CYBER ESSENTIALS

CSTL AWARDED 'CYBER ESSENTIALS PLUS' CERTIFICATION BODY STATUS - WE CAN HELP YOU ACHIEVE CYBER DEFENCE RECOGNITION.

COMPUTER SECURITY TECHNOLOGY LTD.
8-9 Lovat lane, London, London. EC3R 8DW.
Tel: 0207 621 9740.
Email: info@cstl.com
WWW.CSTL.COM

Customer: - REDACTED -

Extract of Summary and Key details of Symantec.cloud Health check Report

Specialist Partner

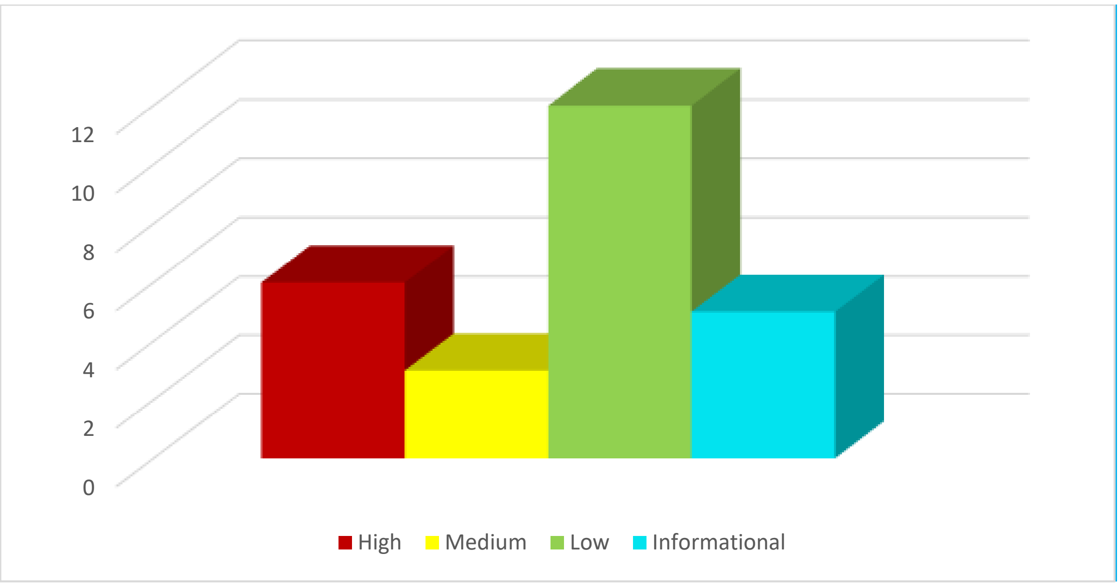
- ✓ 19 years' Symantec reseller
- ✓ Most Certified Tech Services Team
- ✓ Pre and Post technical expertise
- ✓ GOLD Partner Accreditation
- ✓ MASTER Consulting delivery approval.

VERSION: 1-1

STATUS: CUSTOMER FACING – REDACTED.

0. Summary of Recommendations

This section contains a list of the key findings that have been identified. More details can be found further in the Recommendations section (§2). Each finding has a recommendation, rationale and priority rating. The criticality is colour coded and categorised as High, Medium, Low or Informational.



0.1. Environment Rating

Rating: Fair
Justification: A number of high-criticality recommendations have been made, but nothing that would greatly degrade the service if not implemented.

0.2. Overview of Recommendations

Recommendation	Rationale	Ref §	Priority
Enable SPF checking for incoming emails.	SPF is the primary method of defence against Email spoofing. Enabling SPF checks confirms that emails sent to - REDACTED -'s domains arrive from legitimate sources.	§ 2.2.1.1	High
Enable DMARC checking on incoming emails.	DMARC is a supplementary method of defence against Email spoofing. Enabling DMARC checks confirms that emails sent to - REDACTED -'s domains arrive from legitimate sources.	§ 2.2.1.1	High
Consider activating Dynamic IP Block List with the action "Quarantine"	Companies and individuals in the dynamic public block list have demonstrated patterns of junk emailing, and activating this setting will add an extra layer of anti-spam protection. Quarantining messages will allow users to retrieve false positive emails.	§ 2.2.1.1	High

Review and consider removing (unless required) Approved Senders	Based on the number of emails seen past month (222,192), spam emails (22,603) only account for around 10% of all mail that Symantec .Cloud has seen. This may be due to the fact that any defined sender (e.g. added as part of support tickets) within the "Approved Senders" list is automatically exempt from Anti-Spam filtering technologies. When a particular sender is trusted, in the event that the sender's address is spoofed, spam will be able to pass the filters. It should be noted that there is an extensive list of whitelisted domains; domain whitelisting should only be used in exceptional circumstances, and should be removed upon the discovery and resolution of the underlying fault. IP addresses also change over time so whitelisted IP addresses may no longer be relevant for companies that have a less email-focussed infrastructure and should be reviewed.	§ 2.2.1.2	High
Consider whether to amend the Default Email Impersonation Control Settings action from Log Only to Quarantine.	The current setting will not prevent emails identified by this service from being delivered. Quarantining suspect emails will allow false positives to be retrieved by the recipient.	§ 2.2.5	High
Add new policy to block potentially harmful file types	Creating such a rule would allow to strip inbound emails of potentially dangerous attachments (mostly executables and scripts) that are unlikely to appear in regular correspondence and would reduce risk of zero-day threats. This rule could also be extended to macro-enabled documents.	§ 2.2.4	High
Set Cynic Maximum Hold Time to at least 5 minutes	This will help to prevent emails containing time-delayed malicious links (which are not active at the time of sending, but then activate shortly afterwards) from being delivered to users. It will not delay the delivery of the vast majority of mail – only a tiny percentage is forwarded to Cynic for analysis, and of those, many will not need to be held for analysis.	§ 2.2.2	High
Enable non-alphanumeric characters in email quarantine passwords	This setting only applies to quarantine administrator accounts created within Spam Manager. Increasing password complexity requirements ensures that users choose a complex combination of characters that are harder to guess and less prone to brute force attacks.	§ 2.2.4	Medium
Review admin user accounts, make any appropriate changes to permissions if any have more rights than required to fulfil their admin tasks,	Ensures the appropriate level of access to Email Security.Cloud.	§ 2.4.1.1	Medium

and remove any accounts no longer required. - REDACTED -has two accounts – one should be removed unless there is a compelling reason for both to exist.			
Consider activating address registration protection	With the validation feature turned on, emails to non-existent addresses will automatically be rejected, improving protection against spam targeting random popular email addresses.	§ 2.1.1	Low
Consider using Schemus to dynamically update domain email address lists	Although Email Security.Cloud will register an email address the first time an email is sent from it, this risks any email sent to it prior to this happening being blocked. Using Schemus to synch with Active Directory will obviate this risk.	§ 2.1.1	Low
Enable Newsletter / Marketing detection either as ‘Tag Subject and allow’ or ‘Quarantine’.	Enabling Newsletter/Marketing detection should reduce the number of potentially unwanted messages. Groups of recipients that often require, or wish to receive, newsletters may be excluded from these checks.	§ 2.2.1.1	Low
Enter contact details for an administrator who can receive support ticket numbers and notifications for tracking anti-malware **messages that have been submitted for analysis.**	If this information is not provided, Symantec’s Security Response team cannot analyze your user-submitted anti-malware messages or send updates or notifications to your administrator.	§ 2.2.6	Low
Consider enabling DKIM signing for all - REDACTED -’s domains.	DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing. It allows the recipient to check that an email purportedly originating from a specific domain was in fact authorized by the domain’s owner. This will only be of limited benefit, however, as it is reliant upon the receiving end making the necessary checks. Additionally, it may result in forwarded Outlook meeting invitations being incorrectly marked as spoofed.	§ 2.2.7	Low
Review “Policy Based Encryption”, “Encrypt Button” and "Encrypt in the Subject Line" policies and remove if not	These policies apply to a recipient group populated only by a test email address.	§ 2.3.1	Low

required.			
Enable Two Factor Authentication	This setting only applies to administrator accounts created within the Management Portal. Sophisticated network attacks have rendered simple password authentication insufficient to protect an organization against unauthorized access to its network and applications. See	§ 2.4.1.2	Low
Define IP restrictions for console access	Restricting Symantec .Cloud console access to office IP address range prevents any unauthorised logons from outside the network.	§ 2.4.1.2	Low
Consider email size overhead	It is important to note that base64 encoding conversion adds an overhead of up to 33% to message size. This means a setting of 26MB for Maximum email size will actually result in a practical size limit of around 19.5MB.	§ 2.1.2	Informational
Review and consider removing (unless still required) Blocked Senders.	A majority of the entries within the Blocked Senders list are specified by email address. Blocking senders on a per email address basis is very ineffective, and should only be treated as temporary solution. Best practice would be to supply spam samples to Symantec for their Security Response Team to update spam definitions instead.	§ 2.2.1.3	Informational
Enable the “Use global approved image list” and “Use global blocked image list” incoming and outgoing mail settings with the action “Redirect suspected mail to the Image Control administrator”.	Enabling these settings will compare images against a list maintained by Symantec; this will an additional layer of protection to the heuristics setting already activated, which relies on analyzing the content of images to categorize them.	§ 2.2.3	Informational
Consider enabling the “Copy end-user submitted emails to your organization's administrators” setting.	This will grant visibility on suspected spam submitted to Symantec by users and allow the administrator to take any appropriate action.	§ 2.2.6	Informational
Consider deploying the Symantec Email Submission Client if not already in use.	The Symantec Email Submission Client enables customers with Microsoft Exchange environments to submit suspected spam email to Symantec Security Response. The end user moves suspected spam messages to the “Report Spam” folder in their email client, which are then sent to Symantec Security Response for anti-spam research.	§ 2.5.1	Informational

User Impersonation Control		
↳	**Enable User Impersonation Control**	Unchecked

	9	Encrypt in the subject line
Encrypt in the Subject Line	**Apply to:** Outbound mail only **Execute if:** All rules are met **Action:** Redirect to administrator **Notification:** Sender **Contains 2 rules:** Rule for Recipient **Recipients Group:** • PBE Exception ○ Email recipient is in none of the selected groups Rule for Mail **Keyword Lists:** • Custom_GroupF820899B7AE54FFB9D641D1AF91AFB0C ○ Email contains all of the keywords in the selected lists ○ Case sensitive: No ○ Look in: Subject line **Activated:** Yes	

0.3. Advanced Threat Protection: Email. This section details Reports related configuration options for Symantec .Cloud. The section is separated into the below subsection9:

- Anti-Malware Scheduled Reports
- Anti-Spam Scheduled Reports
- Image Control Scheduled Reports
- Spam Quarantine Scheduled Reports

0.3.1.Anti-Malware Scheduled Reports

Recipients	Type of Report
• **- REDACTED -.–redacted- @uk.- REDACTED -.com**	Weekly summary: • Don’t send weekly summary
	Weekly detail: • Don’t send weekly detail
	Monthly summary: • Format: CSV • Elements: ○ Total for all domains ○ Total by domain ○ Malware type for all domains

0.3.2.Anti-Spam Scheduled Reports

Recipients	Type of Report
• **- REDACTED -@a- REDACTED -.co.uk**	Weekly summary: • Don’t send weekly summary
	Monthly summary: • Format: Text • Elements: ○ Total for all domains ○ Total by domain

0.3.3.Image Control Scheduled Reports

Recipients	Type of Report
• **- REDACTED -@a- REDACTED -.co.uk**	Weekly summary: • Don’t send weekly summary
	Weekly detail: • Don’t send weekly summary
	Monthly summary: • Format: Text • Elements: ○ Total for all domains ○ Total by domain ○ Top 20 image recipients ○ Top 20 image senders

0.3.4.Spam Quarantine Scheduled Reports

Recipients	Type of Report
• **None configured**	Weekly summary: • Don’t send weekly summary
	Monthly summary: • Don’t send monthly summary

1. Environment Statistics

This section details the current environment statistics.

Email Services	Value
Emails Scanned (past month)	222,192
Emails Identified as Spam (past month)	22,603
Emails Identified as Malware (past month)	1,340
Emails Identified by Image Control (past month)	62
Emails Triggering Data Protection rules (past month)	1661
Email Advanced Threat Protection incidents (past month)	0

2. Recommendations

This section defines proposed changes to the Symantec .Cloud environment and is separated into the following headings:

- Users and Groups
- Email Services
- Data Protection Services
- Administration/Support
- Symantec .Cloud Tool add-ons

Only recommendations and their rationale are detailed in this section. Settings that should remain unchanged are omitted.

2.1. Users and Groups

This section details the recommendations for Email Address Registrations, User Groups and Message Size.

2.1.1. Address Registration

Recommendation: Consider using Schemus to dynamically update domain email address lists
Rationale: Although Email Security.Cloud will register an email address the first time an email is sent from it, this risks any email sent to it prior to this happening being blocked. Using Schemus to synch with Active Directory will obviate this risk.
Priority: Low

2.1.2. Message Size

Recommendation: Consider email size overhead
Rationale: It is important to note that base64 encoding conversion adds an overhead of up to 33% to message size. This means a setting of 26MB for Maximum email size will actually result in a practical size limit of around 19.5MB.
Priority: **Informational**

2.2. Email Services

2.2.1. Anti-Spam

2.2.1.1. Detection Settings

Setting	Value
Approved Senders	**No Recommended Changes.**
Spoofed Sender Detection	
↳ **Use SPF**	**Recommendation:** Enable SPF checking for incoming emails. **Rationale:** SPF is the primary method of defence against Email spoofing. Enabling SPF checks confirms that emails sent to -REDACTED -'s domains arrive from legitimate sources.

		Note: Enabling SPF checks does not require one to set one's own SPF records, but creating SPF policies and setting domain records is recommended, however. **Priority:** High
↳	**Use DMARC**	**Recommendation:** Enable DMARC checking on incoming emails. **Rationale:** DMARC is a supplementary method of defence against Email spoofing. Enabling DMARC checks confirms that emails sent to - REDACTED -'s domains arrive from legitimate sources. **Note:** Enabling DMARC checks does not require one to set one's own DMARC records, but creating SPF policies and setting domain records is recommended, however. **Priority:** High
Responsive Spam Detection		
↳	**Use dynamic IP block List**	**Recommendation:** Consider activating with the action "Quarantine" **Rationale:** Companies and individuals in the dynamic public block list have demonstrated patterns of junk emailing, and activating this setting will add an extra layer of anti-spam protection. Quarantining messages will allow users to retrieve false positive emails. **Priority:** High
↳	**Use signaturing system**	No recommendations
Predictive Spam Detection (Skeptic Heuristics)		
Newsletter / Marketing Detection		**Recommendation**: Enable Newsletter / Marketing detection either as 'Tag Subject and allow' or 'Quarantine'. **Rationale**: Enabling Newsletter/Marketing detection should reduce the number of potentially unwanted messages. Groups of recipients that often require, or wish to receive, newsletters may be excluded from these checks. **Priority:** Low

2.2.1.2. Approved Senders

Recommendation: Review and consider removing (unless required) Approved Senders
Rationale: Based on the number of emails seen past month (219,958), spam emails (22375) only account for around 10% of all mail that Symantec .Cloud has seen. This may be due to the fact that any defined sender (e.g. added as part of support tickets) within the "Approved Senders" list is automatically exempt from Anti-Spam filtering technologies. When a particular sender is trusted, in the event that the sender's address is spoofed, spam will be able to pass the filters. It should be noted that there is an extensive list of whitelisted domains; domain whitelisting should only be used in exceptional circumstances, and should be removed upon the discovery and resolution of the underlying fault. IP addresses also change over time so whitelisted IP addresses may no longer be relevant for companies that have a less email-focussed infrastructure and should be reviewed.

Additionally, it is advisable to have a process for regular reviews of White and Black Lists to ensure that protection is maintained and remains relevant.

Note: using domains as Approved Senders has further implications and it does not ensure the source IP address belongs to the perceived sending domain; this means that when a domain is spoofed even if SPF/DMARC is enabled, emails will bypass Anti-Spam filters.

Priority: High

2.2.1.3. Blocked Senders

Recommendation: Review and consider removing (unless still required) Blocked Senders.
Rationale: A majority of the entries within the Blocked Senders list are specified by email address. Blocking senders on a per email address basis is very ineffective, and should only be treated as temporary solution. Best practice would be to supply spam samples to Symantec for their Security Response Team to update spam definitions instead.

Priority: Informational

2.2.2.Anti-Malware

Recommendation: Set Cynic Maximum Hold Time to at least 5 minutes
Rationale: This will help to prevent emails containing time-delayed malicious links (which are not active at the time of sending, but then activate shortly afterwards) from being delivered to users. It will not delay the delivery of the vast majority of mail – only a tiny percentage is forwarded to Cynic for analysis, and of those, many will not need to be held for analysis.
Priority: High

2.2.3.Image Control

Recommendation: Enable the "Use global approved image list" and "Use global blocked image list" incoming and outgoing mail settings with the action "Redirect suspected mail to the Image Control administrator".
Rationale: Enabling these settings will compare images against a list maintained by Symantec; this will an additional layer of protection to the heuristics setting already activated, which relies on analyzing the content of images to categorize them.
Priority: Informational

2.2.4.Email Quarantine

Setting		Value
↳	**Character types required in a password:**	**Recommendation:** Enable non-alphanumeric characters **Rationale:** This setting only applies to quarantine administrator accounts created within Spam Manager. Increasing password complexity requirements ensures that users choose a complex combination of characters that are harder to guess and less prone to brute force attacks. **Priority:** Medium

2.2.5.Email Impersonation Control Settings

Recommendation: Consider whether to amend the Default Settings action from Log Only to Quarantine**.**

Rationale: The current setting will not prevent emails identified by this service from being delivered. Quarantining suspect emails will allow false positives to be retrieved by the recipient.
Priority: High

2.2.6.Email Submission Settings

Recommendation: Consider enabling the "Copy end-user submitted emails to your organization's administrators" setting.
Rationale: This will grant visibility on suspected spam submitted to Symantec by users and allow the administrator to take any appropriate action.
Priority: Informational

Recommendation: Enter contact details for an administrator who can receive support ticket numbers and notifications for tracking anti-malware messages that have been submitted for analysis.
Rationale: If this information is not provided, Symantec's Security Response team cannot analyze your user-submitted anti-malware messages or send updates or notifications to your administrator.
Priority: Low

2.2.7.Outbound DKIM Signing Settings

Recommendation: Consider enabling DKIM signing for all - REDACTED -'s domains.
Rationale: DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing. It allows the recipient to check that an email purportedly originating from a specific domain was in fact authorized by the domain's owner. This will only be of limited benefit, however, as it is reliant upon the receiving end making the necessary checks. Additionally, it may result in forwarded Outlook meeting invitations being incorrectly marked as spoofed.
Priority: Low

2.3.Data Protection Services

This section details recommendations for the Data Protection service related configuration options for Symantec .Cloud.

2.3.1. Email Policies

Recommendation: Add new policy to block potentially harmful file types
Rationale: Creating such a rule would allow to strip inbound emails of potentially dangerous attachments (mostly executables and scripts) that are unlikely to appear in regular correspondence and would reduce risk of zero-day threats. This rule could also be extended to macro-enabled documents.
Priority: High

Recommendation: Review "Policy Based Encryption", "Encrypt Button" and "Encrypt in the Subject Line" policies and remove if not required.
Rationale: These policies apply to a recipient group populated only by a test email address.
Priority: Low

Recommendation: Review “Incompetent Leader” policy and remove if not required.
Rationale: This policy applies to a single external email address and may no longer be required.
Priority: Low

2.4. Administration/Support

This section details Administration and Support related configuration options for Symantec .Cloud.

2.4.1. Administration

Settings for User Management and Access Control.

2.4.1.1. User Management

Recommendation: Review admin user accounts, make any appropriate changes to permissions if any have more rights than required to fulfil their admin tasks, and remove any accounts no longer required. - REDACTED -has two accounts – one should be removed unless there is a compelling reason for both to exist.
Rationale: Ensures the appropriate level of access to Email Security.Cloud.
Priority: Medium

2.4.1.2. Access Control

Setting	Value
Password policy	**No changes recommended**
↳ **Passwords expires after**	
↳ **Passwords can be re-used after**	
Two Factor Authentication (2FA)	**Recommendation:** Enable Two Factor Authentication **Rationale:** This setting only applies to administrator accounts created within the Management Portal. Sophisticated network attacks have rendered simple password authentication insufficient to protect an organization against unauthorized access to its network and applications. **Priority:** Low
IP Restrictions	**Recommendation:** Define IP restrictions for console access **Rationale:** Restricting Symantec .Cloud console access to office IP address range prevents any unauthorised logons from outside the network. **Priority:** Low

2.5. Symantec .Cloud Tool add-ons

Supplementary tools are available to the customer for Symantec .Cloud.

- Schemus Synchronisation Tool
- Symantec Email Submissions Client

2.5.1. Symantec Email Submissions Client

Recommendation: Consider deploying the Symantec Email Submission Client if not already in use.

Rationale: The Symantec Email Submission Client enables customers with Microsoft Exchange environments to submit suspected spam email to Symantec Security Response. The end user moves suspected spam messages to the “Report Spam” folder in their email client, which are then sent to Symantec Security Response for anti-spam research.
Priority: Informational

- ***REST OF REPORT - REDCATED –***

COMPUTER SECURITY TECHNOLOGY LTD.
8-9 Lovat lane, London, London. EC3R 8DW.
Tel: 0207 621 9740.
Email: info@cstl.com
WWW.CSTL.COM