Global vision.

Local knowledge.

Cisco Connect Dubrovnik

Croatia · 28.03.2019

Cisco Email Security

Zaštitite svoj najosjetljiviji dio sustava od napada

Vedran Franjić
System Engineer Sales
29.03.2019.

Agenda

- Email importance
- Multilayer approach
- DP and APP
- Securing o365
- Architecture
- Intelligence
- Licensing

Email Importance

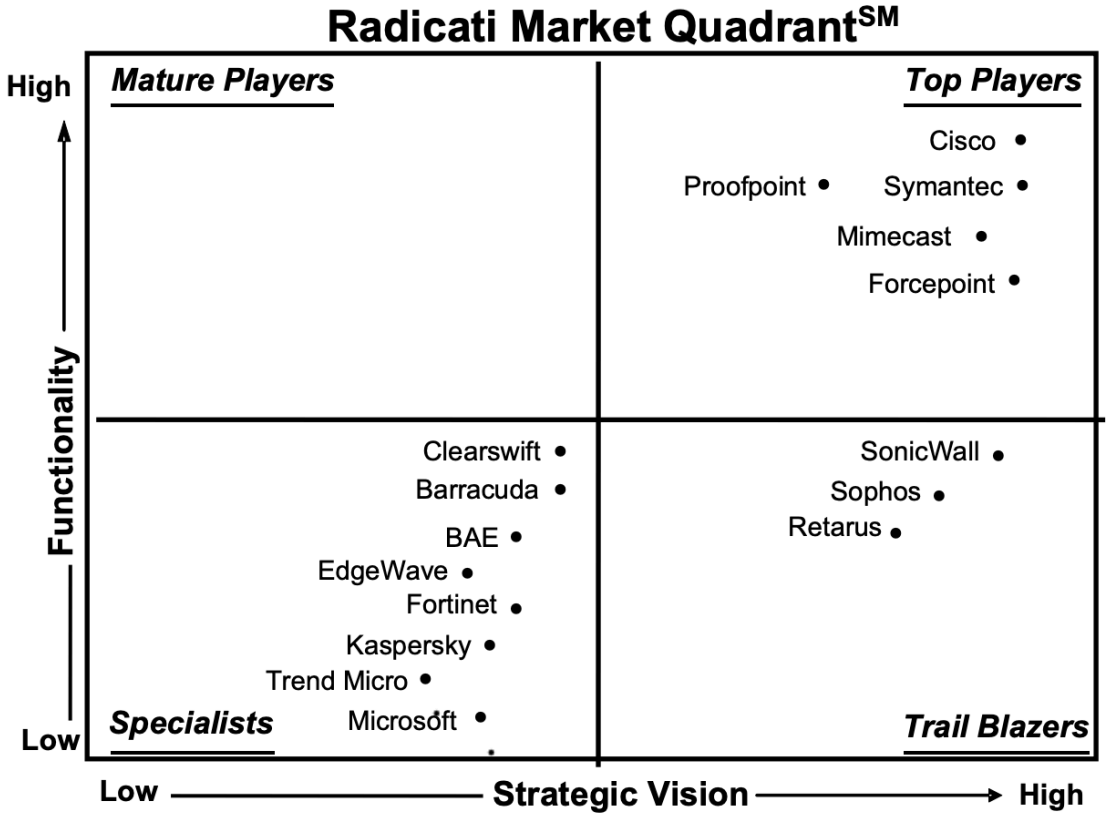


Figure 3: Secure Email Gateway Market Quadrant, 2018*

Grad [redacted] uplatio prevarantu 50.000

R.I.
15.9.2018.

Foto: 123rf, gradonacelnik.hr

NEKOLIKO tvrtki i institucija u Hrvatskoj dobilo je tijekom srpnja lažne mailove u kojima ih se traži da na inozemni račun uplate veće iznose.

Pročelnik za financije Grada [redacted] bio je jedan od njih. 9 srpnja dobio je e-mail u kojem gradonačelnik [redacted] od njega traži da izvrši hitnu uplatu na bankovni račun naveden u mailu. Pročelnik je s računa Grada prebacio 50.000 eura na navedeni račun.

"U Odjel za financije stigla je poruka s upitom možemo li obaviti plaćanje u inozemstvo. Počinitelj prijevare u zabludu je doveo našeg službenika tako što se predstavio u moje ime, napravio lažni mail s podacima kao da sam to ja", objašnjava gradonačelnik [redacted] Počinitelj mu nije hakirao mail, nego adresu s koje je poslao svoj mail nazvao gradonačelnikovim imenom. "Na taj mail pročelnik je odgovorio upitom na koji račun, komu i koji iznos, provjerio u banci može li ići uplata, dobio instrukcije za plaćanje i ono je odrađeno", objašnjava za Glas Slavonije gradonačelnik [redacted]

Podsjećajući na proceduru kako se obavljaju plaćanja, [redacted] dodaje kako se taj dan, do tada, on i pročelnik nisu vidjeli ni čuli. Oko 14.30 sati, nastavlja, pročelnik mu na mail šalje potvrdu o uplati.

"Bilo mi je malo čudno. Prvo se činilo da je nama netko nešto platio iz Britanije, no potom vidim da smo mi

Email was not built with security

It’s easy for attackers

95% of breaches start with email

Attackers Use Multiple Ways to Get In

Malware

Ransomware detections up 90% in 2018[1]

Business Email Compromise (BEC)

$5.3 Billion in losses[2]

Phishing

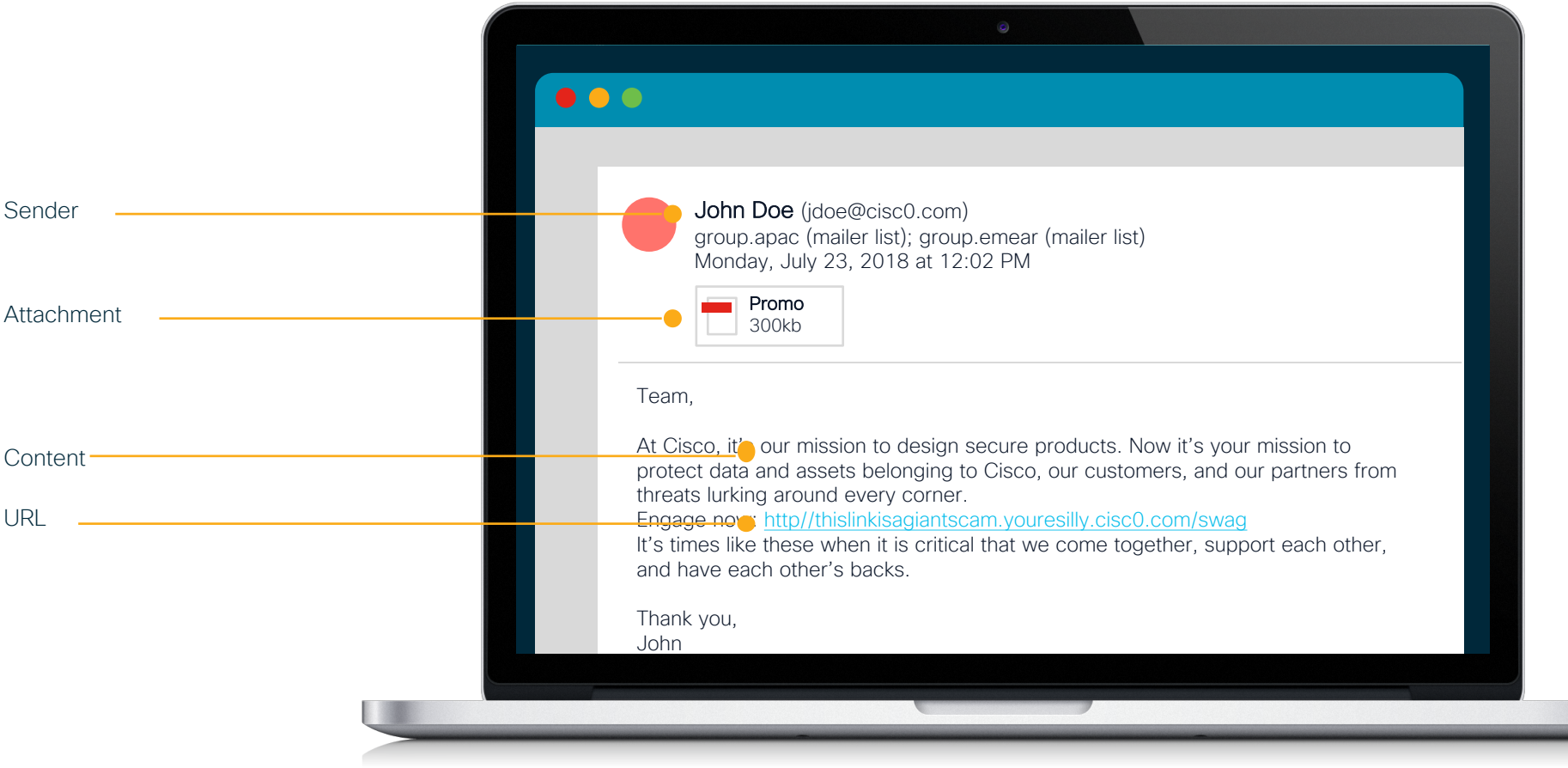
$9.1 Billion in 2018[3]

Domain Compromise

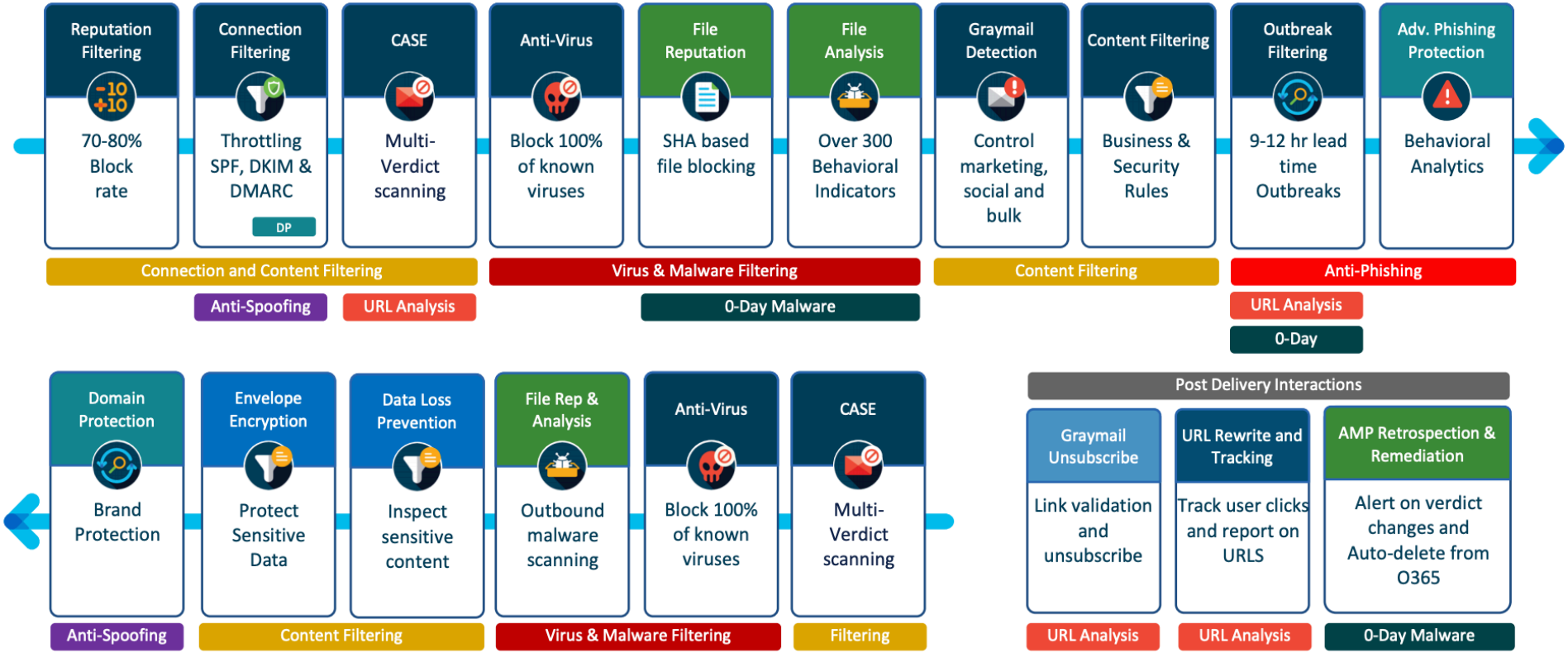
54% of legitimate domains used in phishing campaigns[4]

Multilayered Approach

Solution: Protect Every Part of An Incoming Email

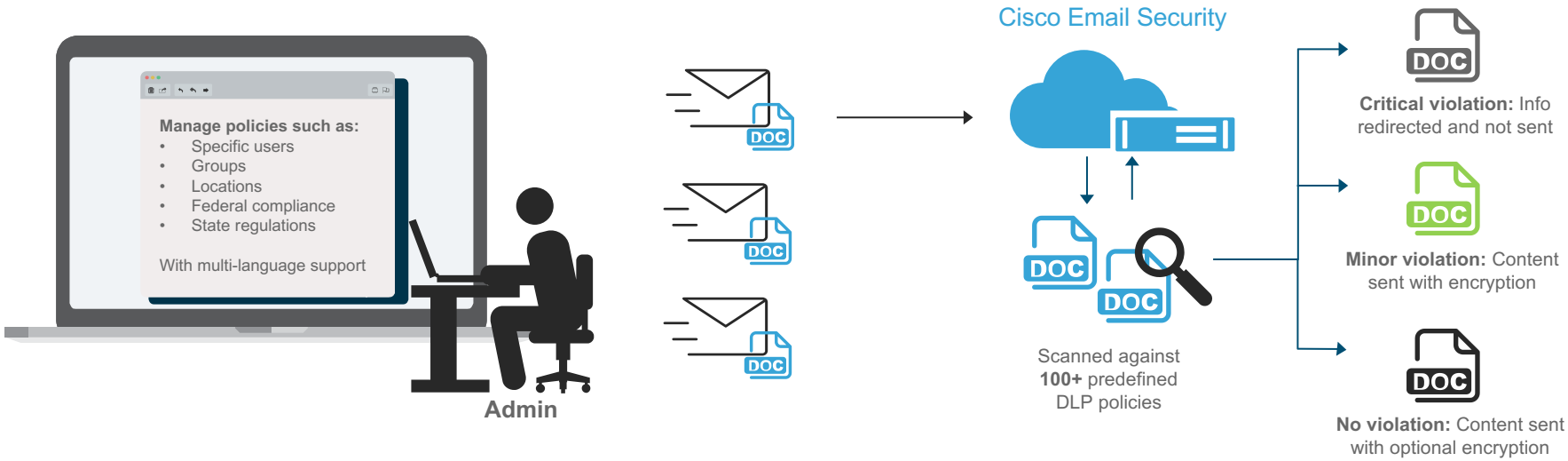


Quick Review: Email Pipeline



Protect personal information and IP

Data Loss Prevention (DLP)



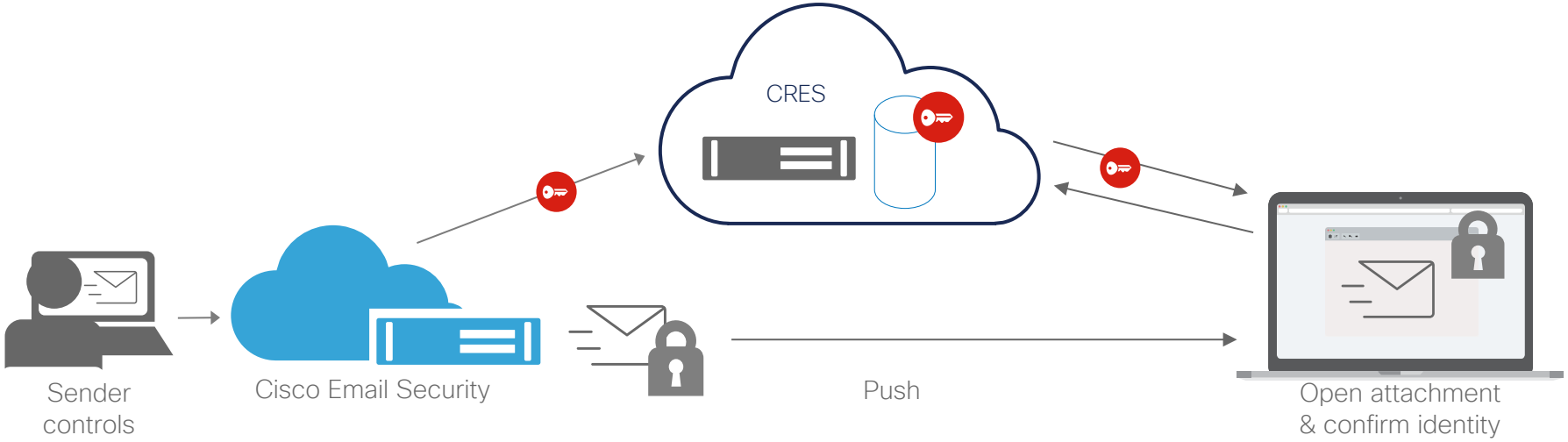
Control what leaves the network and customize policies

Scan email content for sensitive information

Prevent data exfiltration automatically

Extend security to external communications

Cisco Registered Envelope Service (CRES)



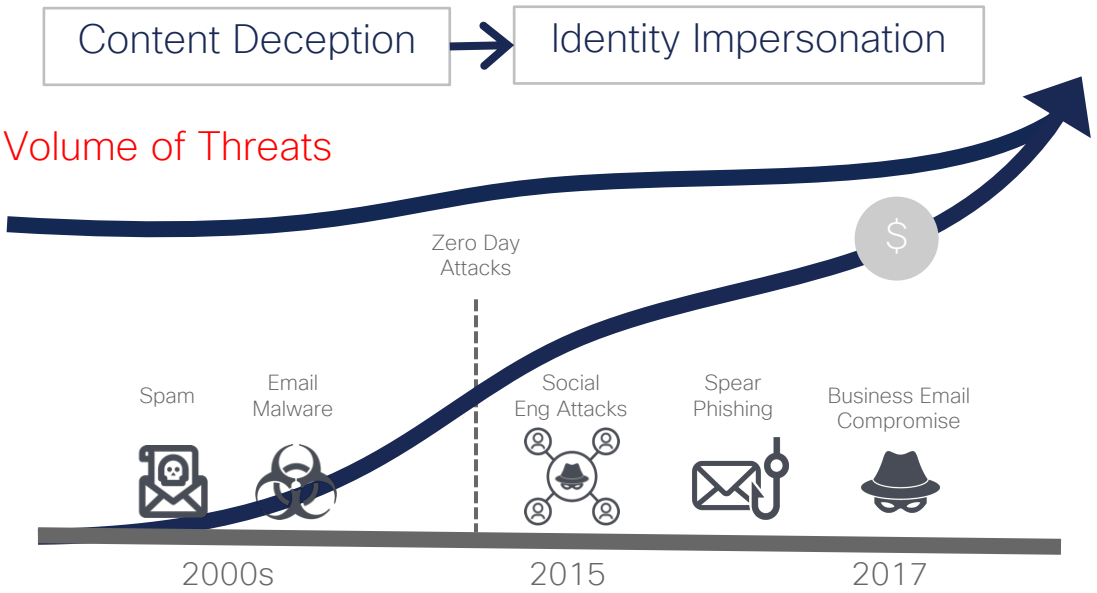
Scan messages for keywords, policies, and sender

Apply authentication mechanisms to access encryption keys

Maintain control over your sent messages

DP and APP

Advanced phishing attacks use identity impersonation

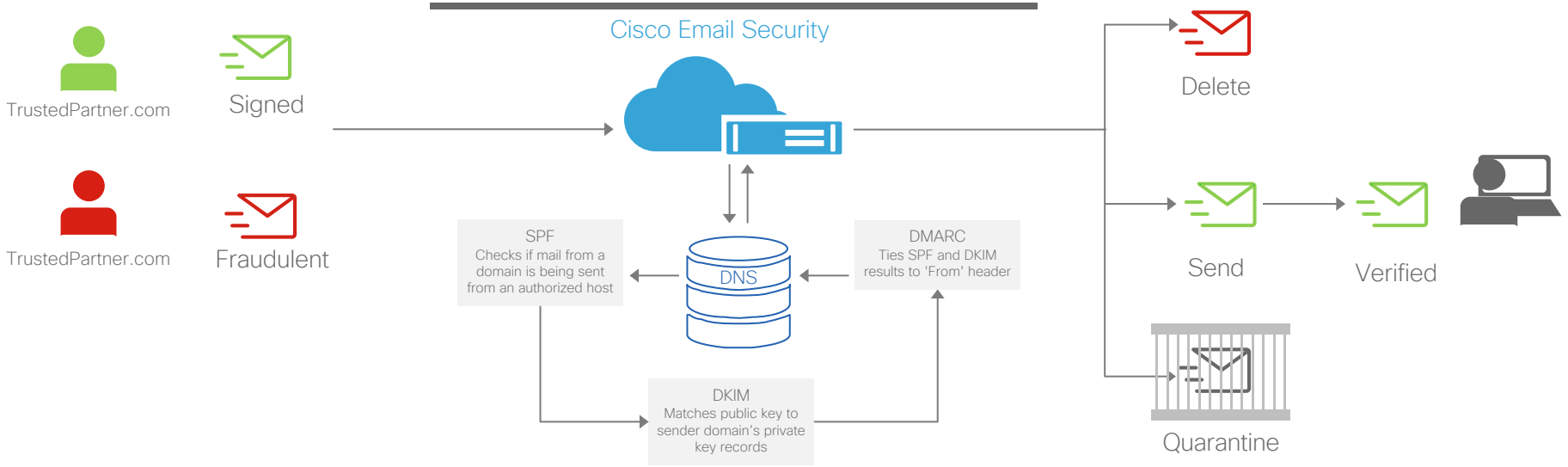


30% open malicious emails
13% click on malicious attachments
3:45 until first user is compromised

Sources: CSOonline.com, Cybersecurity ventures, Nucleus Research, FBI I3C (Jan '15 – Dec '16)

Block fraudulent senders

DMARC, DKIM and SPF

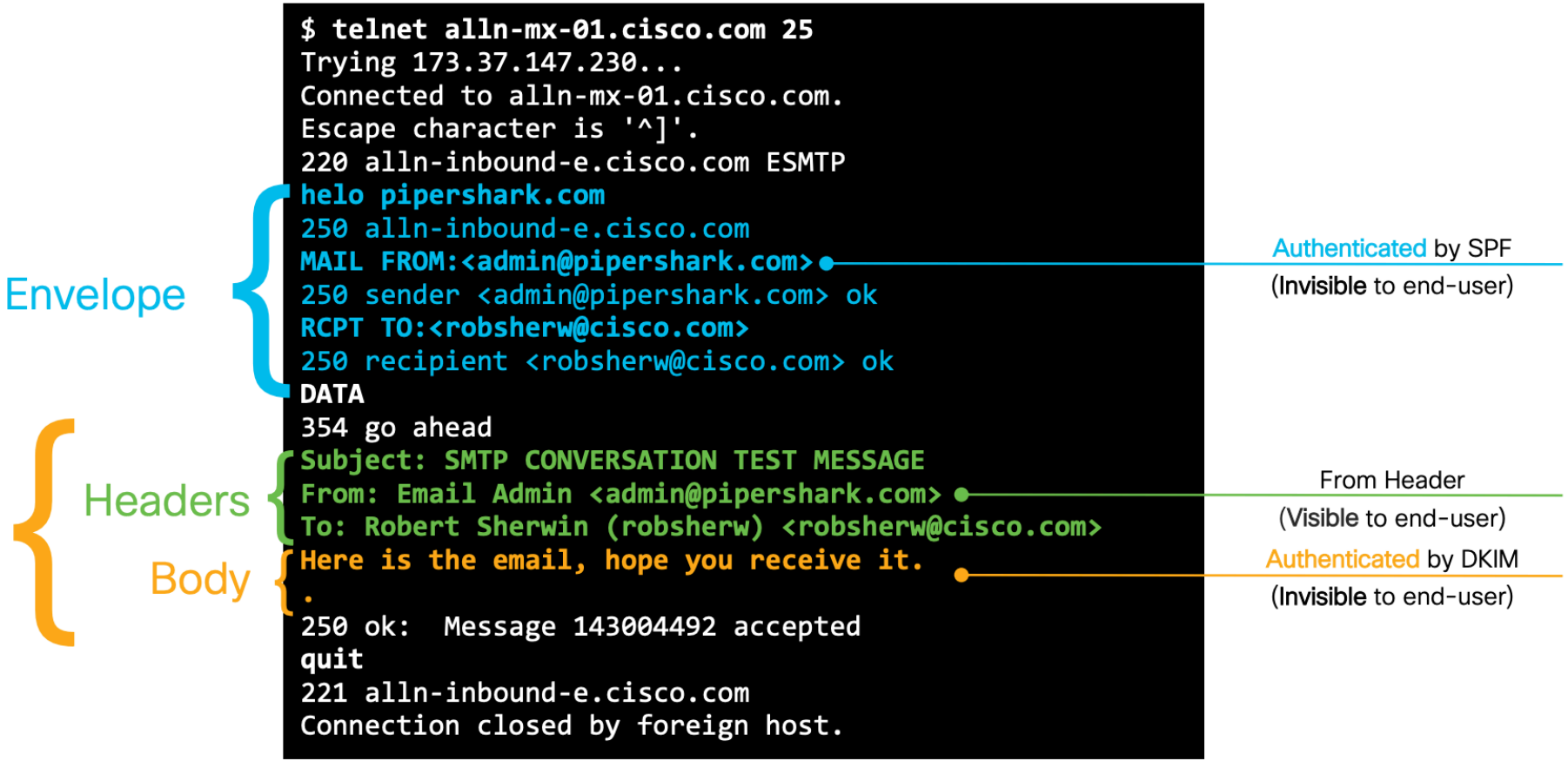


Determine whether a sender is reputable

Inspect sender details on inbound messages

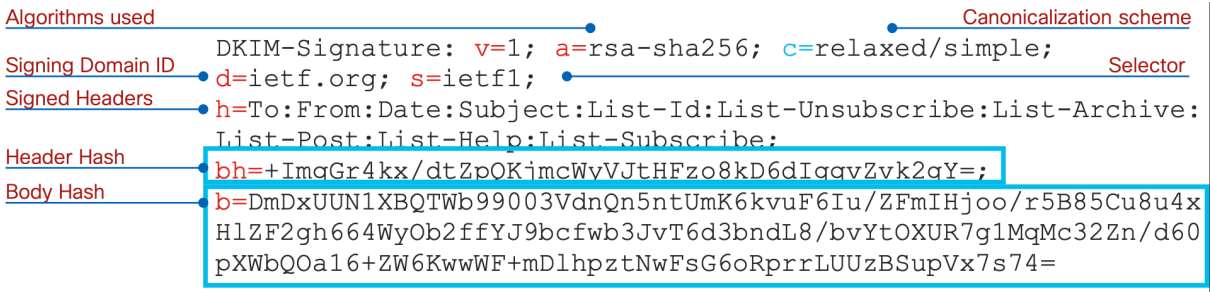
Block invalid senders and identify next steps

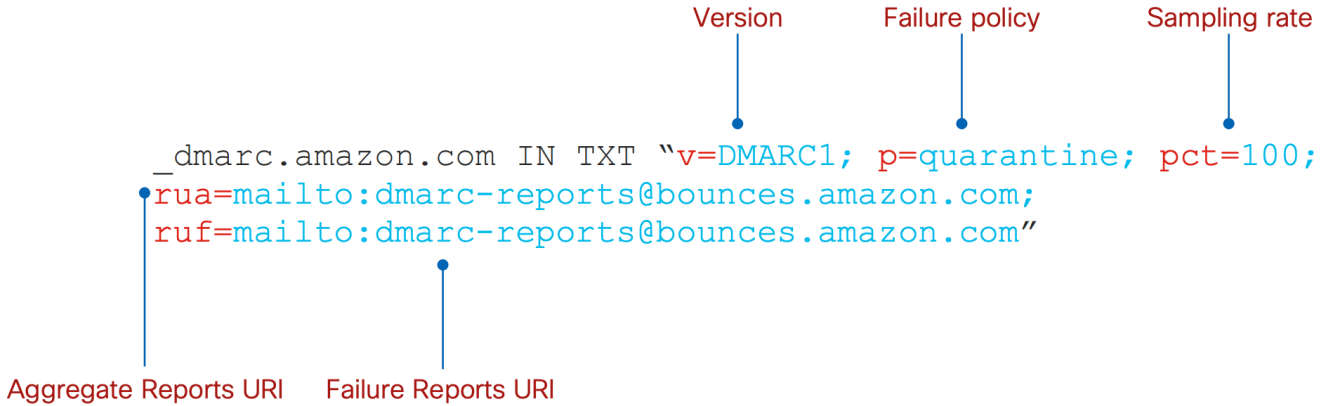
What gets authenticated?



DMARC, DKIM and SPF

```
dhs.gov IN TXT "v=spf1 ip4:216.81.91.184 ip4:216.81.85.157
include:spf.protection.outlook.com -all"
```





Email Authentication Overview

SPF

- Authenticates Message Path
- Authorized senders in DNS

DKIM

- Authenticates Message Content
- Public Encryption keys in DNS

DMARC

Reliable

Visibility

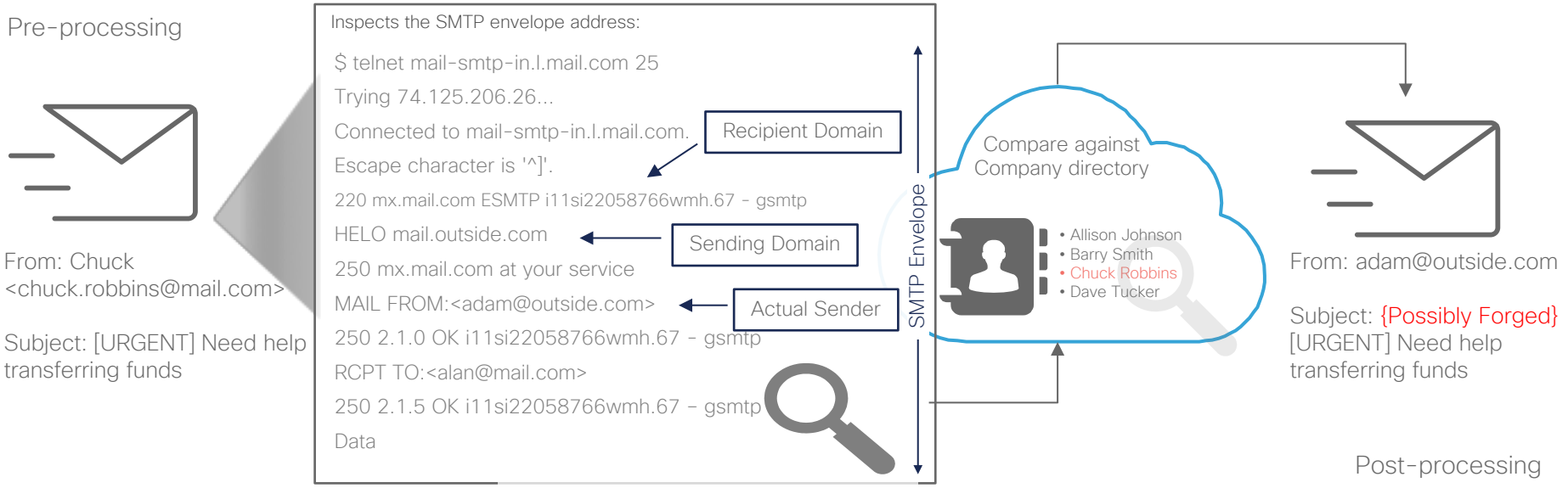
Action-Based Policies

RUA

RUF

Forged Email Detection

FBI defines it as Business Email Compromise (BEC)



Inspect SMTP envelope for True sender address

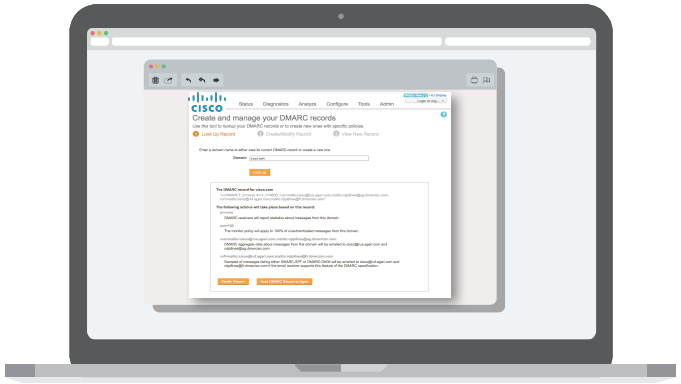
Match sender address against company directory

Send appended mail to warn users of potential forgery

Record a log of attempts and actions taken

Protect your brand

Cisco Domain Protection



Cisco Domain Protection

Protect your brand

- Easily analyze, update and take action against those misusing your domain to send malicious email
- Validate those who use your domain appropriately

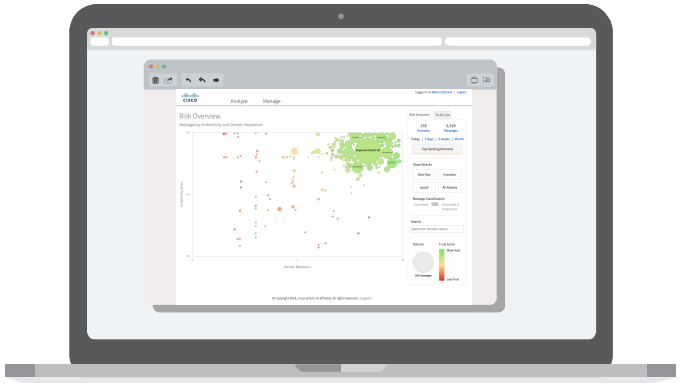
Automate DMARC authentication

- Drive to DMARC Enforcement with proven tools and services

Block attackers from using your domain

Protect against fraudulent senders

Advanced Phishing Protection



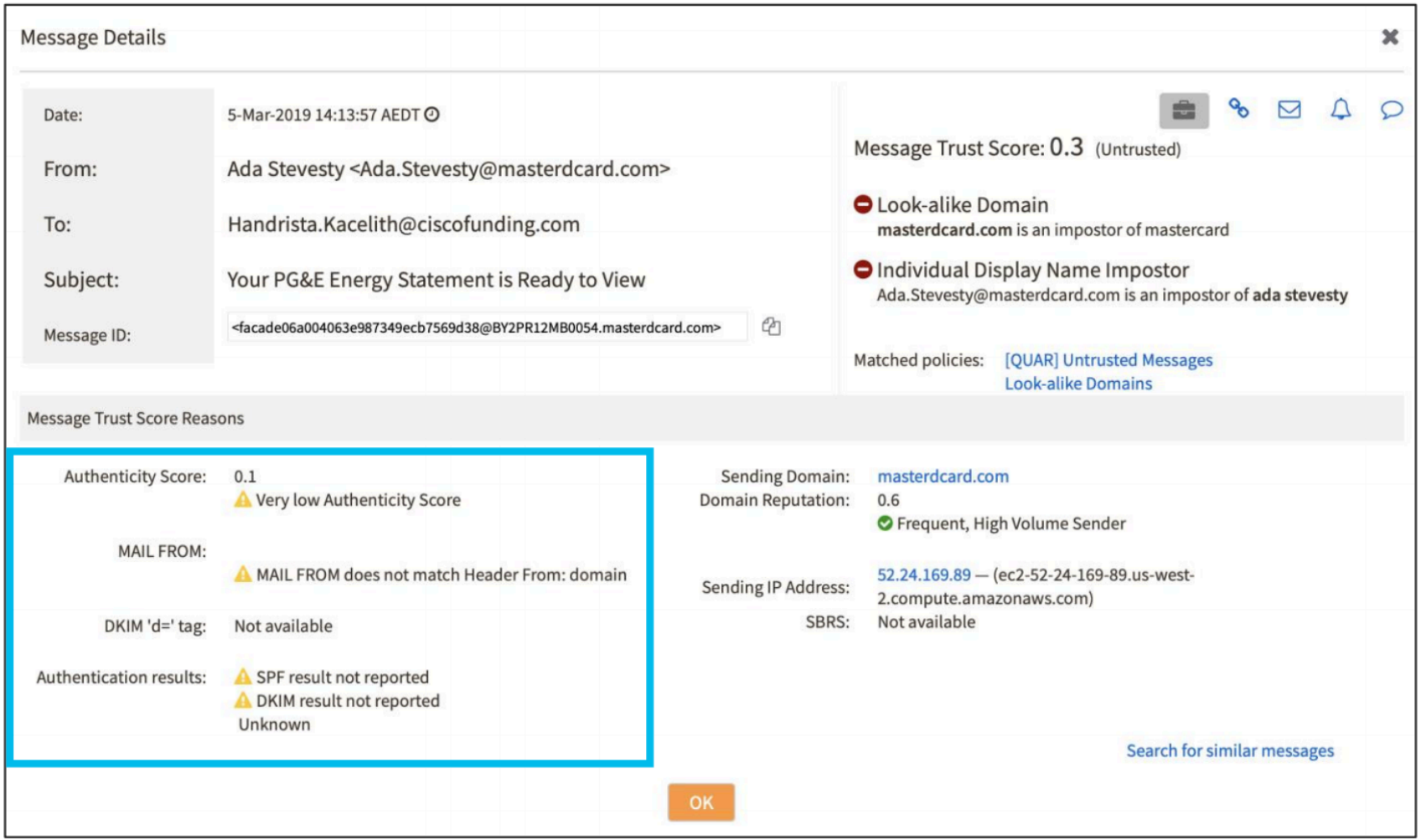
Advanced Phishing Protection

Local intelligence

- Learns and authenticates identities and behavioral relationships for enhanced protection

Reduce business email compromise

- Discerns which emails carry targeted phishing attacks and only legitimate emails get delivered

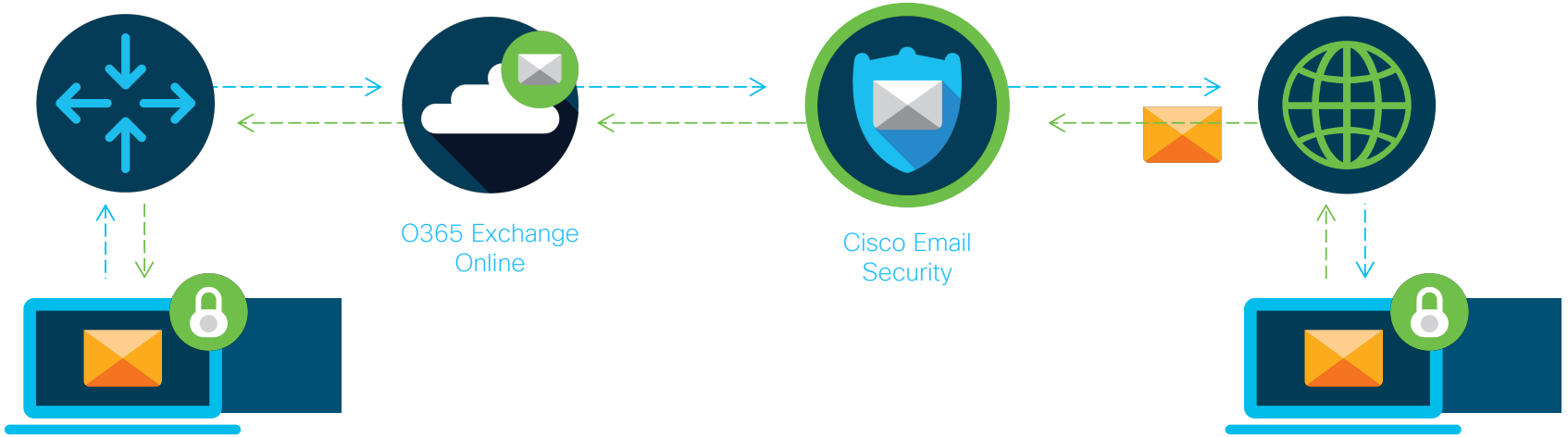

Message Details
Date:
5-Mar-2019 14:13:57 AEDT
From:
Ada Stevesty <Ada.Stevesty@masterdcard.com>
To:
Handrista.Kacelith@ciscofunding.com
Subject:
Your PG&E Energy Statement is Ready to View
Message ID:
<facade06a004063e987349ecb7569d38@BY2PR12MB0054.masterdcard.com>
Message Trust Score: 0.3 (Untrusted)
Look-alike Domain
masterdcard.com is an impostor of mastercard
Individual Display Name Impostor
Ada.Stevesty@masterdcard.com is an impostor of ada stevesty
Matched policies:
[QUAR] Untrusted Messages
Look-alike Domains
Message Trust Score Reasons
Authenticity Score:
0.1
Very low Authenticity Score
MAIL FROM:
MAIL FROM does not match Header From: domain
DKIM 'd=' tag:
Not available
Authentication results:
SPF result not reported
DKIM result not reported
Unknown
Sending Domain:
masterdcard.com
Domain Reputation:
0.6
Frequent, High Volume Sender
Sending IP Address:
52.24.169.89 — (ec2-52-24-169-89.us-west-2.compute.amazonaws.com)
SBRS:
Not available
Search for similar messages
OK

Secure o365

O365 – E3	Cisco Email Security w/O365
✓ Anti-spam filters	✓ Anti-spam filters
✓ Anti-virus protection	✓ Anti-virus protection*
✓ Policy enforcement	✓ Policy enforcement
✓ Disaster recovery	✓ Disaster recovery
✓ Directory services	✓ Directory services
✓ Advanced Threat Protection (Safe Links, Safe Attachments)*	✓ Graymail detection
✓ Message tracking (limited)	✓ Outbreak Filters
✓ Email encryption (cloud-based only)	✓ Message tracking
✓ Data loss prevention	✓ Email encryption (cloud and on premise)
	✓ Advanced Malware Protection
	✓ Detailed reporting
	✓ Zero-day incident management
	✓ Data loss prevention

*Anti-virus provided by O365
*Only with E5

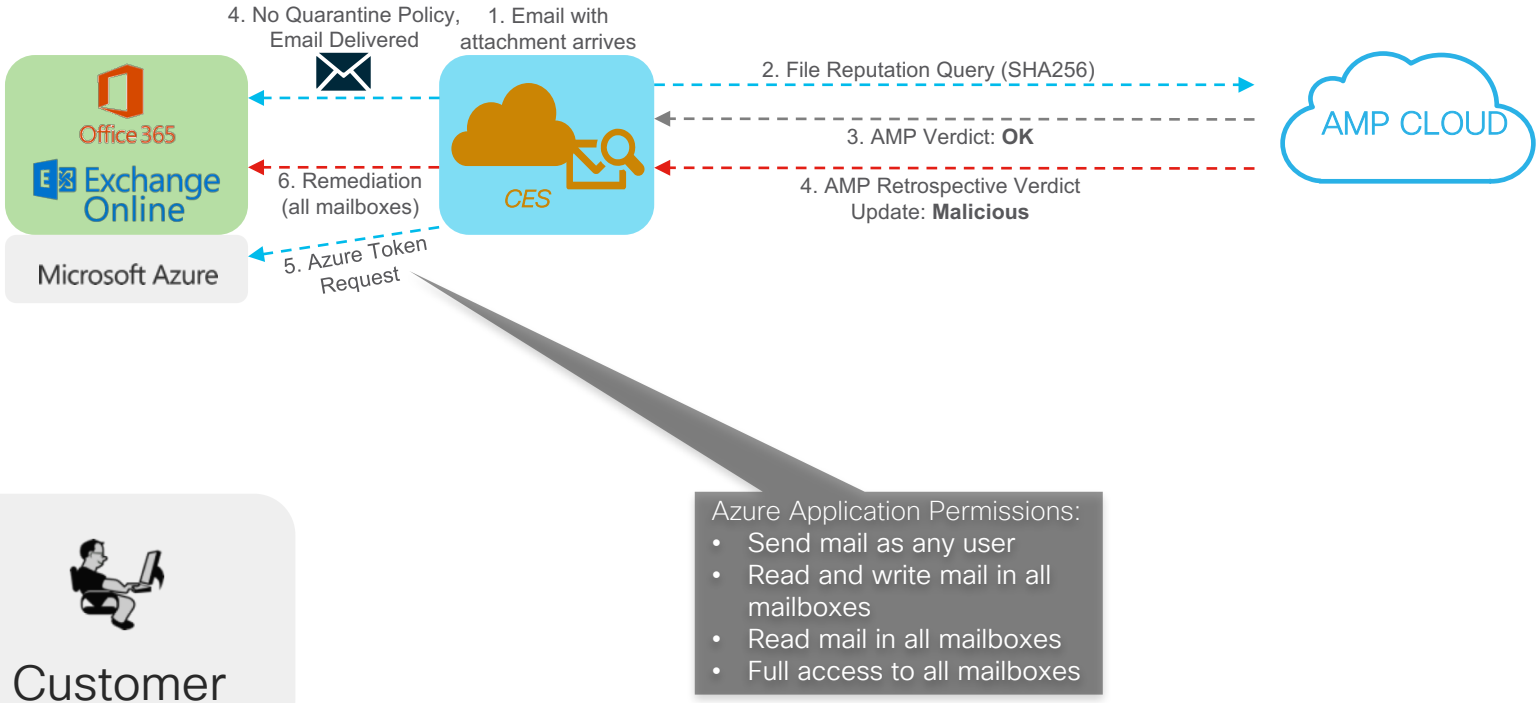
Easily Integrate with Office 365



Outbound Traffic

Inbound Traffic

AMP Retrospective Event Flow

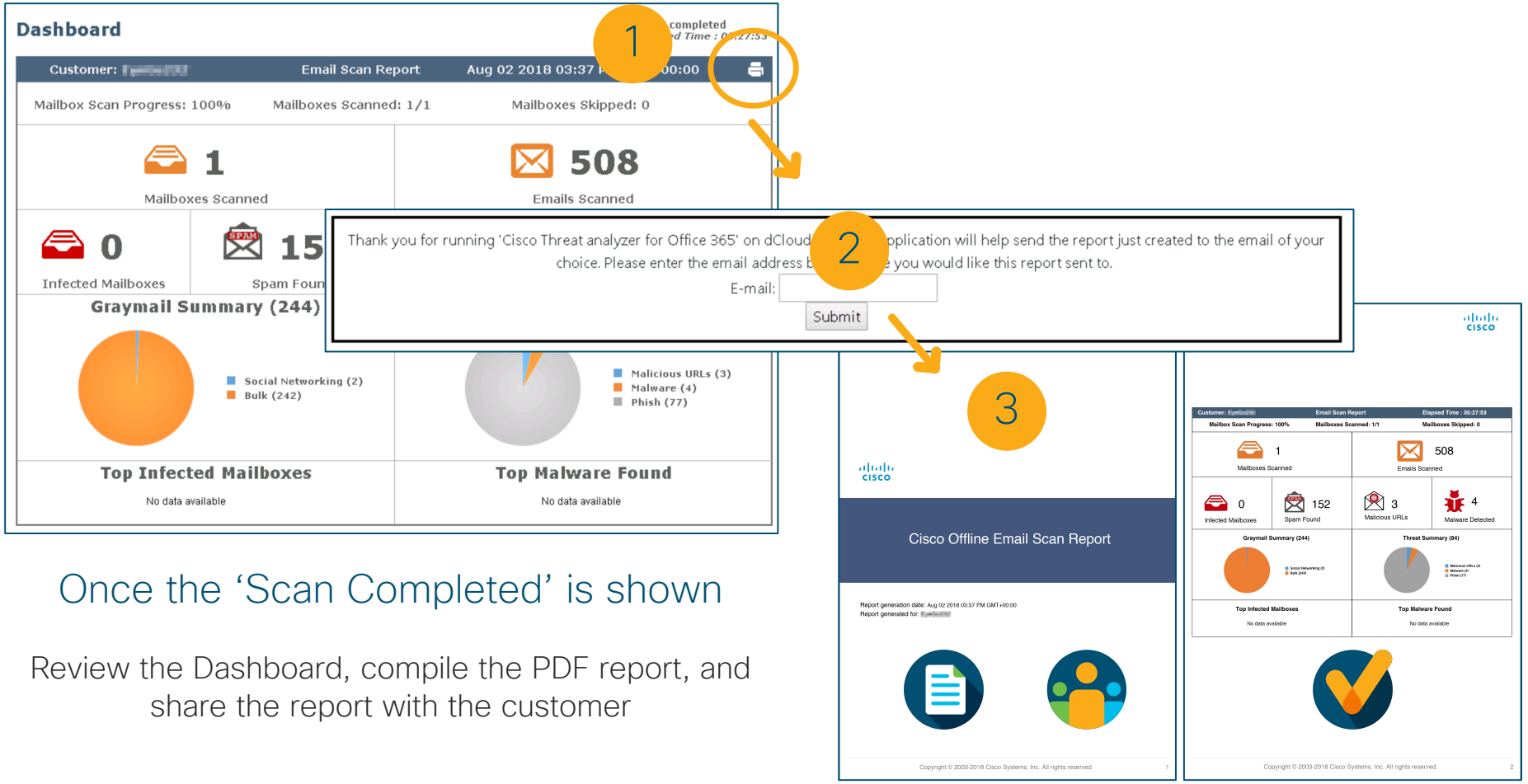


Cisco Threat Analyzer For o365

A free assessment tool to identify security gaps

Visibility into threats gone undetected

Summary scan report with details



Once the ‘Scan Completed’ is shown

Review the Dashboard, compile the PDF report, and share the report with the customer

Arhitecture

Don’t compromise on features when making a choice

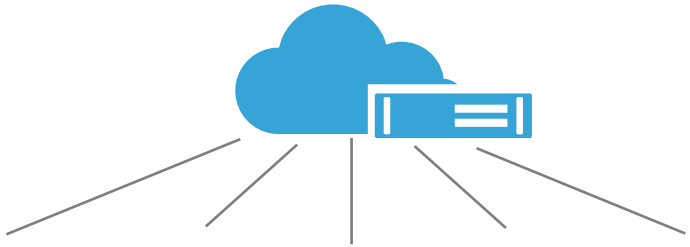
Cloud

On-Premises
(Physical or Virtual)

Hybrid

Cluster

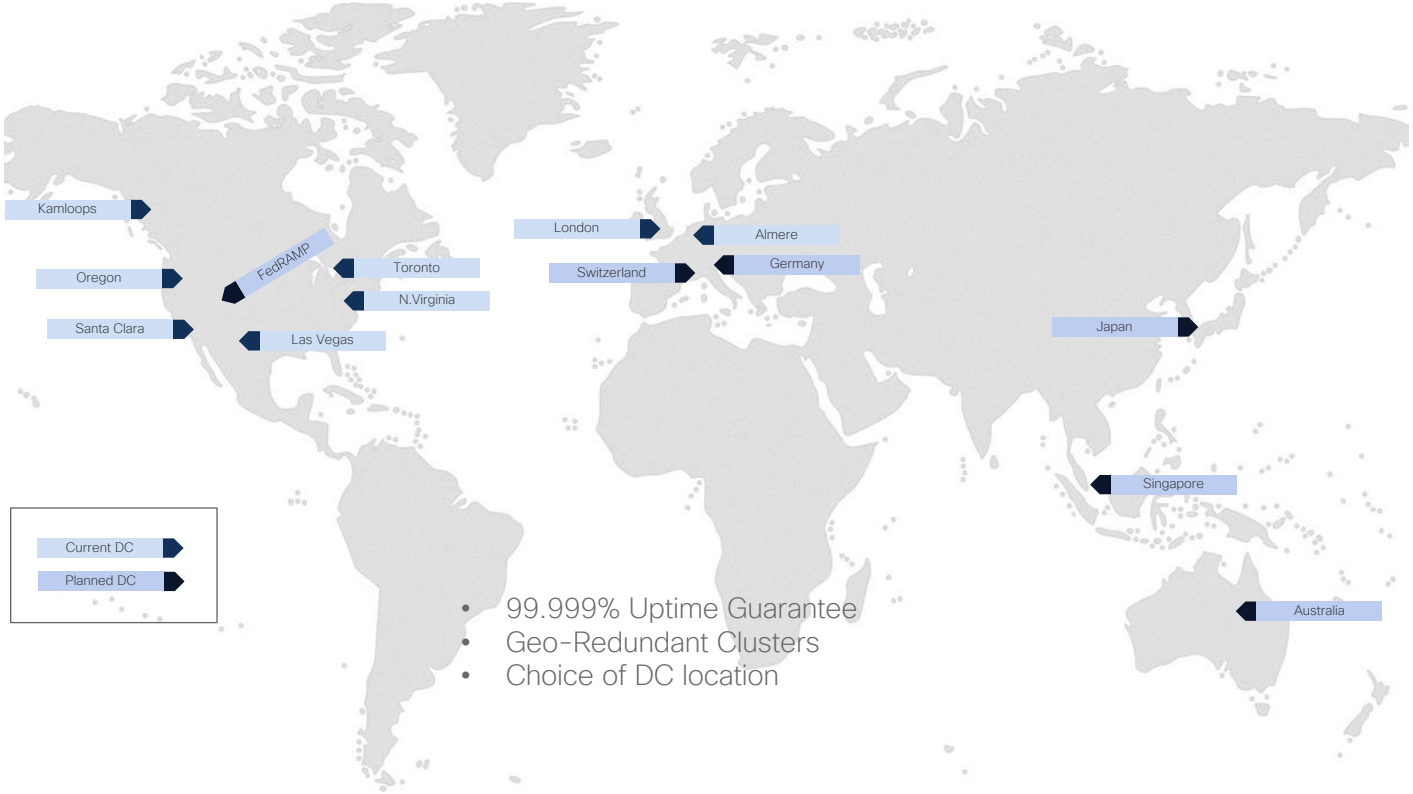
Transition to the cloud with confidence



Cisco Email Security

- Integrate easily with O365
- Deliver 99.999% availability
- Prevent shared-fate with compute instances
- Increase dedicated instances up to 50% at no cost
- Migrate to new deployment options easily

CES: New Datacenters



- 99.999% Uptime Guarantee
- Geo-Redundant Clusters
- Choice of DC location

4 new DCs launched in:

- Toronto
- Kamloops
- Oregon (AWS)
- N. Virginia (AWS)

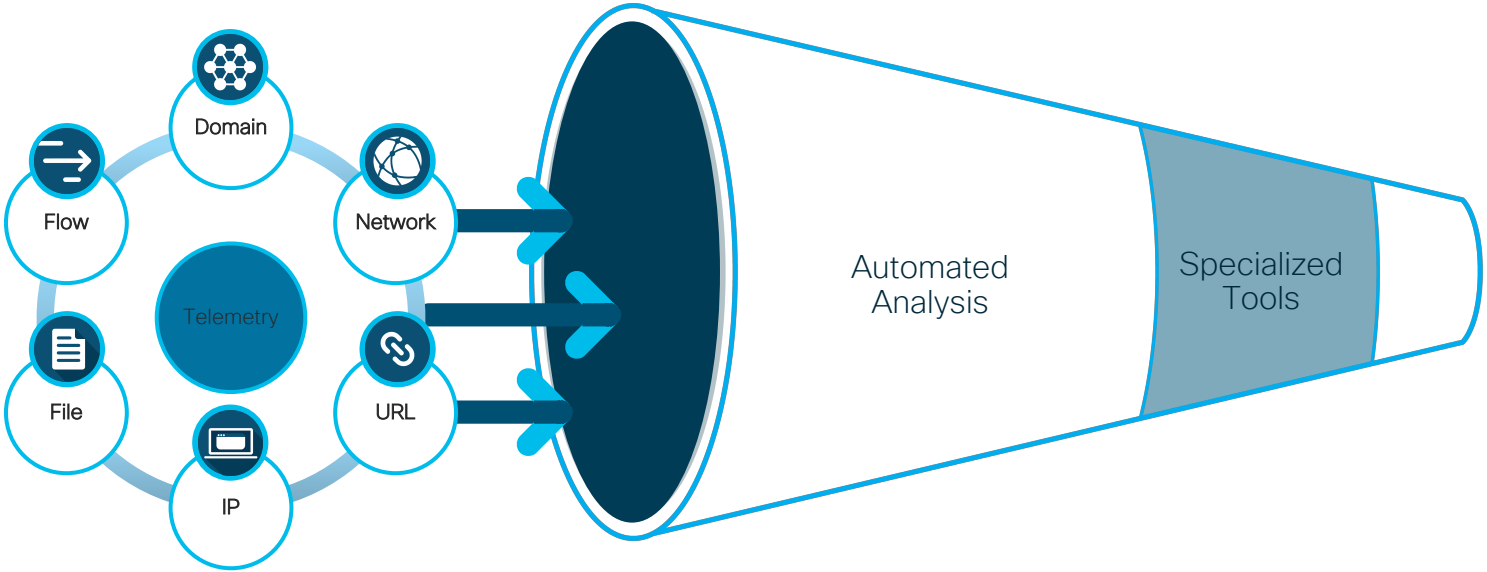
Additional sites

- Switzerland
- Germany
- Australia (x2)
- Japan
- Singapore

Threat Inteligence

The Foundation: Superior Threat Intelligence from Cisco Talos

Visibility across all vectors from a best in class portfolio



The Foundation: Cisco Talos Continued

1.5M

New daily malware samples

600B

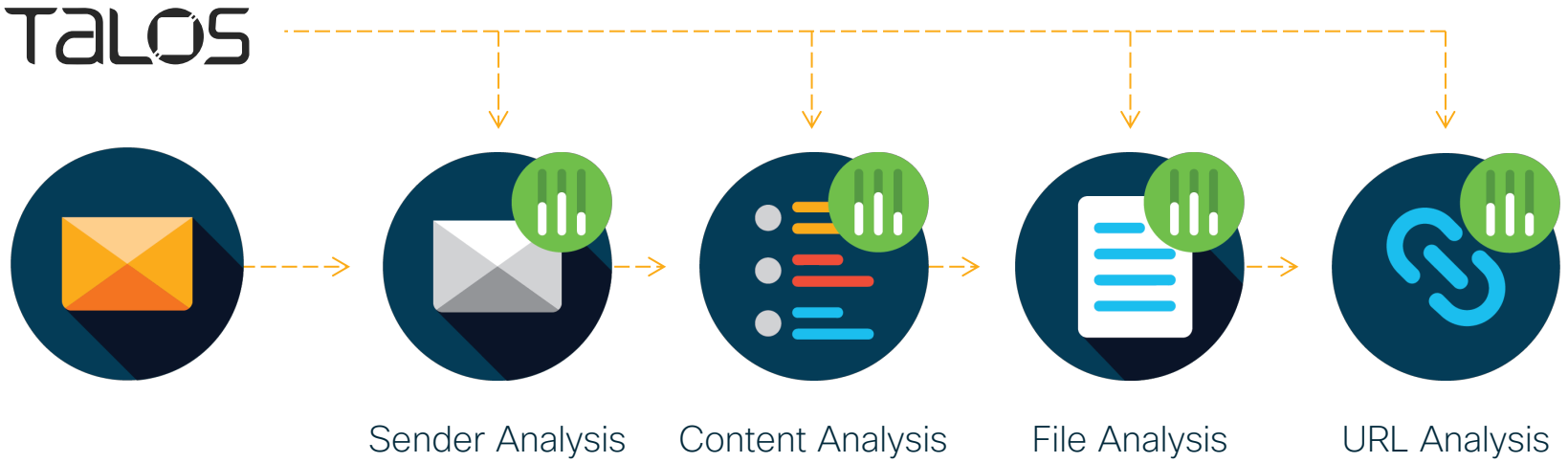
Daily email messages

16B

Daily web requests

Talos on Cisco Email Security

Monitors 600 billion emails per day to provide more broad visibility



Licensing

Product Offering: Licensing

- 1. Choose deployment

  ESA, vESA, CES

- 2. Choose Bundle

  Inbound: Anti-spam + Virus + Outbreak filters

  Outbound: Data Loss Prevention + Encryption

  Premium: Inbound + Outbound

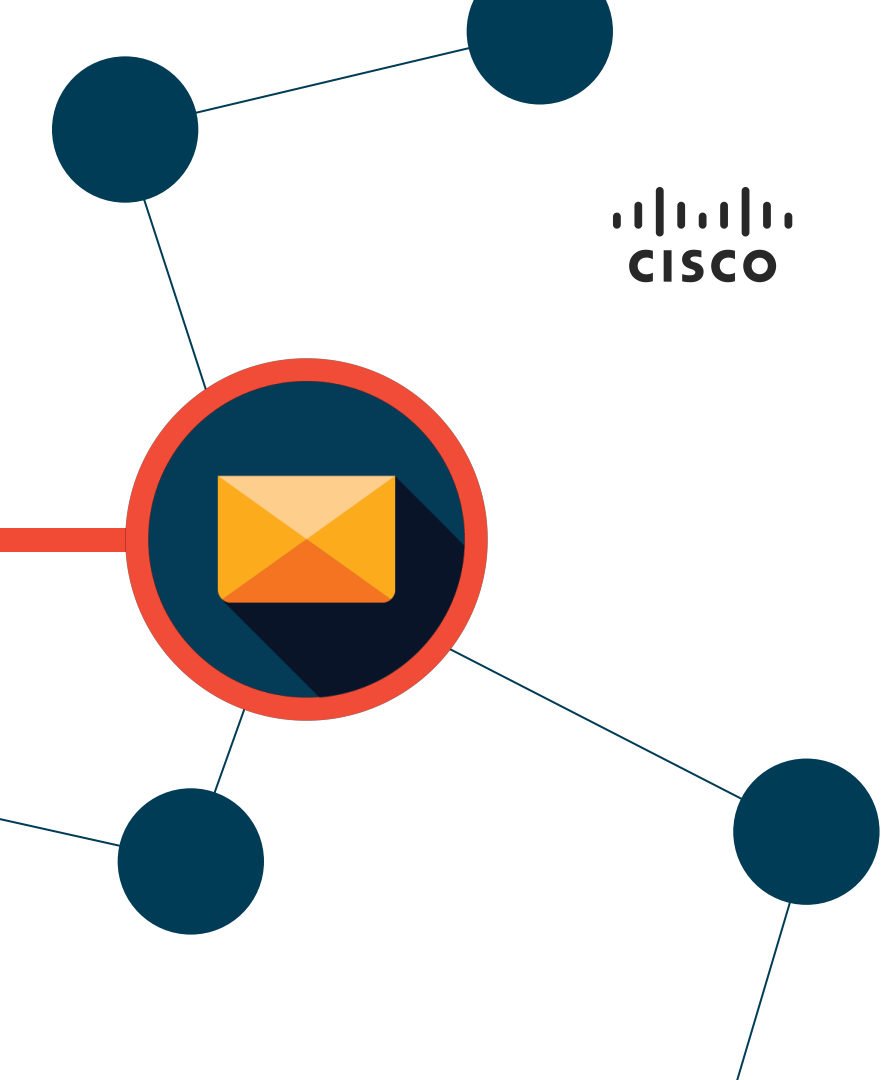
- 3. Choose add-on

  AMP – Advanced Malware Protection

  GSU – Graymail Safe-Unsubscribe

  DP – Domain Protection

  APP – Advanced Phishing protection



Proof of Value:

1. Cloud Email Security
2. On-premise Email Security
3. Advance Phishing Protection
4. Cisco Threat Analyzer o365

Cisco Email Security – Zaštitite svoj najosjetljiviji dio sustava od napada

CISCO