CISCO
SECURE

CISCO The bridge to possible

Americas PIW

How continued innovation helped Cloud Mailbox outgrow its name

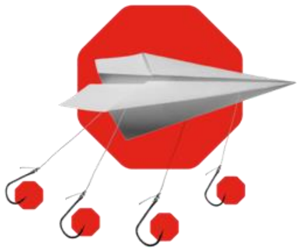
Sérgio Pinto – TME Secure Email

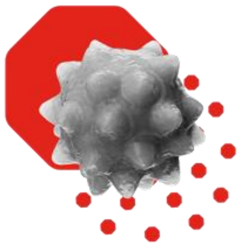
November 2022

Agenda

- What is Email Threat Defense
- Deployment
- Efficacy and New Detectors
- Reporting and Dashboards
- APP EoS and New ETD Connector

Email is still the #1 threat vector





Cisco Secure Email | Secure your business

91%

Attacks

Begin with Email

* industry phishing report

$2.5

Billion

Losses from Phishing, BEC, EAC, Spoofing in 2021

* FBI 2021 IC3 Report

3,729

Businesses

Halted by Ransomware in 2021

* FBI 2021 IC3 Report

Email Threat Defense

Secure Email deployment models

Flexible to fit your environment

On-Premise

Hardware or Virtual Machines

Hybrid

Best of both worlds

Cloud

Agile, Scalable, Secure

Cloud Mailbox → Cisco Secure Email Threat Defense

Why Change?

- Cloud Mailbox name provided impression we host mailboxes
- Cloud Mailbox as evolved to advanced threat detection and more support for threat response
- Email Threat Defense aligned to long term strategy of product line
- Name Change on Oct 25
- No Changes to ordering or PIDs

Email Threat Defense

Cloud-native email security platform that focuses on

Visibility

- ✓ All messages
- ✓ Search / Triage
- ✓ Open APIs

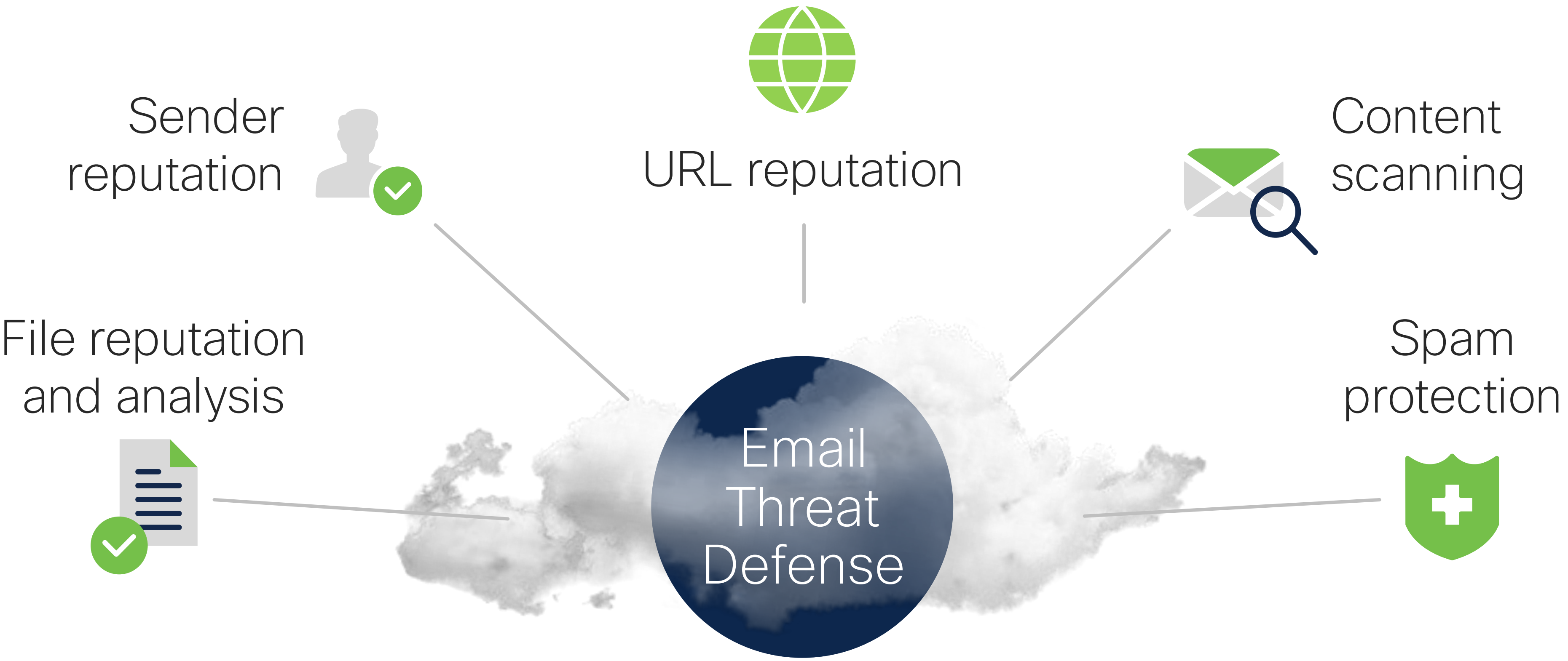
Simplicity

- ✓ Deployment
- ✓ Configuration
- ✓ Management

Integration

- ✓ Talos Intelligence
- ✓ MS APIs
- ✓ Cisco Threat Response

ETD: Comprehensive Attack Protection



Sender reputation

URL reputation

Content scanning

File reputation and analysis

Email Threat Defense

Spam protection

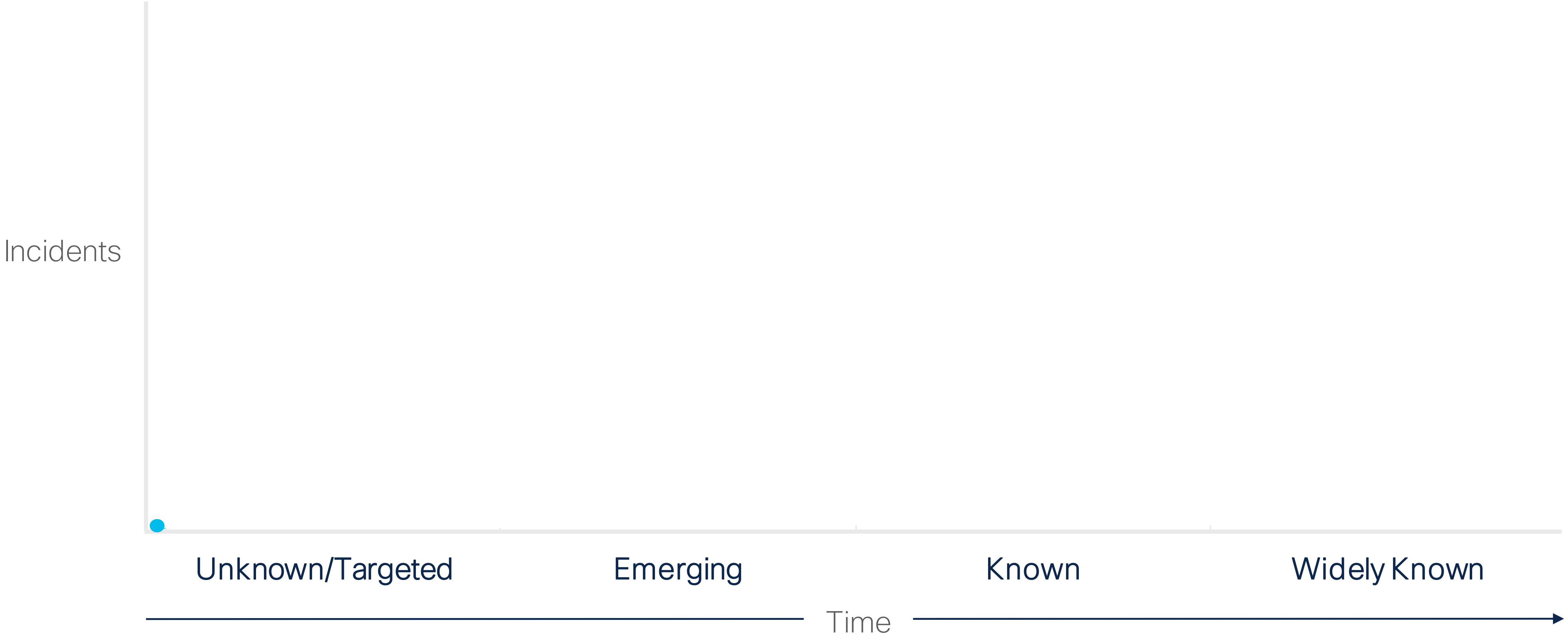
Malware

Phishing / BEC

Internal Threats

Account Takeover

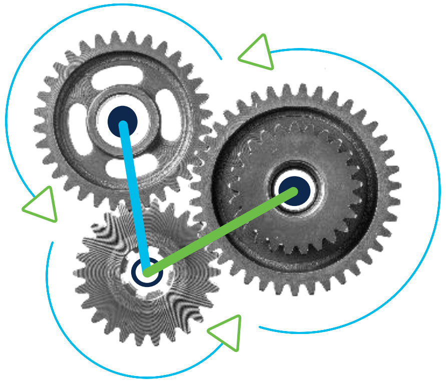
Completes Coverage of advanced threat life cycle



Deploying ETD

Email Threat Defense: Easy to Deploy

Two-Step deployment



Instant Tracking & Reporting

No Risk to mail delivery

Highlights

- ✓ Fully Functional in 5 mins
- ✓ No Operational Risk
- ✓ No Changes to mail flow or DNS
- ✓ Track all messages, including Internal

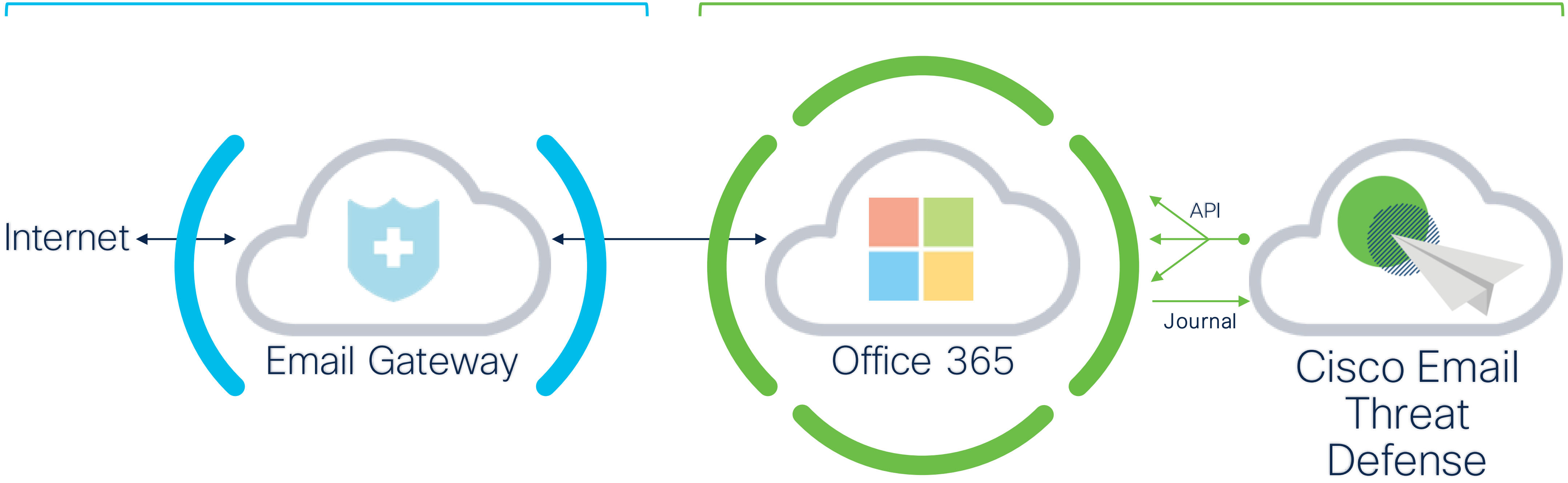
Completes Visibility & Protection for all messages

Traditional Email Gateway

Only sees inbound and outbound messages that cross the perimeter – excludes internal

Cisco Email Threat Defense

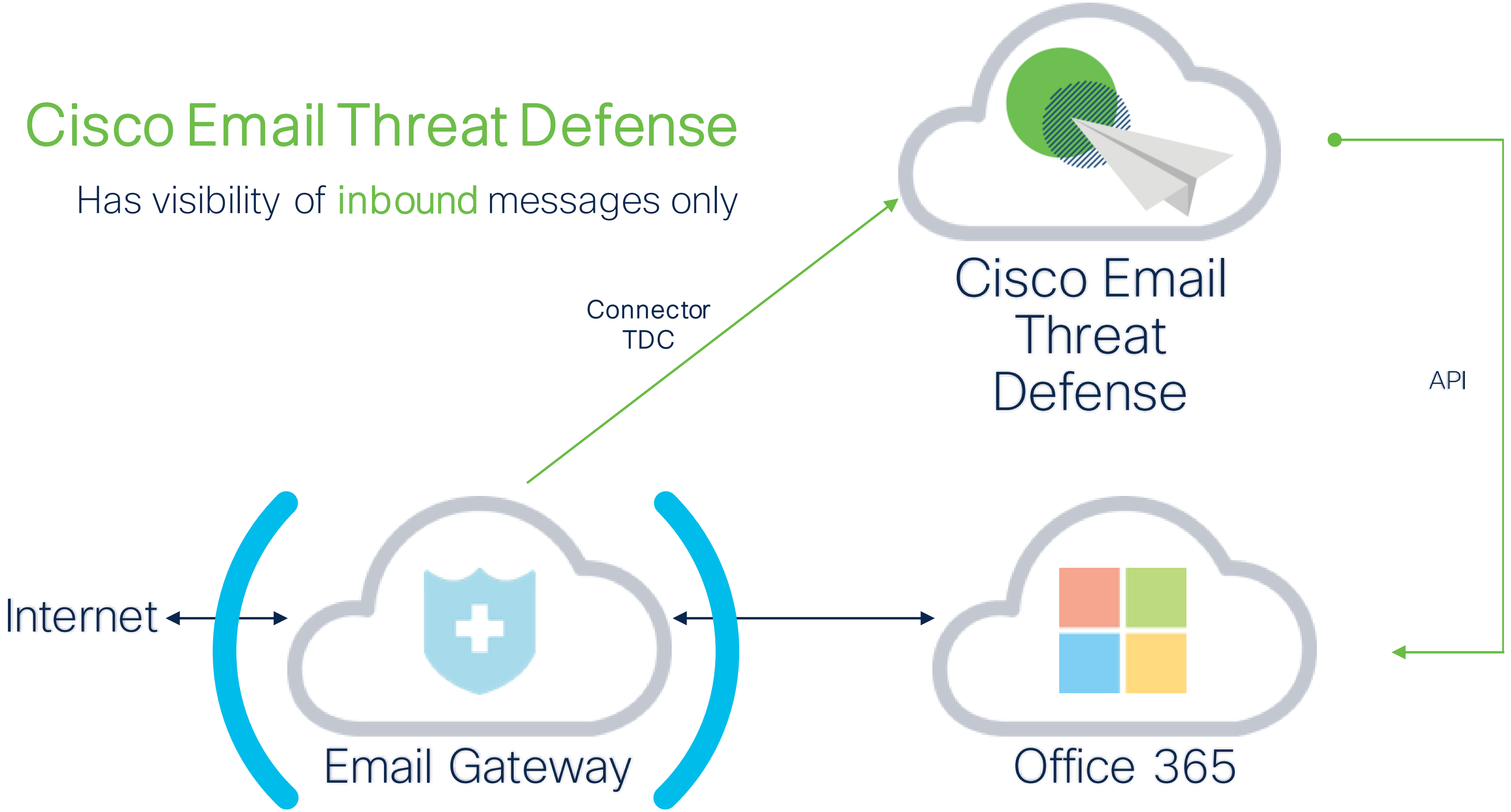
Has complete visibility of all messages, including internal, in addition to inbound and outbound messages



Completes Visibility & Protection for all messages

Cisco Email Threat Defense

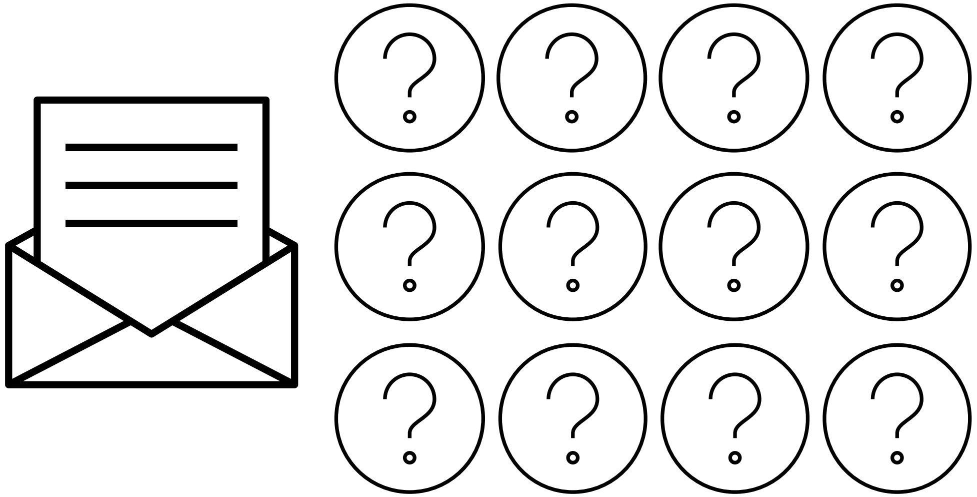
Has visibility of inbound messages only

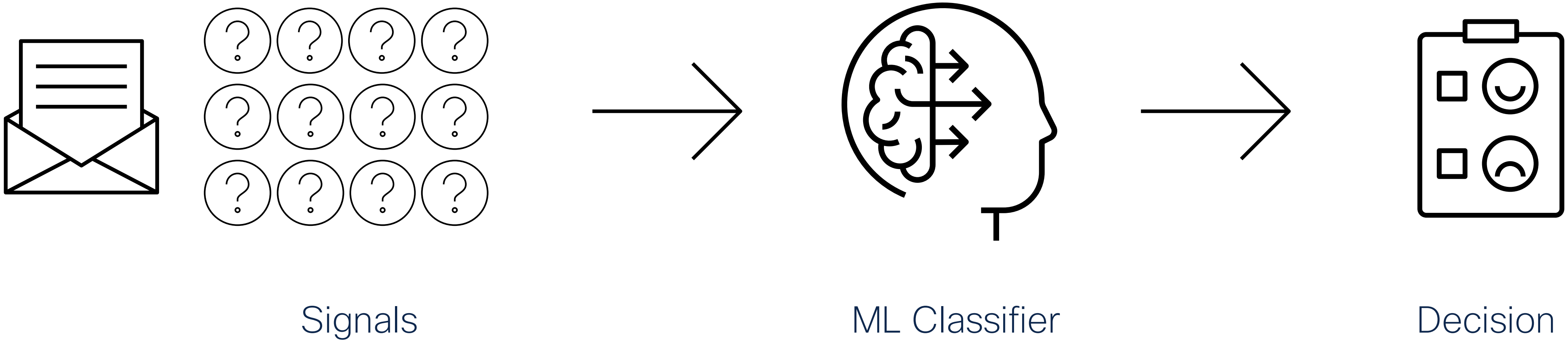


Efficacy & Detectors

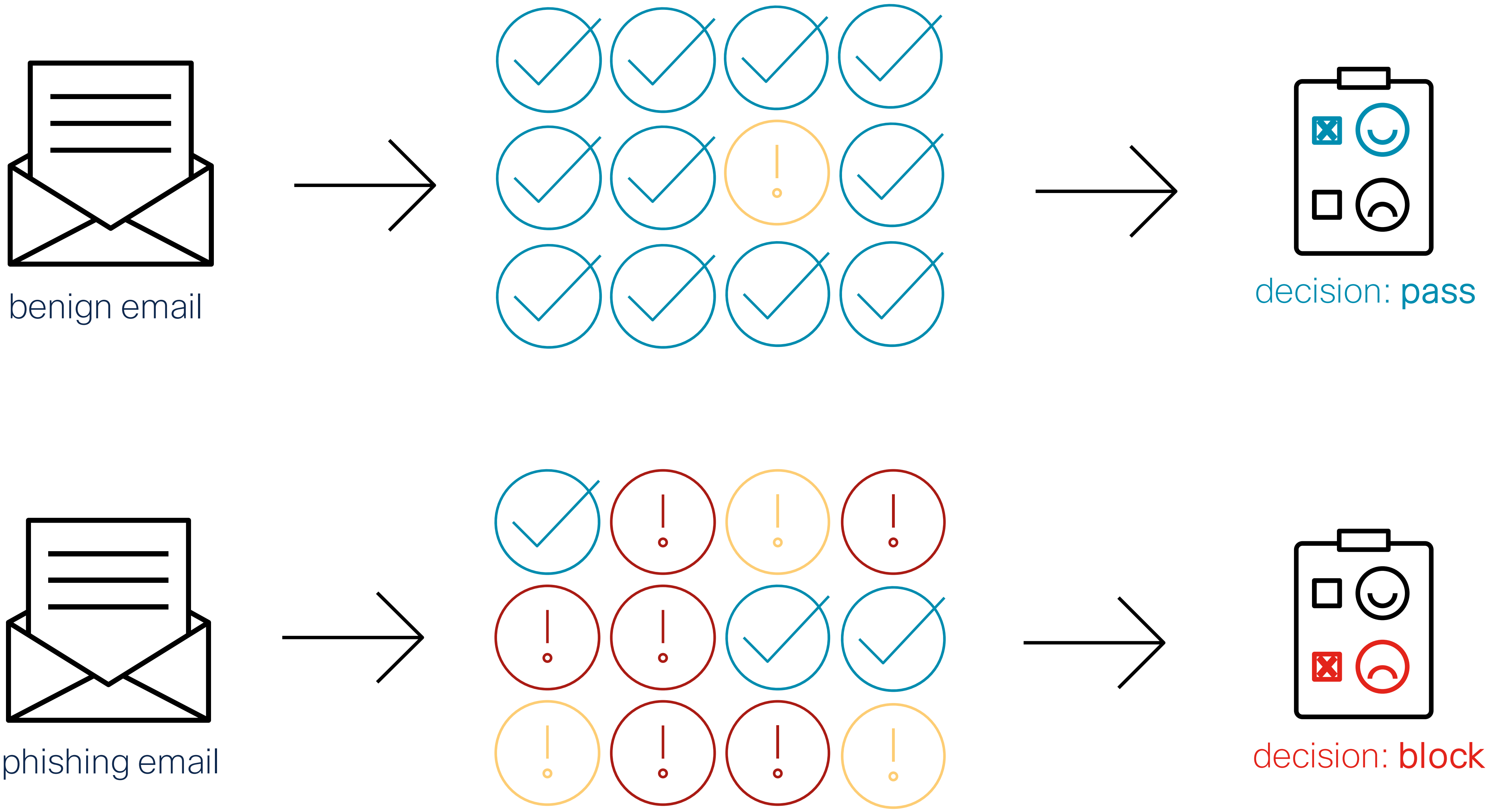
How does it work?

Each email is checked for a variety of independent signals





The final verdict is then given by aggregating the signals

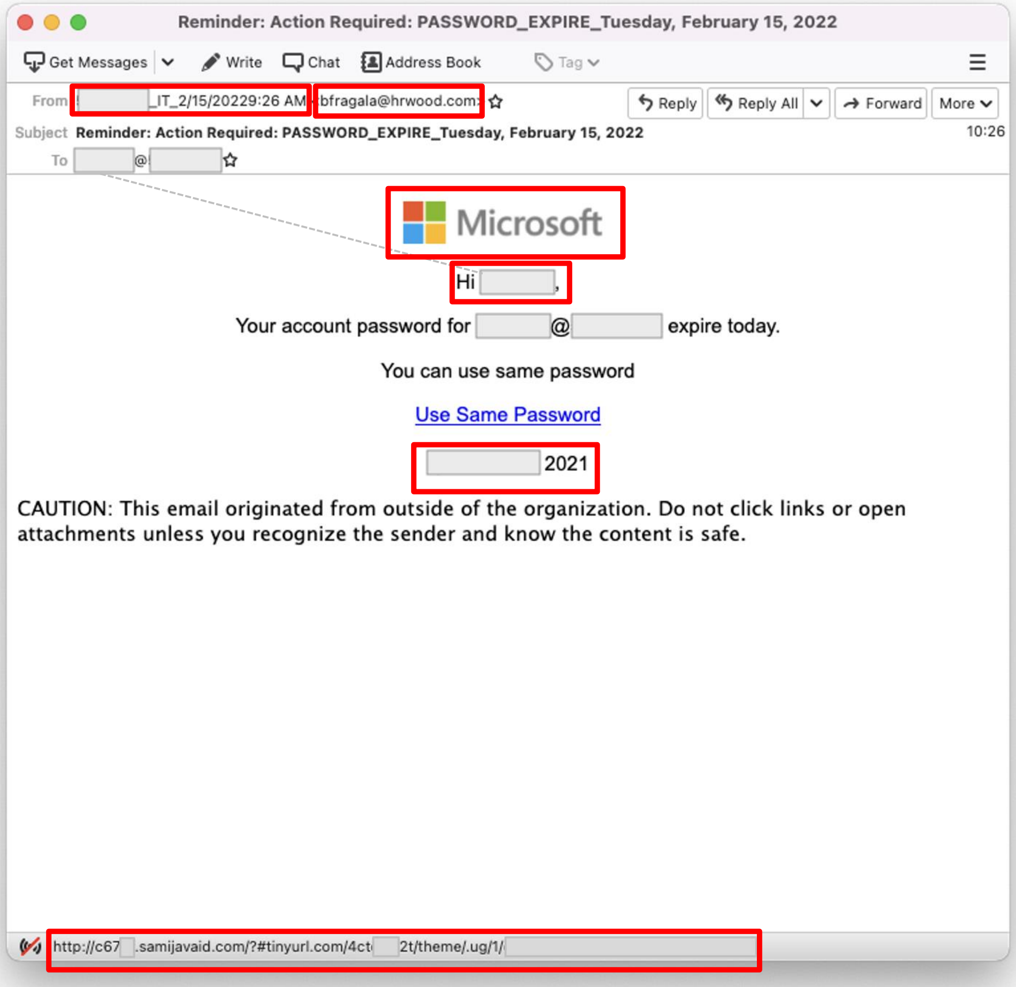


benign email

decision: **pass**

phishing email

decision: **block**



Reminder: Action Required: PASSWORD_EXPIRE_Tuesday, February 15, 2022

From [redacted] IT_2/15/20229:26 AM bfragala@hrwood.com

Subject Reminder: Action Required: PASSWORD_EXPIRE_Tuesday, February 15, 2022 10:26

To [redacted]@[redacted]

Microsoft

Hi [redacted],

Your account password for [redacted]@[redacted] expire today.

You can use same password

Use Same Password

[redacted] 2021

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

http://c67[redacted].samijavaid.com/?#tinyurl.com/4ct[redacted]2t/theme/.ug/1/[redacted]

Sender text is unusual

Greets person by username

Link contains suspicious patterns

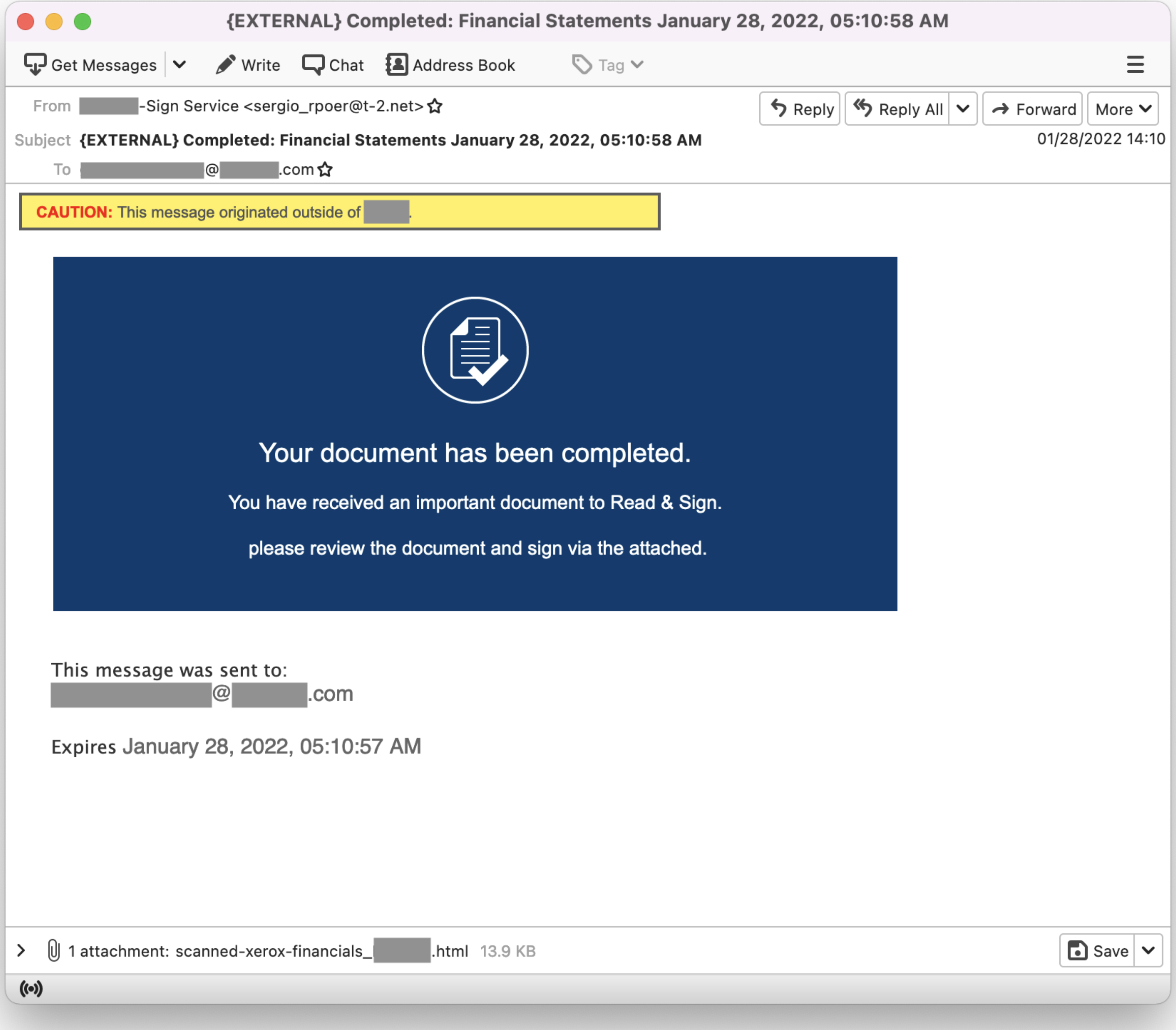
Sender domain has low reputation

Impersonates Microsoft

Impersonates the recipient company

Brand impersonation

Impersonates DocuSign



{EXTERNAL} Completed: Financial Statements January 28, 2022, 05:10:58 AM

From [redacted]-Sign Service <sergio_rpoer@t-2.net>

Subject **{EXTERNAL} Completed: Financial Statements January 28, 2022, 05:10:58 AM**

01/28/2022 14:10

To [redacted]@[redacted].com

CAUTION: This message originated outside of [redacted].

Your document has been completed.

You have received an important document to Read & Sign.

please review the document and sign via the attached.

This message was sent to:
[redacted]@[redacted].com

Expires January 28, 2022, 05:10:57 AM

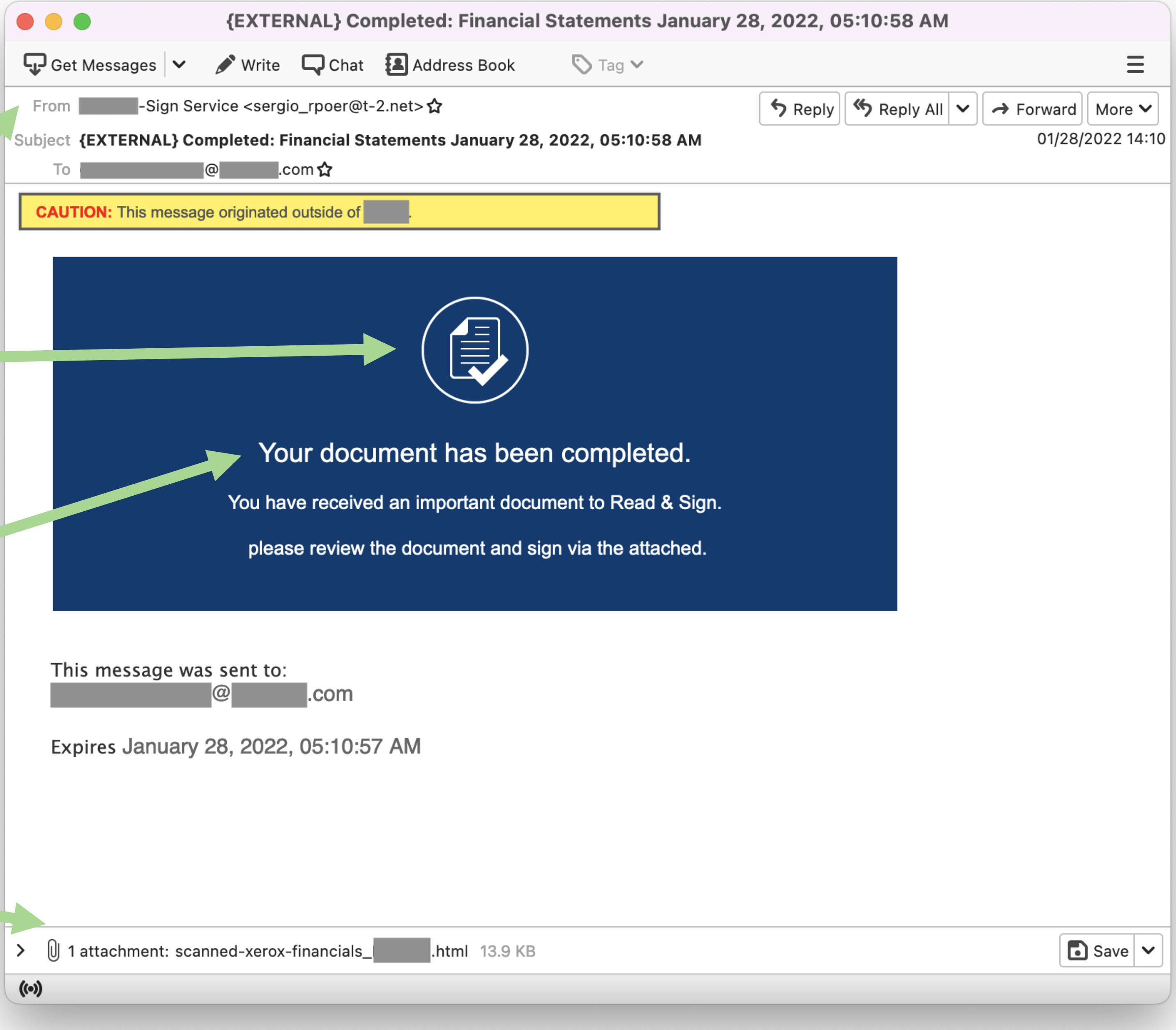
1 attachment: scanned-xerox-financials_[redacted].html 13.9 KB

Brand impersonation

Detection of Docusign logo without a Docusign domain

Semantic intent understanding

HTML attachment unlike what Docusign usually sends



{EXTERNAL} Completed: Financial Statements January 28, 2022, 05:10:58 AM

From [redacted]-Sign Service <sergio_rpoer@t-2.net>

Subject {EXTERNAL} Completed: Financial Statements January 28, 2022, 05:10:58 AM

To [redacted]@[redacted].com

01/28/2022 14:10

CAUTION: This message originated outside of [redacted].

Your document has been completed.

You have received an important document to Read & Sign.

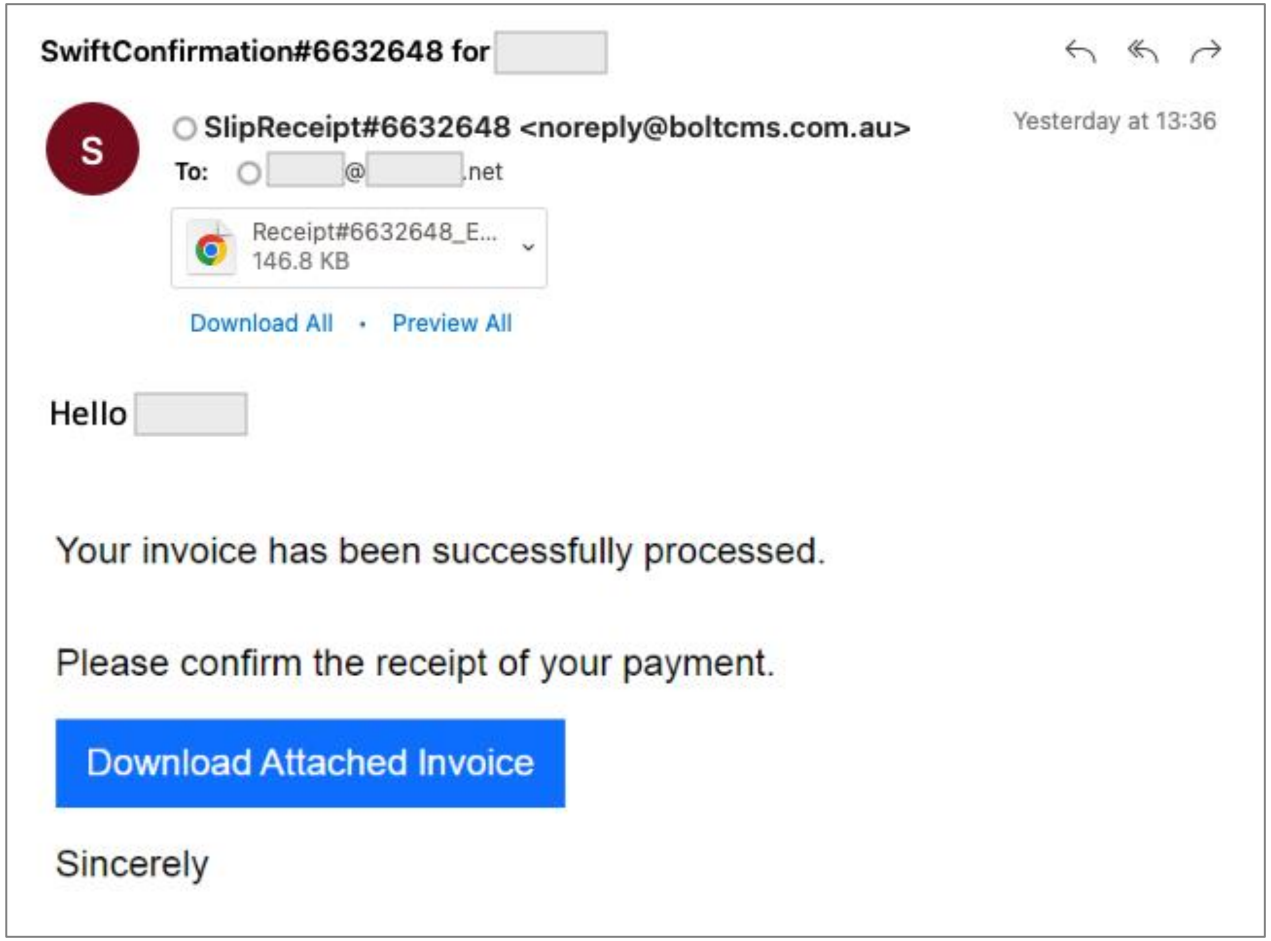
please review the document and sign via the attached.

This message was sent to:
[redacted]@[redacted].com

Expires January 28, 2022, 05:10:57 AM

1 attachment: scanned-xerox-financials_[redacted].html 13.9 KB

Call-to-Action



SwiftConfirmation#6632648 for [redacted]

S

○ **SlipReceipt#6632648 <noreply@boltcms.com.au>**

Yesterday at 13:36

To: ○ [redacted]@[redacted].net

Receipt#6632648_E...
146.8 KB

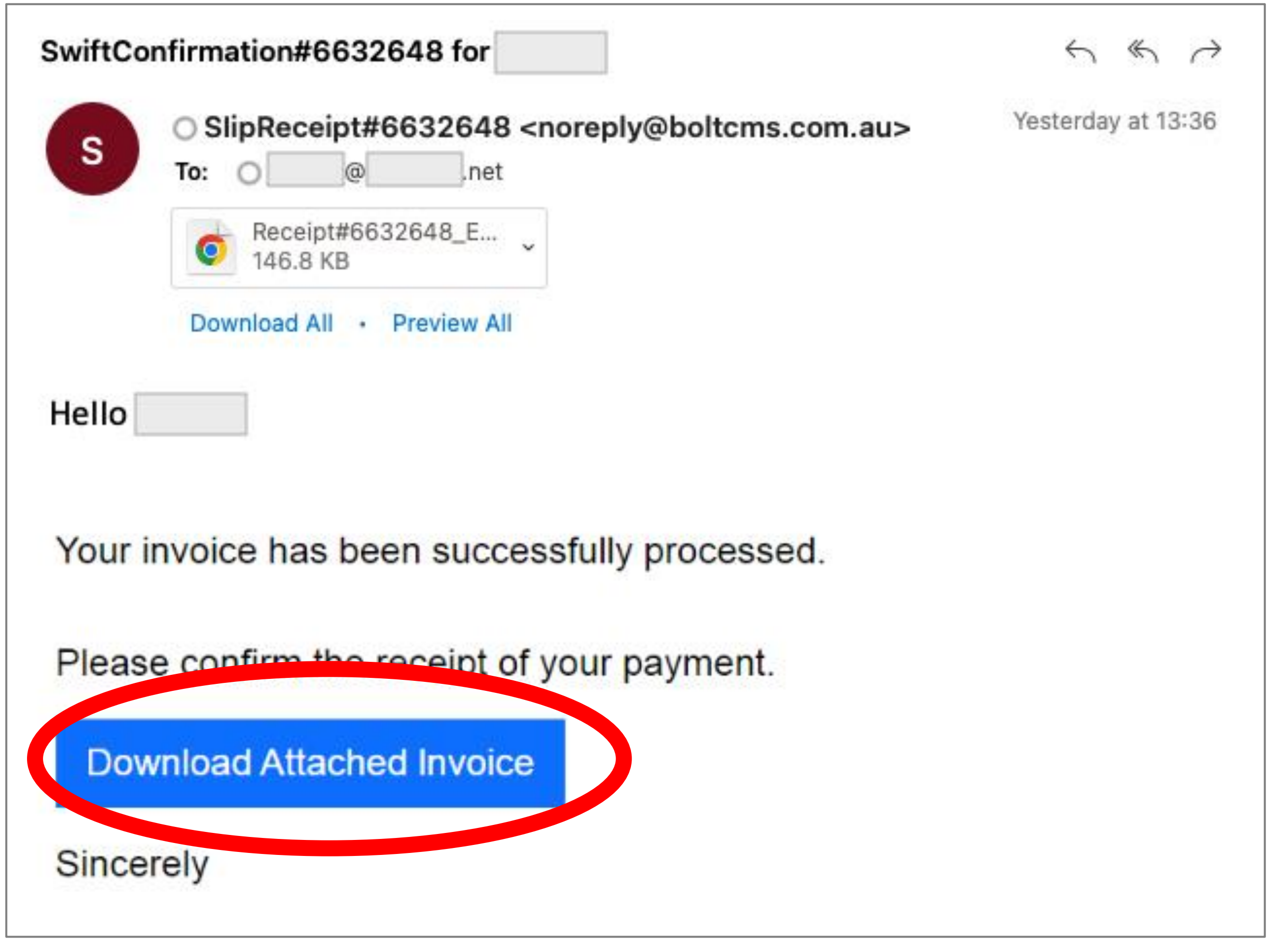
Hello [redacted]

Your invoice has been successfully processed.

Please confirm the receipt of your payment.

Sincerely

Call-to-Action



SwiftConfirmation#6632648 for [redacted]

○ **SlipReceipt#6632648 <noreply@boltcms.com.au>**

Yesterday at 13:36

To: ○ [redacted]@[redacted].net

Receipt#6632648_E...
146.8 KB

Download All • Preview All

Hello [redacted]

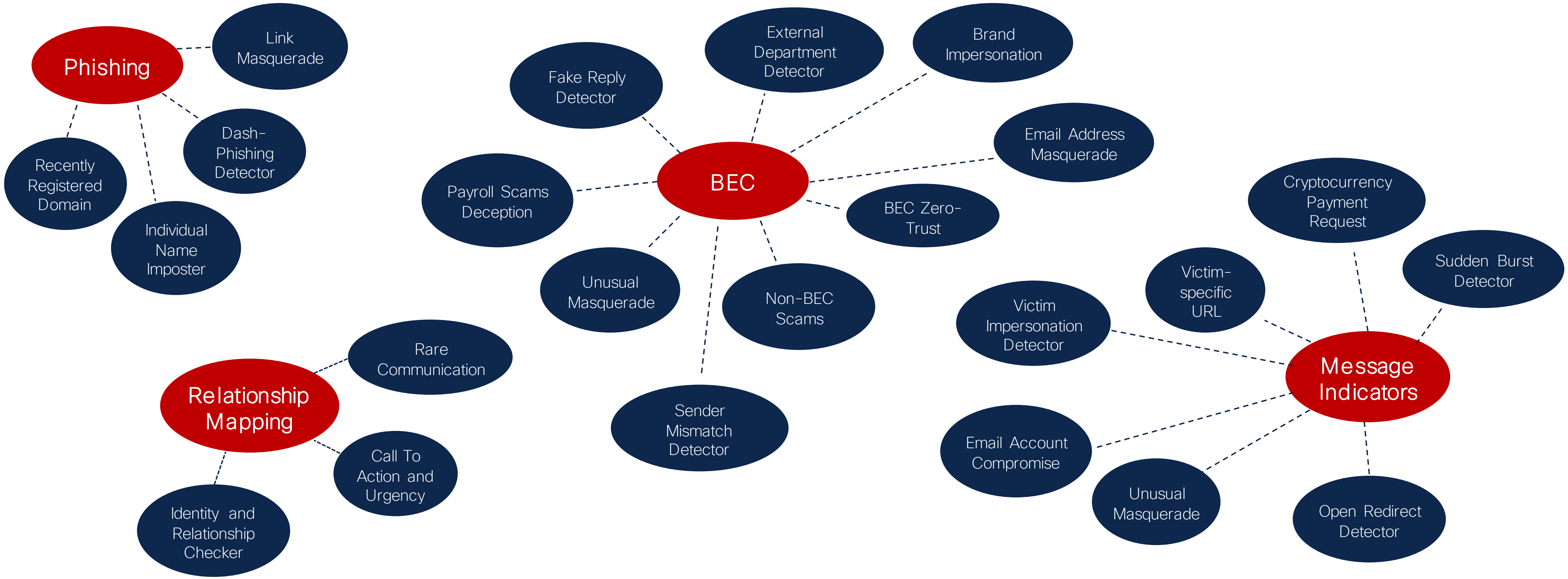
Your invoice has been successfully processed.

Please confirm the receipt of your payment.

Sincerely

Layering Detections using Machine Learning

The creation of mini-engines or *detectors* that identify techniques and behaviors using ML and NLP. The combination of detectors reveal the intent of the message.



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

Impactful reporting

Threat Data Today

Indicators of Compromise

Server IP: 148.221.56.4

Feedex.com

Reply To: Support@wellsfargo.sdf.com

SHA: bf407c05c8c8434550b9e2c54a0e4a7078e8fce91b5b80dc90f0d6fc814fddad

From Address

Client IP Address

Malicious Techniques

Fake Reply

Individual Name Imposter

Credential Phishing

Rare Communication

Link Masquerade

Cryptocurrency Payment

Payroll Scam

Urgency

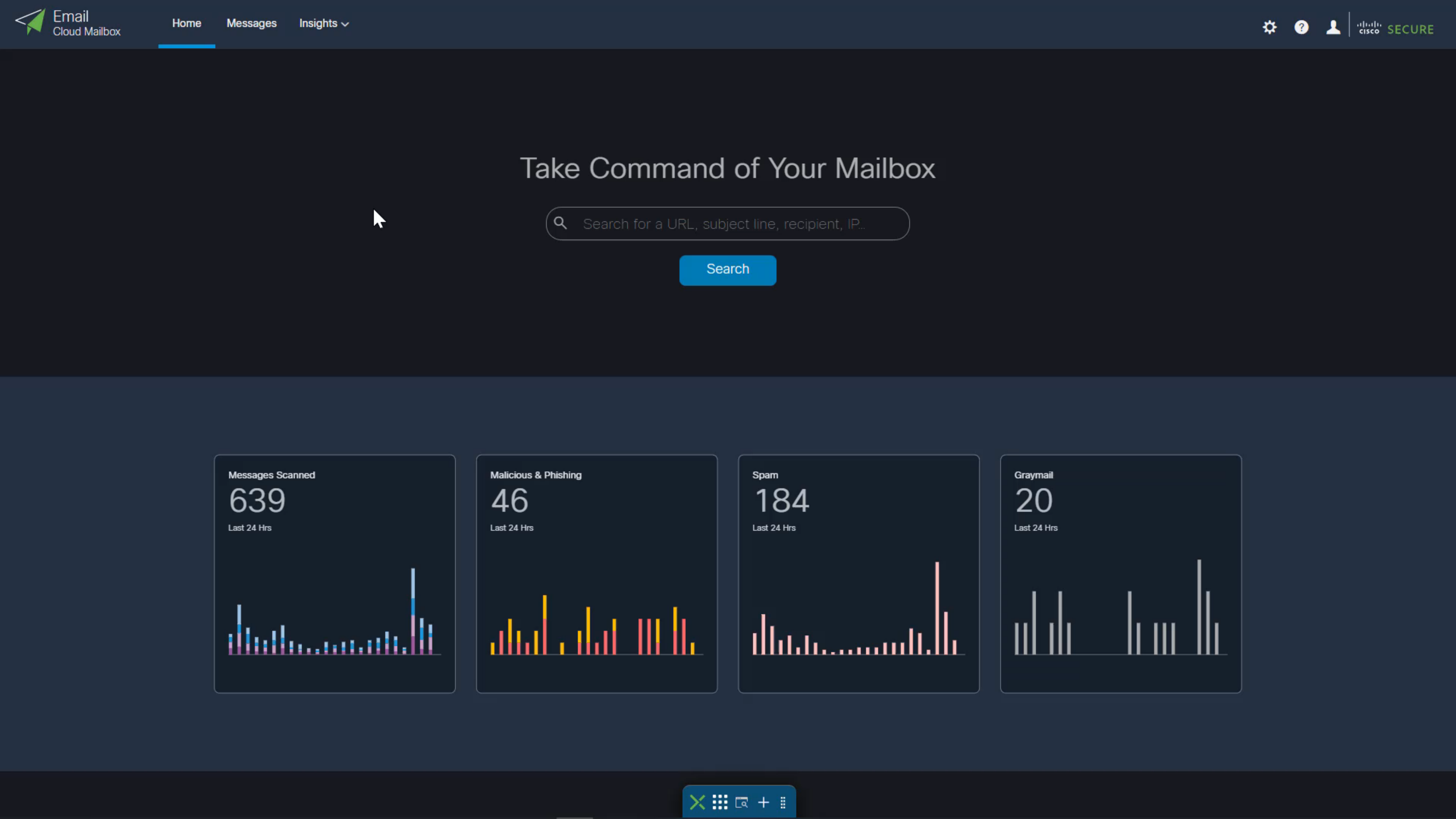
Address Masquerade

Dash-Phishing

Victim-specific URL

Brand Impersonation

Account Takeover



Take Command of Your Mailbox

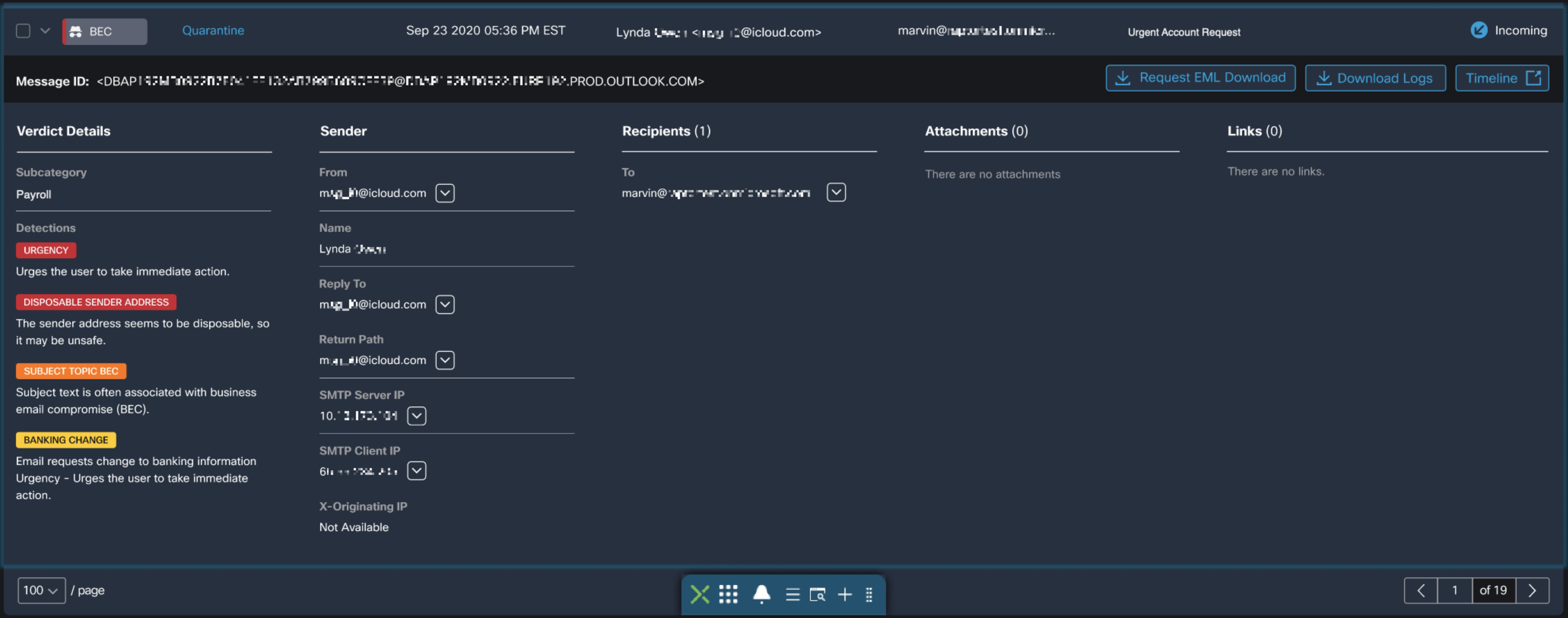
Search for a URL, subject line, recipient, IP...

Messages Scanned
639
Last 24 Hrs

Malicious & Phishing
46
Last 24 Hrs

Spam
184
Last 24 Hrs

Graymail
20
Last 24 Hrs



□ BEC Quarantine Sep 23 2020 05:36 PM EST Lynda [redacted] <[redacted]@icloud.com> marvin@[redacted]... Urgent Account Request Incoming

Message ID: <DBAP[redacted]@[redacted].PROD.OUTLOOK.COM>

Verdict Details

Subcategory
Payroll

Detections

URGENCY
Urges the user to take immediate action.

DISPOSABLE SENDER ADDRESS
The sender address seems to be disposable, so it may be unsafe.

SUBJECT TOPIC BEC
Subject text is often associated with business email compromise (BEC).

BANKING CHANGE
Email requests change to banking information Urgency - Urges the user to take immediate action.

Sender

From
m[redacted]@icloud.com

Name
Lynda [redacted]

Reply To
m[redacted]@icloud.com

Return Path
m[redacted]@icloud.com

SMTP Server IP
10.[redacted]

SMTP Client IP
6[redacted]

X-Originating IP
Not Available

Recipients (1)

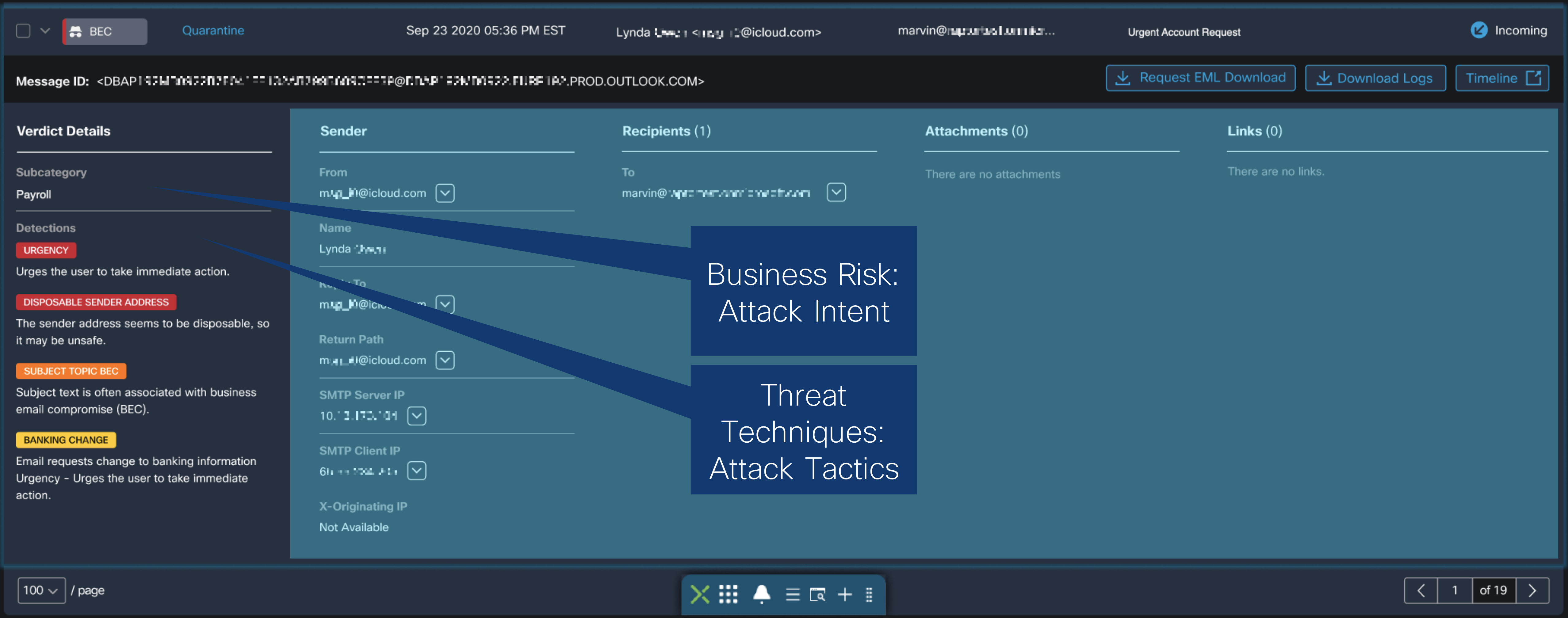
To
marvin@[redacted]

Attachments (0)

There are no attachments

Links (0)

There are no links.



Sep 23 2020 05:36 PM EST | Lynda [redacted] <[redacted]@icloud.com> | marvin@[redacted]... | Urgent Account Request

Message ID: <DBAP[redacted].PROD.OUTLOOK.COM>

Verdict Details

Subcategory
Payroll

Detections

URGENCY
Urges the user to take immediate action.

DISPOSABLE SENDER ADDRESS
The sender address seems to be disposable, so it may be unsafe.

SUBJECT TOPIC BEC
Subject text is often associated with business email compromise (BEC).

BANKING CHANGE
Email requests change to banking information Urgency - Urges the user to take immediate action.

Sender

From
m[redacted]@icloud.com

Name
Lynda [redacted]

Reply-To
m[redacted]@icloud.com

Return Path
m[redacted]@icloud.com

SMTP Server IP
10.[redacted]

SMTP Client IP
6[redacted]

X-Originating IP
Not Available

Recipients (1)

To
marvin@[redacted]

Attachments (0)

There are no attachments

Links (0)

There are no links.

100 / page

1 of 19

Business Risk: Attack Intent

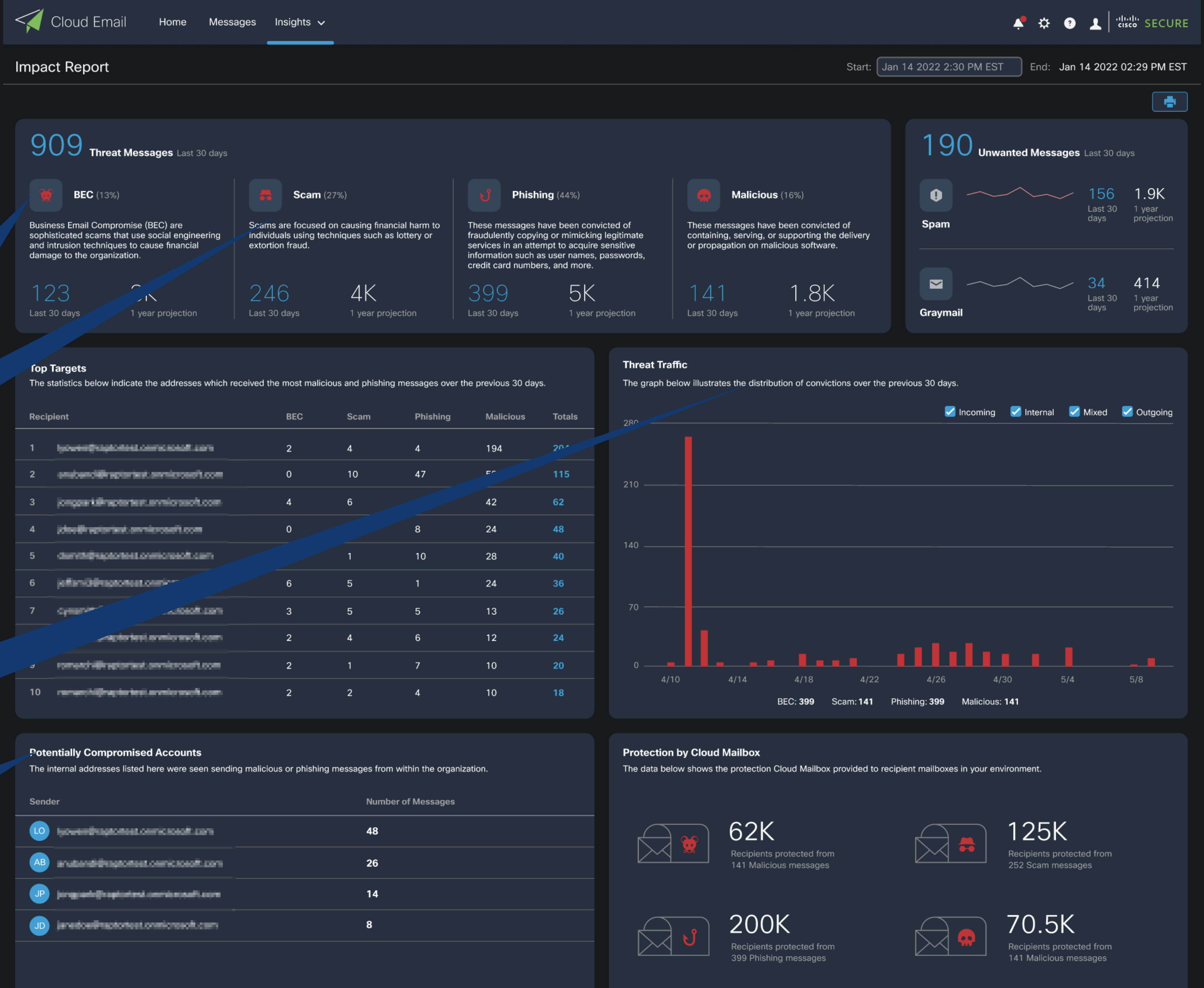
Threat Techniques: Attack Tactics

Business Email Compromise

Scam

Simplified Threat Reporting

Account Take Over Candidates



Impact Report

Start: Jan 14 2022 2:30 PM EST End: Jan 14 2022 02:29 PM EST

909 **Threat Messages** Last 30 days

BEC (13%)

Business Email Compromise (BEC) are sophisticated scams that use social engineering and intrusion techniques to cause financial damage to the organization.

123 Last 30 days — 2K 1 year projection

Scam (27%)

Scams are focused on causing financial harm to individuals using techniques such as lottery or extortion fraud.

246 Last 30 days — 4K 1 year projection

Phishing (44%)

These messages have been convicted of fraudulently copying or mimicking legitimate services in an attempt to acquire sensitive information such as user names, passwords, credit card numbers, and more.

399 Last 30 days — 5K 1 year projection

Malicious (16%)

These messages have been convicted of containing, serving, or supporting the delivery or propagation on malicious software.

141 Last 30 days — 1.8K 1 year projection

190 **Unwanted Messages** Last 30 days

Spam — 156 Last 30 days — 1.9K 1 year projection

Graymail — 34 Last 30 days — 414 1 year projection

Top Targets

The statistics below indicate the addresses which received the most malicious and phishing messages over the previous 30 days.

	Recipient	BEC	Scam	Phishing	Malicious	Totals
1	[redacted]	2	4	4	194	204
2	[redacted]	0	10	47	[illegible]	115
3	[redacted]	4	6	[illegible]	42	62
4	[redacted]	0	[illegible]	8	24	48
5	[redacted]	[illegible]	1	10	28	40
6	[redacted]	6	5	1	24	36
7	[redacted]	3	5	5	13	26
[illegible]	[redacted]	2	4	6	12	24
9	[redacted]	2	1	7	10	20
10	[redacted]	2	2	4	10	18

Threat Traffic

The graph below illustrates the distribution of convictions over the previous 30 days.

☑ Incoming ☑ Internal ☑ Mixed ☑ Outgoing

BEC: **399** Scam: **141** Phishing: **399** Malicious: **141**

Potentially Compromised Accounts

The internal addresses listed here were seen sending malicious or phishing messages from within the organization.

Sender		Number of Messages
LO	[redacted]	48
AB	[redacted]	26
JP	[redacted]	14
JD	[redacted]	8

Protection by Cloud Mailbox

The data below shows the protection Cloud Mailbox provided to recipient mailboxes in your environment.

62K Recipients protected from 141 Malicious messages

125K Recipients protected from 252 Scam messages

200K Recipients protected from 399 Phishing messages

70.5K Recipients protected from 141 Malicious messages

What about APP/Email Phishing Defense?

Positioning Guide

- APP/Agari was added because it brought value and features to the email security
- Significant investments were done into CM/ETD
- APP vendor became a “competitor” due to acquisition(Help Systems)
- APP is not free of challenges/limitations. We closed the gap within ETD
- ETD has proven to have more efficacy in stopping threats and more visibility(scans entire email)
- ETD is easier to deploy(no sensor), easier to support(TAC)
- APP End-of-Sale Dec 14 / End-of-Support Oct 31, 2027

Key takeaways

- Cloud Mailbox is now Email Threat Defense
- ETD is an easy-to-deploy, full feature secure email solution with ML/AI support
- Advanced reporting provides more visibility

Security Partner Discounts – Deal Registration

Security Domain	Security Hunting/Teaming	New Account Breakaway or Competitive	Partner-led 'One Year on Us' Discount w/ Credit
Secure Firewall (incl. Virtual)	up to 65%	72%	n/a
Secure Email	up to 65%	68%	79%
Secure Endpoint	up to 65%	68%	79%
Secure Web Appliance	up to 65%	68%	n/a
Cisco Kenna	up to 65%	n/a	76%
Secure Workload	up to 60%	n/a	73%
Identity Services Engine	up to 60%	64%	76%
Secure Network Analytics	up to 60%	64%	76%
Cloud Security (Umbrella)	up to 60%	n/a	73%
Secure Access by Duo	up to 35%	n/a	57%
Secure Email Threat Defense	up to 30%	n/a	53%

↑ up to 76%*

Take Back Incentive*

Earn a +4% incremental discount when migrating from Cisco Firewalls or Competitive Firewalls

* Discounts are exclusive to only Sustainability Specialized Partners

All discounts are for direct/distributor pricing, and all 2-tier partners must negotiate directly with their distributor.

For more info: visit Security Deal Registration

More Information

Useful and updated Information

- Mailer: ask-secure-email@cisco.com
- TME SharePoint site: https://cisco.sharepoint.com/sites/SecureEmail/
- Free 30-day Trial
  https://cs.co/cmd-trial

Q&A

cisco SECURE