
cisco Live!
Let's go
#CiscoLive

The bridge to possible

You've Got Mail!

What should your email security solution look like?

Sérgio Pinto, Secure Email TME Technical Leader
@sergio_s_pinto

BRKSEC-1029

Cisco Webex App

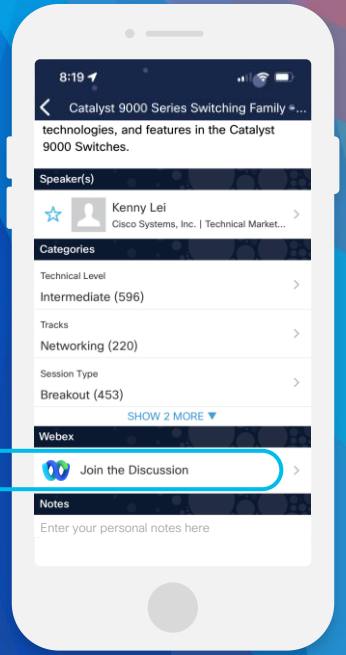
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.

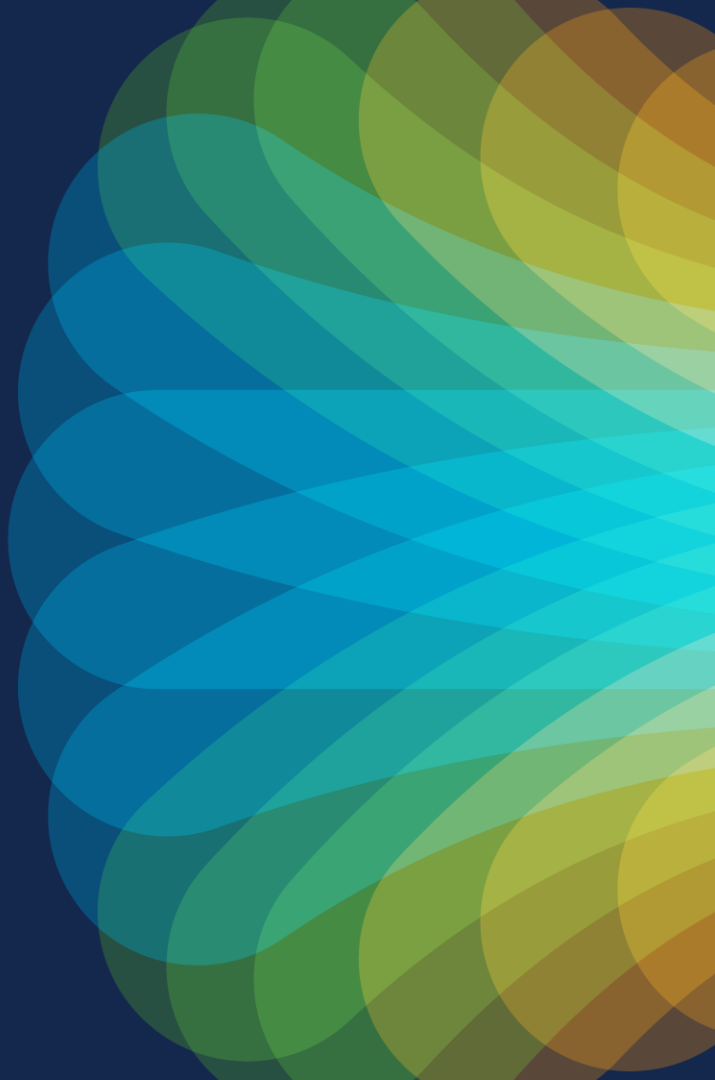


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1029

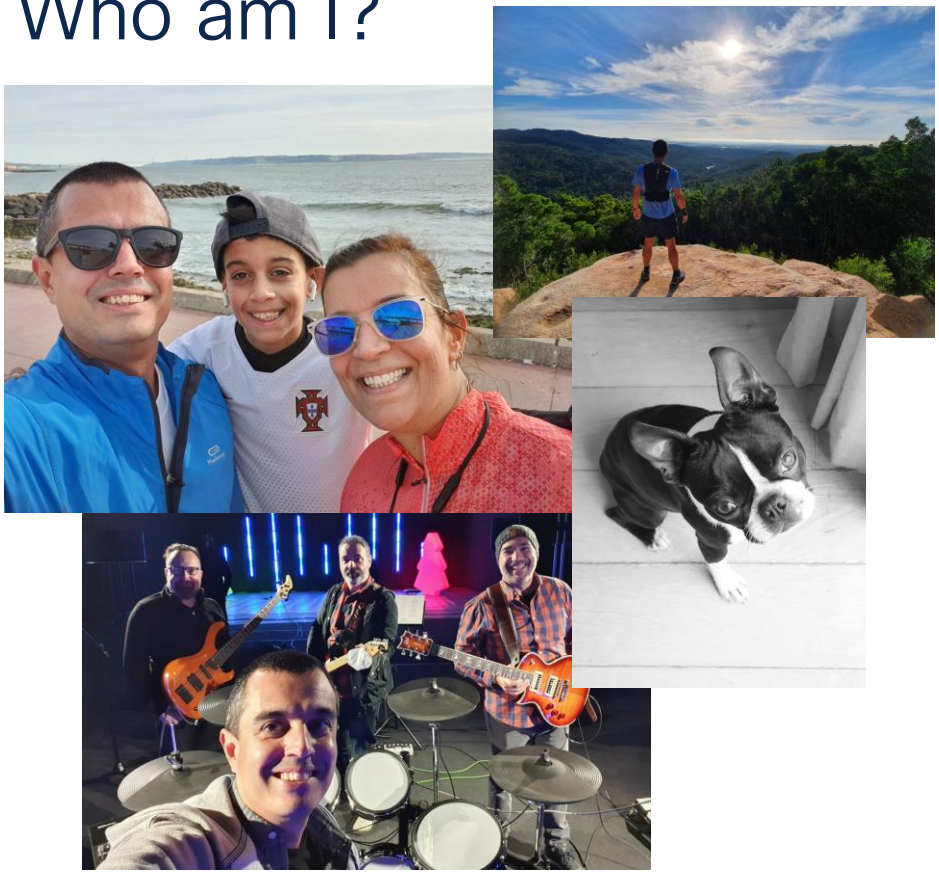
Agenda

- Who am I?
- Why should you care about email security?
- What are the best practices?
- 3 stages of email security
- Call to action
- Conclusion

Who am I?



Who am I?



Secure Email Technical Marketing Engineer

Married, Father, and dog lover (recently)

15+ years in Cisco across Sales and Eng

Cisco Live and External events speaker

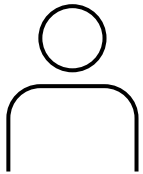
Sports enthusiast (Krav Maga, Running, Padel)

Music lover (I play Guitar, Drums, and Piano)

Based out of Lisbon, Portugal

Why should you care about email security?

#1 information transport model



3.9B users

Growing to
4.5B in 2024

300 Billion

Email sent daily

58%

The first thing they
check in the
morning

Source: www.statista.com

Easy to spoof & impersonate

From:
Miguel
USA

Dear John Doe,

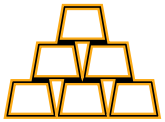
This is Miguel from NY City.
I hope this letter finds you well.

Regards
Sergio

Brand / Data / Financial loss

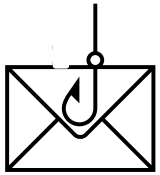
500.000

Complaints per year



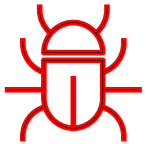
$10.3B

Financial Damage



300.000

Phishing victims with $52M in damage



$2.7B

Loss due to BEC attacks

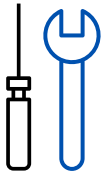
Source: FBI IC3 report - www.ic3.gov

What are the best practices?

What are best practices

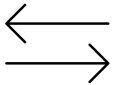
Analyse

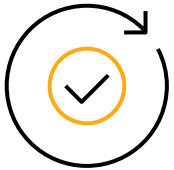
Know your environment and requirements



Tune

Fine tune the configuration to meet your requirements





Monitor

Keep an eye for the results produced after the tuning

The recommendations presented during this session are general guidelines

Protection Phases

Protection phases

Connection

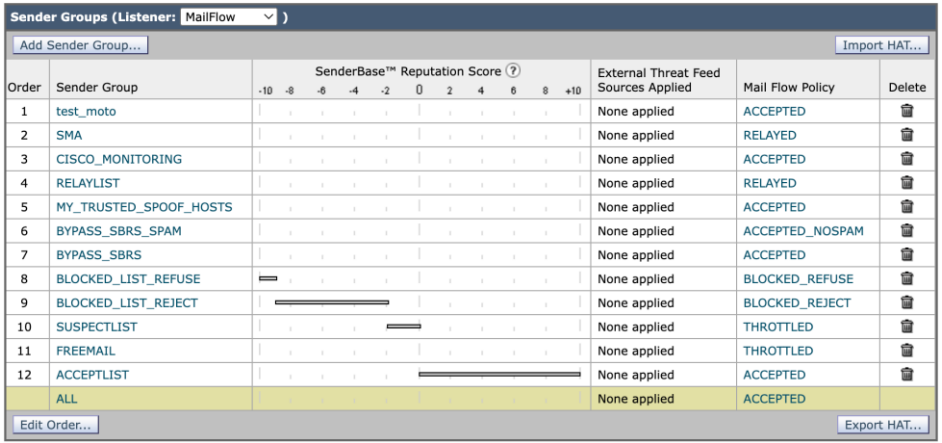
Connected

Post-Delivery

Connection

Sender Based Reputation

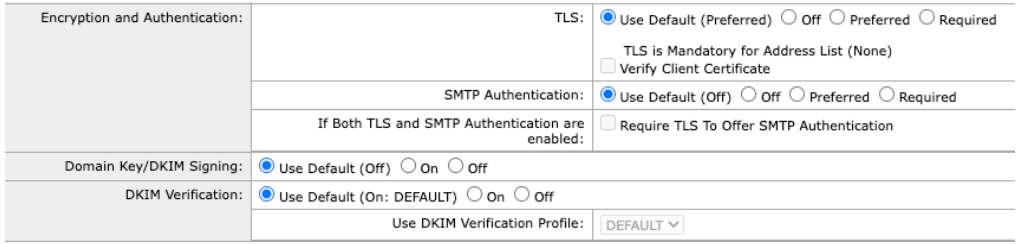
- Refuse or Reject all low-reputation sender
- Create a suspicious reputation-policy
- Throttle freemail senders (limit the number of messages/recipients)

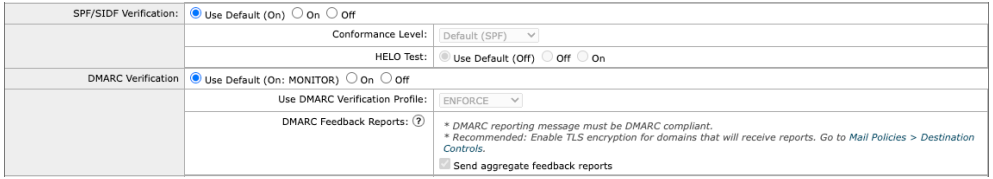


Reputation can block 80-90% of connections on the gateway

Connection checks

- Set Transport Layer Security (TLS) to preferred
- Enable Sender Policy Framework (SPF)
- Enable DomainKeys Identified Mail (DKIM)
- Enable Domain-based Message Authentication, Reporting, and Conformance (DMARC) Verification and Send Aggregate Feedback Reports





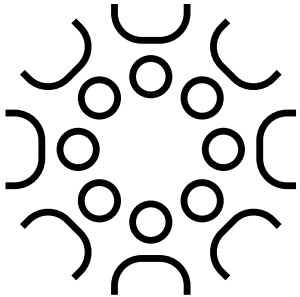
Connected

What should we use?

Anti-virus

Content Filters

File Reputation and Analysis



Safe Printing

BEC protection

URL Manipulation

Phishing prevention

Reputation

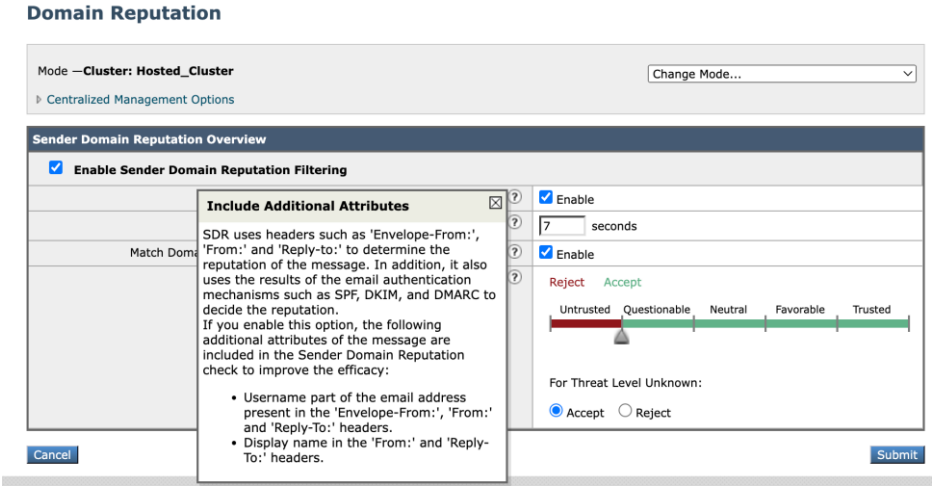
Anti-spam

AI/ML analysis

Dictionaries

Sender based reputation

- Cisco Talos Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on a sender's domain and other attributes.



Make sure to enable the sending of additional attributes

Incoming/outgoing Mail Policies

- Apply Policy per sender or recipient domain/address
- Activate features as required per polity

- Apply content filters per policy

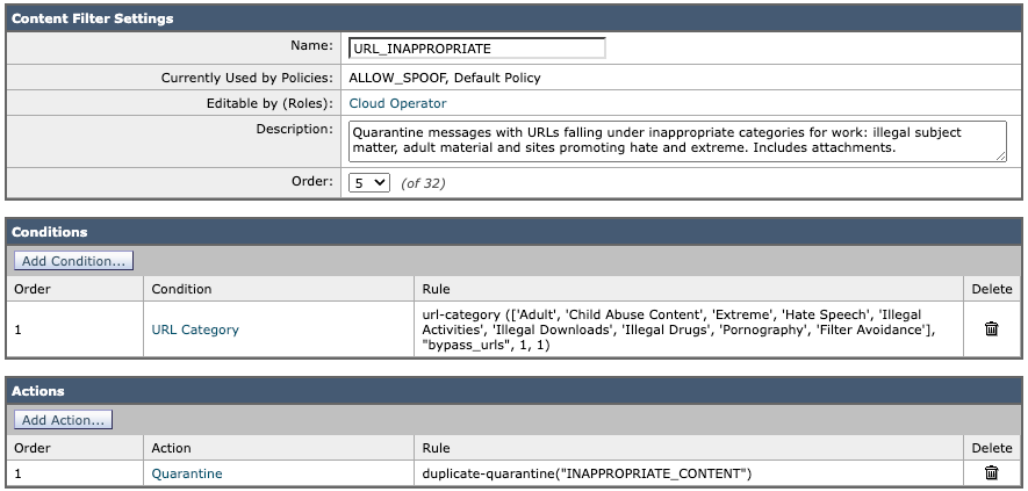
Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	BLOCKED_LIST	Disabled	Disabled	Disabled	Disabled	BLOCKED_LIST_QUARANTINE	Disabled	
2	ALLOWED_LIST	IronPort Anti-Spam Positive: Deliver Suspected: Deliver	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Deliver ...	File Reputation Malware File: Deliver Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	To-Pass-Quarantine Send-to-sec-proxy sent-to-external-proxy Safe-Print-files	Retention Time: Virus: 1 day Other: Deliver without quarantining	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR AU-Header-translation ...	(use default)	
4	motofanzxr	Disabled	Disabled	(use default)	(use default)	Disabled	Disabled	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL SPF_SOFTFAIL ...	Retention Time: Virus: 1 day Other: Deliver without quarantining	

Content filtering

- Content filters allow you to inspect the intricate details of an email and take actions
- Can be created inbound and outbound



Content Filter Settings

Name:	URL_INAPPROPRIATE
Currently Used by Policies:	ALLOW_SPOOF, Default Policy
Editable by (Roles):	Cloud Operator
Description:	Quarantine messages with URLs falling under inappropriate categories for work: illegal subject matter, adult material and sites promoting hate and extreme. Includes attachments.
Order:	5 (of 32)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Category	url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("INAPPROPRIATE_CONTENT")	

Content Filtering

- Make sure to enable:
  - URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT

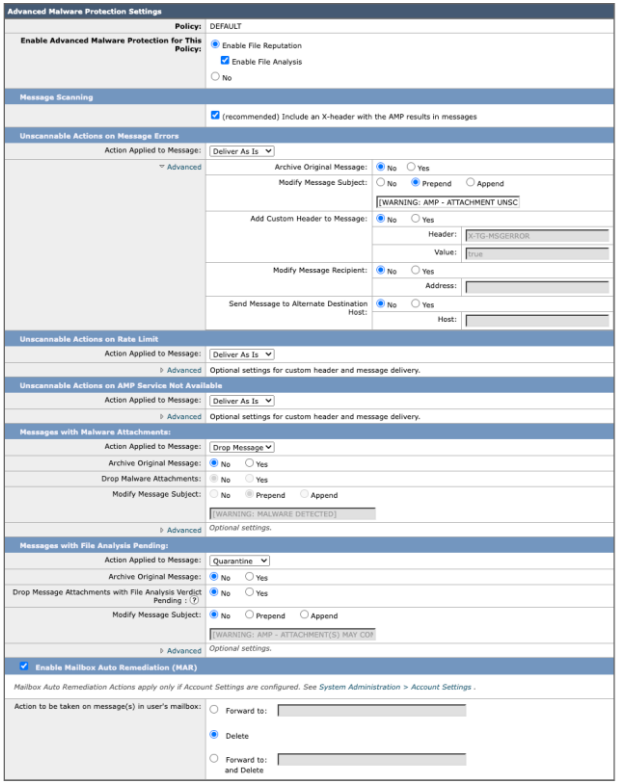
Content Filters

Order	Filter Name	Description	Enable
1	To-Pass-Quarantine		☐
2	delay		☐
3	URL_QUARANTINE_MALICIOUS	Quarantine messages with known malicious URLs. Includes attachments.	☑
4	URL_REWRITE_SUSPICIOUS	Sample policy: Re-write URLs on the cusp of malicious reputation to be scanned a...	☑
5	URL_INAPPROPRIATE	Quarantine messages with URLs falling under inappropriate categories for work: i...	☑
6	DKIM_FAILURE	quarantine a copy of mail failing DKIM verification	☑
7	URL_PROXY_CONTROL		☐
8	SPF_HARDFAIL	quarantine a copy of messages with hardfail response from SPF.	☑
9	URL_MANIPULATION		☐
10	SPF_SOFTFAIL	quarantine a copy of messages with soft fail response on SPF *expect false posit...	☑
11	EXECUTIVE_SPOOF	Identify potential spoofed email from high value sources like an executive	☑
12	DOMAIN_SPOOF	rule to look for external spoofs	☑
13	SDR	rule to monitor sender domain reputation data	☑
14	TG_RATE_LIMIT	used to count # TG upload failed due to rate limit - uploads denied	☑

More details about these Content filters:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html

File reputation and analysis

- File SHA reputation base lookup
- Cloud-based analysis for unknown file reputation
- Drop or quarantine the message
- Notify users of the unscannable attachments(due to error, upload limit)

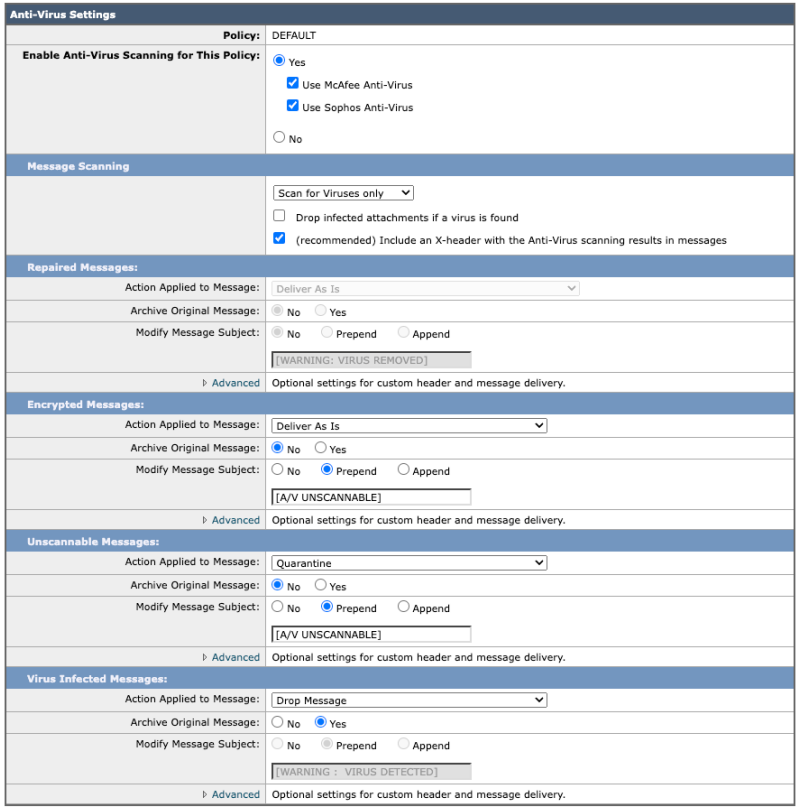


For Unscannable Actions on Message Errors, use Advanced and Add Custom Header to Message, X-TG-MSGERROR, value: True.

For Unscannable Actions on Rate Limit, use Advanced and Add Custom Header to Message, X-TG-RATELIMIT, value: True.

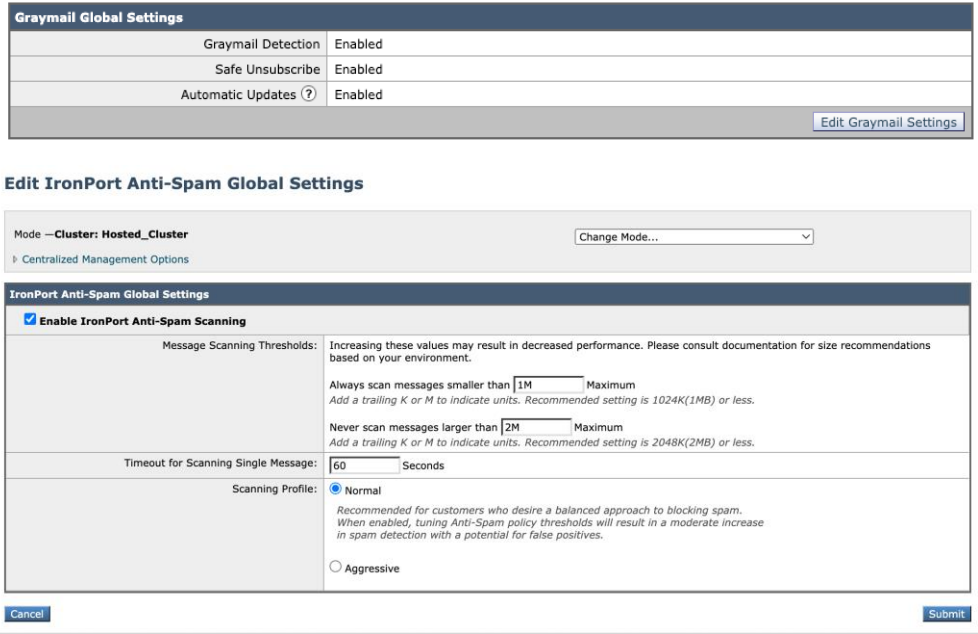
Anti-virus

- Leverage more than one AV engine
- Use this to identify, not repair
- Quarantine or drop infected messages
- Notify users of the unscannable attachments



Anti-spam

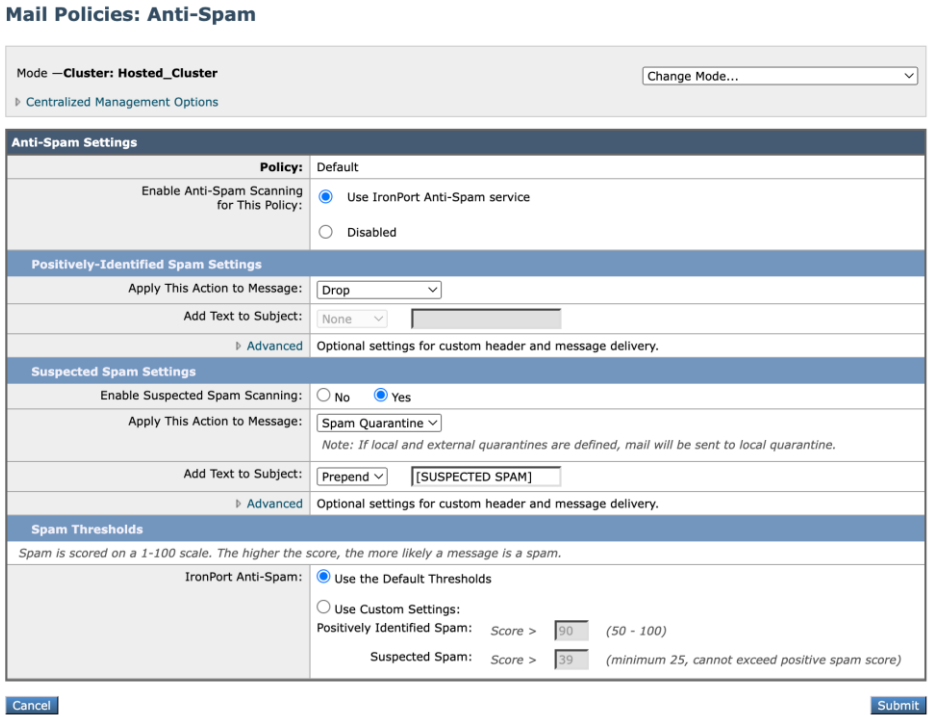
- Make sure you have anti-spam and graymail enabled
- Adjust the settings to always scan messages smaller than 1M
- Never scan messages larger than 2M



According to Cisco Talos, most spam captures as between 512KB and 896KB

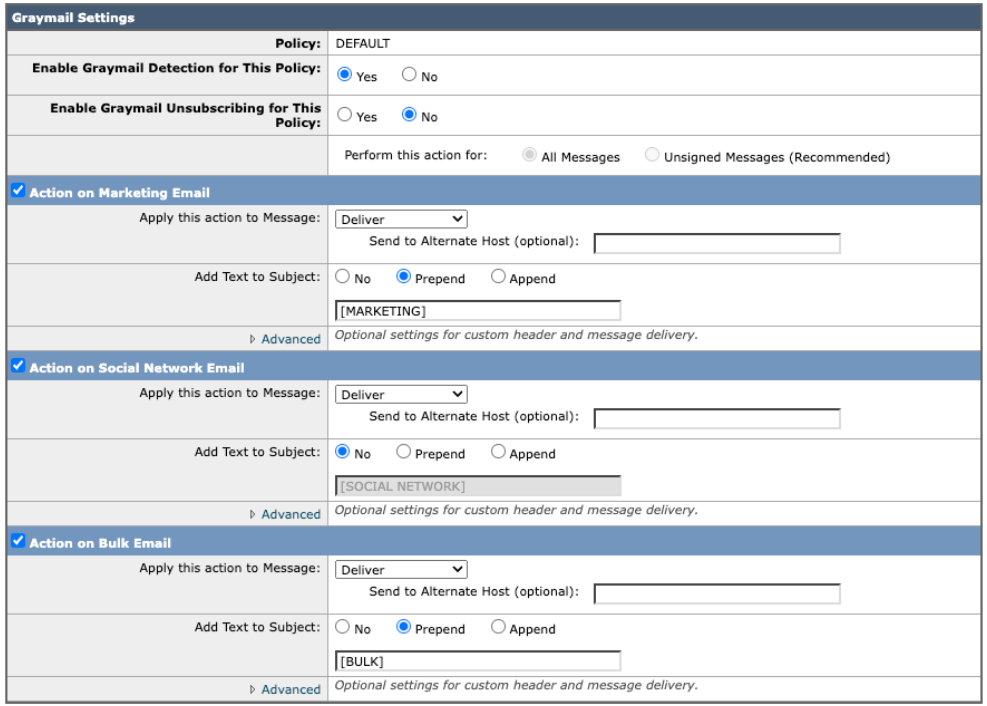
Anti-spam (per policy)

- Drop positively-identified messages
- Prepend on subject to inform the user and/or quarantine the message
- Adjust the Spam Thresholds for more aggressive policy



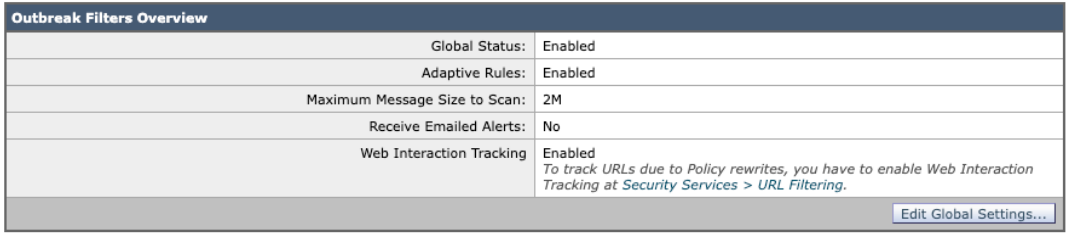
Graymail

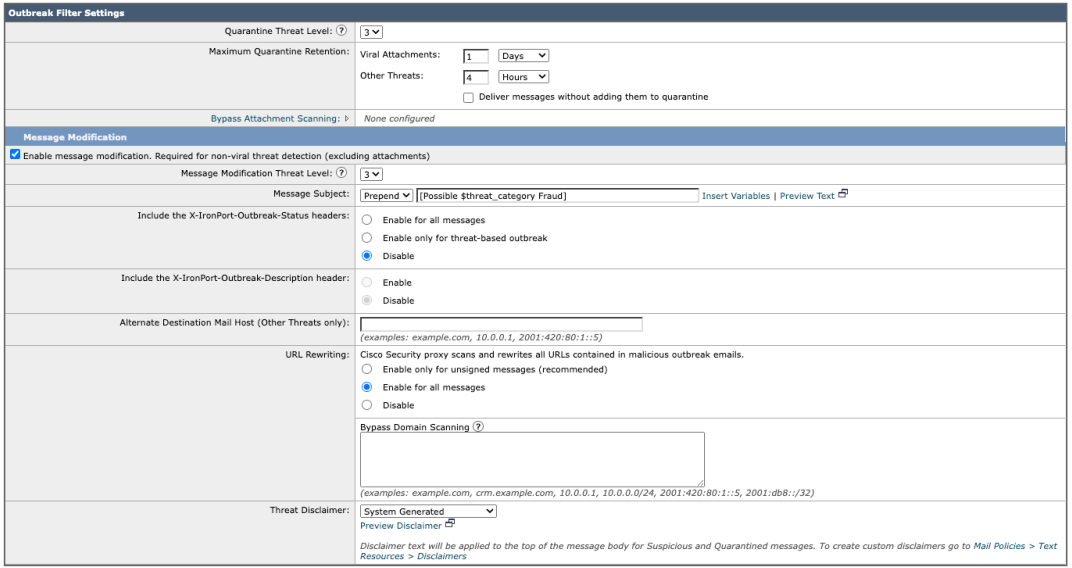
- Scanning is enabled for each verdict (Marketing, Social, Bulk), with Prepend for Add Text to Subject and action is Deliver.
- For Action on Bulk Mail, use Advanced and Add Custom Header (optional): X-Bulk, value: True.



Outbreak filters

- Outbreak filters protect your network from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur.
- Used to enable URL rewriting and safe-browsing
- Make sure it is enabled and used by the policy and max message size set to 2M





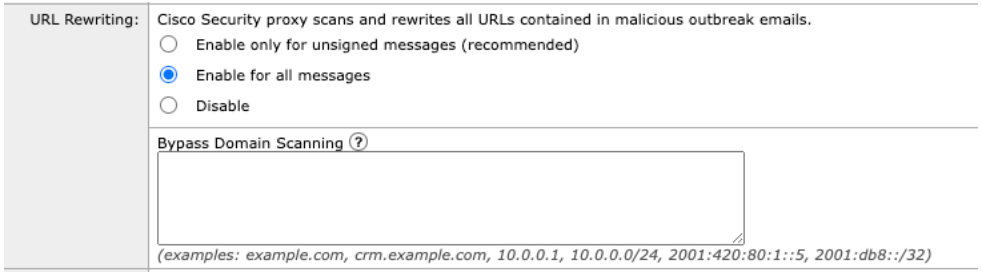
Outbreak filters

- These are the threat levels/risk provided by this service

Level	Risk	Meaning
0	None	There is no risk that the message is a threat.
1	Low	The risk that the message is a threat is low.
2	Low/Medium	The risk that the message is a threat is low to medium. It is a “suspected” threat.
3	Medium	Either the message is part of a confirmed outbreak or there is a medium to large risk of its content being a threat.
4	High	Either the message is confirmed to be part of a large-scale outbreak or its content is very dangerous.
5	Extreme	The message’s content is confirmed to be part of an outbreak that is either extremely large scale or large scale and extremely dangerous.

URL rewriting

- Outbreak filters can rewrite URLs to redirect traffic to potentially harmful websites through a web security proxy, which either warns users that the website they are attempting to access may be malicious or blocks the website completely.



URL rewriting can also be used in content filters for specific categories, reputations, sites, etc.

Cloud URL analysis

- Cisco Talos Intelligence Cloud Services analyses URLs. This cloud service integrates existing WBRS information with a variety of different analysis techniques. By actively analyzing many facets of a URL, from the structure of the URL itself to information about the domain and even page contents, Cisco Talos Intelligence Cloud Services provides the ability to detect and deliver intelligence on a variety of URL-based attacks

- Enable Service Logs
- Enable Outbreak filters
- Enable Web Interaction Tracking

No user or admin additional configurations are required to levarage CUA

Dictionaries

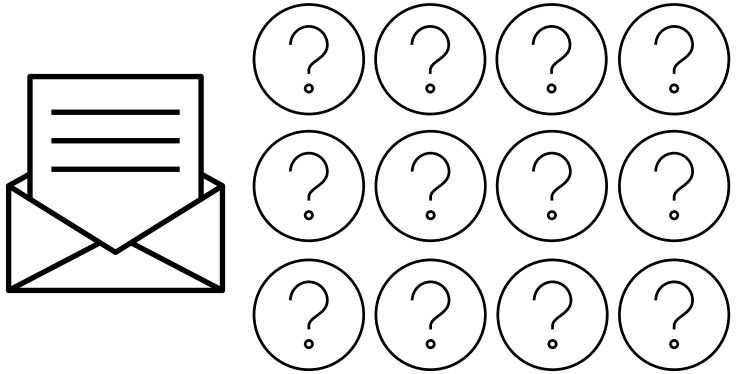
- Enable and review Profanity and Sexual_Content Dictionary
- Create Executive_FED dictionary for Forged Email Detection with all executive names
- Create additional dictionaries for restricted or other keywords as you see needed for your policies, environment, security control©

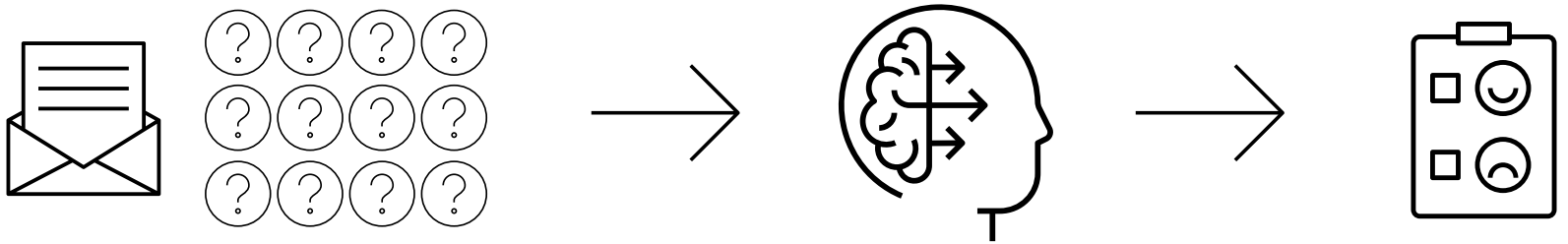
URL filtering

- Enable Security Services > URL Filtering
- Enable URL Category and Reputation Filters
- Enable Web Interaction Tracking in URL Filtering

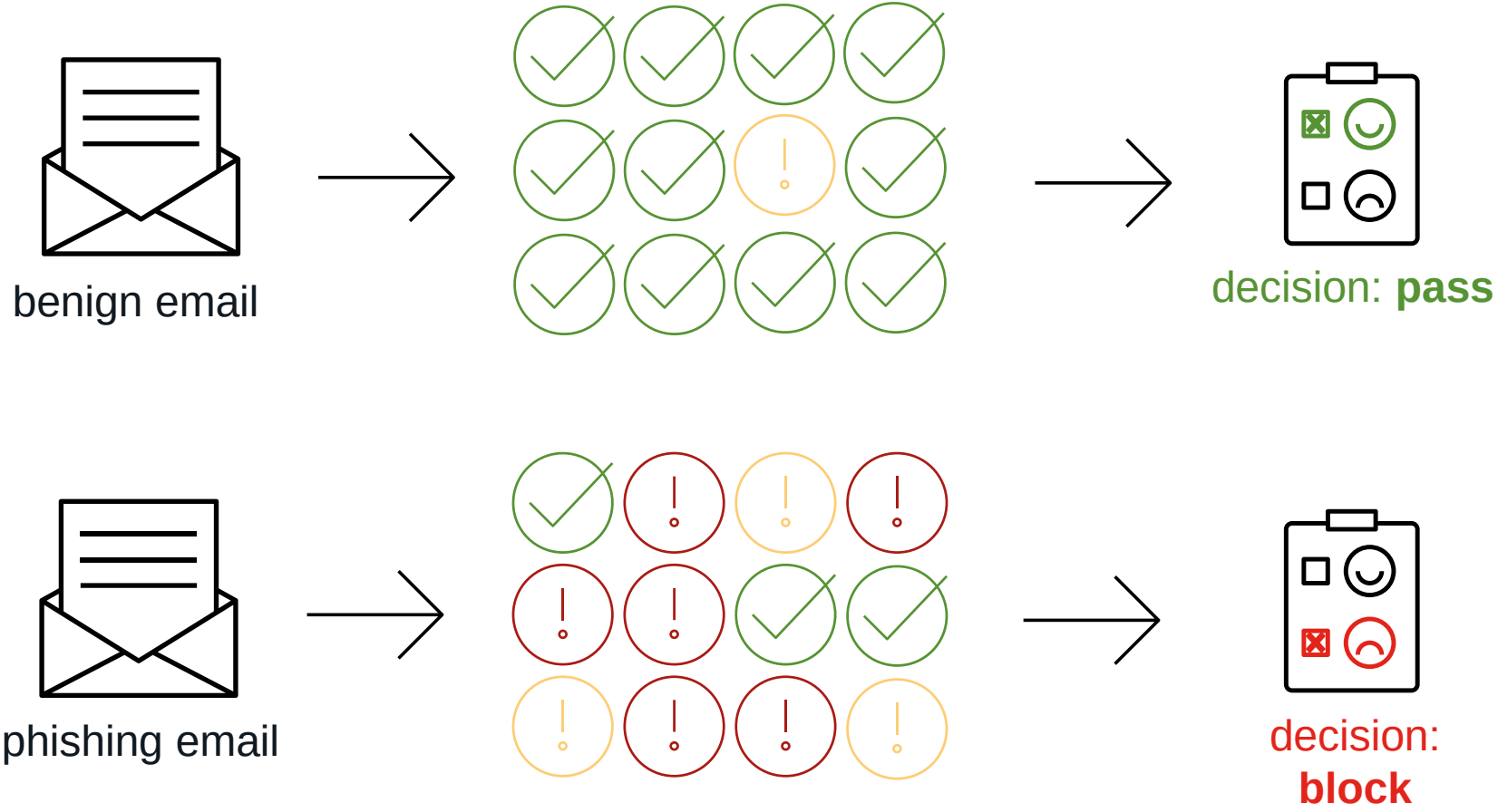
URL Filtering Overview	
URL Category and Reputation Filters:	Enabled
Cisco Web Security Services connection status:	Connected
URL Allowed List:	bypass_urls
Web Interaction Tracking:	Enabled *To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking at Security Services > Outbreak Filters.*
URL Retrospective service status	Connected.

Each email is checked for a variety of independent signals

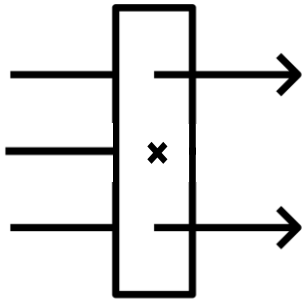




The final verdict is then given by aggregating the signals

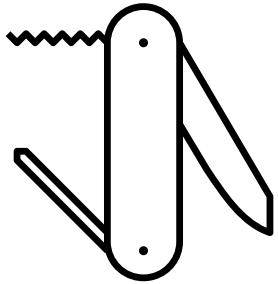


Why behavioral detection works in email security



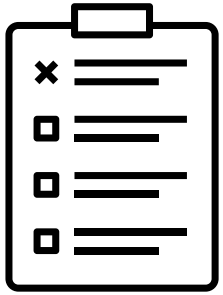
Precise

Blocks phishing attempts, yet allow legitimate emails



Evolutive

Catches ever-changing variations of attack patterns

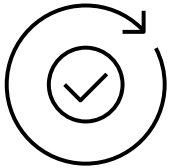


Interpretable

Tells you why an email was flagged

Post-Delivery

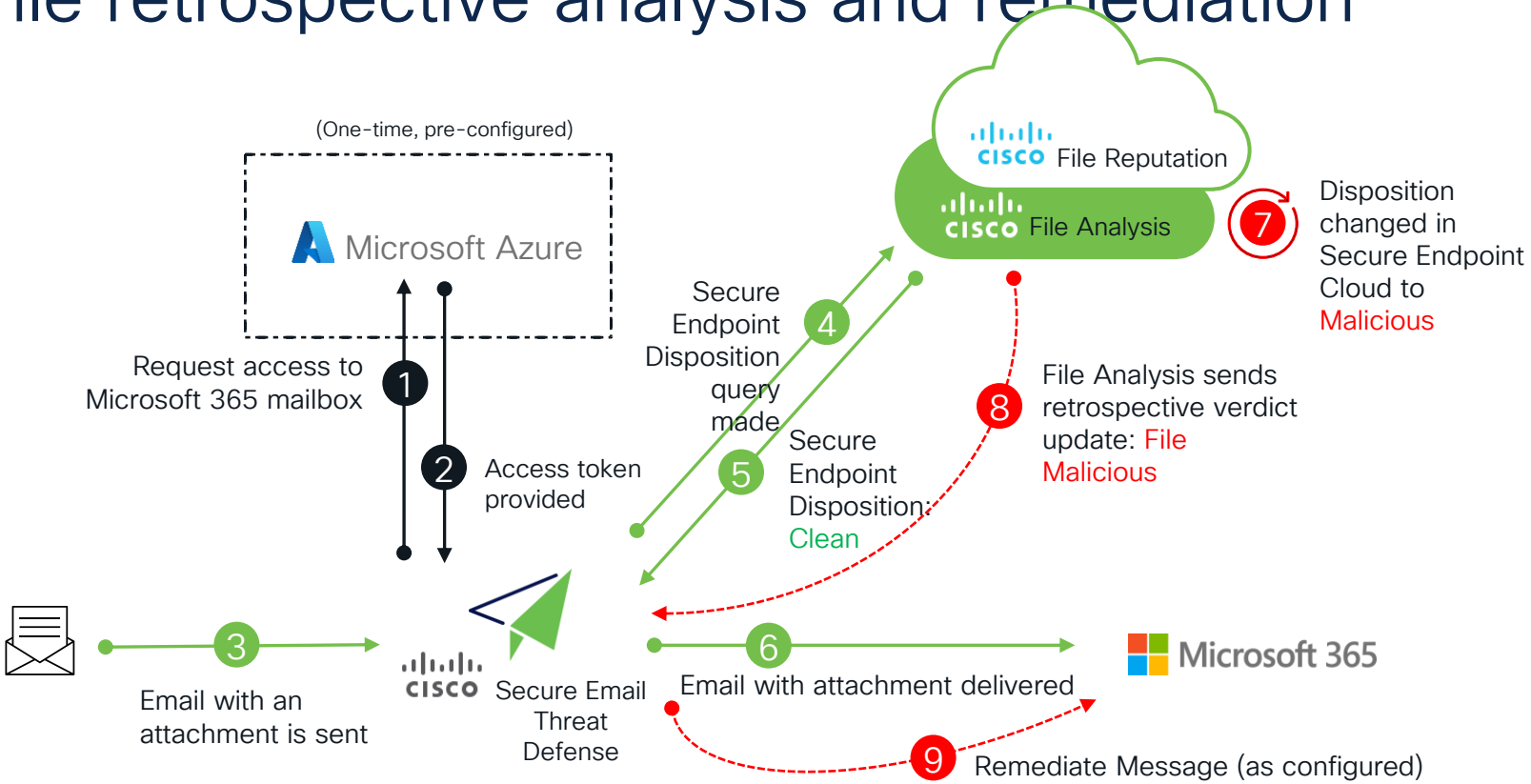
What should we use?



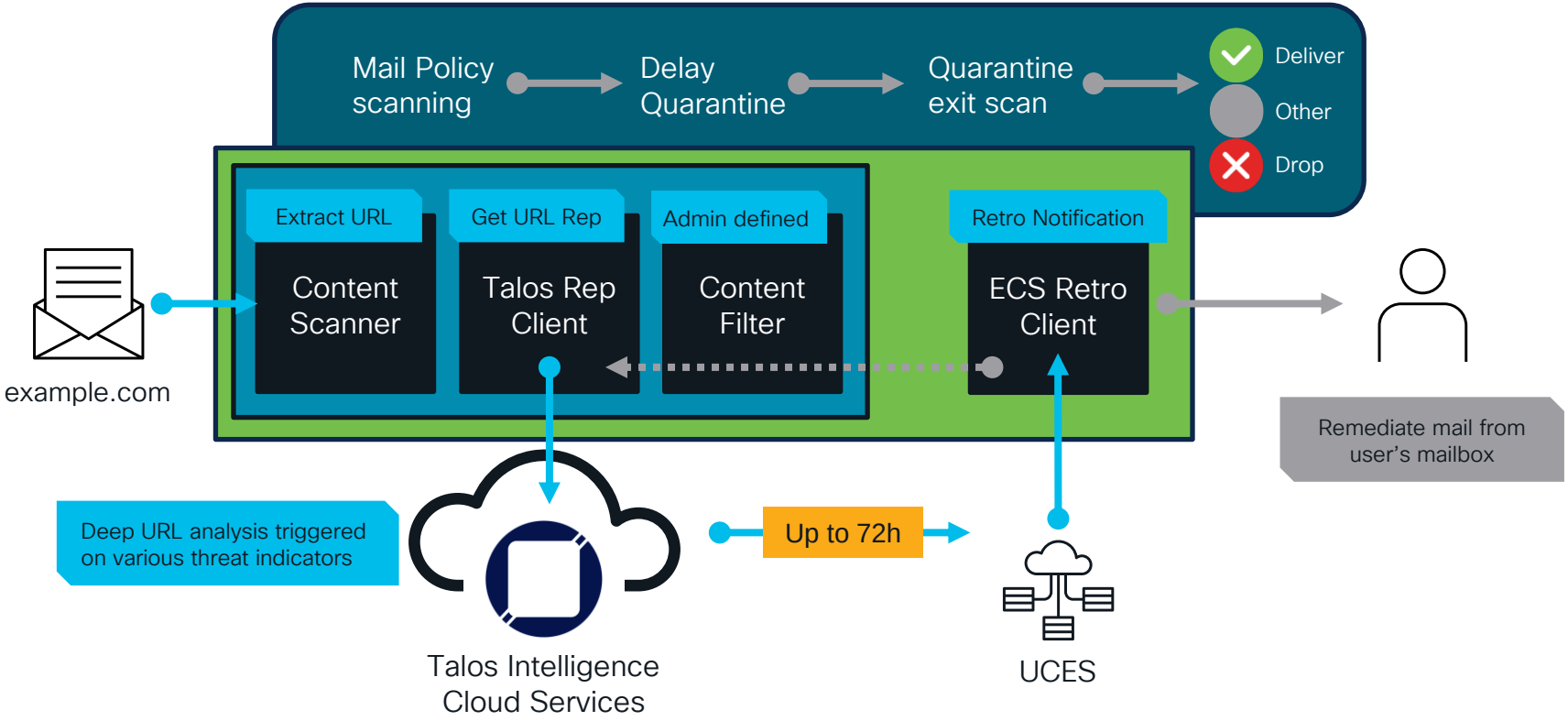
Retrospective analysis

Secure Browsing

File retrospective analysis and remediation



URL retrospective analysis and remediation



Call to action

Call to action

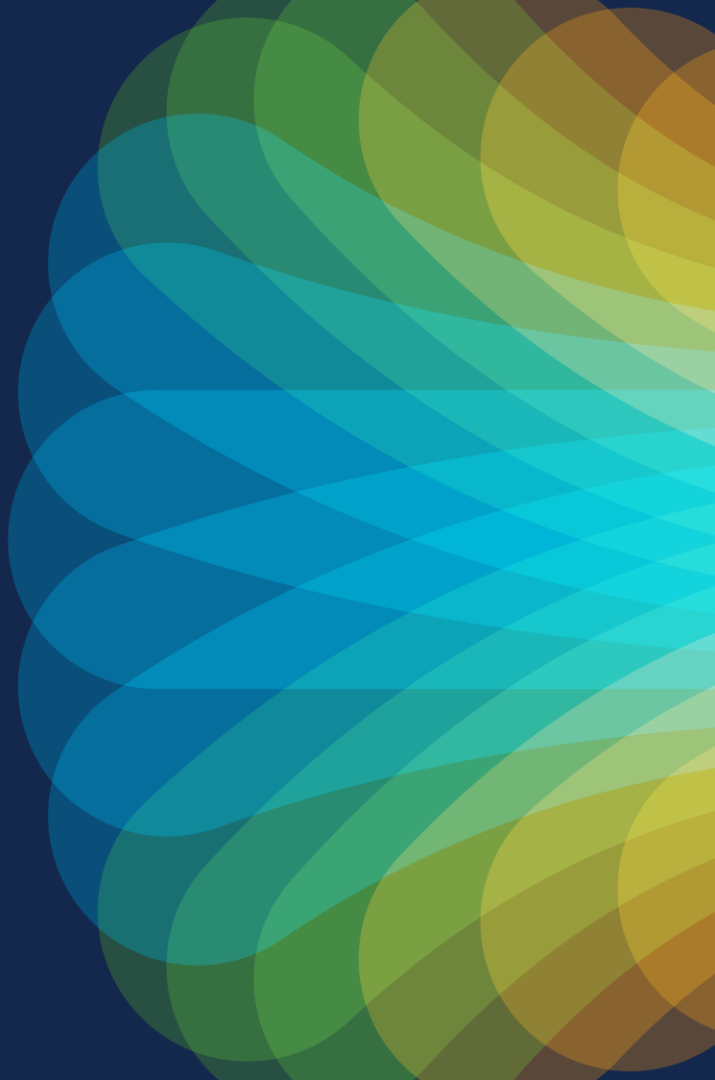
1. Make sure your solution covers the 3 stages of protection
   - Connection
   - Connected
   - Delivered
2. Fine-tune your solution according to the best practices to achieve efficacy
3. Run a POC with Cisco Secure Email Threat Defense:
   - https://cs.co/etd-trial
   - https://order.ces.cisco.com/eval/#

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you




cisco Live!
Let's go
#CiscoLive