



EMAIL SECURITY HEALTH CHECK REPORT


MicroAge[®]

cStor[™]

The Digital Transformation Experts[®]

Email Security Health Check Report



TABLE OF CONTENTS

- OVERVIEW AND CONTACTS.....3
- 1. EXECUTIVE SUMMARY DASHBOARD4
- 2. ACCOUNT REVIEW5
- 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

Email Security Health Check Report

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

Email Security Health Check Report

1. EXECUTIVE SUMMARY DASHBOARD

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

At A Glance

- All Threats correctly stopped/blocked
- Protection Features bring utilized
- Minor Housekeeping items for upkeep

Executive Summary

There are 139 Findings or reccomendations

Accounting Configuration 0 High/ 0 Medium/ 5 Low

Services Configuration 0 High/ 1 Medium/ 1 Low

Directories Configuration 0 High/ 0 Medium/ 1 Low

Gateway Configuration 0 High/ 0 Medium/ 139 Low

Recommendations

There are **0 Urgent** Recommendations

There are **0 High** Recommendations

There are **1 Medium** Recommendations

There are **146 Low** Recommendations

Report Card

Grading Scale

95 – 100%	A
94 – 85%	B
84 and Below	C

A

Email Security Health Check Report

Account and Support Details



Customer Details

Customer Name	REDACTED
Mimecast ID	
Account Code	
Database Code	

Product Details

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

Support Details

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

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**

Email Security Health Check Report

Account Settings > Account Settings

FINDINGS:

RECOMMENDATIONS: None

Account Settings

Account Name	<input type="text" value="REDACTED"/>
Mimecast ID	<input type="text"/>
Account Code	<input type="text"/>
Database Code	<input type="text"/>
Account Status	Enabled
DNS Authorization Code	<input type="text"/>
Minimum Retention (Compliance Protect)	<input type="checkbox"/>
Maximum Retention (Days)	<input type="text"/>
Maximum Retention Validated	Yes
Maximum Retention (Days) for Instant Message	<input type="text"/>
Number of Users	<input type="text"/>
Pause Inbound Deliveries	<input type="checkbox"/>
Warning Message After (Attempts)	<input type="text"/>
Bounce Message After (Attempts)	<input type="text"/>
Ingestion Partner	<input type="checkbox"/>
API Export (Case Review)	<input type="checkbox"/>

Email Security Health Check Report

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.

^ User Access and Permissions

Administration Console Timeout	1 hour(s) 
Allow Weak Ciphers for Secure Receipt	<input type="checkbox"/> 
Send BCC to Mail Server	<input checked="" type="checkbox"/> 
SMTP Submission Override	<input type="checkbox"/> 
POP Services Override	<input type="checkbox"/> 
Force Mimecast Personal Portal v3	<input checked="" type="checkbox"/> 
Display Sender Avatar to External Users	<input checked="" type="checkbox"/> 
Admin IP Ranges (CIDR n.n.n.n/x)	<input type="text"/> 
Content Administrators Default View	Metadata 
Targeted Threat Protection Authentication	<input type="checkbox"/> 
Security Passphrase	<input type="text"/> 

Email Security Health Check Report

Account Settings > Password Complexity and Expiration

FINDINGS:

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

^ Password Complexity and Expiration

Password Complexity

- Minimum password length ?
- Include at least one lowercase alphabetical character (a-z) ?
- Include at least one uppercase alphabetical character (A-Z) ?
- Include at least one numeric character (0-9) ?
- Include at least one non-alphanumeric (!@#\$.,) ?

Password Expiry and Lock

- Password expiration ?
- Use System Default ?
- Account lockout threshold ?
- Account lockout duration ?

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**

Email Security Health Check Report

Services > Continuity

FINDINGS: Continuity not setup

RECOMMENDATION (Med): Setup Continuity to ensure High Availability

Services > Continuity

Description	Affected Group	Type	Status
No data was found for this selection			

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
365 O365 Sync and Recover	O365 Sync and Recover PHX OU	PHX	Enabled with errors
365 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**

Email Security Health Check Report

Directories > Profile Groups

FINDINGS: Reviewed all groups

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

The screenshot shows the 'Directories > Profile Groups' interface. At the top left, there is a navigation breadcrumb 'Directories > Profile Groups' and a hamburger menu icon. Below this is an 'Edit group' section with a search bar containing the text 'Root'. The main content area displays a list of folders under the 'Root' category. The folders are listed in two columns. The left column includes: 2 factor Auth, Admin group (1), Admin Hold Emails (1), Administrator Alerts, Blocked Senders (1032), Bosch Domain List (1), Bosch User Email Allow (1), Bypass Greylisting (2), Bypass RBL (2), Bypass RBL QuickBooks (42), and Bypass Spam Scanning (6). The right column includes: Bypass Spam Scanning (6), Bypass URL Protection, CCERT Alerts URL Notification Bypass (7), Redacted User Email Allow (1), Content Bypass, DNS Authentication Bypass (31), External Forwarding O365 (3), Helpdesk Alerts URL Notification Bypass (5), Inbound to O365 Route (21), IP Permitted External (1040), IP Permitted Internal (3), IT Employees (8), MCG Google Anti-Spoof Bypass (44), and NDR/Termed Empl (2). The 'Content Bypass' folder is highlighted with a mouse cursor.

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**

Email Security Health Check Report

mimecast®

At a Glance

Headline Statistics



7. SECURE EMAIL GATEWAY



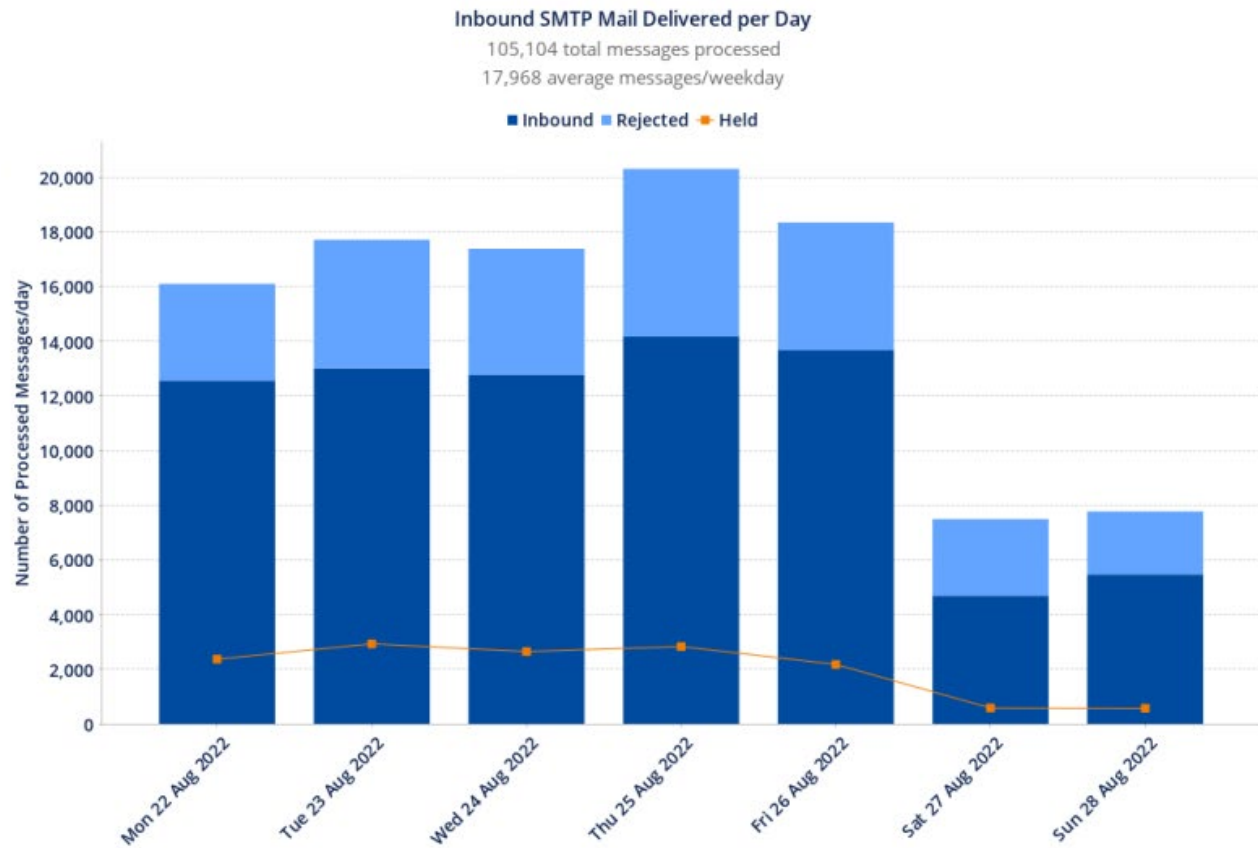
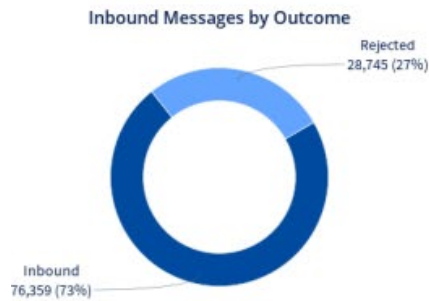
Mimecast Secure Email Gateway protects organizations and employees from spear-phishing, malware, spam, and zero-day attacks by combining innovative applications and policies with multiple detection engines and intelligence feeds to keep sophisticated attackers out.

Secure Email Gateway Highlights

Email Security Health Check Report

Inbound SMTP Overview

Secure Email Gateway



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.

Email Security Health Check Report

Top Inbound Non-TLS Sender Domains

Secure Email Gateway

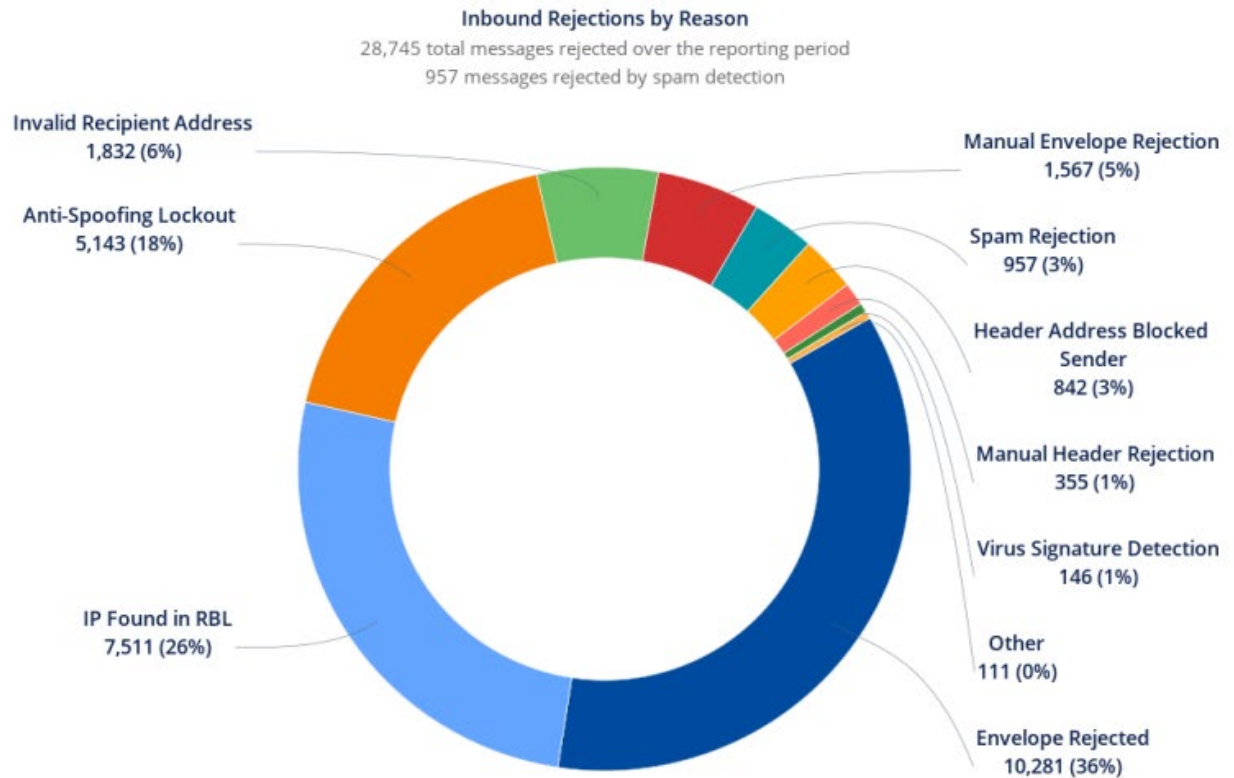
Rank	Domain	Mail Count
1	[REDACTED]	402
2	[REDACTED]	254
3	[REDACTED]	212
4	[REDACTED]	79
5	[REDACTED]	69
6	[REDACTED]	64
7	[REDACTED]	59
8	[REDACTED]	47
9	[REDACTED]	46
10	[REDACTED]	44
11	[REDACTED]	41
12	[REDACTED]	36
13	[REDACTED]	36
14	[REDACTED]	33
15	[REDACTED]	29
16	[REDACTED]	27
17	[REDACTED]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

Email Security Health Check Report

Inbound Rejections

Secure Email Gateway

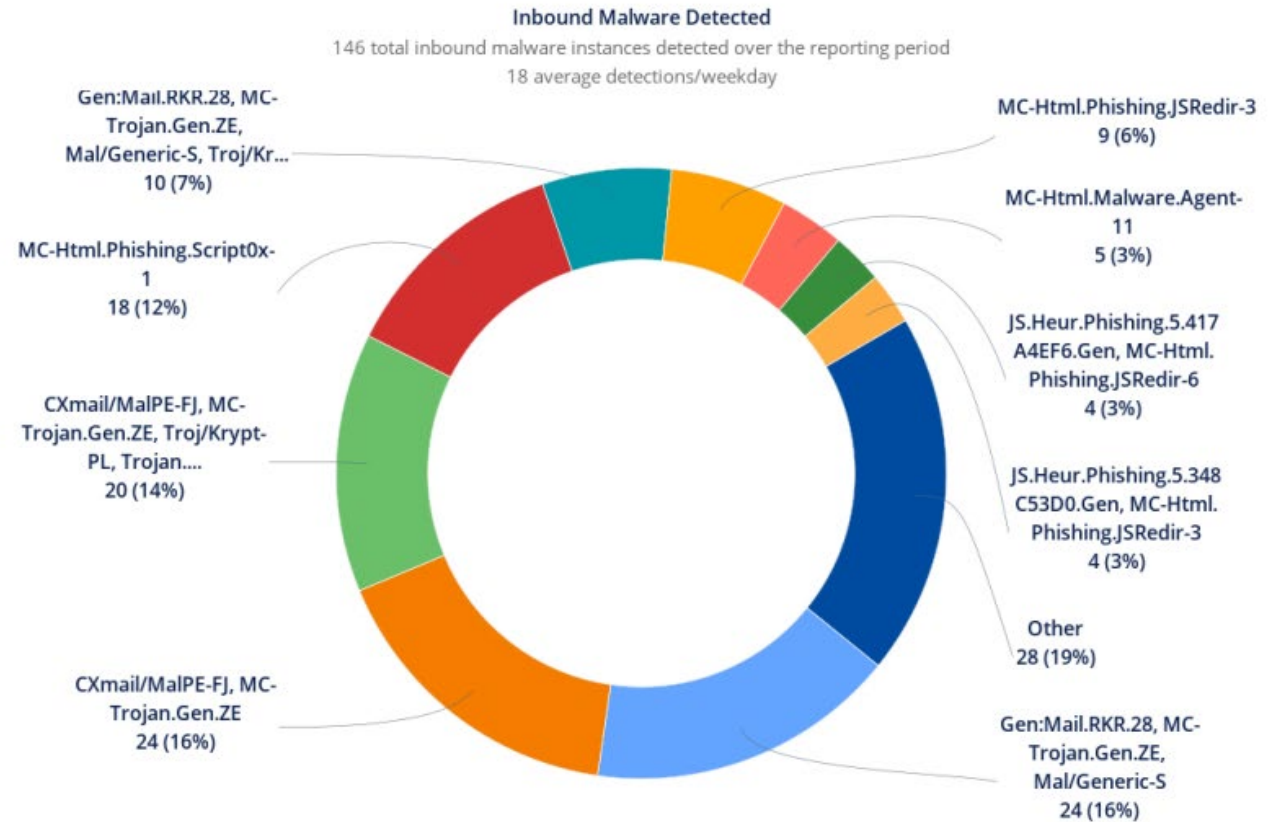


The distribution of rejection reasons for the rejections shown in the Inbound SMTP Overview chart. The count increments (+1) for each recipient. Excludes temporary errors and failed connection attempts. Recent logs can be found in the Administration Console under [Message Center - Rejected and Deferred](#).

Email Security Health Check Report

Top Inbound Malware

Secure Email Gateway

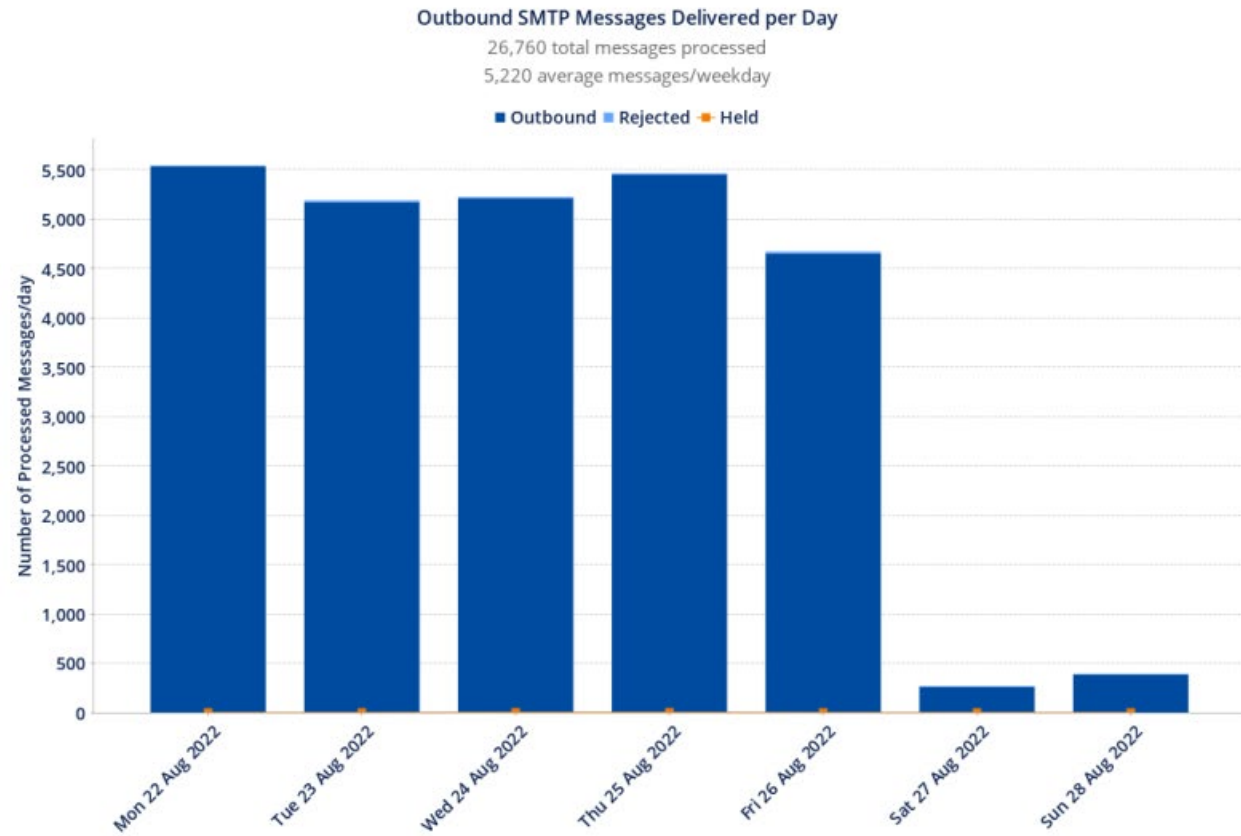
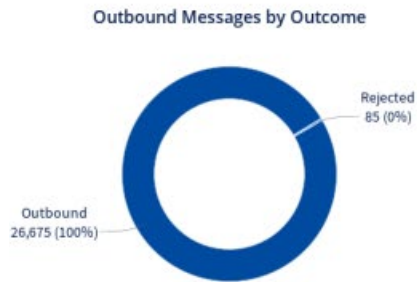


The distribution of malware detected in inbound mail. The count increments (+1) for each recipient. Details about the Malware Detections can be found in the [Threat Dashboard](#).

Email Security Health Check Report

Outbound SMTP Overview

Secure Email Gateway



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.

Email Security Health Check Report

Top Outbound Non-TLS Recipient Domains

Secure Email Gateway

mimecast®

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.

Email Security Health Check Report

mimecast

Top Attachment Types

Secure Email Gateway

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

Email Security Health Check Report

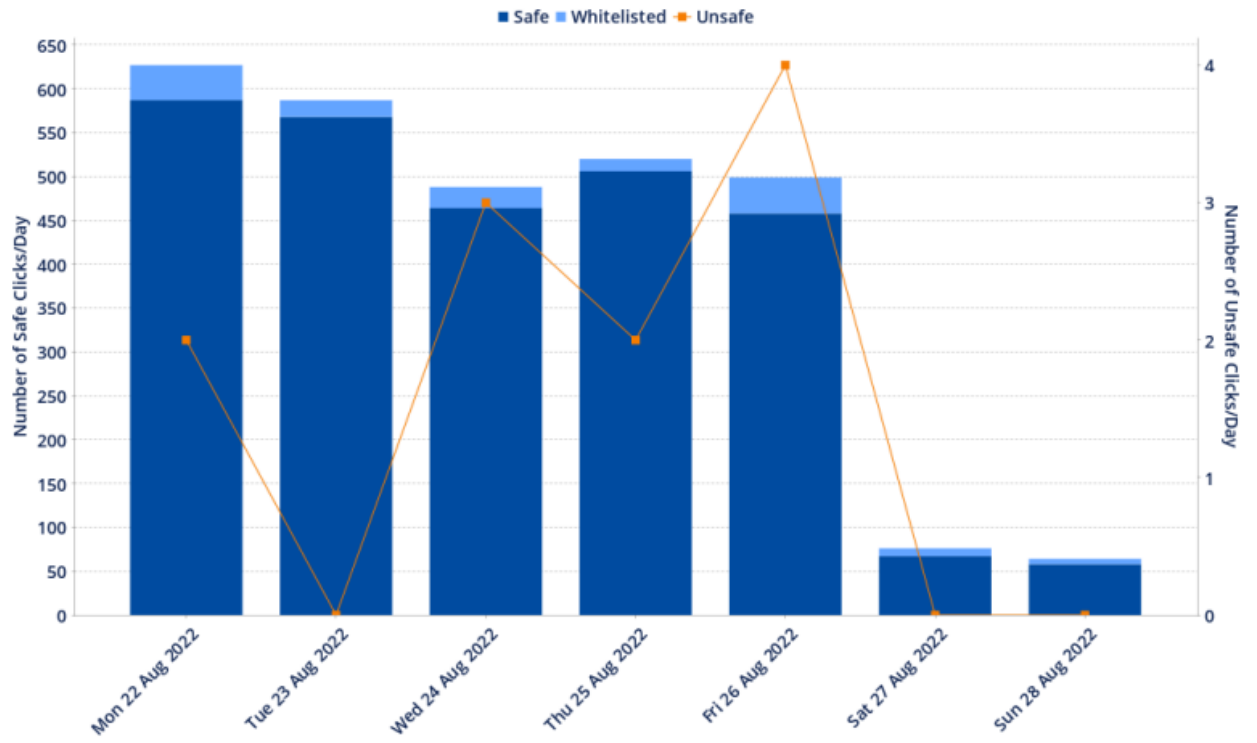
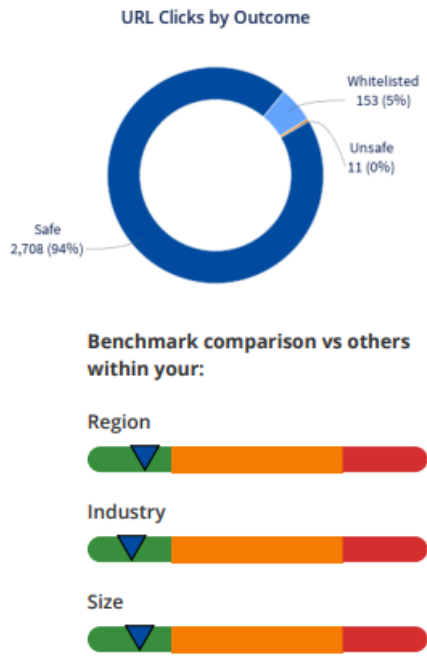
URL Clicks

URL Protect

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.

Email Security Health Check Report

Top URL Clickers by Severity and Volume

URL Protect

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

Email Security Health Check Report

Attachment Protect Sandboxing

Attachment Protect

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

Sandboxed Attachments by Outcome



Benchmark comparison vs others within your:

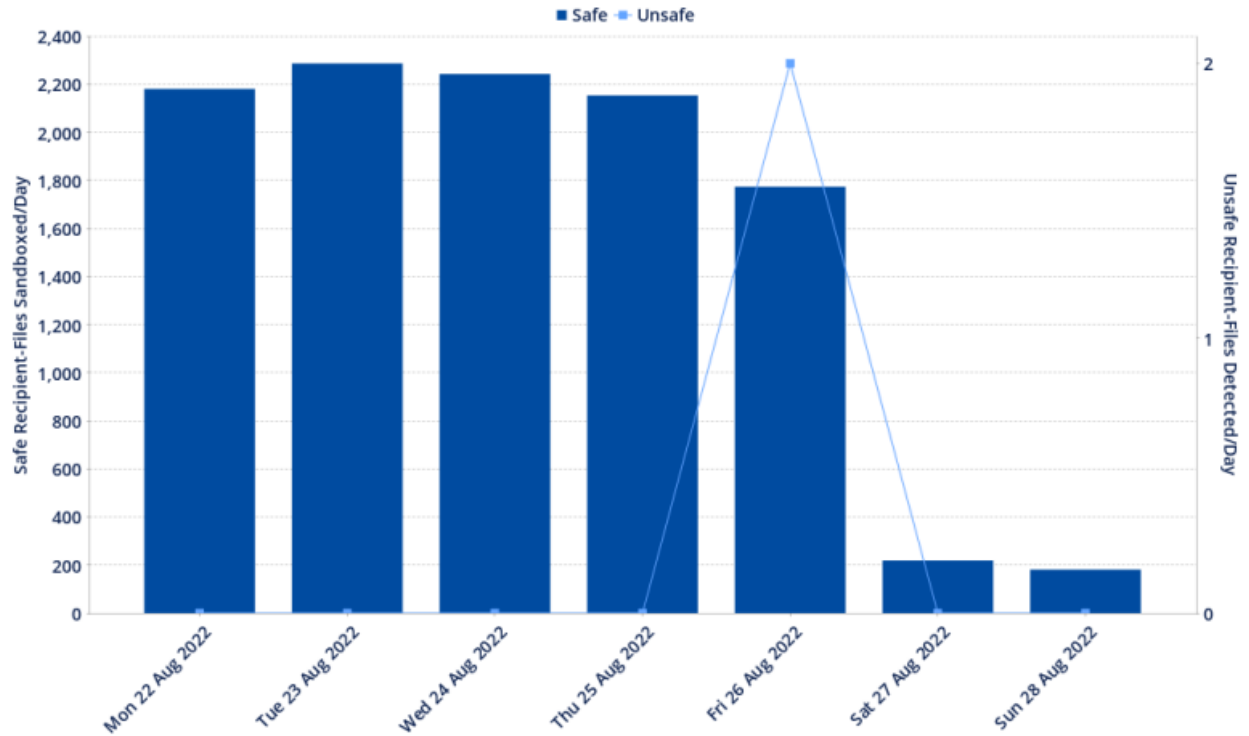
Region



Industry



Size



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.

Email Security Health Check Report

mimecast®

Sandboxed File Types

Attachment Protect

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

Email Security Health Check Report



Top Sandbox Filenames by Severity and Volume

Attachment Protect

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]	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.

Email Security Health Check Report

Top Sandbox Users by Severity and Volume

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

Email Security Health Check Report

Impersonation Protect Detections

Impersonation Protect

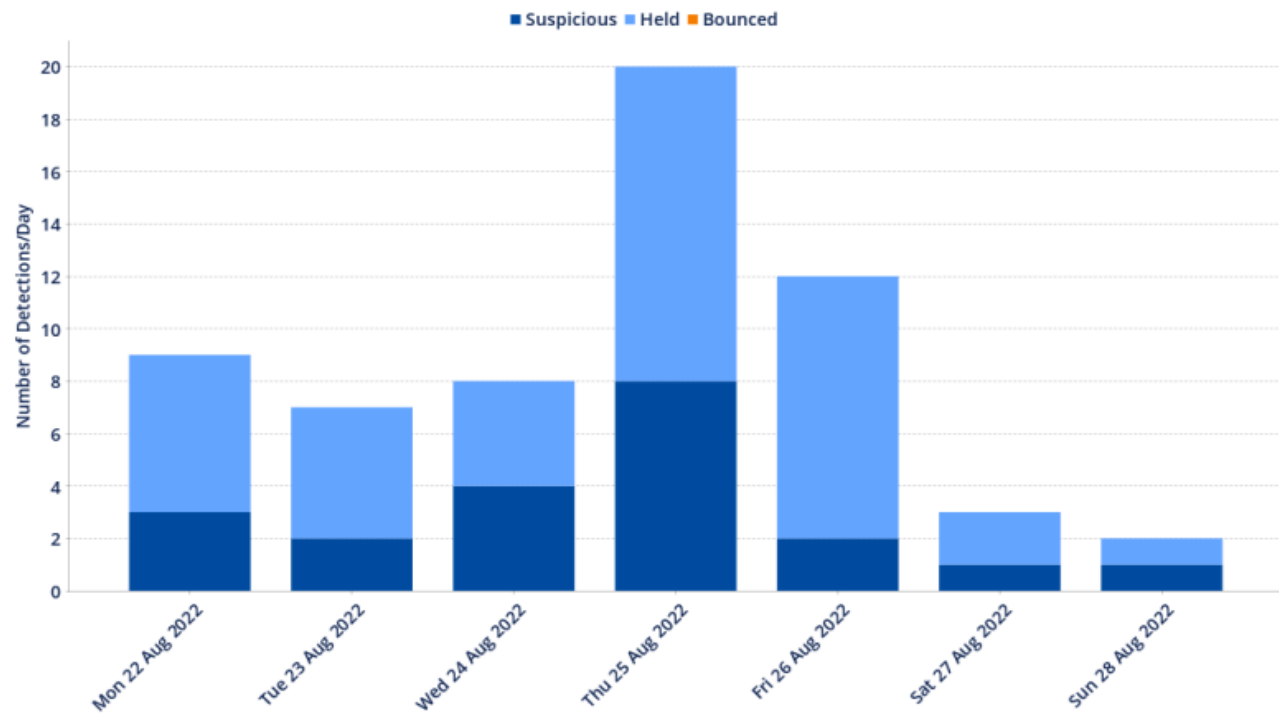
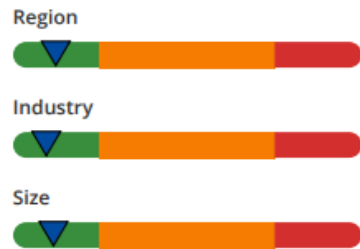
Detections by Impersonation Protect per Day

61 total messages detected
11 average messages/weekday

Impersonation Detections by Outcome



Benchmark comparison vs others within your:



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.

Email Security Health Check Report



Top Impersonation Protect Targets

Impersonation Protect

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.

```
PS C:\windows\system32> Resolve-DnsName -name Redacted -type MX
Name                                     Type  TTL  Section  NameExchange
-----
Preference
-----
Redacted                                MX    86393 Answer  us-smtp-inbound-2.mimecast.com
10
Redacted                                MX    86393 Answer  us-smtp-inbound-1.mimecast.com
10

PS C:\windows\system32> Resolve-DnsName -name Redacted -type MX
Name                                     Type  TTL  Section  NameExchange
-----
Preference
-----
Redacted                                MX    14   Answer  us-smtp-inbound-1.mimecast.com
10
Redacted                                MX    14   Answer  us-smtp-inbound-2.mimecast.com
10

PS C:\windows\system32> Resolve-DnsName -name Redacted -type MX
Name                                     Type  TTL  Section  NameExchange
-----
Preference
-----
Redacted                                MX    1800 Answer  us-smtp-inbound-2.mimecast.com
10
Redacted                                MX    1800 Answer  us-smtp-inbound-1.mimecast.com
```

Recommendation: None

Email Security Health Check Report

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
Gv4E4cyBKEnMGFnHSo_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-sC8rDRC1UU}
Redacted  TXT   600  Answer   {m12g41j3k68mnng4s6pp972qqwzjq1z3}
    
```

Recommendation: None

Email Security Health Check Report

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' separated by "-".

Email Security Health Check Report

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.

Email Security Health Check Report

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

Email Security Health Check Report

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.



Thank You!