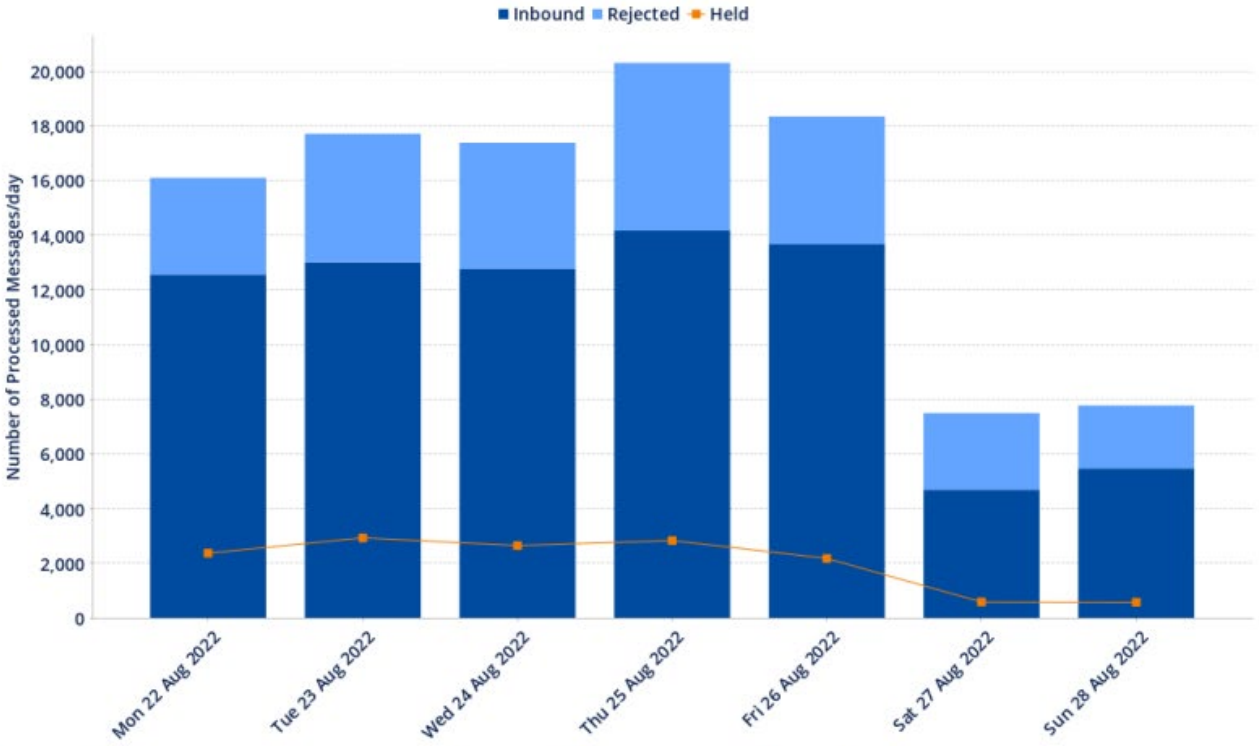
Inbound Messages by Outcome



Inbound SMTP Mail Delivered per Day

105,104 total messages processed

17,968 average messages/weekday



The volume of inbound routed messages delivered by Mimecast to internal recipients, grouped by outcome. Where a message is addressed to multiple recipients, the counts increments (+1) for each recipient.

Top Inbound Non-TLS Sender Domains

mimecast

Secure Email Gateway

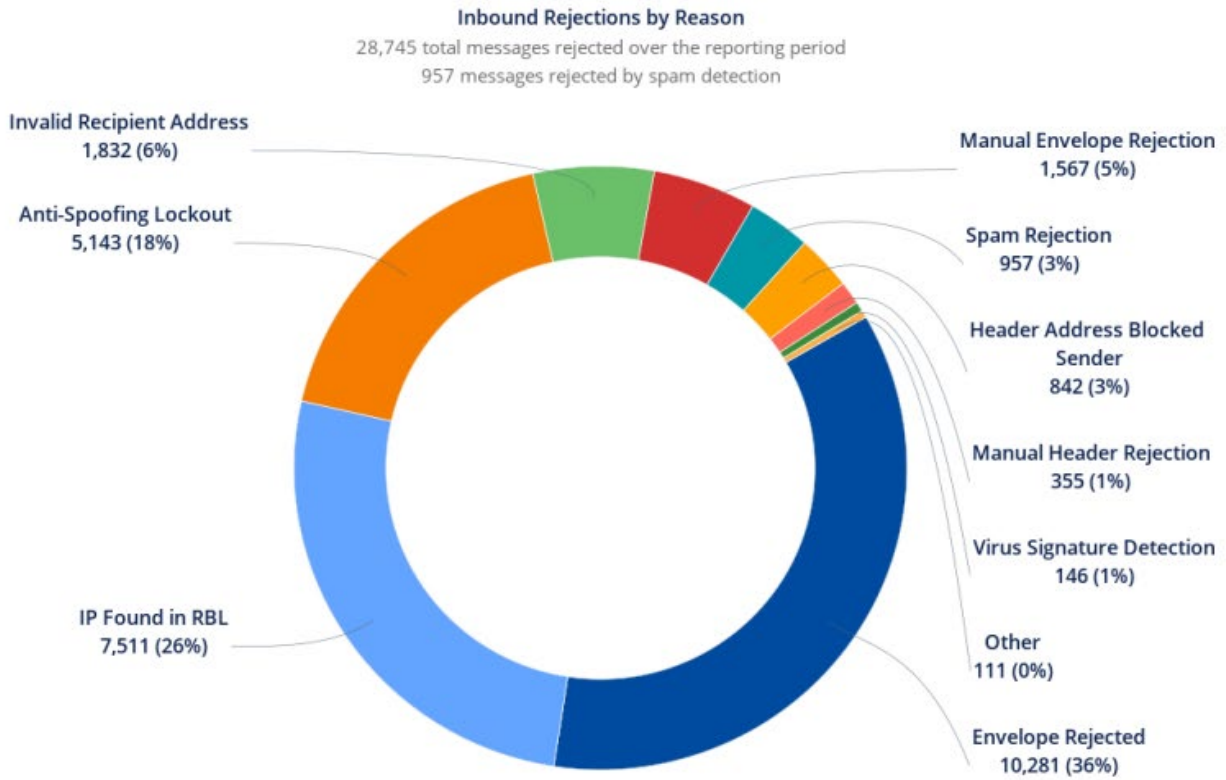
Rank	Domain	Mail Count
1	[redacted]	402
2	[redacted]	254
3	[redacted]	212
4	[redacted]	79
5	[redacted]	69
6	[redacted]	64
7	[redacted]	59
8	[redacted]	47
9	[redacted]	46
10	[redacted]	44
11	[redacted]	41
12	[redacted]	36
13	[redacted]	36
14	[redacted]	33
15	[redacted]	29
16	[redacted]	27
17	[redacted]	27
18	[redacted]	23
19	[redacted]	23
20	[redacted]	21

This table is intended to help you identify the top 3rd party domains which send mail without negotiating TLS.

Inbound Rejections

Secure Email Gateway

mimecast

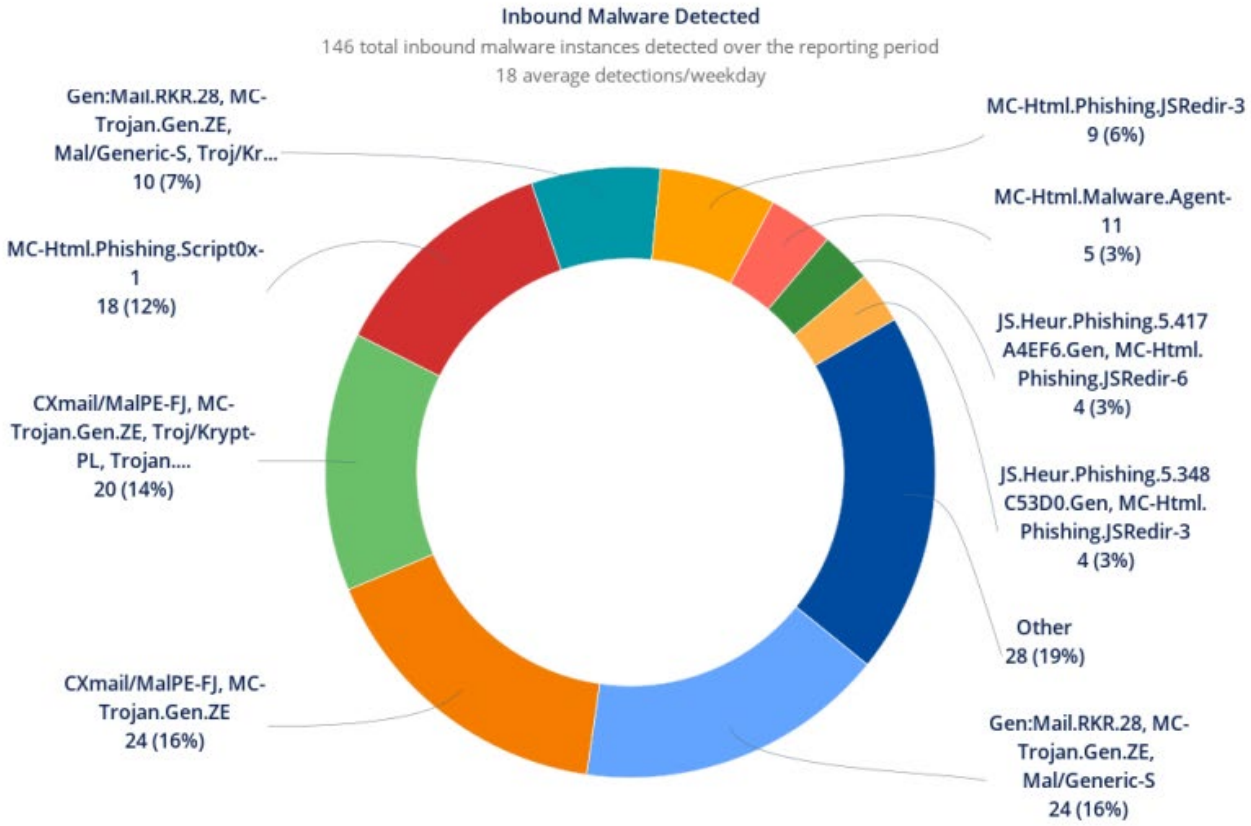


The distribution of rejection reasons for the rejections shown in the Inbound SMTP Overview chart. The count increments (+1) for each recipient. Excludes temporary errors and failed connection attempts. Recent logs can be found in the Administration Console under Message Center - Rejected and Deferred.

Top Inbound Malware

Secure Email Gateway

mimecast



The distribution of malware detected in inbound mail. The count increments (+1) for each recipient. Details about the Malware Detections can be found in the Threat Dashboard.

Outbound SMTP Overview

Secure Email Gateway

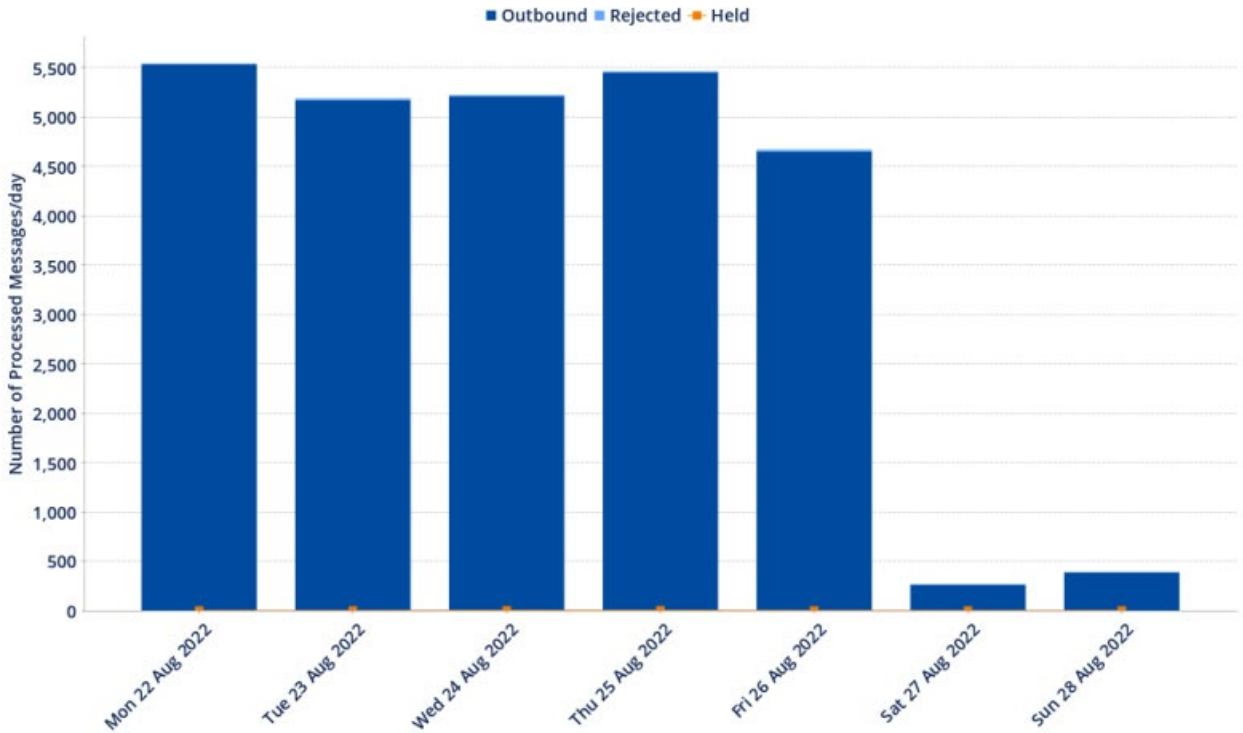
mimecast

Outbound Messages by Outcome

Outbound SMTP Messages Delivered per Day

26,760 total messages processed

5,220 average messages/weekday



The volume of outbound messages delivered by Mimecast to external recipients, grouped by outcome. Where a message is addressed to multiple recipient, the counts increments (+1) for each recipient.

Top Outbound Non-TLS Recipient Domains

mimecast

Secure Email Gateway

Rank	Domain	Mail Count
1	[redacted]	53
2	[redacted]	28
3	[redacted]	17
4	[redacted]	16
5	[redacted]	14
6	[redacted]	13
7	[redacted]	13
8	[redacted]	13
9	[redacted]	13
10	[redacted]	12
11	[redacted]	11
12	[redacted]	11
13	[redacted]	11
14	[redacted]	10
15	[redacted]	10
16	[redacted]	10
17	[redacted]	9
18	[redacted]	9
19	[redacted]	8
20	[redacted]	7

This table is intended to help you identify the top 3rd party domains which have accepted mail without TLS encryption.

Top Attachment Types

Secure Email Gateway

mimecast

Rank	File Type	Total Size
1	Acrobat	16.6 GB
2	Image	1.7 GB
3	Compressed Archive	1.0 GB
4	Microsoft Word	618.3 MB
5	Microsoft Excel	179.1 MB
6	Microsoft PowerPoint	104.8 MB
7	Video	44.0 MB
8	Other	28.4 MB
9	Binary File	23.3 MB
10	Text File	19.1 MB
11	Rich Text File	11.8 MB
12	Drawing	8.4 MB
13	HTML File	7.6 MB
14	Microsoft Office	6.4 MB
15	Audio	6.3 MB
16	Electronic Mail	3.8 MB
17	MatLab	2.1 MB
18	Calendar File	1.0 MB
19	Electronic Business Card	187.1 kB
20	Open Office Document	24.3 kB

The cumulative size of files processed by Mimecast in this period, grouped by file type. The file types shown are derived from common MIME types, aggregated for easier reading.

8. URL PROTECT

Targeted Threat Protection - **URL Protection** is an advanced Mimecast service, that builds on the security gateway services to protect your organization against the growing threat posed by advanced phishing and spear phishing attacks in inbound mail. It works by rewriting all URLs in inbound messages.

URL Protect Highlights

URL Clicks

URL Protect

mimecast

URL Clicks by Outcome

Benchmark comparison vs others within your:

Region

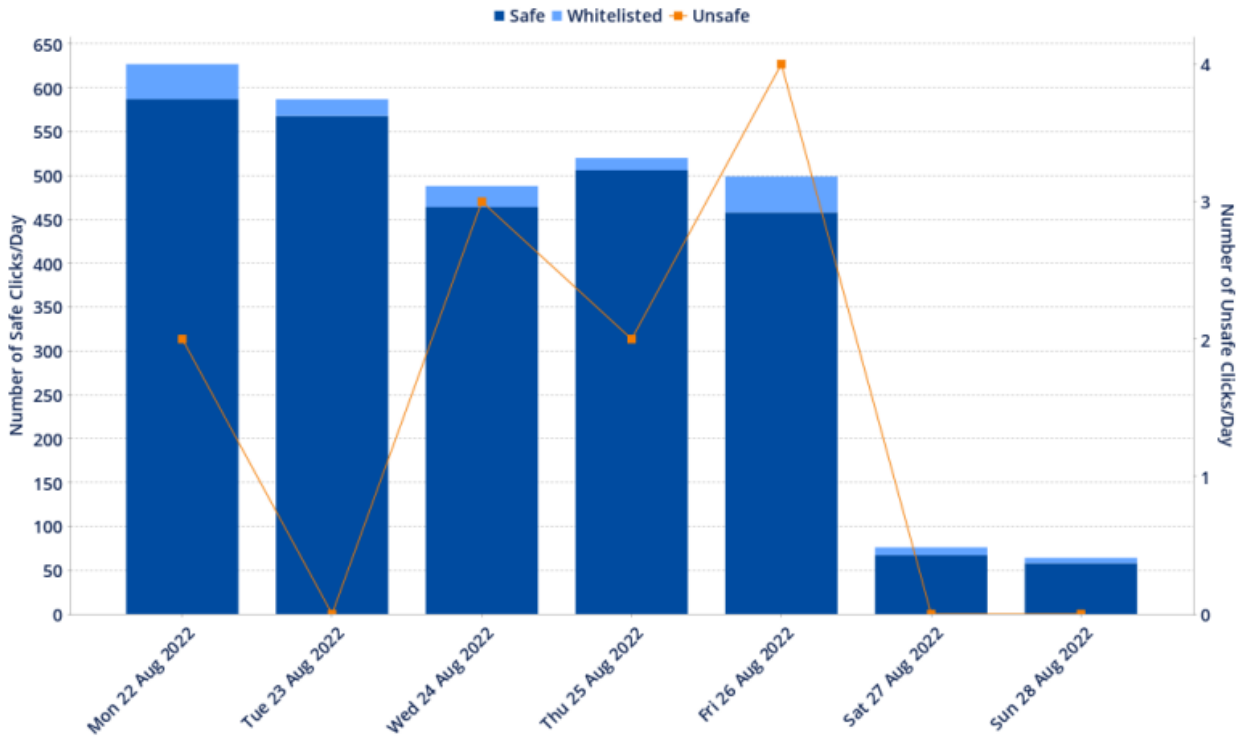
Industry

Size

Number of Safe (bars) and Unsafe (line) URL Clicks per Day

2,872 clicks analyzed; 11 unsafe clicks detected

In this period, 1 in 261 clicks were unsafe



The number of URL clicks per day by outcome. Unsafe clicks are charted on a second axis with a smaller scale for easier reading. The benchmarking charts show how your business compares with other Mimecast customers. The calculation is based on the total number of unsafe URL clicks detected per user across the same reporting period for comparable organizations, identified by industry, region and size.

Top URL Clickers by Severity and Volume

URL Protect

mimecast

User	Safe Count	Unsafe Count	Total	Unsafe Click Rate
[redacted]	17	3	20	1 in 7
[redacted]	2	1	3	1 in 3
[redacted]	5	1	6	1 in 6
[redacted]	1	1	2	1 in 2
[redacted]	6	1	7	1 in 7
[redacted]	2	1	3	1 in 3
[redacted]	3	1	4	1 in 4
[redacted]	4	1	5	1 in 5
[redacted]	1	1	2	1 in 2
[redacted]	62	0	62	
[redacted]	56	0	56	
[redacted]	47	0	47	
[redacted]	45	0	45	
[redacted]	43	0	43	
[redacted]	42	0	42	
[redacted]	37	0	37	
[redacted]	36	0	36	
[redacted]	35	0	35	
[redacted]	30	0	30	
+534 Other Users	2,387	0	2,387	
Grand Total	2,861	11	2,872	1 in 261

The most active URL-clicking users in this period, by outcome. Ordered by descending incidence of unsafe clicks and then by overall clicks.

9. ATTACHMENT PROTECT

Mimecast Targeted Threat Protection – **Attachment Protect** provides a layered defense against malicious email attachments by combining static file analysis, instant safe file previewing, and next generation attachment sandboxing for advanced protection from spear-phishing and other targeted email attacks.

Attachment Protect Highlights

Attachment Protect Sandboxing

Attachment Protect

mimecast

Sandboxed Attachments by Outcome

Benchmark comparison vs others within your:

Region

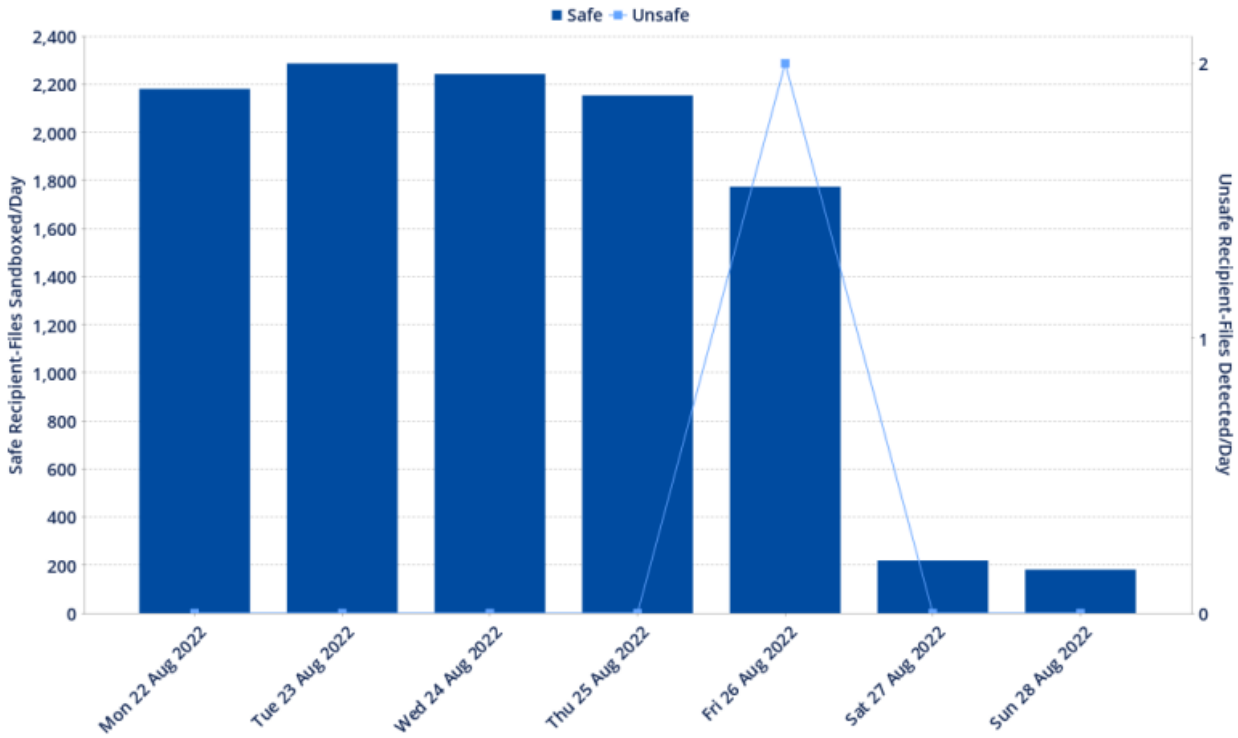
Industry

Size

Number of Safe (bars) and Unsafe (line) Sandboxed Attachments per Day

11,041 attachments sandboxed; 2 unsafe attachments detected

In this period, 1 in 5,520 attachments were unsafe



The number of sandboxed attachments per day by outcome. Unsafe attachments are charted on a second axis with a smaller scale for easier reading. The benchmarking charts show how your business compares with other Mimecast customers. The calculation is based on total unsafe attachments per user across the same reporting period for comparable organizations, identified by industry, region and size.

Sandboxed File Types

Attachment Protect

mimecast

File Type	Safe Count	Unsafe Count	Total	Unsafe File Rate
Acrobat	9,125	2	9,127	1 in 4,564
Microsoft Excel	751	0	751	
Other	514	0	514	
Microsoft Word	427	0	427	
Text File	127	0	127	
Compressed Archive	60	0	60	
Rich Text File	14	0	14	
Microsoft PowerPoint	13	0	13	
Electronic Mail	5	0	5	
Open Office Document	3	0	3	
Grand Total	11,039	2	11,041	1 in 5,520

Top Sandbox Filenames by Severity and Volume

Attachment Protect

mimecast

Filename	Safe Count	Unsafe Count	Total	Unsafe File Rate
[redacted]	0	1	1	1 in 1
[redacted]	0	1	1	1 in 1
[redacted]	43	0	43	
[redacted]	43	0	43	
[redacted]	41	0	41	
[redacted]	31	0	31	
[redacted]	24	0	24	
[redacted]	24	0	24	
[redacted]	19	0	19	
[redacted]	16	0	16	
[redacted]	16	0	16	
[redacted]	14	0	14	
[redacted]	14	0	14	
[redacted]	14	0	14	
[redacted]	14	0	14	
[redacted]	14	0	14	
[redacted]	14	0	14	
[redacted]	14	0	14	
[redacted]	13	0	13	
+6,417 Other Filenames	10,671	0	10,671	
Grand Total	11,039	2	11,041	1 in 5,520

The most common filenames encountered by our sandboxes, by outcome. Ordered by descending incidence of unsafe files and then by overall volume.

Top Sandbox Users by Severity and Volume

mimecast

Attachment Protect

User	Safe Count	Unsafe Count	Total	Unsafe File Rate
[redacted]	31	1	32	1 in 32
[redacted]	21	1	22	1 in 22
[redacted]	790	0	790	
[redacted]	188	0	188	
[redacted]	114	0	114	
[redacted]	109	0	109	
[redacted]	107	0	107	
[redacted]	98	0	98	
[redacted]	89	0	89	
[redacted]	81	0	81	
[redacted]	74	0	74	
[redacted]	74	0	74	
[redacted]	74	0	74	
[redacted]	72	0	72	
[redacted]	71	0	71	
[redacted]	69	0	69	
[redacted]	66	0	66	
[redacted]	66	0	66	
[redacted]	65	0	65	
+750 Other Users	8,780	0	8,780	
Grand Total	11,039	2	11,041	1 in 5,520

The most targeted recipients of files submitted for sandboxing by outcome. Ordered by descending incidence of unsafe volume and then by overall volume.

10. IMPERSONATION PROTECT

Impersonation Protect is an advanced email security technology that protects employees against targeted social engineering attacks in email, often called whaling or CEO Fraud. Backed by comprehensive protection from Mimecast's threat intelligence infrastructure and Messaging Security teams.

Impersonation Protect Highlights

Impersonation Protect Detections

Impersonation Protect

mimecast

Impersonation Detections by Outcome

Benchmark comparison vs others within your:

Region

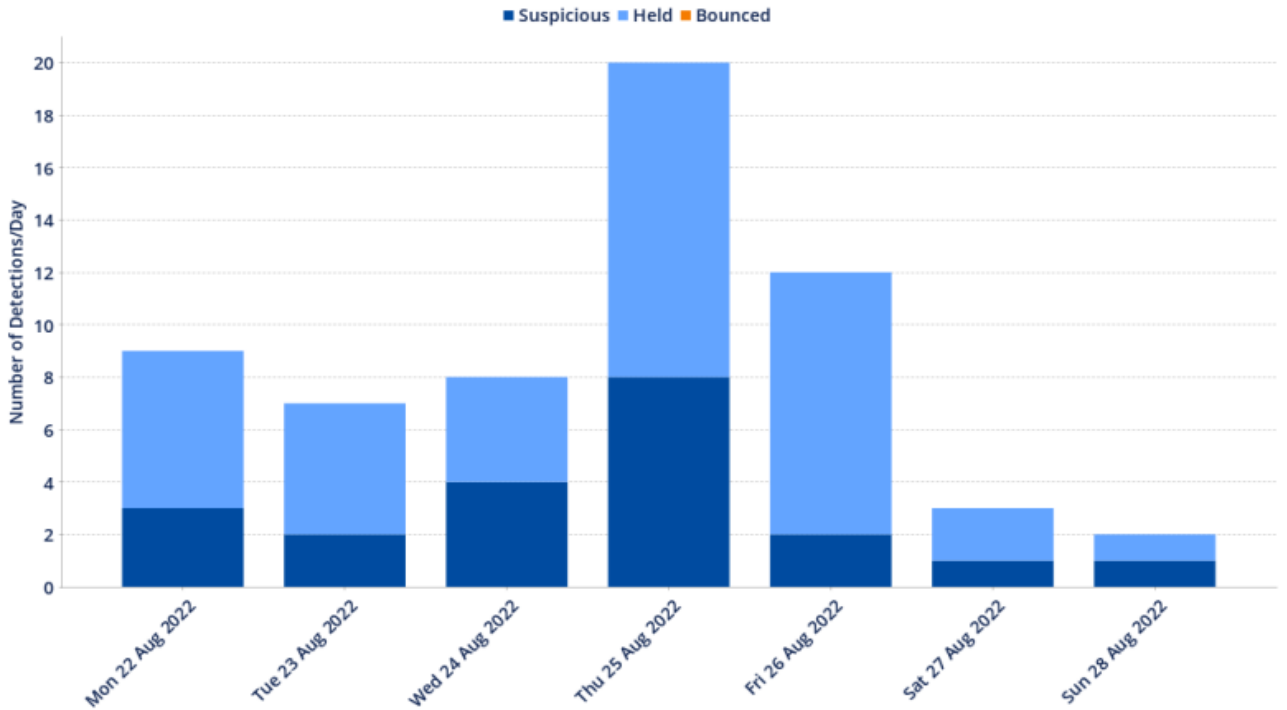
Industry

Size

Detections by Impersonation Protect per Day

61 total messages detected

11 average messages/weekday



The count of messages which trigger at least one Impersonation Detect policy. If these numbers are unexpectedly high or low then we recommend you review your Policy Definitions. The benchmarking charts show how your business compares with other Mimecast customers. The calculation is based on the total number of impersonation detections per user across the same reporting period for comparable organizations, identified by industry, region and size.

Top Impersonation Protect Targets

Impersonation Protect

mimecast

Rank	Recipient	Mail Count
1	[redacted]	4
2	[redacted]	4
3	[redacted]	4
4	[redacted]	3
5	[redacted]	3
6	[redacted]	2
7	[redacted]	2
8	[redacted]	2
9	[redacted]	2
10	[redacted]	2
11	[redacted]	1
12	[redacted]	1
13	[redacted]	1
14	[redacted]	1
15	[redacted]	1
16	[redacted]	1
17	[redacted]	1
18	[redacted]	1
19	[redacted]	1
20	[redacted]	1

End of Account Assessment

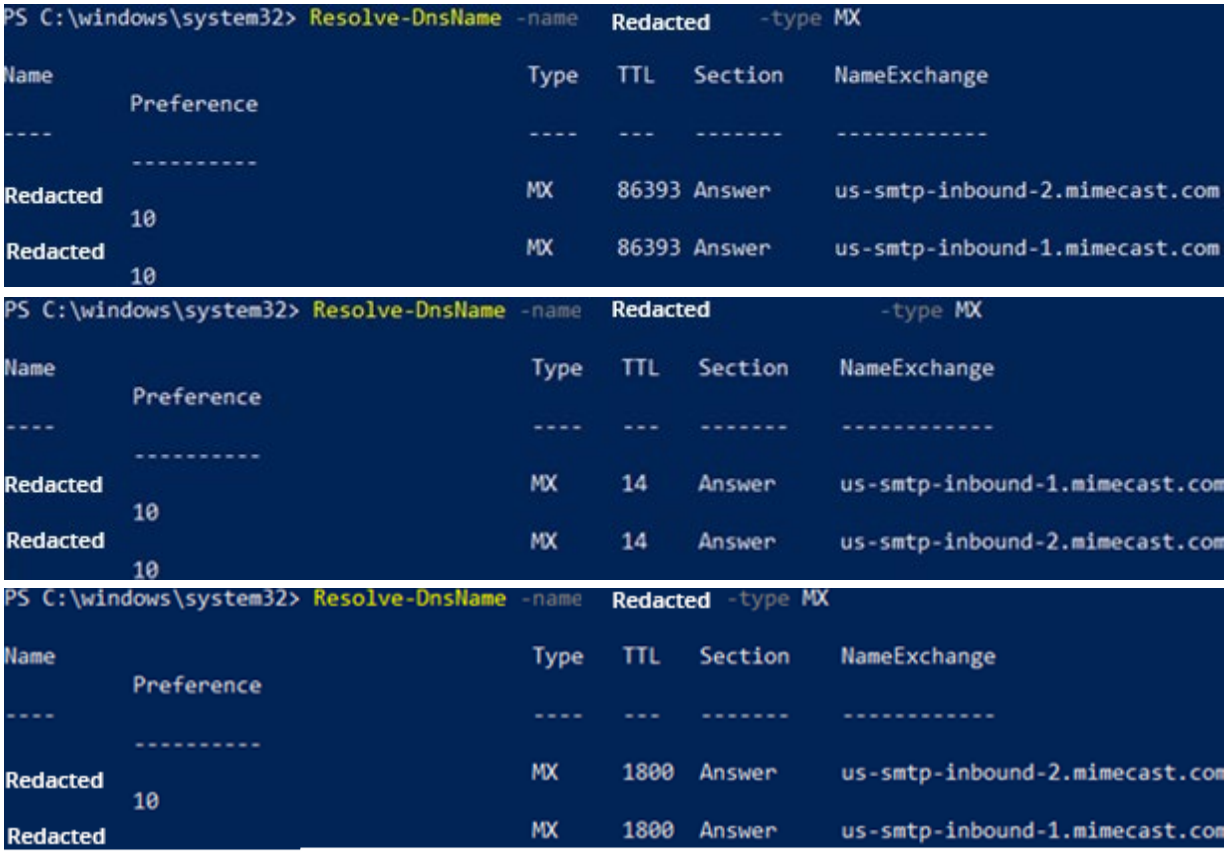
11. UNUSED OR DISABLED FEATURES SUMMARY

See below for details around any discovered Disabled or Unused Features:

Platform	Category	Disabled or Unused Feature Description
Mimecast	Security	Services > Continuity FINDINGS: Continuity not setup
Mimecast	Security	**Data Leak Prevention:** Monitor the details of messages that have had actions applied by Content Examination policies. Mimecast protects against an organization wide data leak, through seamless integration with Microsoft Exchange.

12. ADDITIONAL INFORMATION

MX Record Description: Shows the domain MX records are telling/showing/advertising to other domains to send mail to the records below. This helps identify if the domain has any other records that would allow attackers to bypass security controls.



Recommendation: None

TXT Record Description: Shows that MicroAge.com TXT/SPF record is to authorize specific hosts permission to send emails on behalf of your domain.

```
PS C:\windows\system32> Resolve-DnsName -name  Redacted -type TXT

Name                                 Type   TTL   Section    Strings
----                                 ----   ---   -------    -------
Redacted                             TXT    1800  Answer     {v=spf1
                                                              include:us._netblocks.mimecast.com -all}
```

```
PS C:\windows\system32> Resolve-DnsName -name  Redacted          -type TXT

Name                                 Type   TTL   Section    Strings
----                                 ----   ---   -------    -------
Redacted                             TXT    1800  Answer     {v=spf1
                                                              include:us._netblocks.mimecast.com ~all }
```

```
PS C:\windows\system32> Resolve-DnsName -name  Redacted     -type TXT

Name                                 Type   TTL   Section    Strings
----                                 ----   ---   -------    -------
Redacted                             TXT    600   Answer     {hbpsa4ovjhe877rsnufgccdblj}
Redacted                             TXT    600   Answer     {google-site-verification=DVSwJFbCBQGcFM1
                                                              Gv4E4cyBKhEnMGFnhSo_fbg1KDX0?}
Redacted                             TXT    600   Answer     {v=spf1
                                                              include:us._netblocks.mimecast.com
                                                              include:_spf.google.com
                                                              ip4:216.81.154.183 ip4:72.32.72.85 ~all}
Redacted                             TXT    600   Answer     {teamviewer-sso-verification=7df972eb1cd3
                                                              455d9e222d6918854ef2}
Redacted                             TXT    600   Answer     {dglrqaoebj1eddi1oji2u5iopr}
Redacted                             TXT    600   Answer     {google-site-verification=kP7kX46w5CQ12bu
                                                              B714HtbHqIBaEfdVX-sC8rDRClUU}
Redacted                             TXT    600   Answer     {ml2g41j3k68mnng4s6pp972qqwzjq1z3}
```

Recommendation: None

A **DMARC** policy allows a sender to indicate that their messages are protected and tells a receiver what to do if one of the authentication methods passes or fails, such as send the message to junk/reject the message. DMARC prevents spammers or phishers from using valid organization names for email fraud. It protects the integrity of your brand and increases customer confidence and trust. If reporting is enabled, you can get insight into attempts to spam, phish or even spear phishing using your organization's brand/name.

Recommendation: Updating/Validate current DMARC record off ProofPoint.

```
v=DMARC1; p=reject; rua=mailto: Redacted ,mailto: Redacted ; ruf=mailto: Redacted ,mailto: Redacted ; fo=1;
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto: Redacted	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto: Redacted	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ":".

FINAL RESULT:

Cousin Domains

We scanned for a possible **3168** suspicious domains, and only identified **58** registered. Only the REDACTED URL TLD was scanned.

Scanned 3168 suspicious domains. Identified 58 registered: download as CSV or JSON

PERMUTATION	IP ADDRESS	NAME SERVER	MAIL SERVER
Redacted *original	Redacted United States	Redacted	us-smtp-inbound-1.mimecast.com
Redacted addition	Redacted Italy	Redacted	
Redacted addition	Redacted United States	Redacted	
Redacted addition	Redacted	Redacted	alt1.aspmx.l.google.com
Redacted addition	Redacted	Redacted	
Redacted addition	Redacted United Kingdom	Redacted	mx1-us1.ppe-hosted.com
Redacted addition	Redacted Germany	Redacted	localhost

For further information and a complete breakdown of all domains: Please see REDACTED.

ADDITIONAL INFORMATION

Fuzzer Types

Addition: Adding another letter to the end of the domain

Bitsquatting: Flipping 1 bit in the bit stream, which would make the name look like a typo.

Homoglyph/Punycode: A look alike character in Unicode

Hyphenation: Inserting a hyphen in the domain.

Insertation: Adding an additional character in the domain.

Omission: Removing a character in the domain.

Repetition: Adding the same character that proceeds in the domain.

Replacement: Substituting a character for any character in the domain.

Transposition: Flipping 2 characters right next to each other, in the incorrect order.

Vowel-Swap: Replacing the vowels for another vowel.

TLD-Swap: Replacing 'com' with a few other common TLDs.

13. MANAGEWISE EXPRESS OVERVIEW

This Report was created under the guidelines of your Mimecast ManageWise Express Service engagement. See details below.

The MicroAge **Mimecast ManageWise Express Service** provides support for routine maintenance to help prevent unplanned downtime, optimize system performance, support business needs and free up time to work on key business objectives. It is part of a new breed of IT service, born out of the same economic necessity and technological capacity as on-demand consumer services. It helps relieve tension between IT and the business by striking a healthy balance of stability and agility, providing the resources to keep existing infrastructure strong while enabling business growth.

Delivery

The MicroAge Mimecast ManageWise Express Service is delivered as follows:

Discovery, Assessment, and Health Check

MicroAge engineers engage with designated client personnel to perform an assessment and review. MicroAge will review the client's Mimecast environment against standard methodology and best practices. This is typically completed remotely and should not exceed two business days. Tasks include:

- Assessment of the client's Mimecast implementation
- Review of performance and perceived functionality with the client
- Review overall environment health and adherence to standard best practices
- Document findings and recommendations, then outline a roadmap of tasks for future plans or remediation
- Advise client on any new features or modules not currently in use (i.e., archiving, sync and recover, and resilience)
- Future environment design and planning as needed
- Mimecast environment documentation and technical client documentation, if time permits

Responsibilities

MicroAge Responsibilities

Mimecast ManageWise Express Service as outlined in this service brief

Client Responsibilities

- The client must provide all information requested by the consultant for the completion of services
- The client must provide a knowledgeable contact who is available throughout the service to clarify questions and provide information, access, and passwords when needed
- Adherence to all MicroAge's services terms and conditions located at https://microage.com/salesterms/
- Clients must provide at least two (2) weeks advance notice to schedule service delivery. Service(s) will be scheduled on a mutually agreed date based on consultant resource availability
- Client will provide remote and all needed access to the client's environment to complete services

Shared Responsibilities

- The entire MicroAge service must be completed within the chosen contract term. Otherwise, the order will be automatically terminated and deemed complete
- MicroAge will send the client a confirmation email when the service is complete, providing an opportunity for the client to advise if the service was not delivered satisfactorily. If the client does not submit a written notification of a service performance issue within five (5) business days from receipt of the closure email, the work will be deemed accepted

End of ManageWise Express Overview

14. END OF DOCUMENT

This is the end of the Email Security Health Check Report. A report review can be scheduled at your convenience.
Please direct any questions or requests to your MicroAge Team.