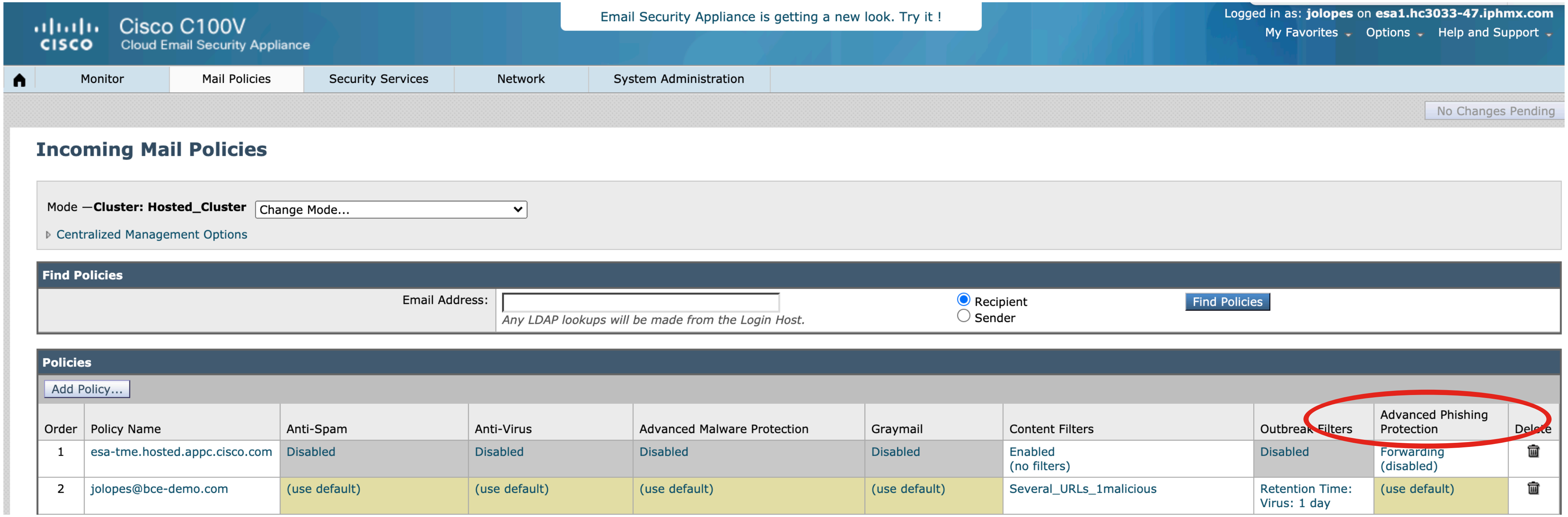
cisco Secure

Cisco Secure Email Phishing Defense

Thomas Jankowsky
Technical Solutions Architect
March 2021

Secure Email Gateway & Phishing Defense Integration



Cisco C100V
Cloud Email Security Appliance
Email Security Appliance is getting a new look. Try it !
Logged in as: **jolopes** on **esa1.hc3033-47.iphmx.com**
My Favorites
Options
Help and Support
Monitor
Mail Policies
Security Services
Network
System Administration
No Changes Pending

Incoming Mail Policies

Mode —**Cluster: Hosted_Cluster** Change Mode...

Centralized Management Options

Find Policies

Email Address: Any LDAP lookups will be made from the Login Host.

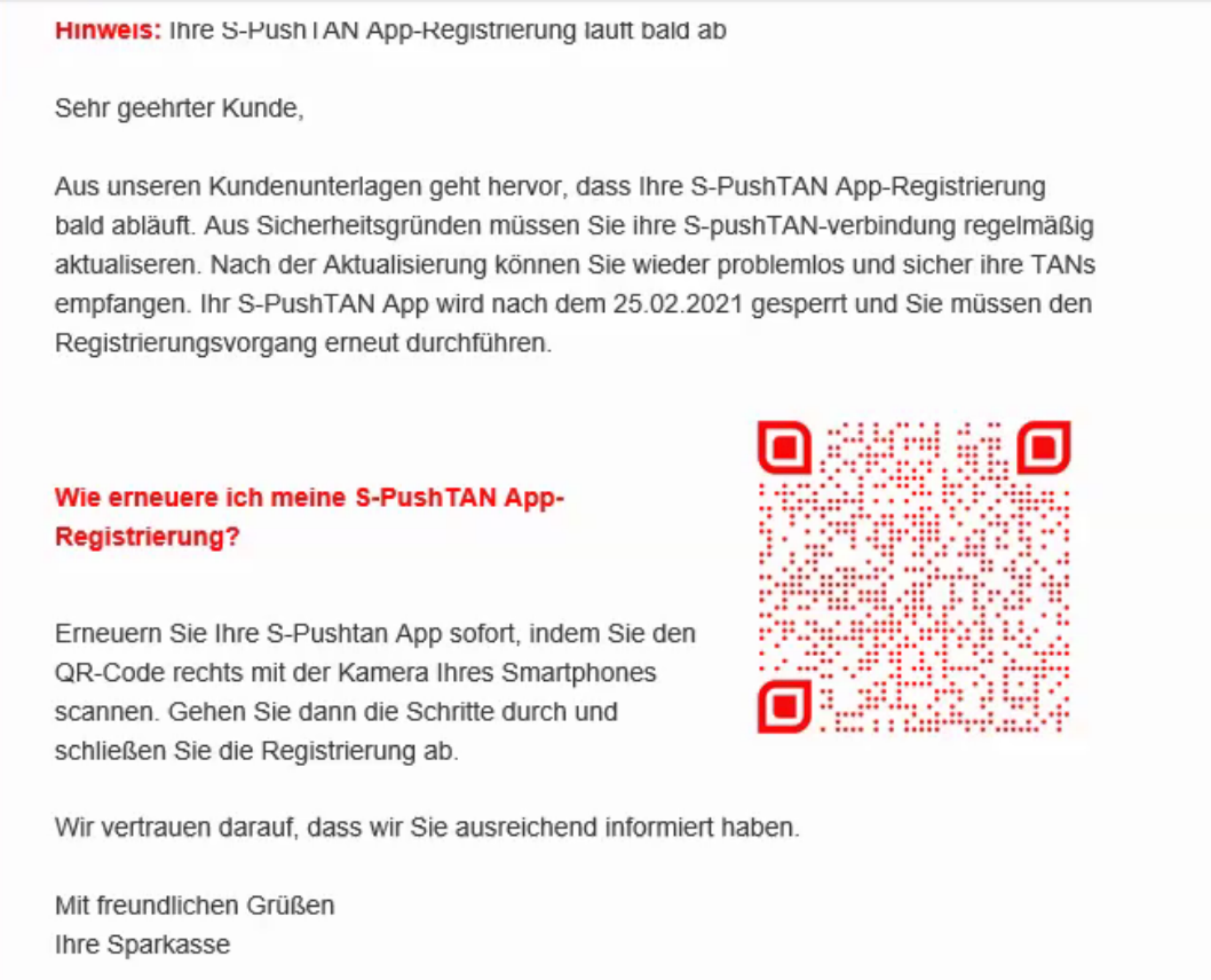
● Recipient
○ Sender

Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	esa-tme.hosted.appc.cisco.com	Disabled	Disabled	Disabled	Disabled	Enabled (no filters)	Disabled	Forwarding (disabled)	🗑
2	jolopes@bce-demo.com	(use default)	(use default)	(use default)	(use default)	Several_URLs_1malicious	Retention Time: Virus: 1 day	(use default)	🗑



Hinweis: Ihre S-PushTAN App-Registrierung läuft bald ab

Sehr geehrter Kunde,

Aus unseren Kundenunterlagen geht hervor, dass Ihre S-PushTAN App-Registrierung bald abläuft. Aus Sicherheitsgründen müssen Sie ihre S-pushTAN-verbindung regelmäßig aktualiseren. Nach der Aktualisierung können Sie wieder problemlos und sicher ihre TANs empfangen. Ihr S-PushTAN App wird nach dem 25.02.2021 gesperrt und Sie müssen den Registrierungsvorgang erneut durchführen.

Wie erneuere ich meine S-PushTAN App-Registrierung?

Erneuern Sie Ihre S-Pushtan App sofort, indem Sie den QR-Code rechts mit der Kamera Ihres Smartphones scannen. Gehen Sie dann die Schritte durch und schließen Sie die Registrierung ab.

Wir vertrauen darauf, dass wir Sie ausreichend informiert haben.

Mit freundlichen Grüßen
Ihre Sparkasse

Cisco Email Security 2021

Email Security

- Email Security Appliance (ESA)
- Cloud Email Security (CES)
- Security Management Appliance (SMA)

Cisco Registered Envelope Service (CRES)

- Email Security Plug-in & Add-in

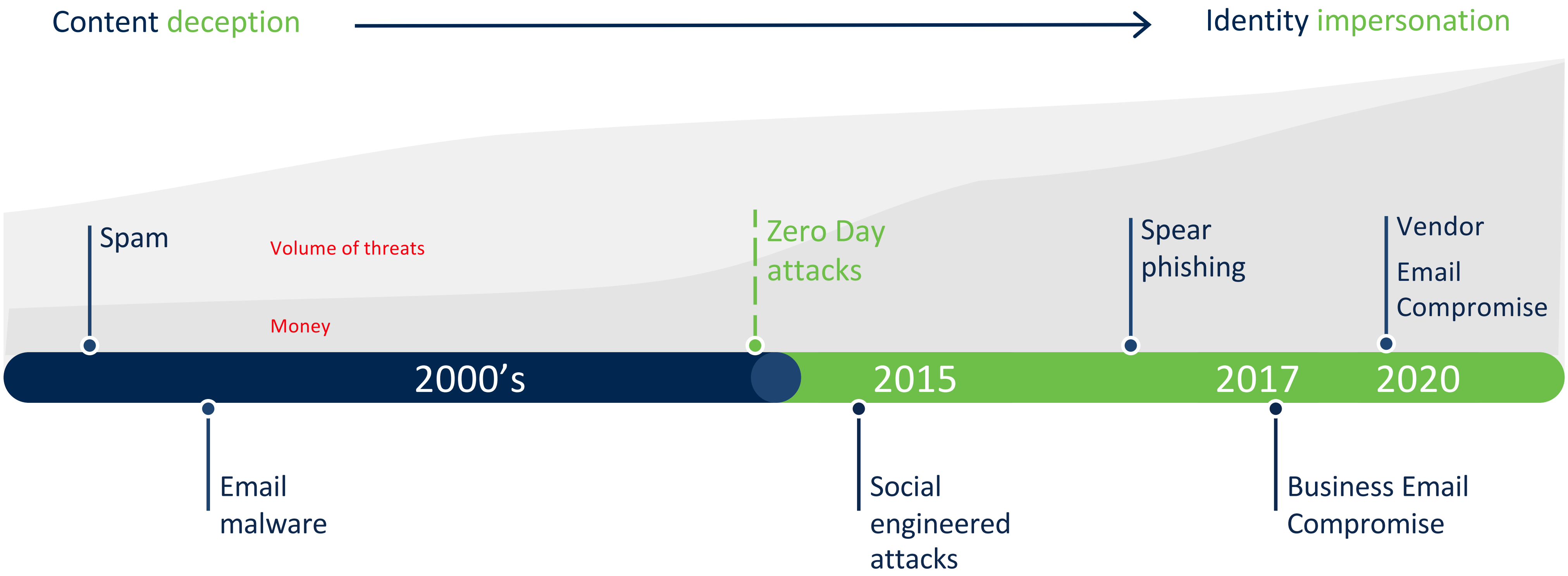
Advanced Phishing Protection (APP)

Domain Protection (DMP)

Cisco Security Awareness (CSA)

Cisco Mailbox Defense (CMD)

Advanced Phishing Attacks use identity impersonation



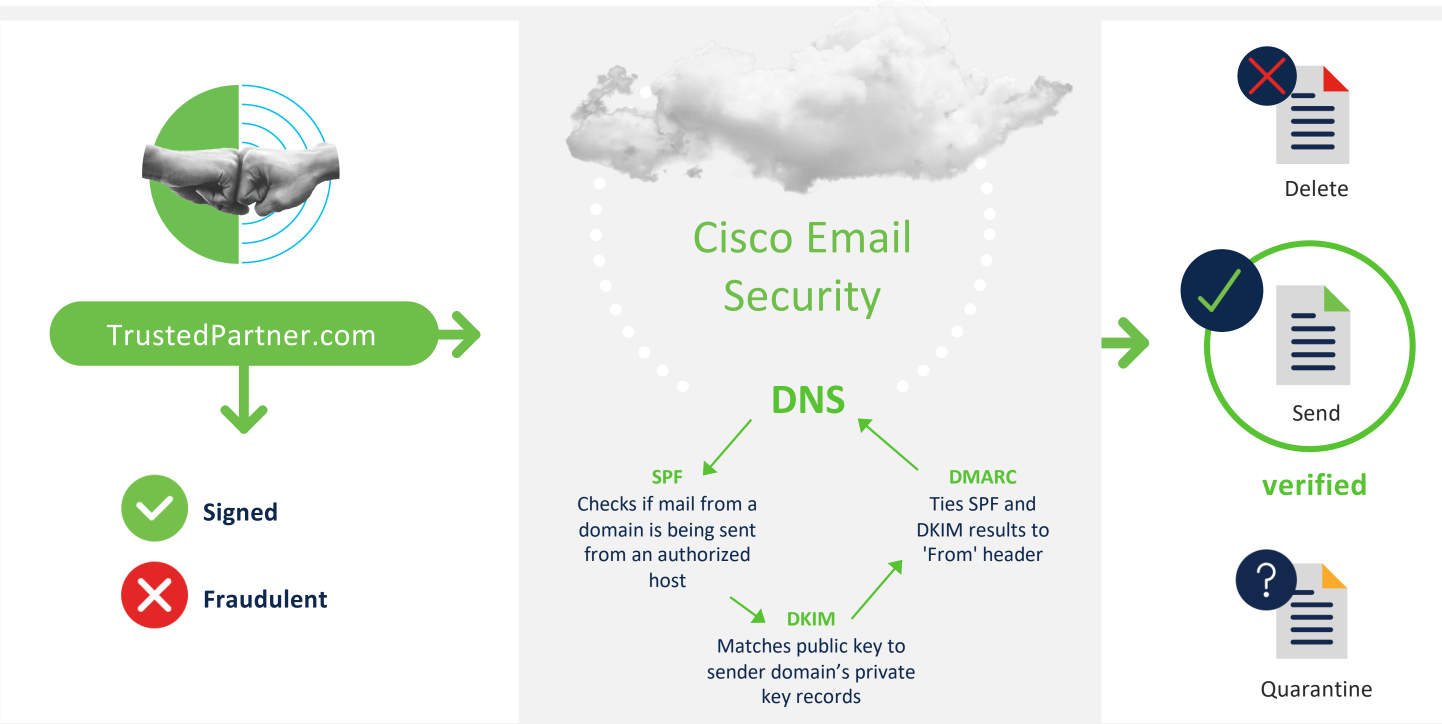
Road to Cisco Phishing Defense

Block fraudulent senders

DMARC, DKIM and SPF

Block fraudulent senders

- Determine whether a sender is reputable
- Inspect sender details on inbound messages
- Block invalid senders and identify next steps



SPF: Checks if mail from a domain is being sent from an authorized host

DKIM: Matches public key to sender domain’s private key records

DMARC: Ties SPF and DKIM results to 'From' header

Forged email detection

FBI defines it as Business Email Compromise (BEC)

Forged Email Detection

- Inspect SMTP envelope for True sender address
- Match sender address against company directory
- Send appended mail to warn users of potential forgery
- Record a log of attempts and actions taken

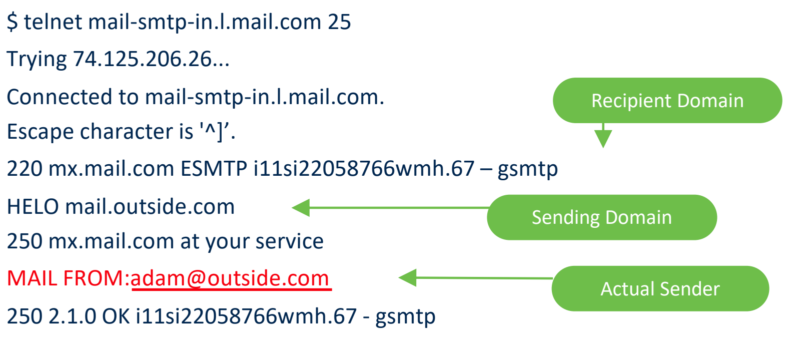
Pre-processing

From: Chuck chuck.robbins@mail.com

Subject: [URGENT]

Need help transferring funds

Inspects the SMTP envelope address



```
$ telnet mail-smtp-in.l.mail.com 25
Trying 74.125.206.26...
Connected to mail-smtp-in.l.mail.com.
Escape character is '^]'.
220 mx.mail.com ESMTP i11si22058766wmh.67 – gsmtp
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM:adam@outside.com
250 2.1.0 OK i11si22058766wmh.67 - gsmtp
```

Post-processing

From: adam@outside.com

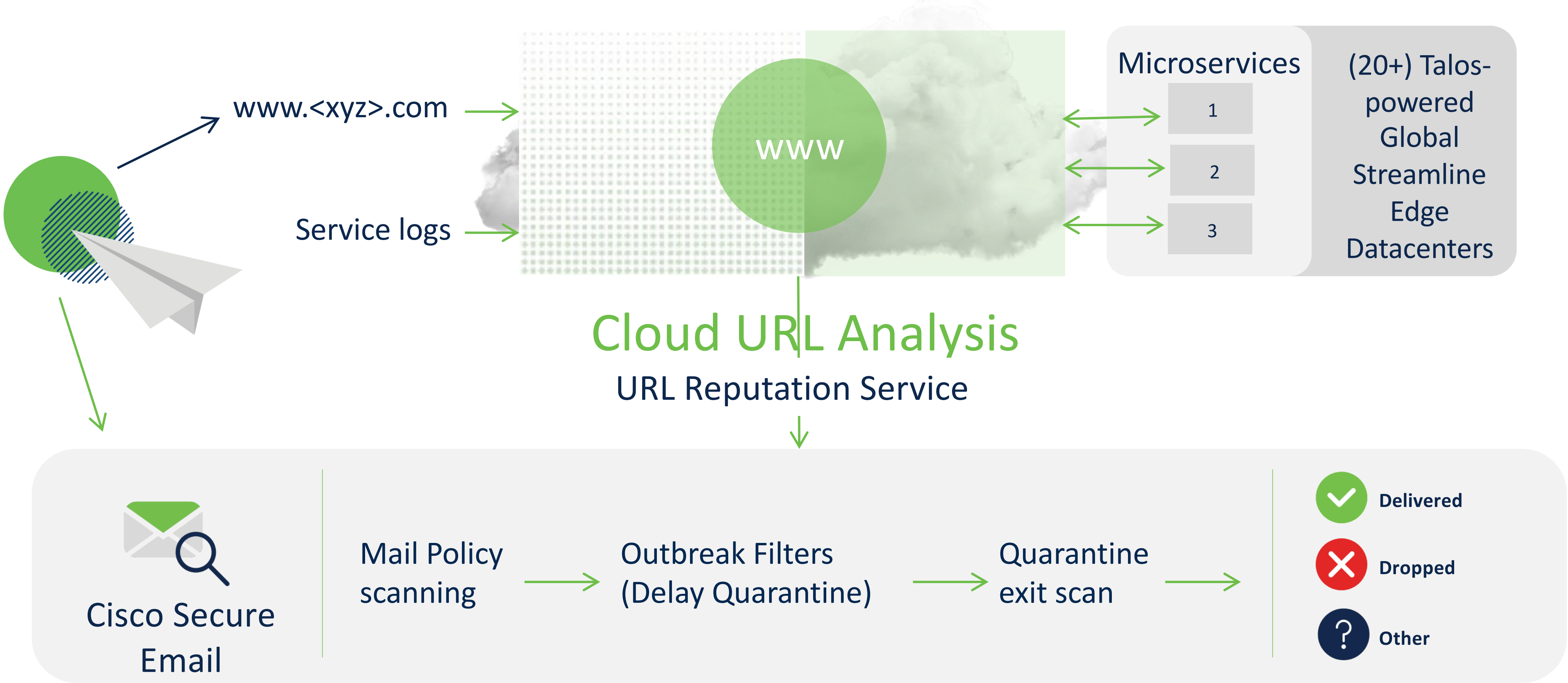
Subject: **{Possibly Forged}** [URGENT]

Need help transferring funds

Compare against Company directory

- Allison Johnson
- Barry Smith
- **Chuck Robbins**
- Dave Tucker

Cloud URL Analysis (CUA)



www.<xyz>.com

Service logs

WWW

Microservices

1

2

3

(20+) Talos-powered Global Streamline Edge Datacenters

Cloud URL Analysis

URL Reputation Service

Cisco Secure Email

Mail Policy scanning

Outbreak Filters (Delay Quarantine)

Quarantine exit scan

✓ Delivered

✗ Dropped

? Other

Cloud URL Analysis (CUA)

How Does it Work

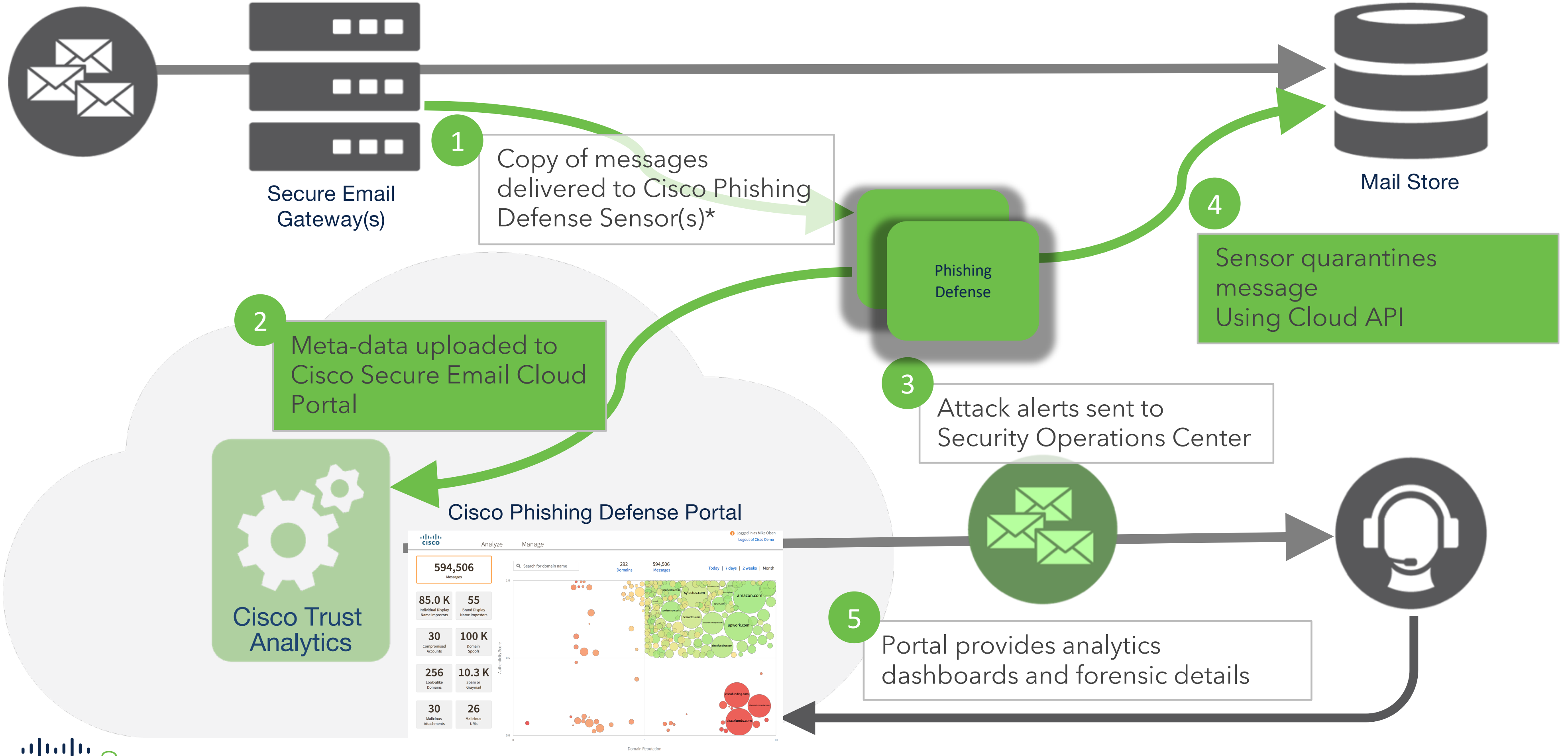
- Handles Credential phishing, Malware, Hailstorm and high-volume offer spam
- Performs out-of-band cloud URL analysis
- Triggered and uses context from new Service Logs, with Per-message context around analyzed URLs
- Leverages URL reputation services to deliver verdicts
- Transparent updates/upgrades - no updates or upgrades on Secure Email Gateway required!

Benefits

- Reduced latency of URL and IP reputation delivery
  - Increasing efficacy against threats
- Reduced platform dependencies
  - Expanding threat protection efficacy and coverage
  - Tackle evolving threat landscape nimbly and transparently (w/o Secure Email Gateway release)
- Service Logs (New in 13.5) replaces Sender Base Network Participation (SBNP)
  - Reducing overhead
  - Increasing context and visibility for threat defense

Cisco Phishing Defense

Cisco Phishing Defense - Deployment Architecture



1 Copy of messages delivered to Cisco Phishing Defense Sensor(s)*

2 Meta-data uploaded to Cisco Secure Email Cloud Portal

3 Attack alerts sent to Security Operations Center

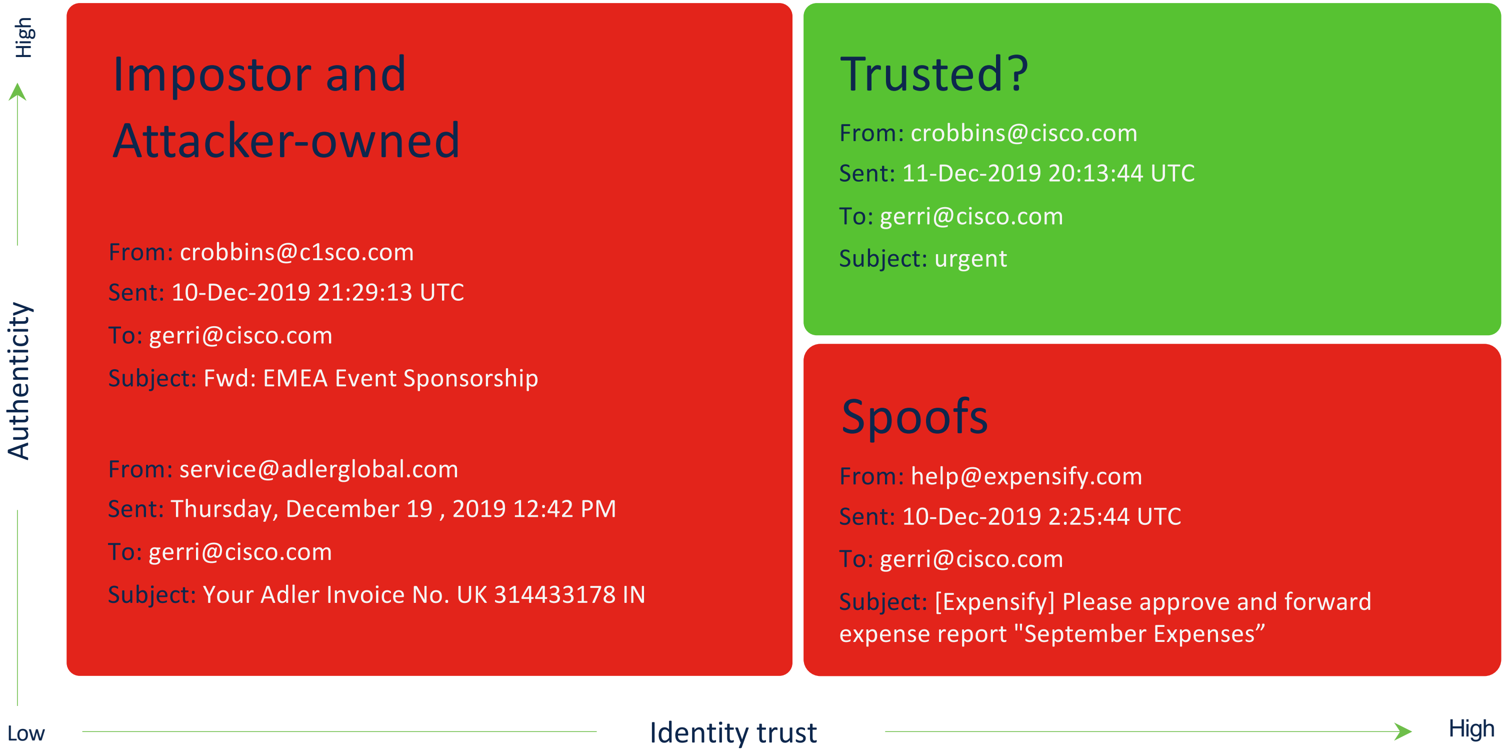
4 Sensor quarantines message Using Cloud API

5 Portal provides analytics dashboards and forensic details

cisco Secure

* AsyncOS 13.5 introduced the sensor within the ESA

Cisco Trust Analytics



High

Authenticity

Low

Identity trust

High

Impostor and Attacker-owned

From: crobbins@c1sco.com
Sent: 10-Dec-2019 21:29:13 UTC
To: gerri@cisco.com
Subject: Fwd: EMEA Event Sponsorship

From: service@adlerglobal.com
Sent: Thursday, December 19 , 2019 12:42 PM
To: gerri@cisco.com
Subject: Your Adler Invoice No. UK 314433178 IN

Trusted?

From: crobbins@cisco.com
Sent: 11-Dec-2019 20:13:44 UTC
To: gerri@cisco.com
Subject: urgent

Spoofs

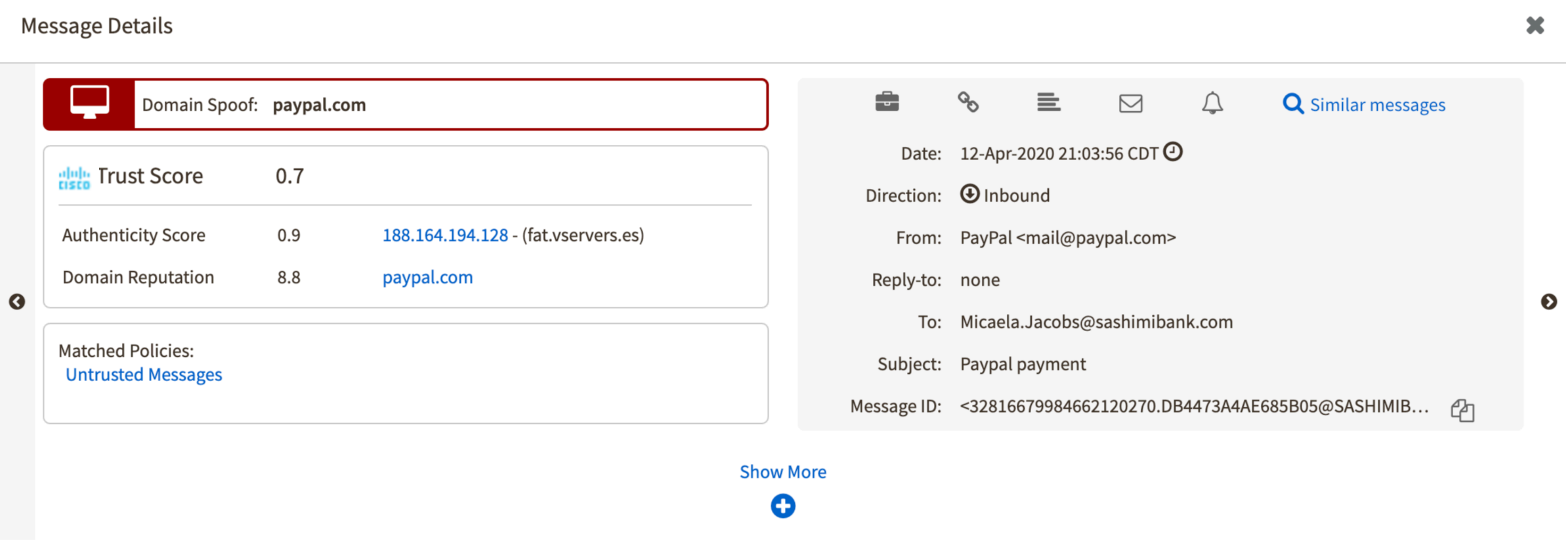
From: help@expensify.com
Sent: 10-Dec-2019 2:25:44 UTC
To: gerri@cisco.com
Subject: [Expensify] Please approve and forward expense report "September Expenses”

Cisco Phishing Defense

DEMO

Phishing Defense: Real World Examples

Domain Spoof - Paypal



Message Details

Domain Spoof: **paypal.com**

Trust Score	0.7	
Authenticity Score	0.9	188.164.194.128 - (fat.vservers.es)
Domain Reputation	8.8	paypal.com

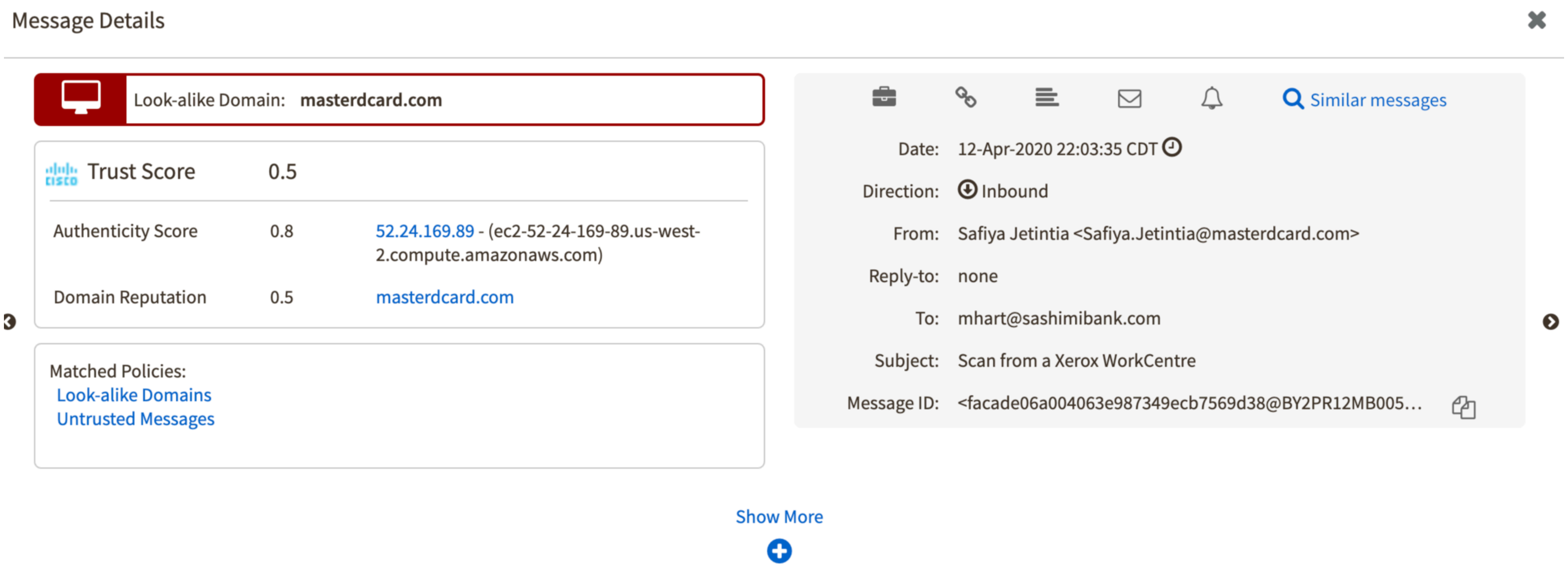
Matched Policies:
Untrusted Messages

Similar messages

Date:	12-Apr-2020 21:03:56 CDT
Direction:	Inbound
From:	PayPal <mail@paypal.com>
Reply-to:	none
To:	Micaela.Jacobs@sashimibank.com
Subject:	Paypal payment
Message ID:	<32816679984662120270.DB4473A4AE685B05@SASHIMIB…

Show More

Real-World Look-Alike Impersonation Example



Message Details

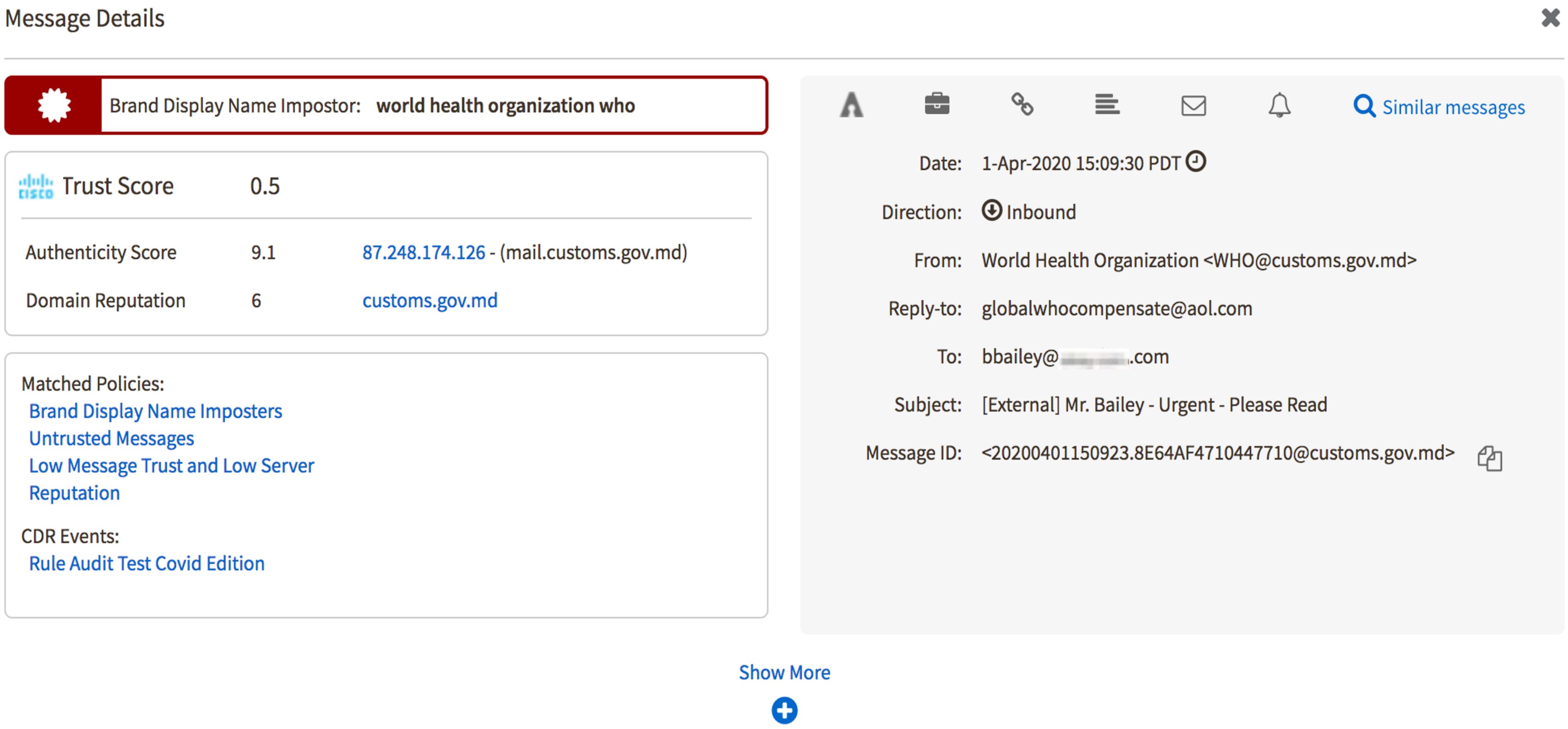
Look-alike Domain: **masterdcard.com**

Trust Score	0.5	
Authenticity Score	0.8	52.24.169.89 - (ec2-52-24-169-89.us-west-2.compute.amazonaws.com)
Domain Reputation	0.5	masterdcard.com

Matched Policies:
Look-alike Domains
Untrusted Messages

Date:	12-Apr-2020 22:03:35 CDT
Direction:	Inbound
From:	Safiya Jetintia <Safiya.Jetintia@masterdcard.com>
Reply-to:	none
To:	mhart@sashimibank.com
Subject:	Scan from a Xerox WorkCentre
Message ID:	<facade06a004063e987349ecb7569d38@BY2PR12MB005...

Real-World Display-Name Imposter Example



Message Details

Brand Display Name Impostor: **world health organization who**

Trust Score	0.5	
Authenticity Score	9.1	87.248.174.126 - (mail.customs.gov.md)
Domain Reputation	6	customs.gov.md

Matched Policies:
- Brand Display Name Imposters
- Untrusted Messages
- Low Message Trust and Low Server Reputation

CDR Events:
- Rule Audit Test Covid Edition

Date: 1-Apr-2020 15:09:30 PDT

Direction: Inbound

From: World Health Organization <WHO@customs.gov.md>

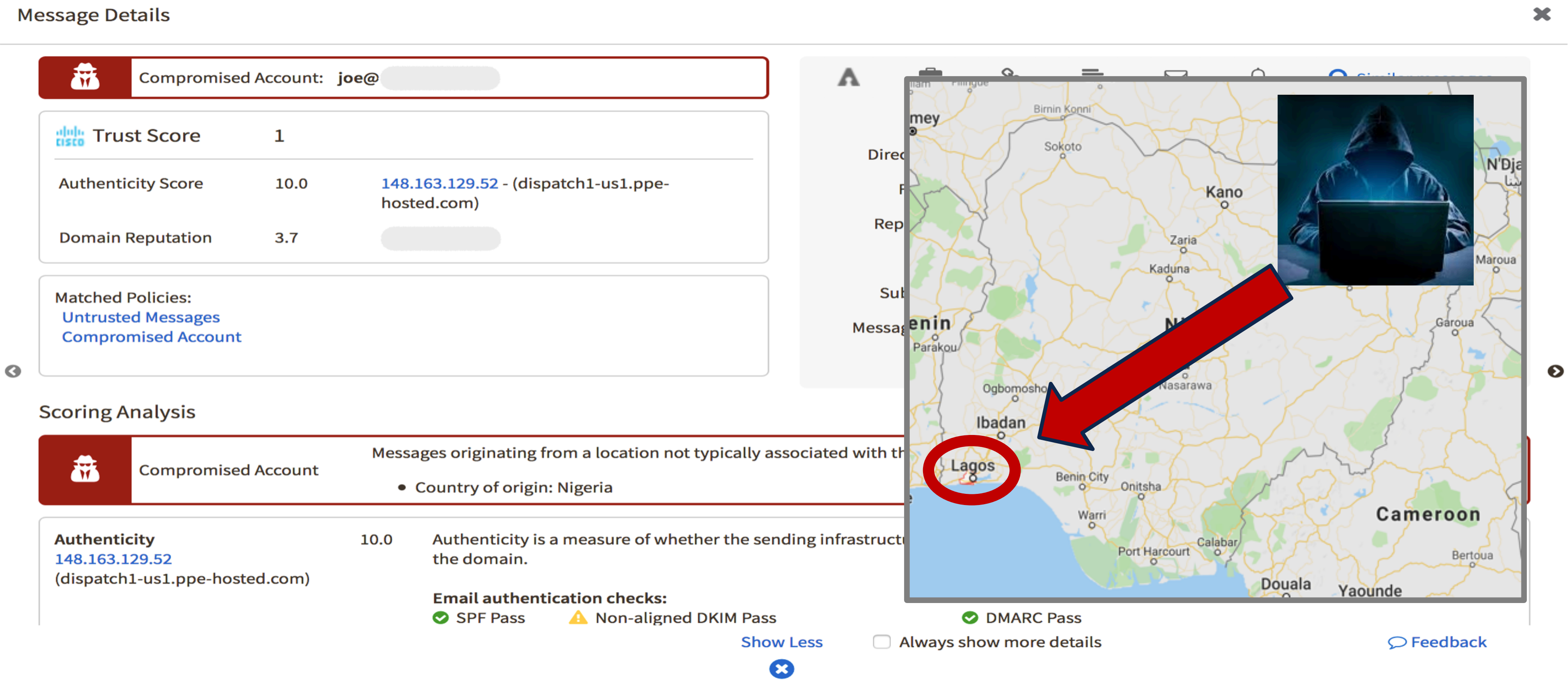
Reply-to: globalwhocompensate@aol.com

To: bbailey@[redacted].com

Subject: [External] Mr. Bailey - Urgent - Please Read

Message ID: <20200401150923.8E64AF4710447710@customs.gov.md>

Real-World Compromised Account Example



Message Details

Compromised Account: joe@[redacted]

Trust Score 1

Authenticity Score	10.0	148.163.129.52 - (dispatch1-us1.ppe-hosted.com)
Domain Reputation	3.7	[redacted]

Matched Policies:
Untrusted Messages
Compromised Account

Scoring Analysis

Compromised Account

Messages originating from a location not typically associated with th

- Country of origin: Nigeria

Authenticity
148.163.129.52
(dispatch1-us1.ppe-hosted.com)

10.0

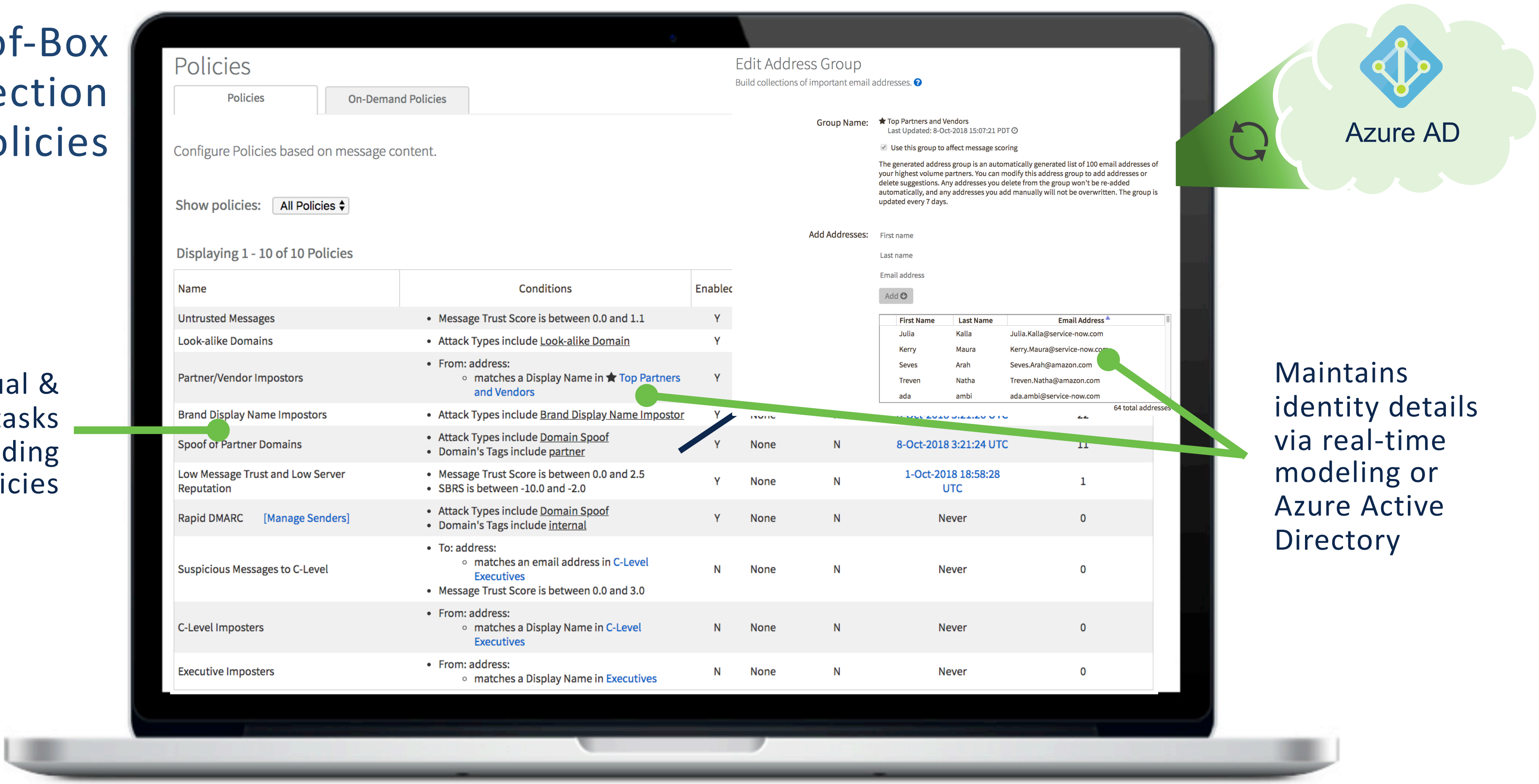
Authenticity is a measure of whether the sending infrastructu
the domain.

Email authentication checks:
✓ SPF Pass ⚠ Non-aligned DKIM Pass ✓ DMARC Pass

Free Up Resources With Policy Automation

Out-of-Box Protection Policies

Automate manual & error prone tasks inherent in building policies



Policies

Policies | On-Demand Policies

Configure Policies based on message content.

Show policies: All Policies

Displaying 1 - 10 of 10 Policies

Name	Conditions	Enabled				
Untrusted Messages	• Message Trust Score is between 0.0 and 1.1	Y				
Look-alike Domains	• Attack Types include Look-alike Domain	Y				
Partner/Vendor Impostors	• From: address: ○ matches a Display Name in ★ Top Partners and Vendors	Y				
Brand Display Name Impostors	• Attack Types include Brand Display Name Impostor	Y				
Spoof of Partner Domains	• Attack Types include Domain Spoof • Domain's Tags include partner	Y	None	N	8-Oct-2018 3:21:24 UTC	11
Low Message Trust and Low Server Reputation	• Message Trust Score is between 0.0 and 2.5 • SBRS is between -10.0 and -2.0	Y	None	N	1-Oct-2018 18:58:28 UTC	1
Rapid DMARC [Manage Senders]	• Attack Types include Domain Spoof • Domain's Tags include internal	Y	None	N	Never	0
Suspicious Messages to C-Level	• To: address: ○ matches an email address in C-Level Executives • Message Trust Score is between 0.0 and 3.0	N	None	N	Never	0
C-Level Imposters	• From: address: ○ matches a Display Name in C-Level Executives	N	None	N	Never	0
Executive Imposters	• From: address: ○ matches a Display Name in Executives	N	None	N	Never	0

Edit Address Group

Build collections of important email addresses.

Group Name: ★ Top Partners and Vendors
Last Updated: 8-Oct-2018 15:07:21 PDT

☑ Use this group to affect message scoring

The generated address group is an automatically generated list of 100 email addresses of your highest volume partners. You can modify this address group to add addresses or delete suggestions. Any addresses you delete from the group won't be re-added automatically, and any addresses you add manually will not be overwritten. The group is updated every 7 days.

Add Addresses: First name

Last name

Email address

Add

First Name	Last Name	Email Address
Julia	Kalla	Julia.Kalla@service-now.com
Kerry	Maura	Kerry.Maura@service-now.com
Seves	Arah	Seves.Arah@amazon.com
Treven	Natha	Treven.Natha@amazon.com
ada	ambi	ada.ambi@service-now.com

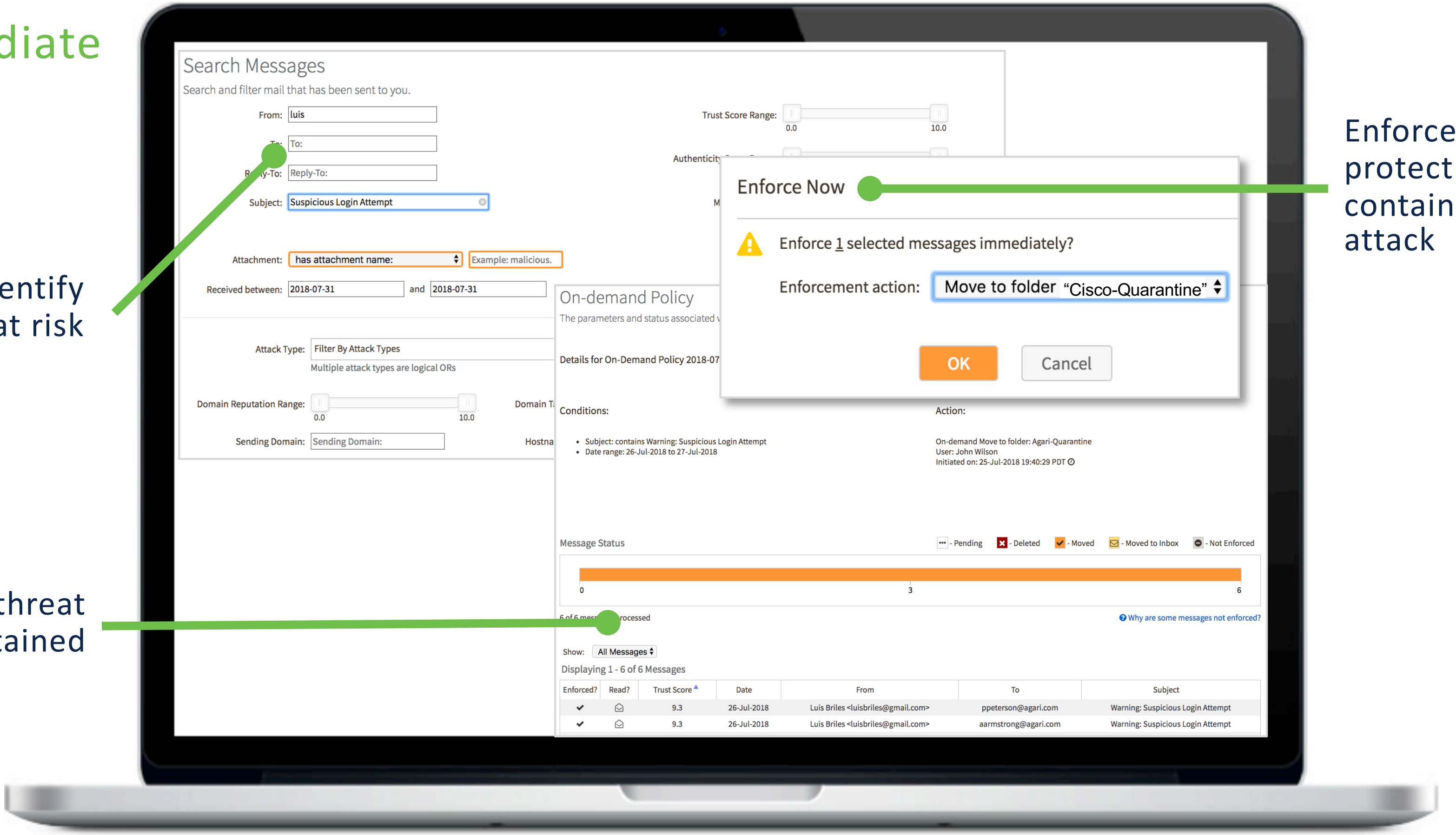
64 total addresses

Maintains identity details via real-time modeling or Azure Active Directory

cisco Secure

Post-Delivery Protection Against Zero-Day Attacks

Search & Remediate



Search Messages

Search and filter mail that has been sent to you.

From: luis

To: To:

Reply-To: Reply-To:

Subject: Suspicious Login Attempt

Attachment: has attachment name: Example: malicious.

Received between: 2018-07-31 and 2018-07-31

Attack Type: Filter By Attack Types

Multiple attack types are logical ORs

Domain Reputation Range: 0.0 10.0

Sending Domain: Sending Domain:

Trust Score Range: 0.0 10.0

Authenticity

Enforce Now

Enforce 1 selected messages immediately?

Enforcement action: Move to folder "Cisco-Quarantine"

On-demand Policy

The parameters and status associated

Details for On-Demand Policy 2018-07

Conditions:

- Subject: contains Warning: Suspicious Login Attempt
- Date range: 26-Jul-2018 to 27-Jul-2018

Action:

On-demand Move to folder: Agari-Quarantine
User: John Wilson
Initiated on: 25-Jul-2018 19:40:29 PDT

Message Status

6 of 6 mess rocessed

Why are some messages not enforced?

Show: All Messages

Displaying 1 - 6 of 6 Messages

Enforced?	Read?	Trust Score	Date	From	To	Subject
✓	✉	9.3	26-Jul-2018	Luis Briles <luisbriles@gmail.com>	ppeterson@agari.com	Warning: Suspicious Login Attempt
✓	✉	9.3	26-Jul-2018	Luis Briles <luisbriles@gmail.com>	aarmstrong@agari.com	Warning: Suspicious Login Attempt

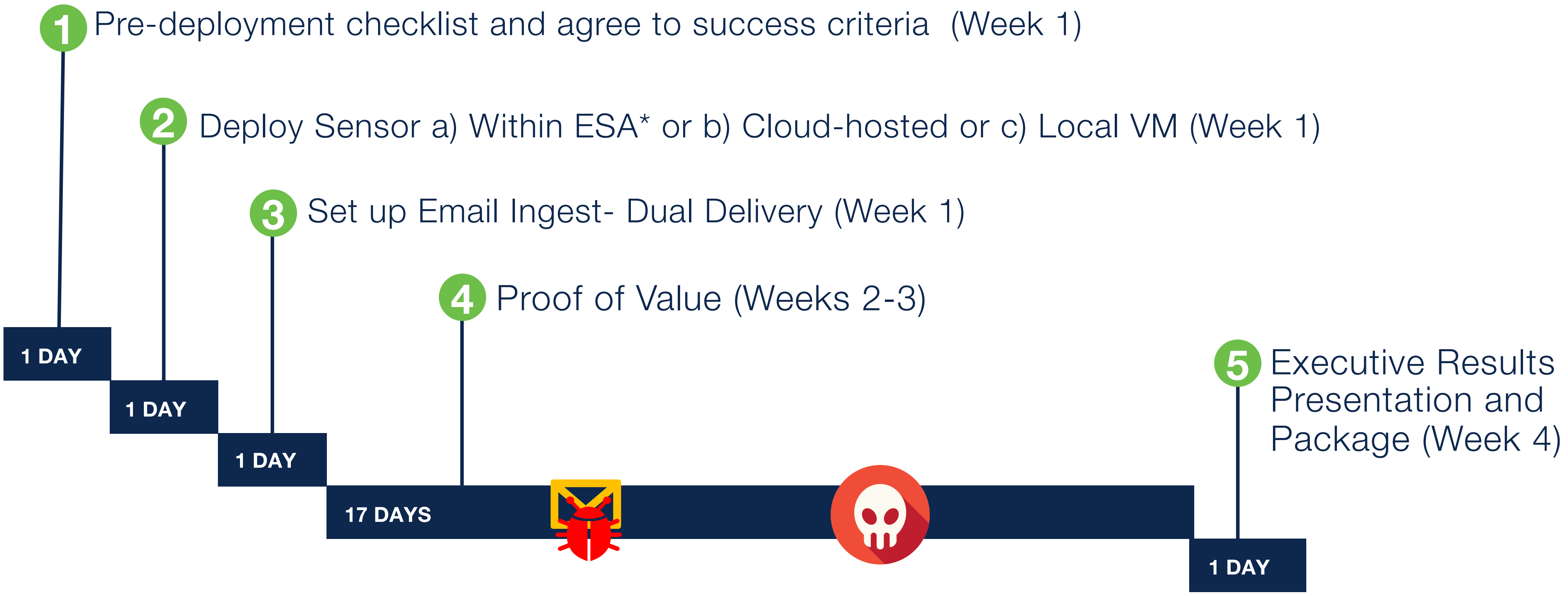
Quickly identify who is at risk

Confirm that the threat has been contained

Enforce protection to contain the attack

Secure

Proving Cisco Phishing Defense - 5 Steps and 4 Weeks



1 Pre-deployment checklist and agree to success criteria (Week 1)

2 Deploy Sensor a) Within ESA* or b) Cloud-hosted or c) Local VM (Week 1)

3 Set up Email Ingest- Dual Delivery (Week 1)

4 Proof of Value (Weeks 2-3)

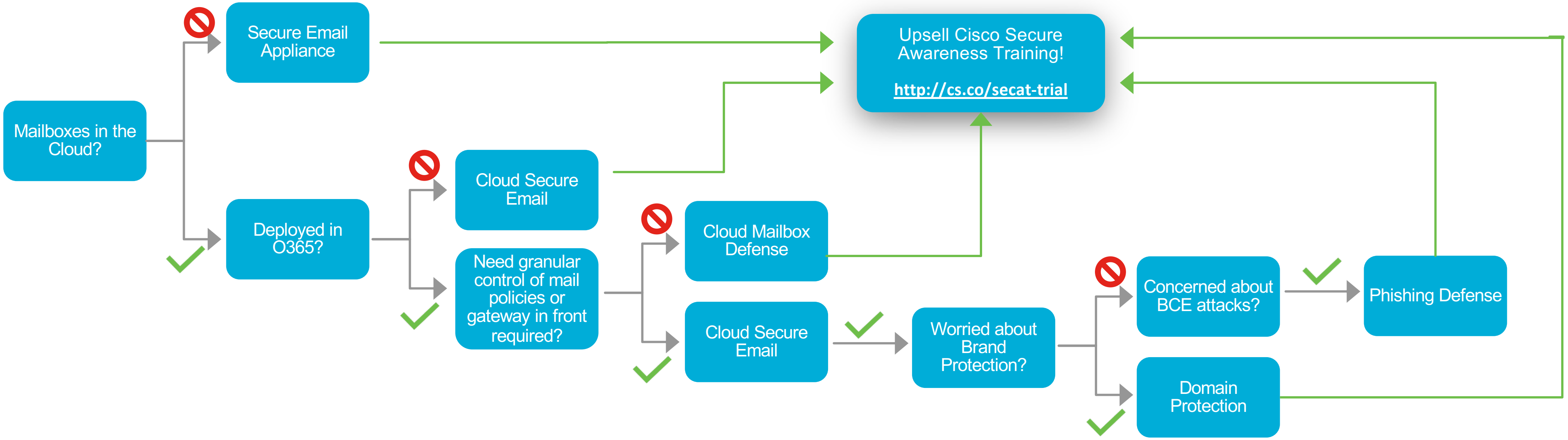
5 Executive Results Presentation and Package (Week 4)

Domain Protection/Phishing Defense PoV Guide

Positioning Guide

	Cloud Mailbox Defense	Secure Email Gateway/Cloud Gateway	Phishing Defense + Domain Protection
O365	✓	✓	✓
On Premises / Hybrid		✓	✓
MX Record Change		✓	
Context / Behavioral Analysis			✓
Spam Protection	✓	✓	
File Reputation	✓	✓	
File Analysis	✓	✓	
Cloud URL Analysis	✓	✓	
Data Loss Prevention		✓	
Email Encryption		✓	
DMARC Automation			✓
Post-Delivery Remediation	✓	✓	✓
Talos Threat Intelligence	✓	✓	
Trajectory and Conversation View	✓		
Brand Protection			✓
Automatic and On-Demand Remediation	✓	✓	✓
Internal Mail Scanning	✓		✓

Secure Email Decision Tree



cisco Secure