

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

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



#CiscoLive

# Cisco Webex App

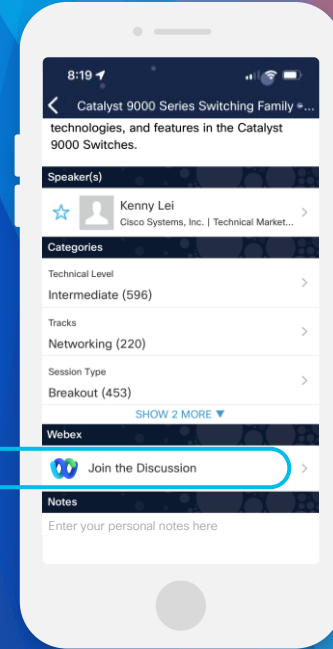
## Questions?

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://cislive.ciscoevents.com/cislivebot/#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)

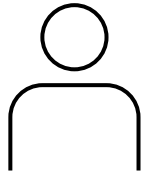
Music lover (I play Guitar, Drums, and Piano)

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



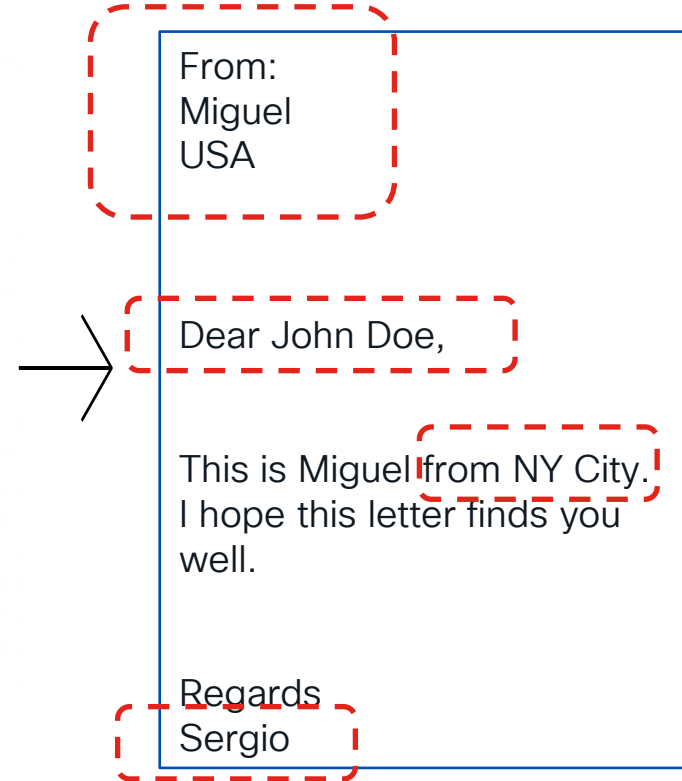
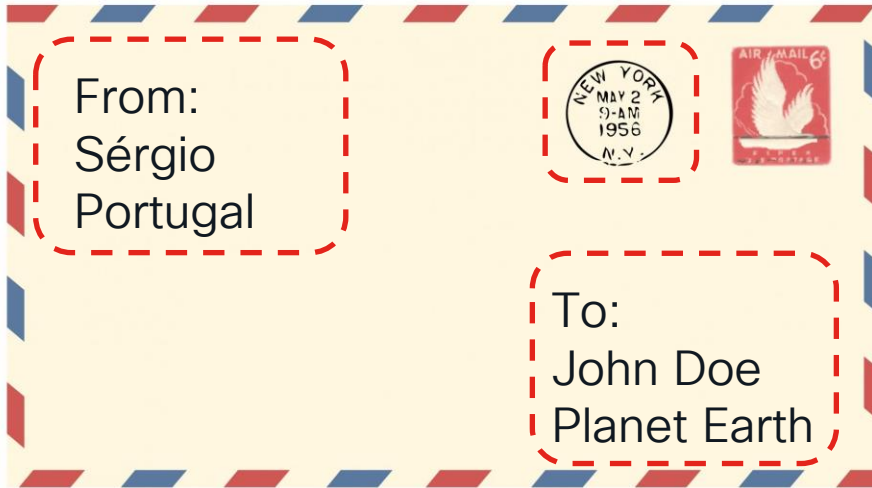
58%

The first thing they  
check in the  
morning

Source: [www.statista.com](https://www.statista.com)



# Easy to spoof & impersonate

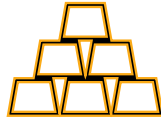


# Brand / Data / Financial loss



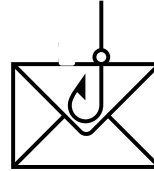
500.000

Complaints  
per year



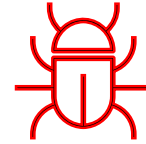
\$10.3B

Financial  
Damage



300.000

Phishing  
victims with  
\$52M in  
damage



\$2.7B

Loss due to  
BEC attacks

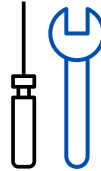
What are the  
best practices?

# What are best practices



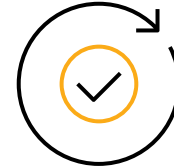
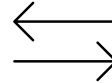
## Analyse

Know your environment and requirements



## Tune

Fine tune the configuration to meet your requirements



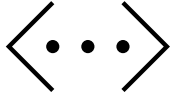
## Monitor

Keep an eye for the results produced after the tuning

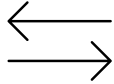
The recommendations presented during this session are general guidelines

# Protection Phases

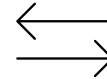
# Protection phases



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)

Sender Groups (Listener: MailFlow)

Add Sender Group... Import HAT...

Order	Sender Group	SenderBase™ Reputation Score ?	External Threat Feed Sources Applied	Mail Flow Policy	Delete
1	test_moto		None applied	ACCEPTED	
2	SMA		None applied	RELAYED	
3	CISCO_MONITORING		None applied	ACCEPTED	
4	RELAYLIST		None applied	RELAYED	
5	MY_TRUSTED_SPOOF_HOSTS		None applied	ACCEPTED	
6	BYPASS_SBRS_SPAM		None applied	ACCEPTED_NOSPAM	
7	BYPASS_SBRS		None applied	ACCEPTED	
8	BLOCKED_LIST_REFUSE		None applied	BLOCKED_REFUSE	
9	BLOCKED_LIST_REJECT		None applied	BLOCKED_REJECT	
10	SUSPECTLIST		None applied	THROTTLED	
11	FREEMAIL		None applied	THROTTLED	
12	ACCEPTLIST		None applied	ACCEPTED	
	ALL		None applied	ACCEPTED	

Edit Order... Export HAT...

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

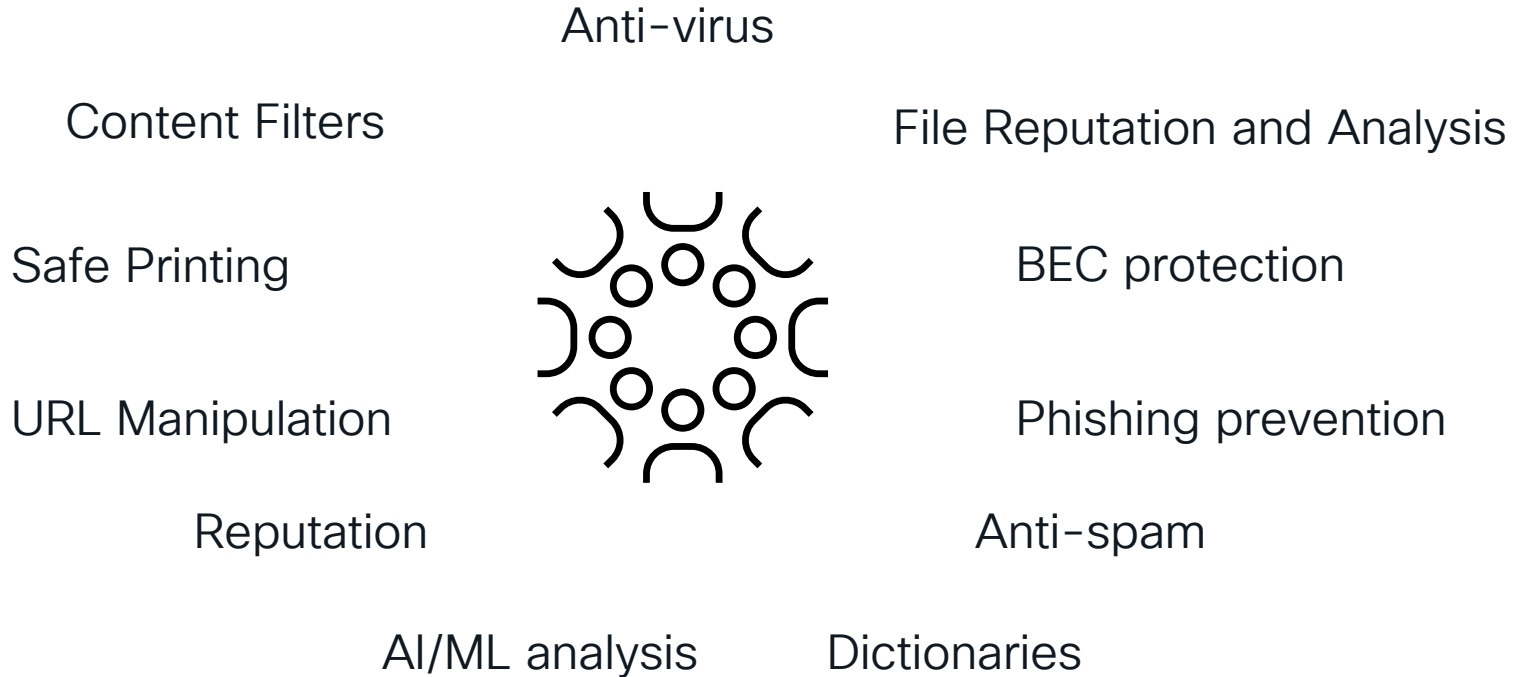
Encryption and Authentication:	TLS:	<input checked="" type="radio"/> Use Default (Preferred) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
		<input type="checkbox"/> TLS is Mandatory for Address List (None) <input type="checkbox"/> Verify Client Certificate
	SMTP Authentication:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication
Domain Key/DKIM Signing:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> On <input type="radio"/> Off	
DKIM Verification:	<input checked="" type="radio"/> Use Default (On: DEFAULT) <input type="radio"/> On <input type="radio"/> Off	
	Use DKIM Verification Profile:	DEFAULT ▼

SPF/SIDF Verification:	<input checked="" type="radio"/> Use Default (On) <input type="radio"/> On <input type="radio"/> Off	
	Conformance Level:	Default (SPF) ▼
	HELO Test:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> On
DMARC Verification	<input checked="" type="radio"/> Use Default (On: MONITOR) <input type="radio"/> On <input type="radio"/> Off	
	Use DMARC Verification Profile:	ENFORCE ▼
	DMARC Feedback Reports: ⓘ	<input checked="" type="checkbox"/> Send aggregate feedback reports <small>* DMARC reporting message must be DMARC compliant. * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies &gt; Destination Controls.</small>

# Connected



# What should we use?



# 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.

**Domain Reputation**

Mode — **Cluster: Hosted\_Cluster** Change Mode...

» Centralized Management Options

---

**Sender Domain Reputation Overview**

☒ **Enable Sender Domain Reputation Filtering**

Match Domains

**Include Additional Attributes** ☒ ?

SDR uses headers such as 'Envelope-From:', 'From:', and 'Reply-to:' to determine the reputation of the message. In addition, it also uses the results of the email authentication mechanisms such as SPF, DKIM, and DMARC to decide the reputation.

If you enable this option, the following additional attributes of the message are included in the Sender Domain Reputation check to improve the efficacy:

- Username part of the email address present in the 'Envelope-From:', 'From:' and 'Reply-To:' headers.
- Display name in the 'From:' and 'Reply-To:' headers.

☒ ? **Enable**

?  seconds

☒ ? **Enable**

? **Reject Accept**

Untrusted Questionable Neutral Favorable Trusted

For Threat Level Unknown:

☒ Accept ☐ Reject

Cancel Submit

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 policy
- 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 Uncannable: Deliver Virus Positive: Deliver ...	File Reputation Malware File: Deliver Pending Analysis: Deliver Uncannable - Message Error: Deliver Uncannable - Rate Limit: Deliver Uncannable - 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	motofanzr	Disabled	Disabled	(use default)	(use default)	Disabled	Disabled	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Uncannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Deliver Uncannable - Message Error: Deliver Uncannable - Rate Limit: Deliver Uncannable - 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		<input type="checkbox"/>
2	delay		<input type="checkbox"/>
3	URL_QUARANTINE_MALICIOUS	Quarantine messages with known malicious URLs. Includes attachments.	<input checked="" type="checkbox"/>
4	URL_REWRITE_SUSPICIOUS	Sample policy: Re-write URLs on the cusp of malicious reputation to be scanned a...	<input checked="" type="checkbox"/>
5	URL_INAPPROPRIATE	Quarantine messages with URLs falling under inappropriate categories for work: i...	<input checked="" type="checkbox"/>
6	DKIM_FAILURE	quarantine a copy of mail failing DKIM verification	<input checked="" type="checkbox"/>
7	URL_PROXY_CONTROL		<input type="checkbox"/>
8	SPF_HARDFAIL	quarantine a copy of messages with hardfail response from SPF.	<input checked="" type="checkbox"/>
9	URL_MANIPULATION		<input type="checkbox"/>
10	SPF_SOFTFAIL	quarantine a copy of messages with soft fail response on SPF *expect false posit...	<input checked="" type="checkbox"/>
11	EXECUTIVE_SPOOF	Identify potential spoofed email from high value sources like an executive	<input checked="" type="checkbox"/>
12	DOMAIN_SPOOF	rule to look for external spoofs	<input checked="" type="checkbox"/>
13	SDR	rule to monitor sender domain reputation data	<input checked="" type="checkbox"/>
14	TG_RATE_LIMIT	used to count # TG upload failed due to rate limit - uploads denied	<input checked="" type="checkbox"/>

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.

The screenshot displays the 'Advanced Malware Protection Settings' configuration page. The 'Policy' is set to 'DEFAULT'. Under 'Enable Advanced Malware Protection for This Policy', the options 'Enable File Reputation' and 'Enable File Analysis' are both checked. The 'Message Scanning' section has a checkbox for '(recommended) Include an X-header with the AMP results in messages' which is checked. The 'Unscannable Actions on Message Errors' section shows 'Action Applied to Message:' set to 'Deliver As Is'. Under the 'Advanced' tab, 'Archive Original Message' is set to 'No', 'Modify Message Subject' is set to 'Prepend' with the value '[WARNING: AMP - ATTACHMENT UNSCANNABLE]', and 'Add Custom Header to Message' is checked with the header 'X-TG-MSGERROR' and value 'True'. The 'Unscannable Actions on Rate Limit' section also shows 'Action Applied to Message:' set to 'Deliver As Is'. The 'Unscannable Actions on AMP Service Not Available' section shows 'Action Applied to Message:' set to 'Deliver As Is'. The 'Messages with Malware Attachments' section shows 'Action Applied to Message:' set to 'Drop Message'. The 'Messages with File Analysis Pending' section shows 'Action Applied to Message:' set to 'Quarantine'. At the bottom, the 'Enable Mailbox Auto Remediation (NAR)' checkbox is checked, and the 'Action to be taken on message(s) in user's mailbox:' is set to 'Delete'.



# 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-Virus Settings	
Policy:	DEFAULT
Enable Anti-Virus Scanning for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	<input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus
Message Scanning	
	Scan for Viruses only
	<input type="checkbox"/> Drop infected attachments if a virus is found
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: VIRUS REMOVED]
	Advanced Optional settings for custom header and message delivery.
Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
	Advanced Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Quarantine
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
	Advanced Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
	Advanced Optional settings for custom header and message delivery.

# 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

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates ?	Enabled

[Edit Graymail Settings](#)

## Edit IronPort Anti-Spam Global Settings

Mode —Cluster: Hosted\_Cluster [Change Mode...](#)

[Centralized Management Options](#)

### IronPort Anti-Spam Global Settings

☒ **Enable IronPort Anti-Spam Scanning**

Message Scanning Thresholds: Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.

Always scan messages smaller than  Maximum  
Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.

Never scan messages larger than  Maximum  
Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.

Timeout for Scanning Single Message:  Seconds

Scanning Profile: ☒ Normal  
Recommended for customers who desire a balanced approach to blocking spam. When enabled, tuning Anti-Spam policy thresholds will result in a moderate increase in spam detection with a potential for false positives.

☐ Aggressive

[Cancel](#) [Submit](#)

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

## Mail Policies: Anti-Spam

Mode —Cluster: Hosted\_Cluster

Change Mode...

Centralized Management Options

Anti-Spam Settings

Policy: Default

Enable Anti-Spam Scanning for This Policy:

☒ Use IronPort Anti-Spam service

☐ Disabled

Positively-Identified Spam Settings

Apply This Action to Message: Drop

Add Text to Subject: None

AdvancedOptional settings for custom header and message delivery.

Suspected Spam Settings

Enable Suspected Spam Scanning: No ☒ Yes

Apply This Action to Message: Spam Quarantine

Note: If local and external quarantines are defined, mail will be sent to local quarantine.

Add Text to Subject: Prepend [SUSPECTED SPAM]

AdvancedOptional settings for custom header and message delivery.

Spam Thresholds

Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.

IronPort Anti-Spam: ☒ Use the Default Thresholds

☐ Use Custom Settings:

Positively Identified Spam: Score > 90 (50 - 100)

Suspected Spam: Score > 39 (minimum 25, cannot exceed positive spam score)

Cancel

Submit

# 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.

Graymail Settings	
Policy:	DEFAULT
Enable Graymail Detection for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input type="radio"/> Yes <input checked="" type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages <input type="radio"/> Unsigned Messages (Recommended)
<b>Action on Marketing Email</b>	
Apply this action to Message:	<div>Deliver</div> <div>Send to Alternate Host (optional):</div>
Add Text to Subject:	<div><input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append</div> <div>[MARKETING]</div>
	<div>Advanced</div> Optional settings for custom header and message delivery.
<b>Action on Social Network Email</b>	
Apply this action to Message:	<div>Deliver</div> <div>Send to Alternate Host (optional):</div>
Add Text to Subject:	<div><input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append</div> <div>[SOCIAL NETWORK]</div>
	<div>Advanced</div> Optional settings for custom header and message delivery.
<b>Action on Bulk Email</b>	
Apply this action to Message:	<div>Deliver</div> <div>Send to Alternate Host (optional):</div>
Add Text to Subject:	<div><input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append</div> <div>[BULK]</div>
	<div>Advanced</div> Optional settings for custom header and message delivery.

# 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 Overview	
Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	2M
Receive Emailed Alerts:	No
Web Interaction Tracking	Enabled <i>To track URLs due to Policy rewrites, you have to enable Web Interaction Tracking at Security Services &gt; URL Filtering.</i>
<a href="#">Edit Global Settings...</a>	

Outbreak Filter Settings	
Quarantine Threat Level: <a href="#">?</a>	3 ▾
Maximum Quarantine Retention:	Viral Attachments: 1 ▾ Days ▾ Other Threats: 4 ▾ Hours ▾ <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▾	None configured
Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: <a href="#">?</a>	3 ▾
Message Subject:	Prepend ▾ [Possible \$threat_category Fraud] <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
	Bypass Domain Scanning <a href="#">?</a> <input type="text"/> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>
Threat Disclaimer:	System Generated ▾ <a href="#">Preview Disclaimer</a> <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies &gt; Text Resources &gt; Disclaimers</small>

# 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:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
	Bypass Domain Scanning <a href="#">?</a> <div></div> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>

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 leverage 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©

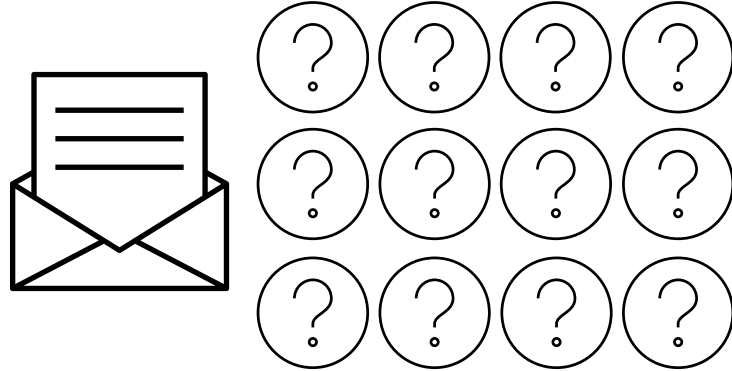
Executive_FED	placeholder (1)
Internal_Domains	@placeholder.com (1)
Profanity	... (128)
Sexual_Content	adult sight, adult site, adult video, adult web, adult-oriented, adults only, ageof21, altsex, ... (235)
Export Dictionary...	

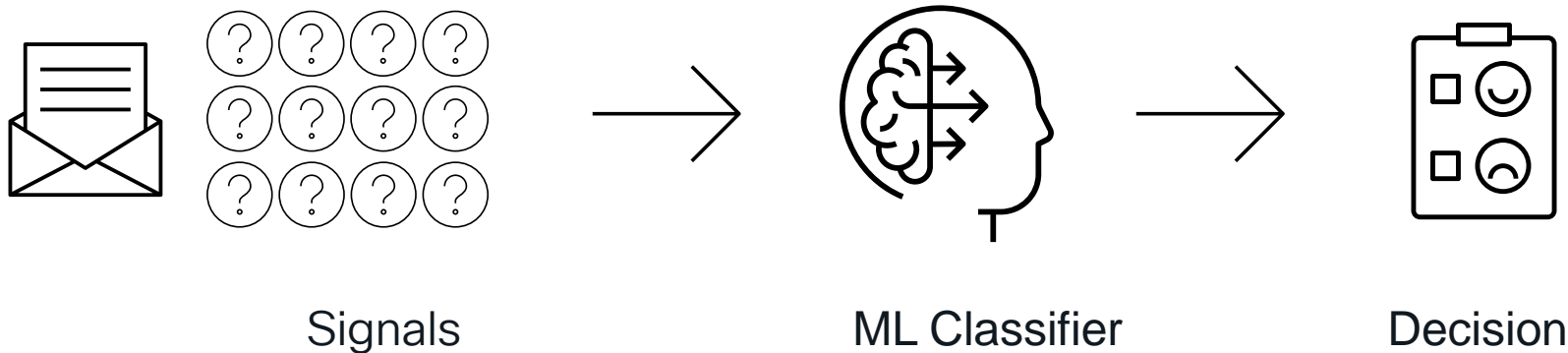
# URL filtering

- 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 <i>To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking at <a href="#">Security Services &gt; Outbreak Filters</a>.</i>
URL Retrospective service status	Connected.

Each email is checked  
for a variety of  
independent signals

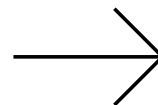
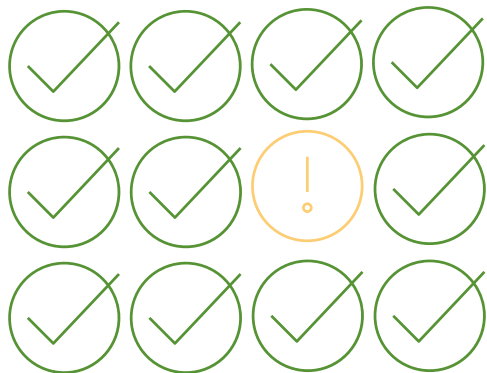
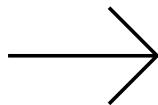




The final verdict is then given  
by aggregating the signals



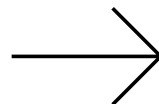
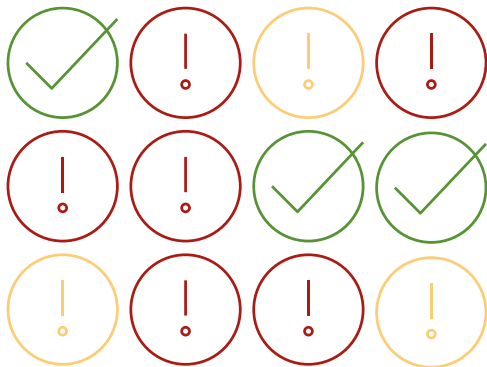
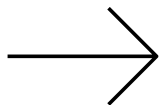
benign email



decision: **pass**

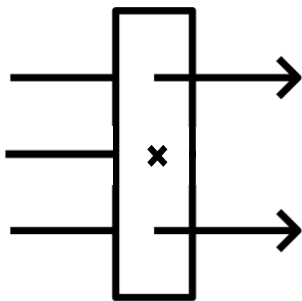


phishing email

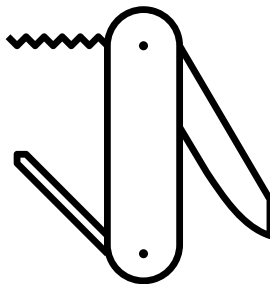


decision:  
**block**

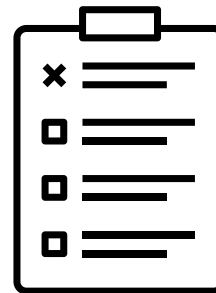
# Why behavioral detection works in email security



Precise  
Blocks phishing attempts,  
yet allow legitimate emails



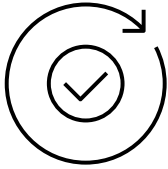
Evolutive  
Catches ever-changing variations of attack patterns



Interpretable  
Tells you why an email was flagged

# Post-Delivery

# What should we use?



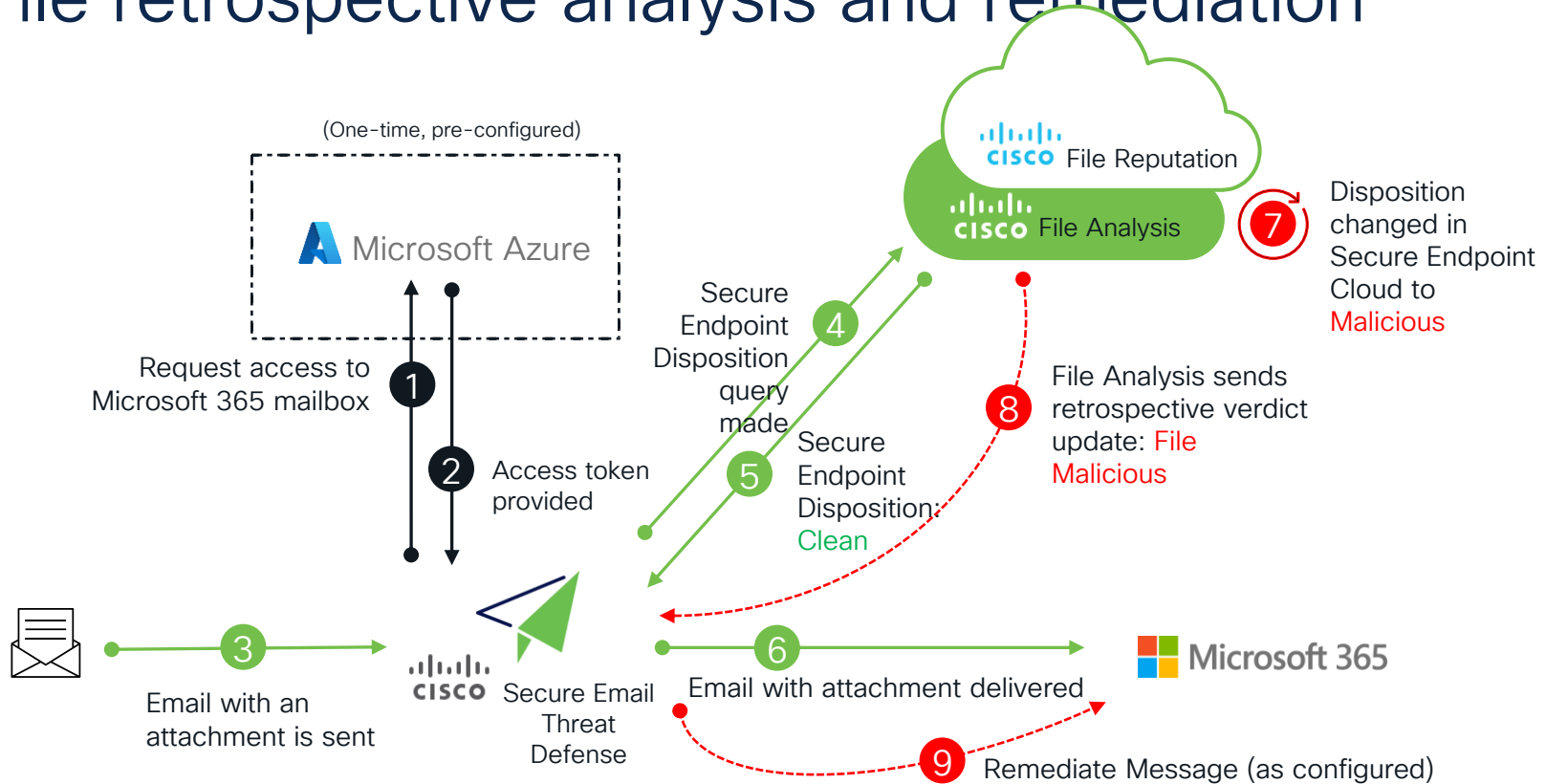
Retrospective analysis



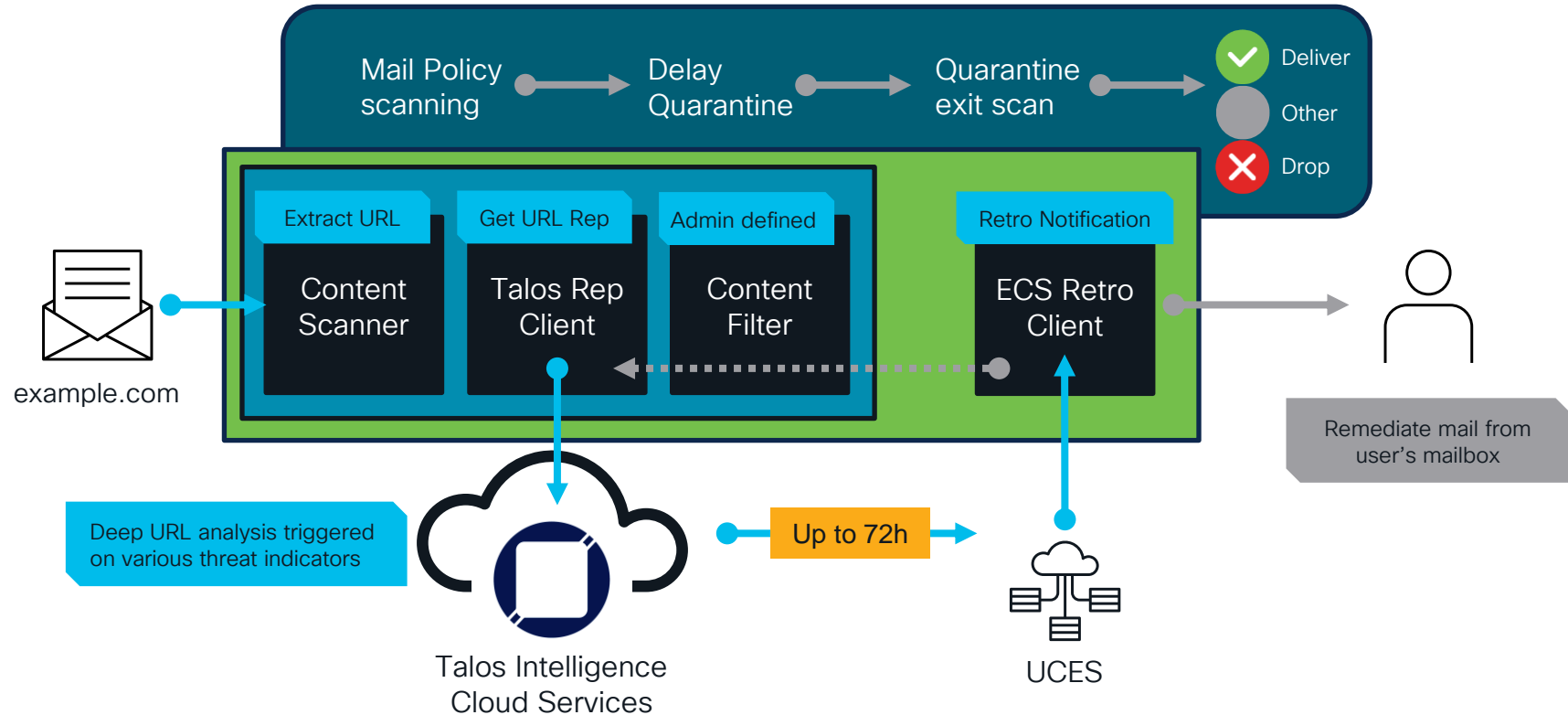
Secure Browsing



# 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](https://www.CiscoLive.com/on-demand)

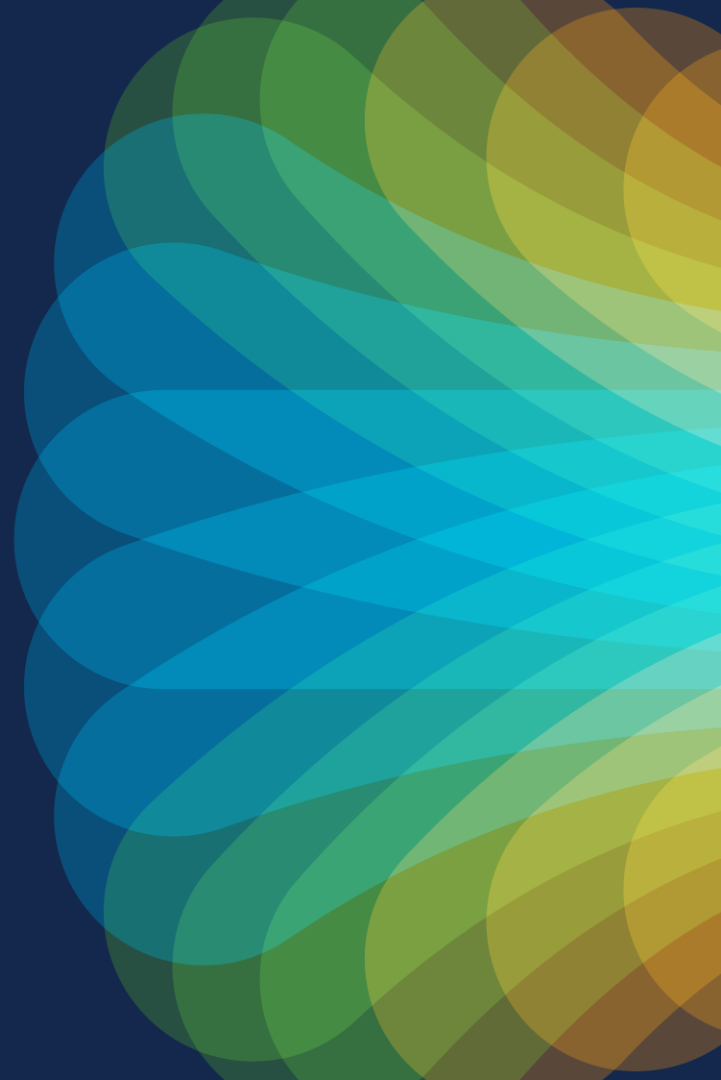


The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, pink, purple, blue, and green. Overlaid on this are large, soft, wavy shapes in shades of orange, red, and yellow, giving the impression of clouds or flowing liquid. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive