Secure solutions for advanced email threats

Threat-centric email security

Alberto Torralba
CSE
October 2016

Email is still the #1 threat vector

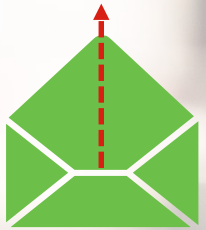
Phishing leaves businesses on the line

Phishing

Spoofing

Ransomware

94%
of phish mail has malicious attachments[1]



30%
of phishing messages are opened[1]

$500M

Loss incurred due to phishing attacks in a year by US companies[2]

[1]2016 Cisco Annual Security Report
[2]2016 Verizon Data Breach Report, Kerbs on Security

Messages contain attachments and URL's

Socially engendered messages are well crafted and specific

Credential "hooks" give criminals access to your systems

Spoofing rates are on the rise

Phishing

Spoofing

Ransomware

$2.3B

In losses from spoofing 2013 - 2015[1]

[1]FBI Warns of Dramatic Increase in Business email scams, 2016

Forged addresses fool recipients

Threat actors extensively research targets

Money and sensitive information are targeted

Ransomware attacks are holding companies hostage

Phishing

Spoofing

Ransomware

Ransomware represents the biggest jump in occurrences of crimeware[1]

9,515
users are paying ransoms per month[2]

$60M

Cost to consumers and companies of a single campaign[2]

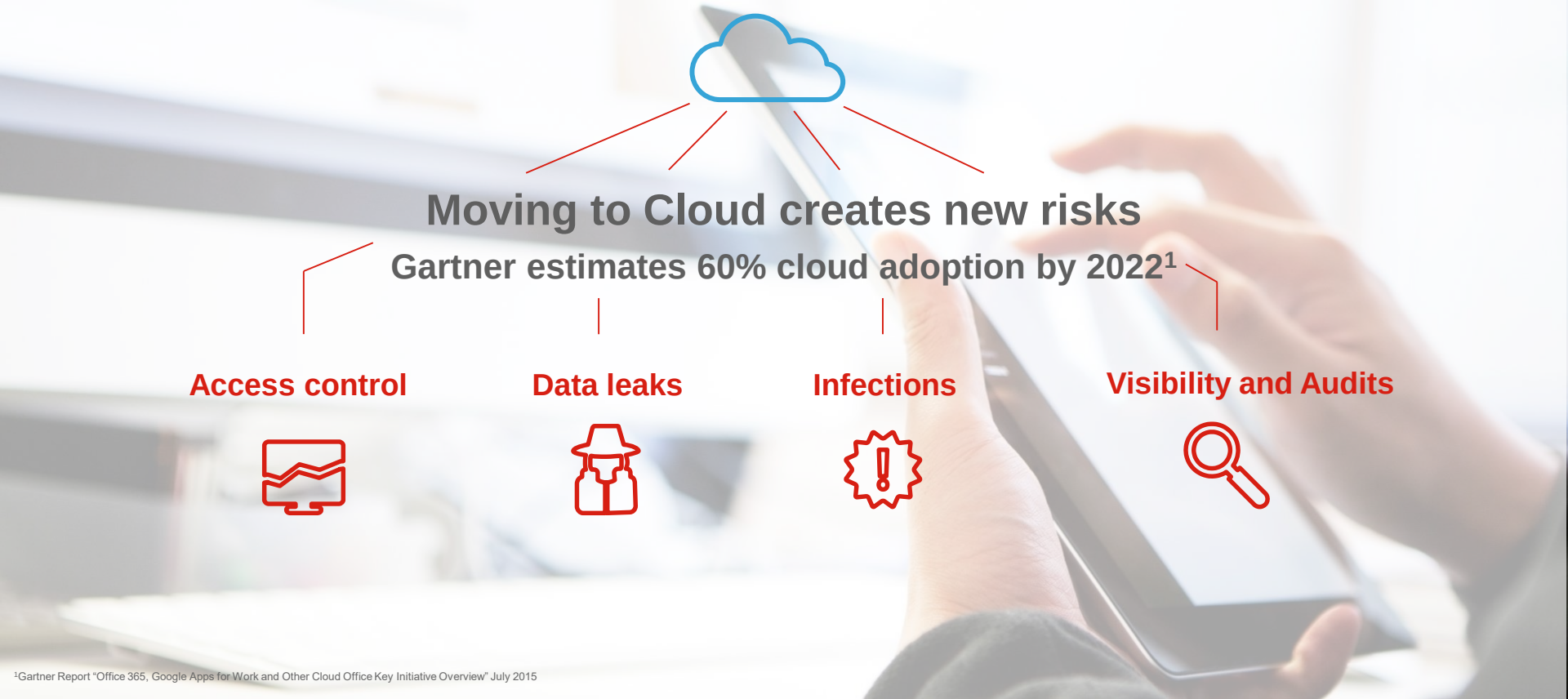
[1]2016 Verizon Data Breach Report, Kerbs on Security
[2]2016 Cisco Annual Security Report

Malware encrypts critical files

Locking you out of your own system

Extortion demands are being paid

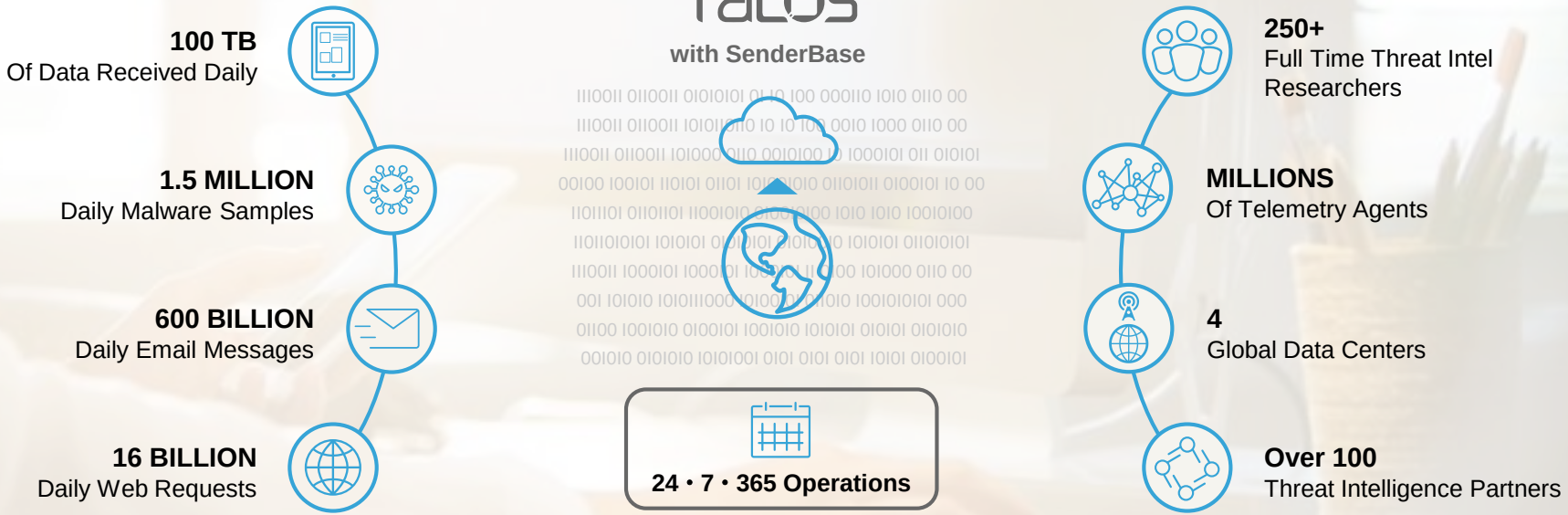
And security is more complex with email moving to the cloud



[1]Gartner Report "Office 365, Google Apps for Work and Other Cloud Office Key Initiative Overview" July 2015

Reduce threats

Cisco Email Security is backed by unrivaled global threat intelligence



Deploy the world's largest email traffic monitoring network

Leverage industry-leading threat analytics

Which is the only threat intelligence that caught a $30M phishing scam

90,000
Targeted victims per day

62%
Of Angler infections delivered ransomware

$19,419
Total ransom collected per server per day

9,000
Unique IP addressed were served exploits in a single day

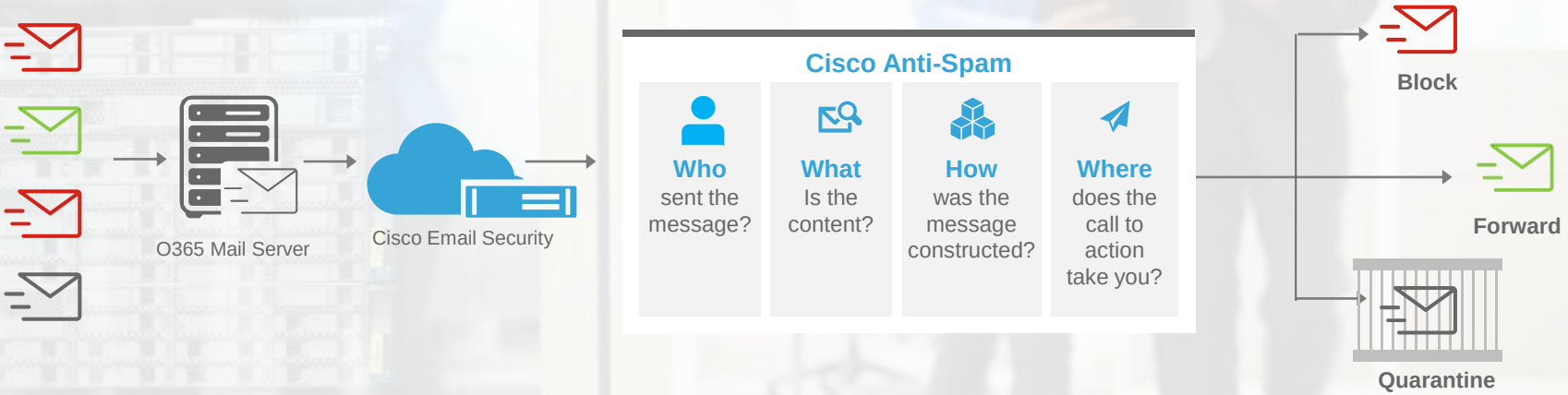
40%
Of users being served exploits were compromised

Talos response:

- **Traced the primary locations for the proxy servers to Dallas and Bavaria**
- **Quarantined the breach at Limestone Networks in Dallas, reducing propagation by 30%**
- **Blacklisted all additional servers and domains associated with Angler**
- **Published community rules for front-end and back-end communication to protect further attacks**

It’s built with industry-leading spam protection

Anti-spam processing / Context Adaptive Scanning Engine (CASE)



Review sender reputation, URL reputation, and message content

Block spam with 99% accuracy with fewer than 1:1M false positives

Quarantine suspicious messages for additional review

And reduces your exposure to the three main components of an email attack

Attachments

URLs

Email content

Attachments

Protect against

Ransomware

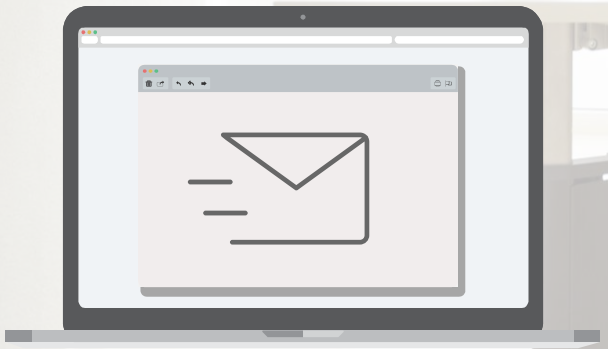
Phishing

Stop the damage from malicious attachments that seem legitimate

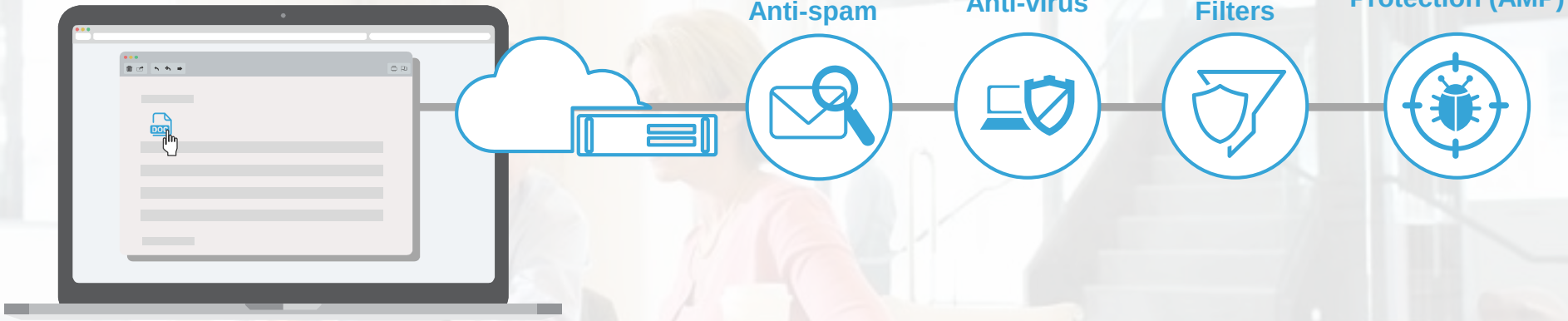
Dave from HR receives an email with a resume attached

Everything looks normal so Dave opens the attachment

An executable file downloads malware without his knowledge

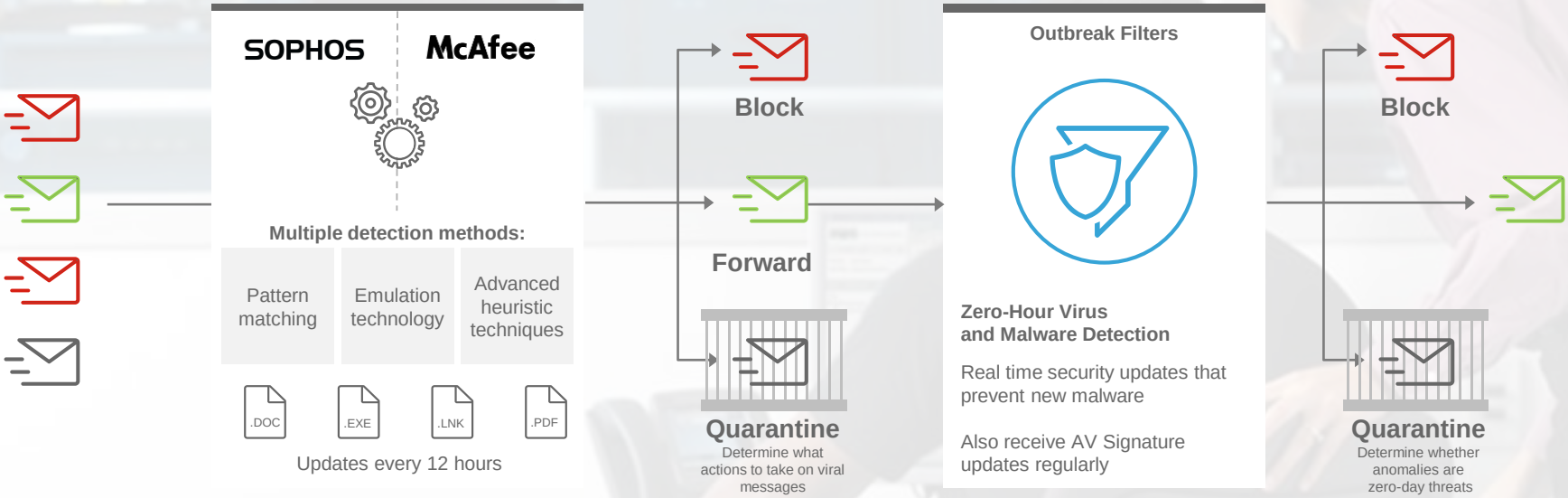


Cisco protects against threats hidden within attachments



Block known and zero-day viruses

Anti-virus processing



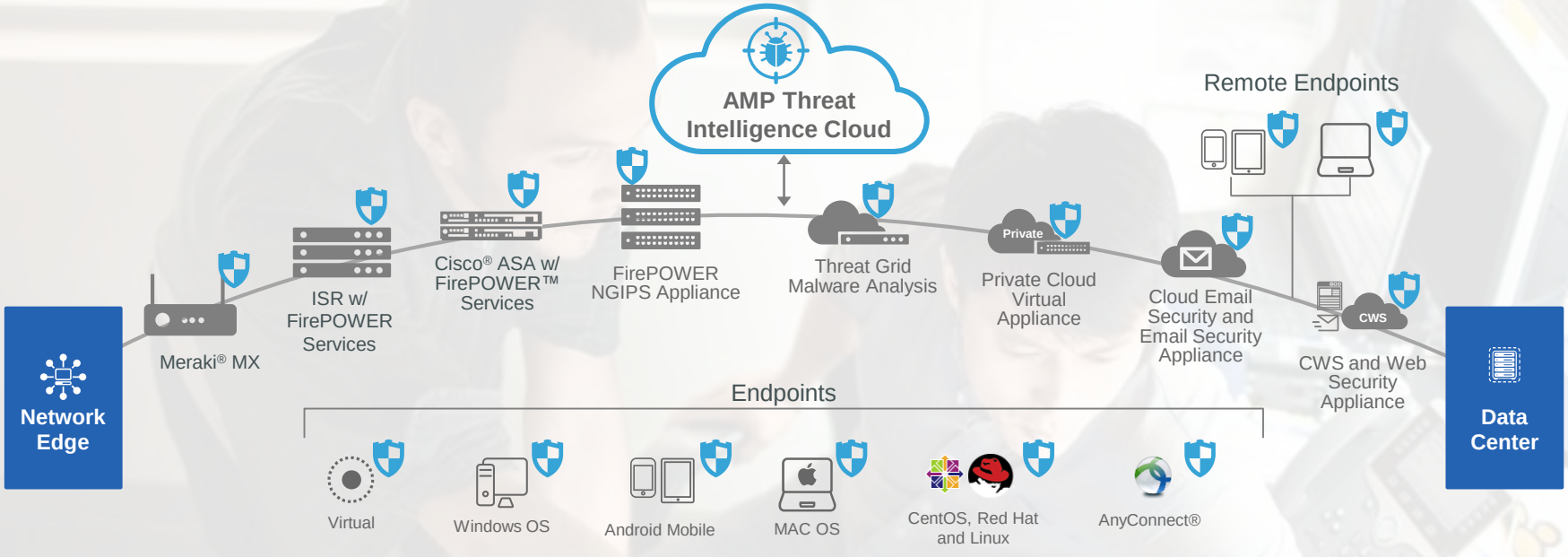
Scan attachments for known viruses

Forward clean emails to additional security checks

Defend against zero-day malware

Detect and contain advanced threats quickly

Advanced Malware Protection (AMP) architecture



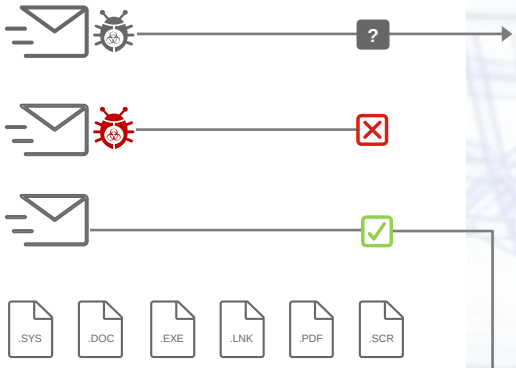
Leverage threat intelligence and dynamic malware analysis

Deploy easily with multiple platform options

Keep tabs on all emails admitted into the environment after analysis

Advanced Malware Protection (AMP)

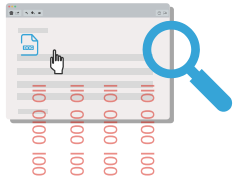
File Reputation



Known Signatures | Fuzzy Fingerprinting | Indications of compromise

File Sandboxing

- Advanced Analytics
- Dynamic analysis
- 560+ indicators



Unknown | Clean | Malicious

File Retrospection

Block known malware

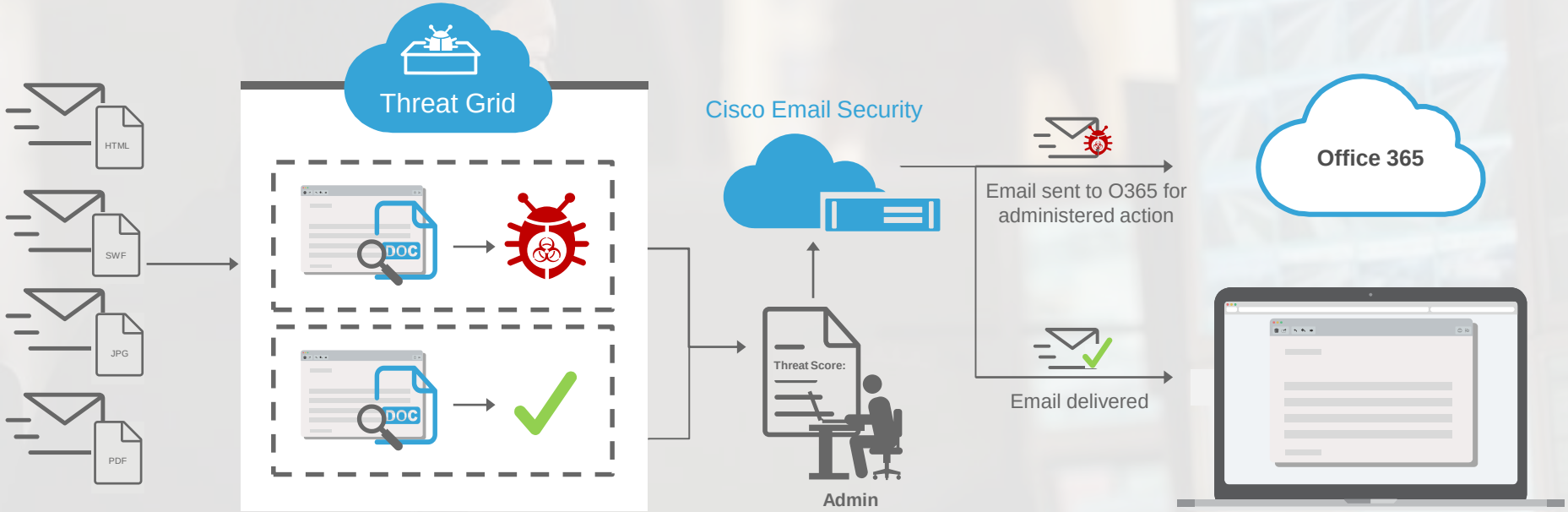
Investigate files safely

Auto-remediate threats in O365

Gain visibility into messages trying to enter the network

Investigate unrecognized attachments safely

AMP Threat Grid for Sandboxing



Upload unknown files to Threat Grid

Examine files with context-driven analysis

Receive threat report and score to guide decision making

Automatically remediate malware for O365 users

Email Content

Protect against

Spoofing

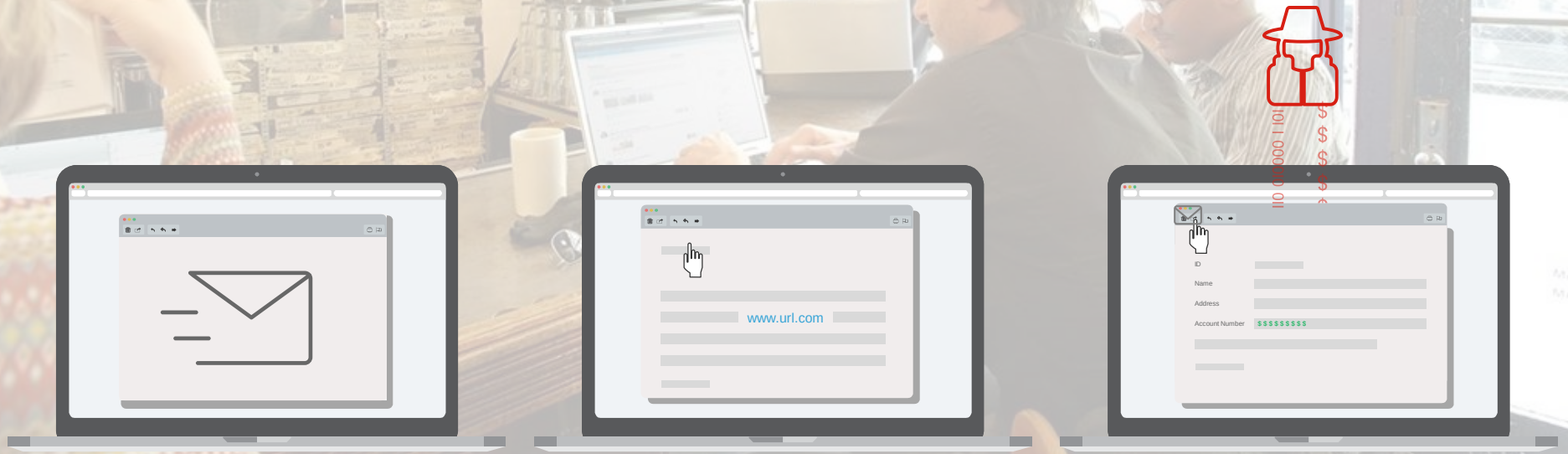
Phishing

Protect your users against Business Email Compromise scams

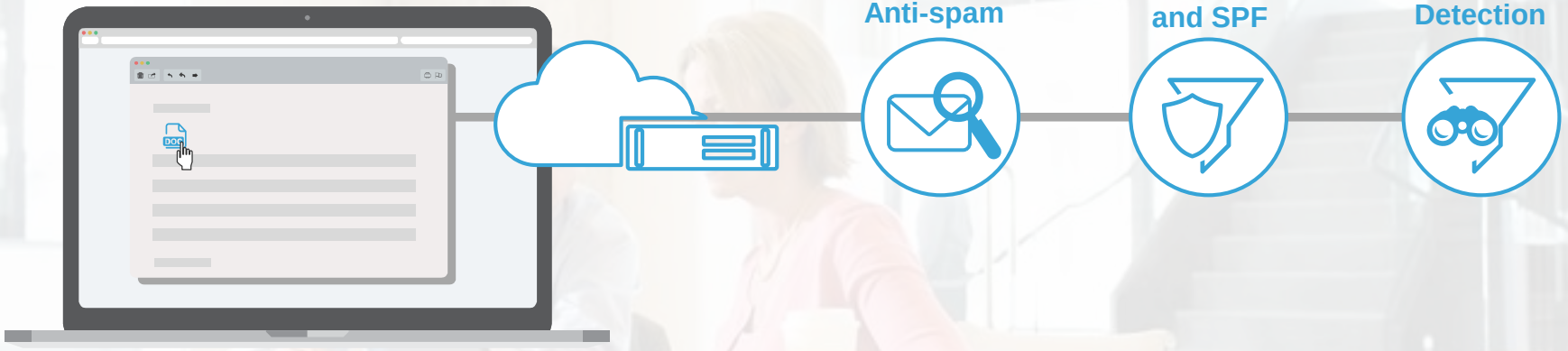
Kevin receives an urgent email from his boss asking to transfer funds

To avoid delays, Kevin sends the payment right away

Kevin unknowingly sent the payment to a fraudster

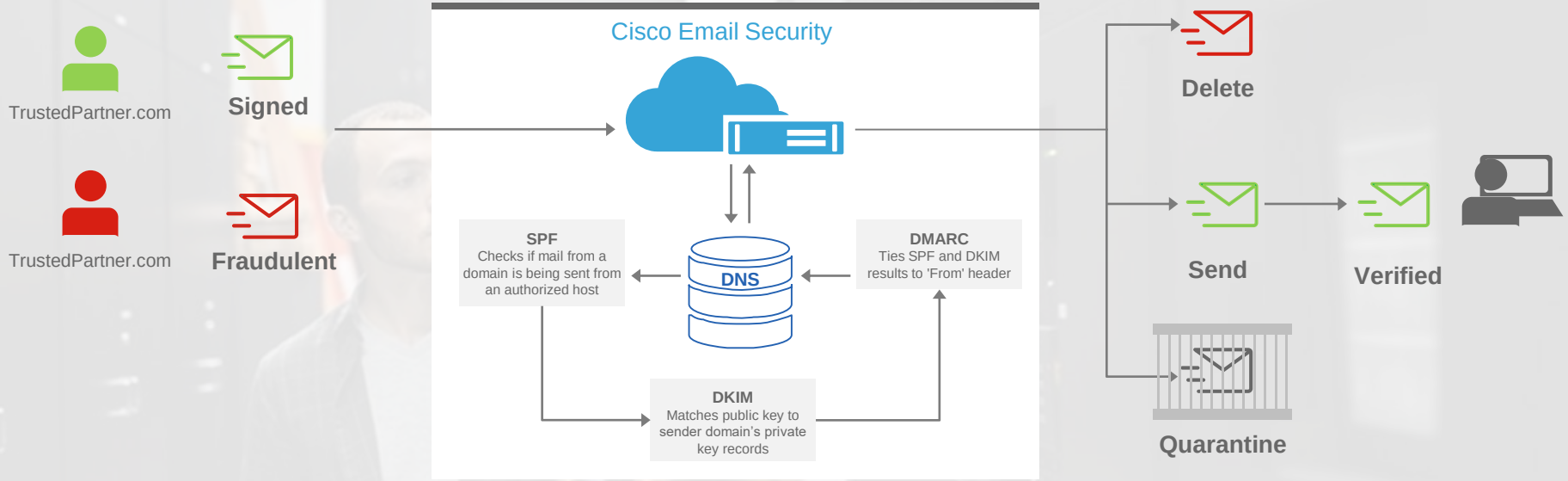


Cisco defends against human error



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

Protect against spoofing attacks

Forged Email Detection

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

RCPT TO:<alan@mail.com>

250 2.1.5 OK i11si22058766wmh.67 – gsmtp

Data

Recipient Domain

Sending Domain

Actual Sender

SMTP Envelope

Compare against Company directory

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

From: adam@outside.com

Subject: {Possibly Forged} [URGENT] Need help transferring funds

Post-processing

Inspect SMTP envelope for 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

Safeguard against sensitive information going to the wrong people

Tina receives an email from HR for a background check

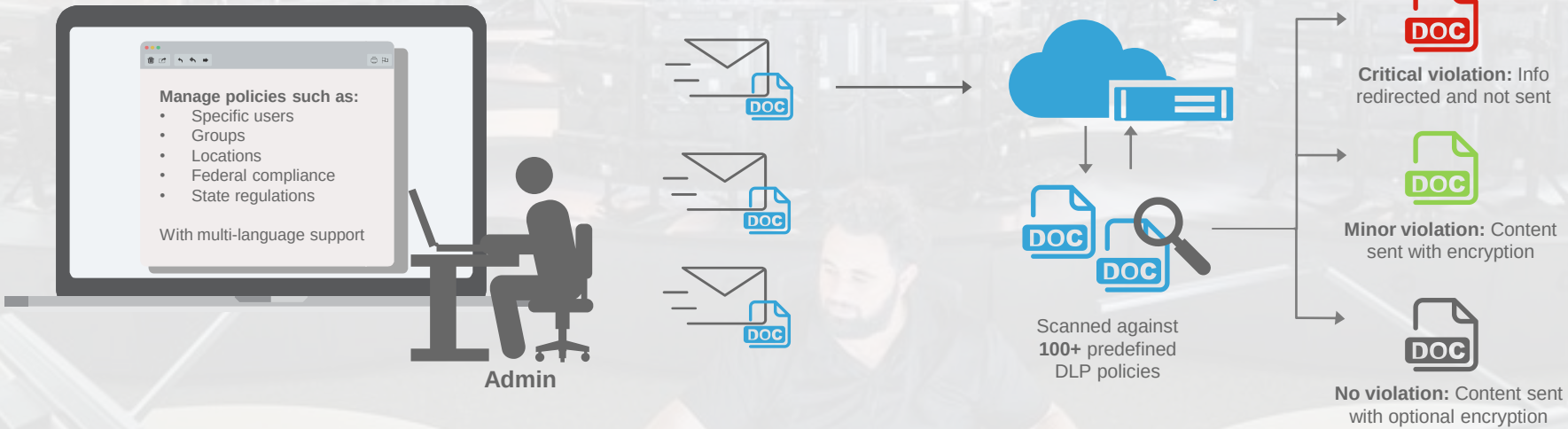
Everything looks legitimate so Tina replies with new hire information

Tina just sent the new hire's personal info into the wrong hands

Cisco catches critical data before it leaves the network

Protect personal information and IP

Data Loss Prevention (DLP)



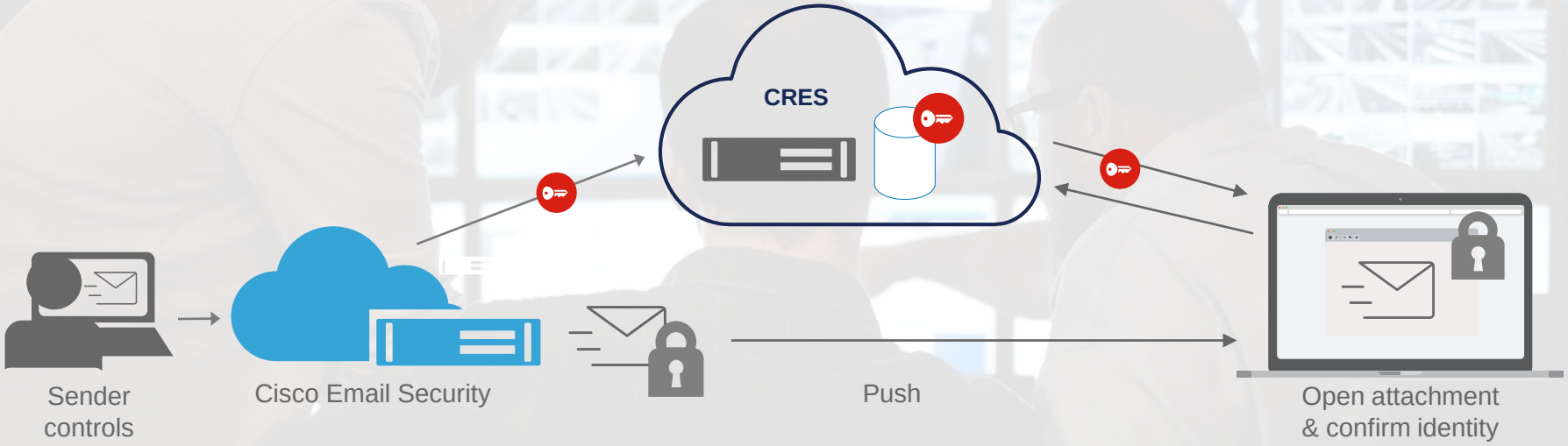
Control what leaves the network and customize policies

Scan email content for sensitive information

Prevent data exfiltration automatically

Extend security to external communications

Cisco Registered Envelope Service (CRES)



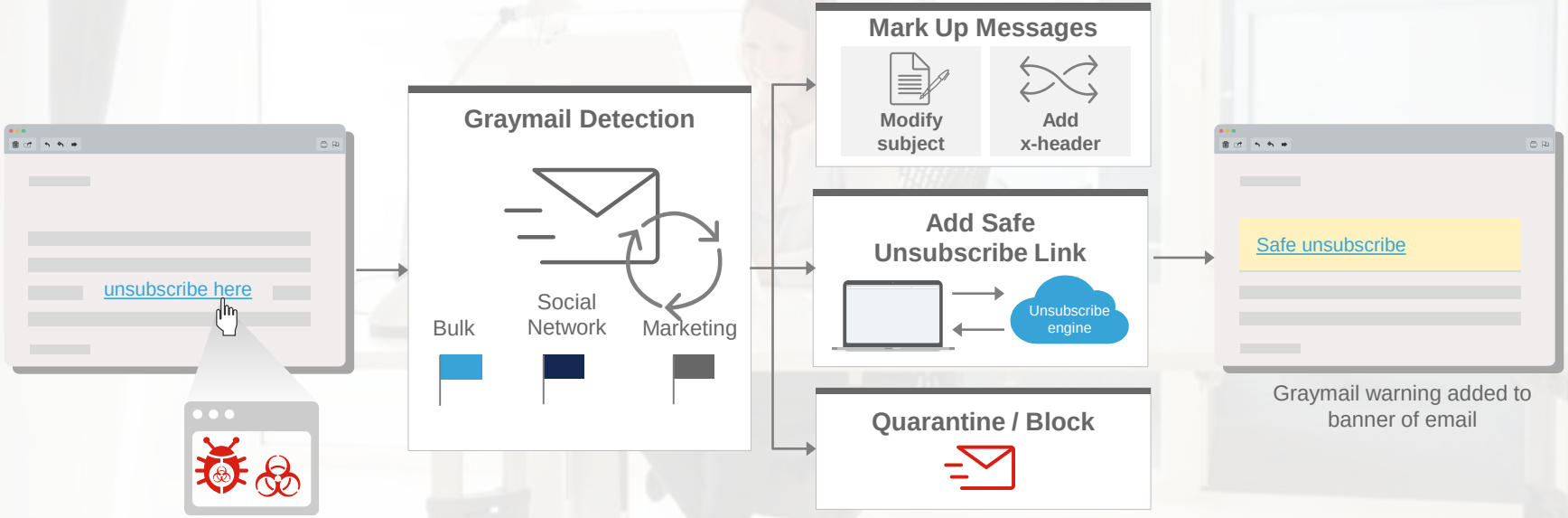
Scan messages for keywords, policies, and sender

Apply authentication mechanisms to access encryption keys

Maintain control over your sent messages

Separate what matters from what doesn’t

Graymail detection and safe unsubscribe



Identify messages that aren’t spam

Categorize incoming bulk, marketing, and social networking emails

Provide users a method to safely unsubscribe

URLs

Protect against

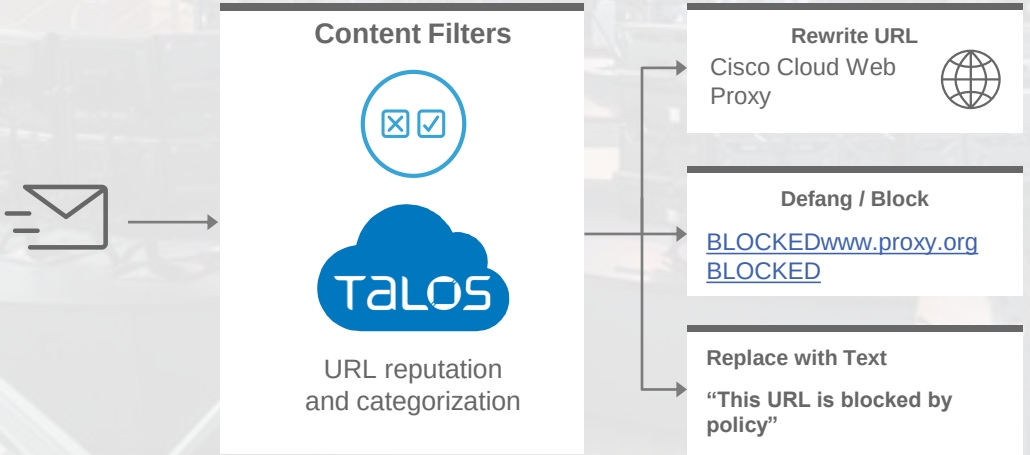
Ransomware

Phishing

Spoofing

Control which emails cross the network

Content Filters

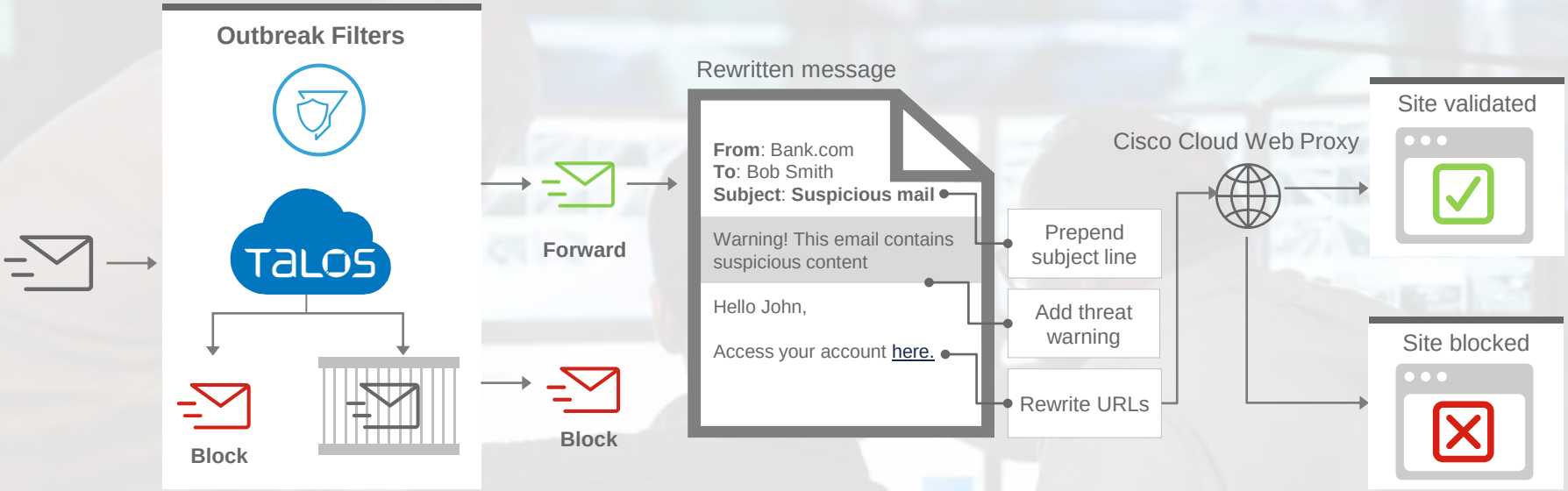


Customize filters in three different ways for additional security

Easily enforce business and compliance policies

Detect targeted or blended attacks automatically

Outbreak Filters



Block all known threats with Talos

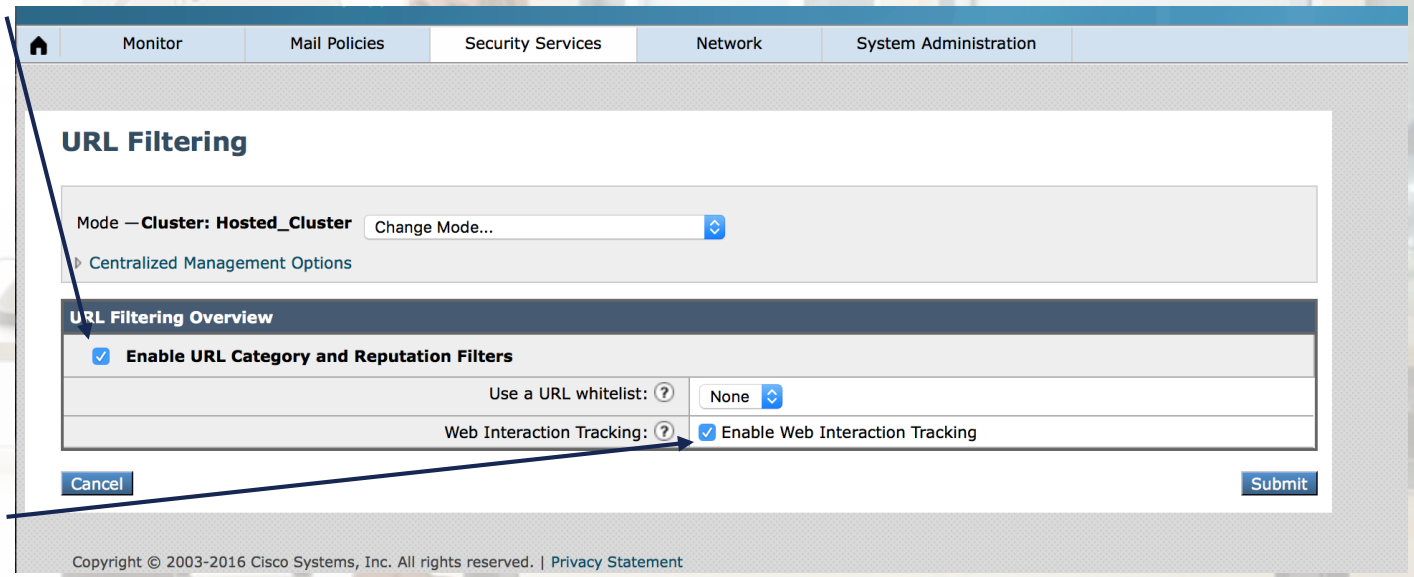
Quarantine emails with suspicious URLs

Modify emails to protect end-user

Redirect traffic to protect from malicious links

How to: Step 1

Enable the service



Web Interaction Tracking: Track the clicks on the links.

How to: Step 2

Using CLI execute two commands.

1.- websecurityadvanceconfig

2.- outbreakconfig
Logging of URLs is currently enabled.

Do you wish to disable logging of URL's? [N]>

```
c100v.secpod.local> websec
websecuritydiagnostics, websecurityadvancedconfig, websecurityconfig
c100v.secpod.local> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[20]>

Enter the URL cache size (no. of URLs):
[810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that should be scanned:
[100]>

Enter the Web security service hostname:
[v2.sds.cisco.com]>

Enter the threshold value for outstanding requests:
[5]>

Do you want to verify server certificate? [Y]>

Enter the default time-to-live value (seconds):
[30]>

Do you want to rewrite all URLs with secure proxy URLs? [N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server:
[Info]>

Enter the default debug log level for URL cache:
[Info]>

Enter the default debug log level for HTTP client:
[Info]>
```

How to: Step 2

websecurityadvanceconfig

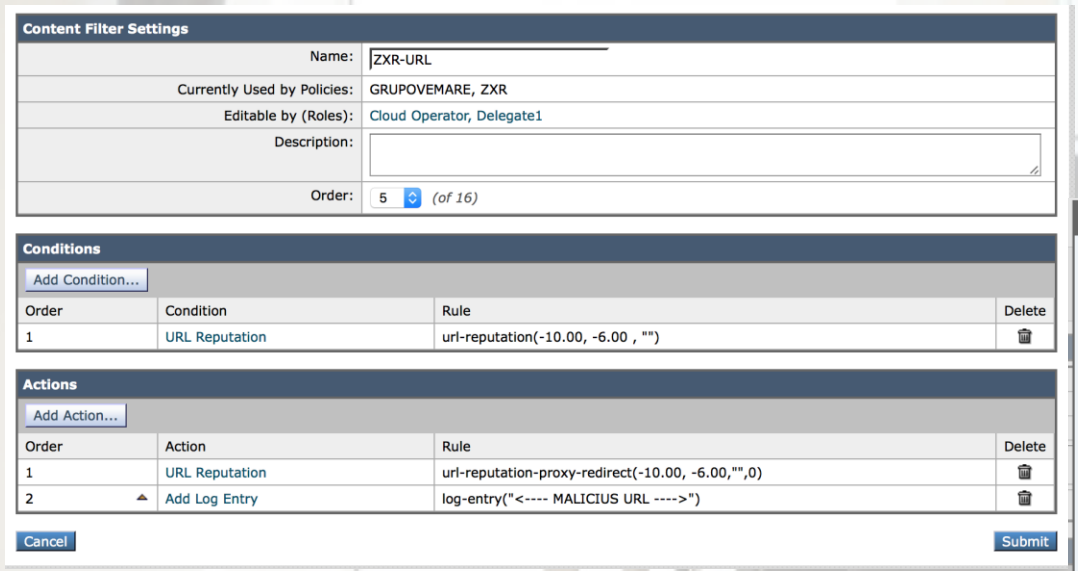
Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[5]> 20

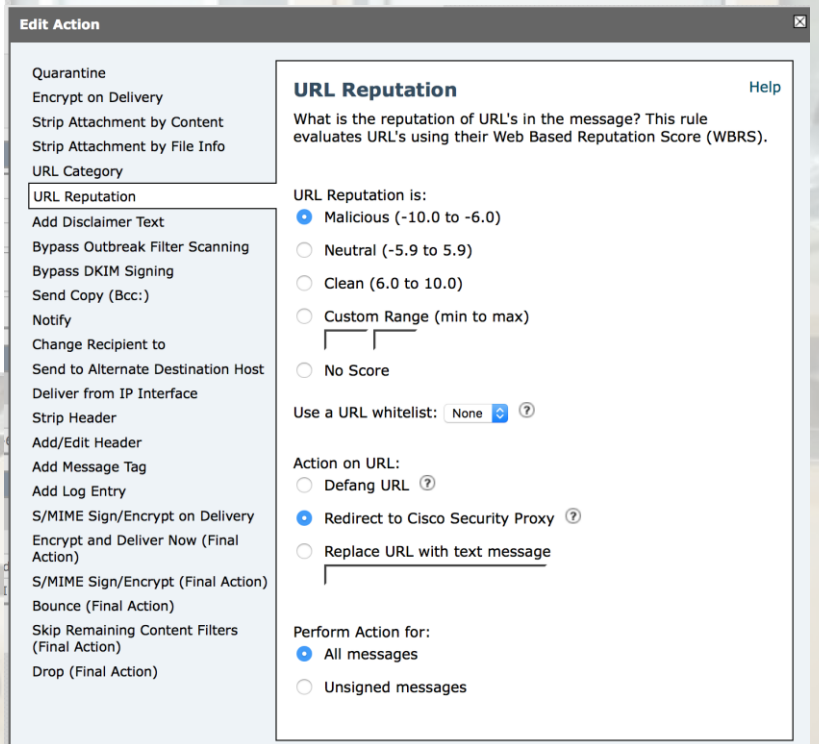
Enter the threshold value for outstanding requests:
[50]>5

Do you want to rewrite all URLs with secure proxy URLs? [Y]>N

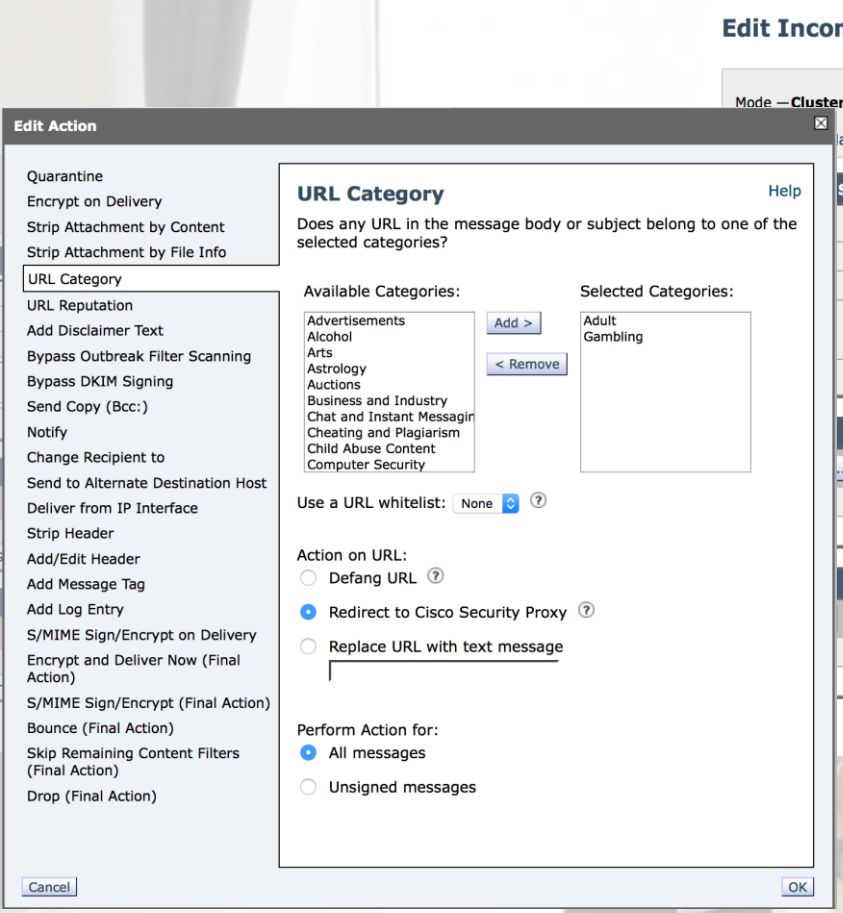
```
c100v.secpod.local> websec
websecuritydiagnostics, websecurityadvancedconfig, websecurityconfig
c100v.secpod.local> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[20]>

Enter the URL cache size (no. of URLs):
[810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that should be scanned:
[100]>

Enter the Web security service hostname:
[v2.sds.cisco.com]>

Enter the threshold value for outstanding requests:
[5]>

Do you want to verify server certificate? [Y]>

Enter the default time-to-live value (seconds):
[30]>

Do you want to rewrite all URLs with secure proxy URLs? [N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server:
[Info]>

Enter the default debug log level for URL cache:
[Info]>

Enter the default debug log level for HTTP client:
[Info]>
```

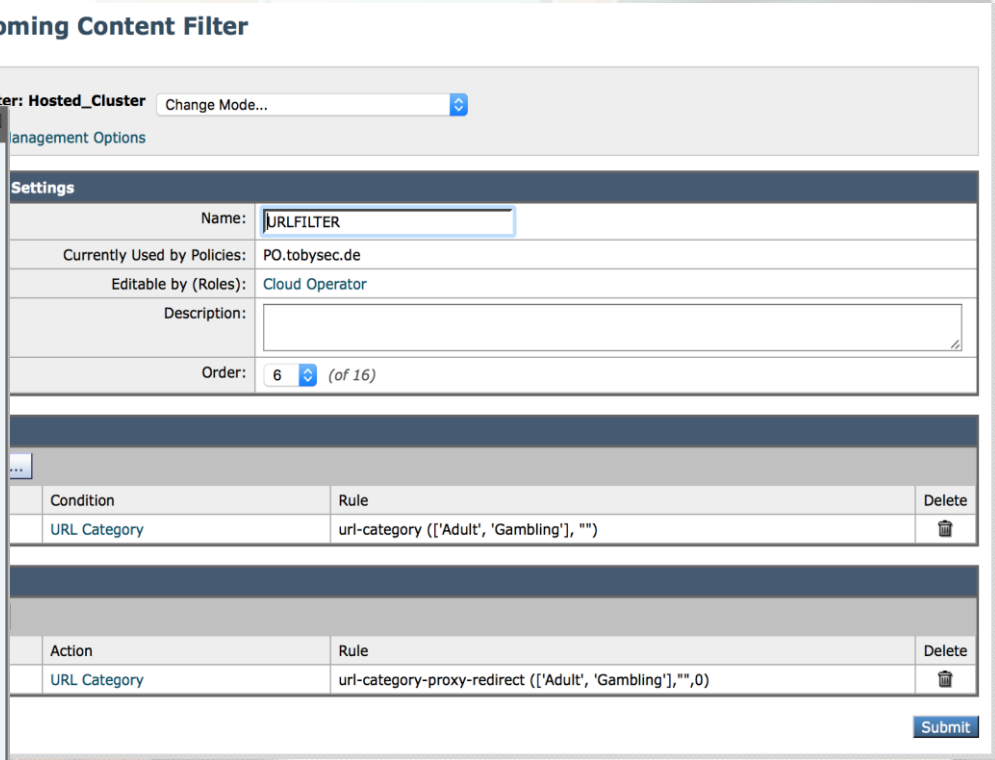
Url Filtering on Email: Web Reputation





Url Filtering on Email: Web Categories

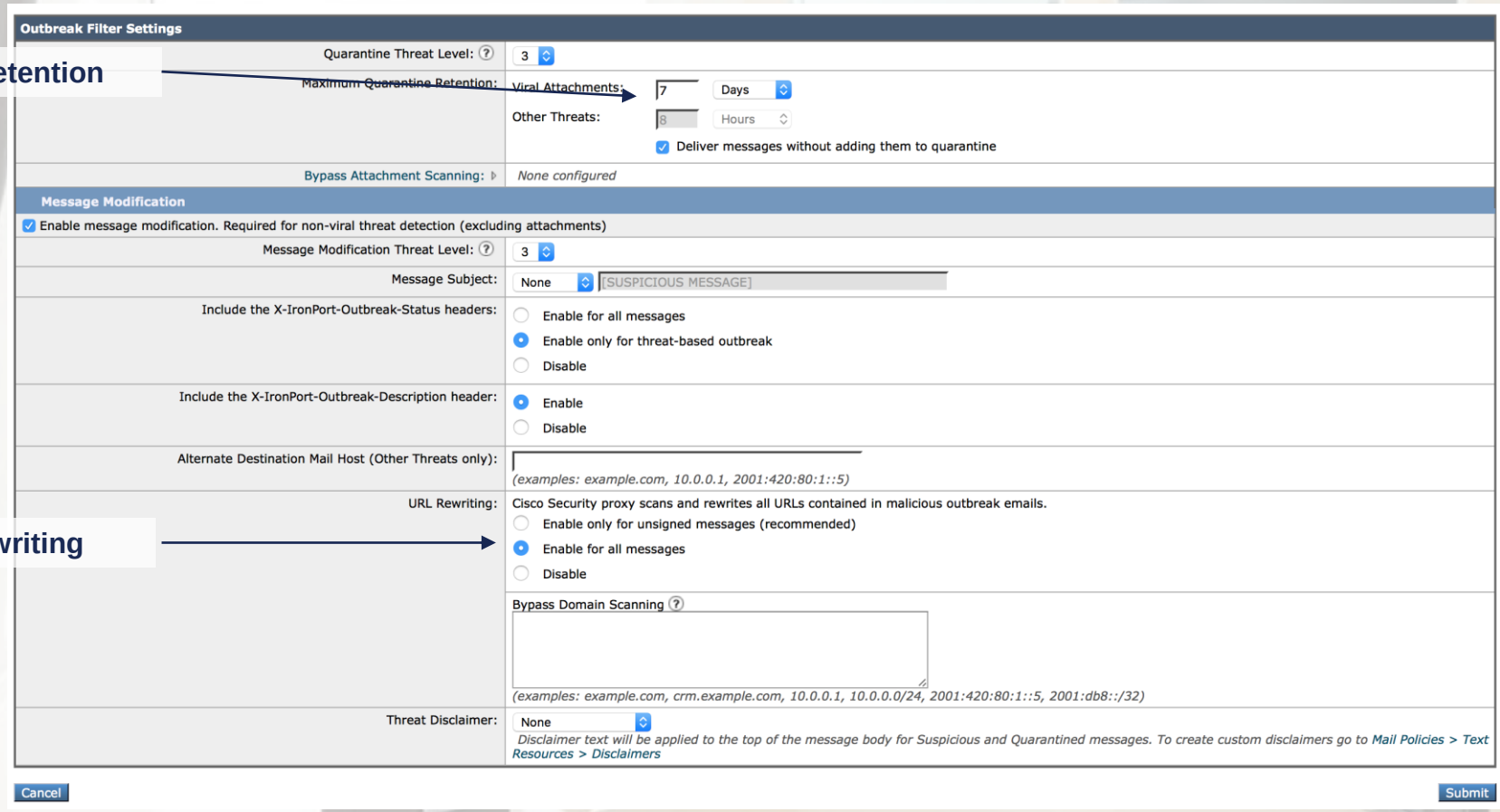




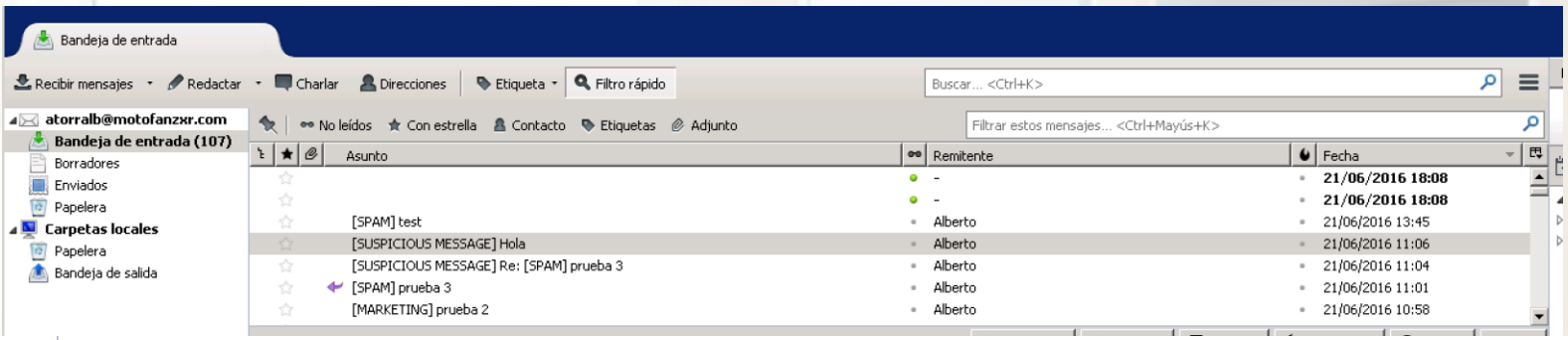
Outbreak Filter & URL

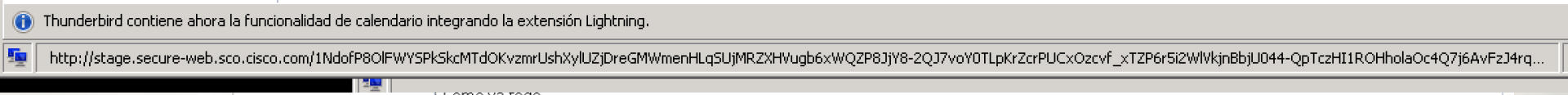
Time retention

Url rewriting



End-User experience





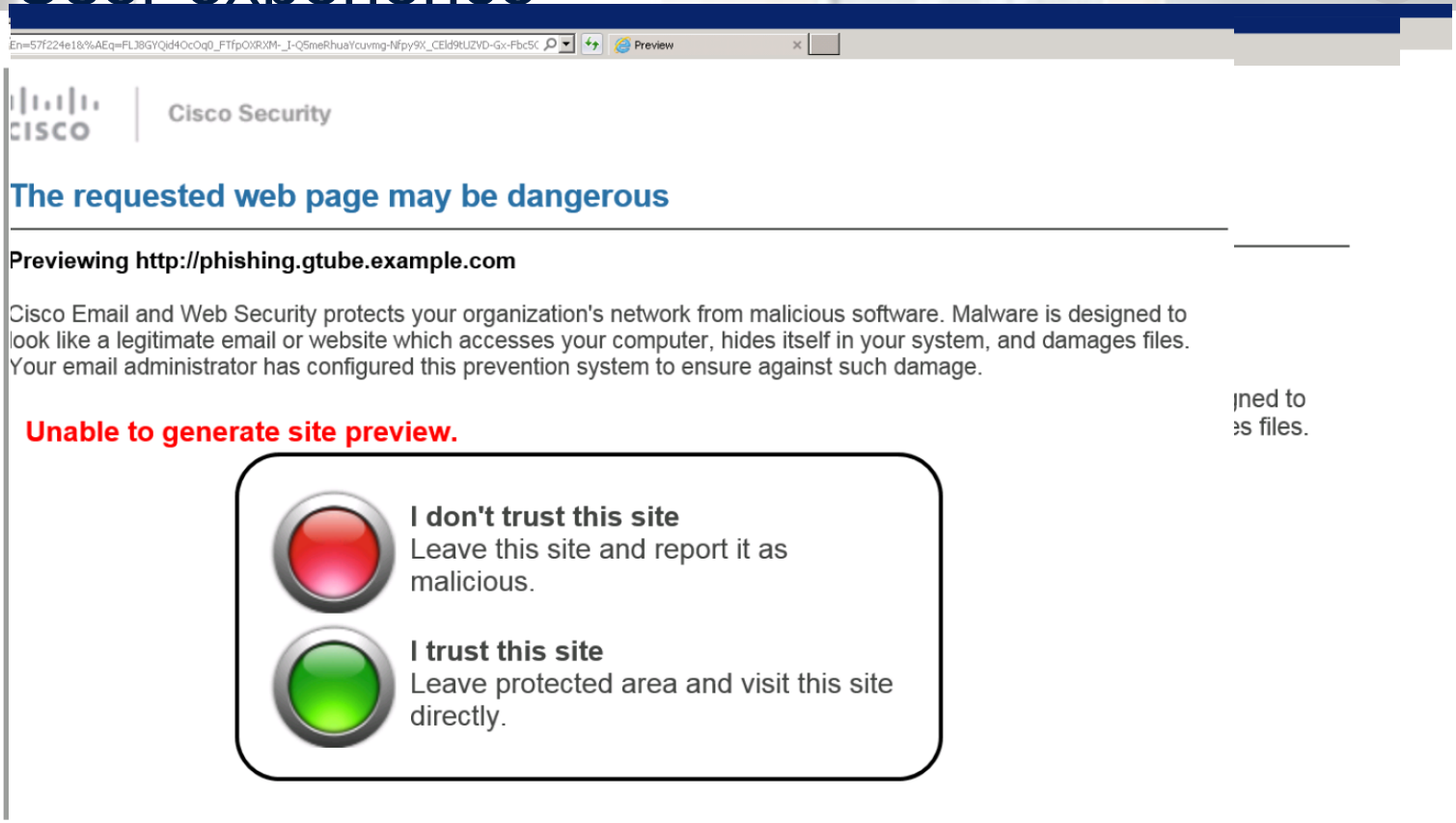
Como va todo
te envío un enlace muy interesante.

http://ihaveabadreputation.com

Alberto

http://stage.secure-web.sco.cisco.com/1NdofP8OlFWYSPkSkcMTdOKvzmrUshXylUZjDreGMWmenHLqSUjMRZXHVugb6xWQZP8JjY8-2QJ7voY0TLpKrZcrPUCxOzcvf_xTZP6r5i2WlVkjnBbjU044-QpTczHI1ROHholaOc4Q7j6AvFzJ4rqtziHoDgWd5luhB-i297Fh8v64b736bIUcvIoQyKpOJkGilVj9BFwvsv4-aw3wW40QE3rqzWYThehYDaMXBsmAsBbv0g4hkDRdh8e7qjN8mwx2BvHWYMD34Q9CwTxgAEvEdiqoMWZGij8rZK-iCufGFKbTl0tMl6zbaCTnFiLCMxG2YsWS_CCq_ROkZt2VN_5X-QrYtfmxpipxXAREKegy-j6Bnt189kClF5Z2dOf35/http%3A%2F%2Fihaveabadreputation.com

End-User experience



End-User experience

Block Page Customization

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

▸ Centralized Management Options

Edit Block Page Customization

☑ **Enable Block Page customization**	
Logo URL:	*(example: http://www.example.com/image.gif)*
Company Name:	
Contact Information:	*(examples: Contact Name, 123-1234-123, user@example.com)*
Default Language: ?	✓ English/United States [en-us]

Italian [it]
Français/France [fr-fr]
日本語 [ja]
Español [es]
русский язык [ru]
漢語繁體 [zh-tw]
한국어 [ko]
汉语简体 [zh-cn]
Deutsch [de-de]
Português/Brasil [pt-br]

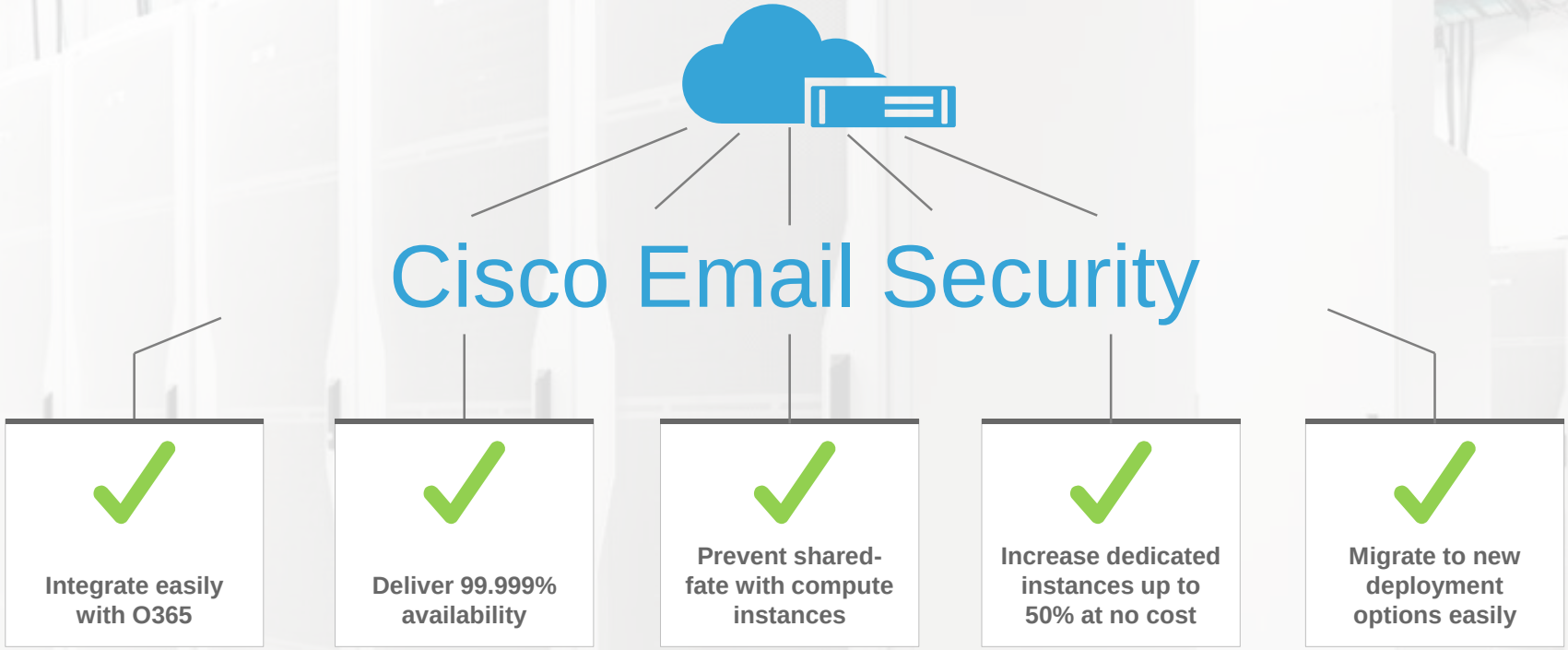
? Preview Block Page Customization

Cancel Submit

DEMO

Support growth

Transition to the cloud with confidence

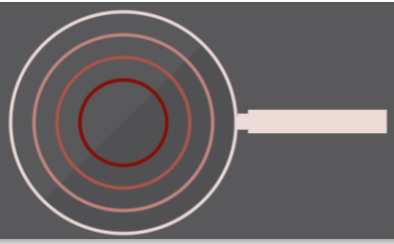


Deploy the configuration that works best for you

Cloud

Hybrid

On Premises



How to benefit from our Free Risk Assessment? Cisco Threat Scan Proof of Value Programme

- With this offer, you will:
  - Gain valuable information on your network including critical attacks
  - Reduce risk and make security a growth engine for your business

- This offer is valid through December 29th, 2016 in Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Luxemburg, Netherlands, Norway, Spain, Sweden, Switzerland and United Kingdom.

- For more information and to request a Threat Scan POV, go to www.cisco.com/go/threatscanpov


CISCO