

Email Security.cloud – Configuring DLP on to your email flow and applying security to your hosted email deployment

Phil Walters

Principal Learning Consultant, Technical Field Enablement

Session Agenda

1 Email Data Loss Prevention.cloud

2 Support for Hosted Email Platforms

3 Self-serve Domains

4 Support for Sender Policy Framework

5 Introduction to the Lab Exercises

Disclaimer

“Any information regarding pre-release Symantec offerings, future updates or other planned modifications is subject to ongoing evaluation by Symantec and therefore subject to change. This information is provided without warranty of any kind, express or implied. Customers who purchase Symantec offerings should make their purchase decision based upon features that are currently available.”

vision



Email Data Loss Prevention.cloud



*Dr. Larry Ponemon, Chairman
and Founder of the Ponemon
Institute*

“ Negligent insiders and malicious attacks are the main causes of data breach. Thirty nine percent of organizations say that negligence was the root cause of the data breaches. ”

Two Approaches to Data Loss Prevention

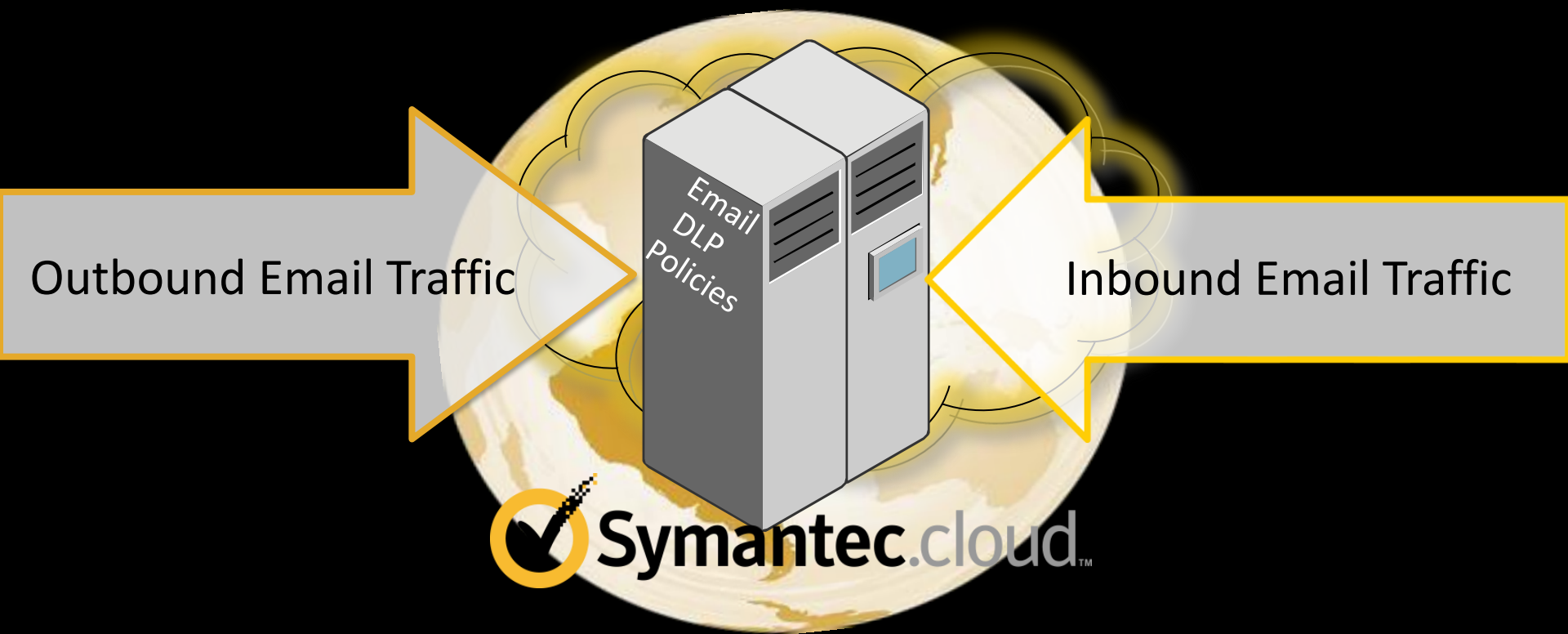
Enterprise DLP

- Single solution for the discovery, detection, enforcement, and remediation across all data channels.
- Includes data at-rest, data in-motion and end-point security.
- Complex to install and manage.

Channel DLP

- DLP over a single data channel e.g. email or web.
- Simple policies.
- Simple deployment.
- Ideally suited for a cloud-based solution.

Email Data Loss Prevention – A Cloud Based Solution



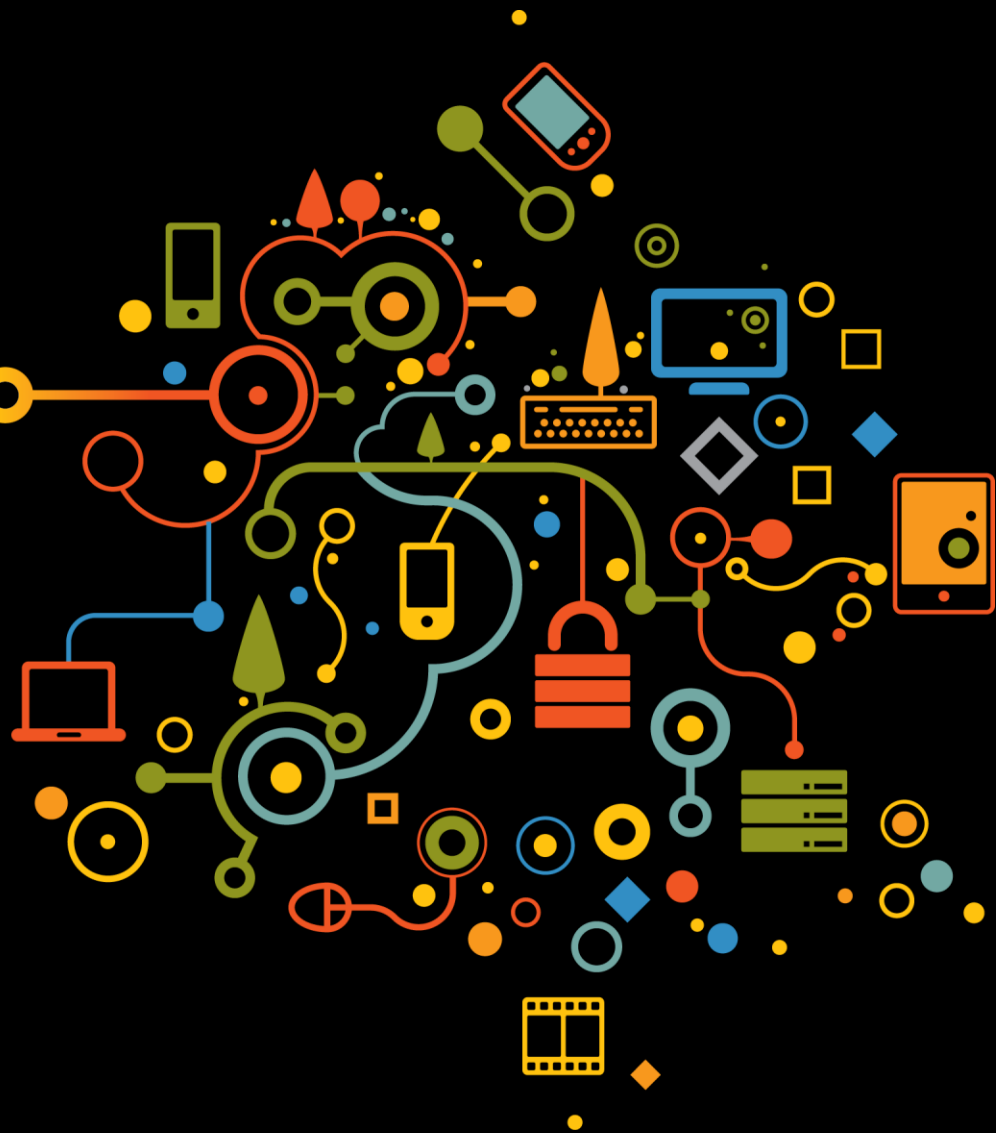
Introducing Email Data Loss Prevention.cloud

- Built upon the Email Security.cloud service with 100% SLA for availability.
- Easy policy builder in the cloud-based management portal.
- Pre-built policy templates for quick policy deployment.
- Pre-built regular expressions for common data types e.g. credit card numbers, social security numbers etc.
- Ability to create regular expressions to match content.
- Detailed reports to view rules matched and matched text.

Details of the New Service

- This service should go live this Summer.
- This is a replacement for the existing Content Control service.
- New customers will be provisioned onto Email Data Loss Prevention.cloud service.
- Existing customers will be migrated from the Content Control service to Email Data Loss Prevention.cloud service at no cost.
- All existing functionality in the Content Control service is mapped to the Email Data Loss Prevention.cloud service.
- Some new functionality is also available e.g. the ability to create regular expressions to pattern match content.

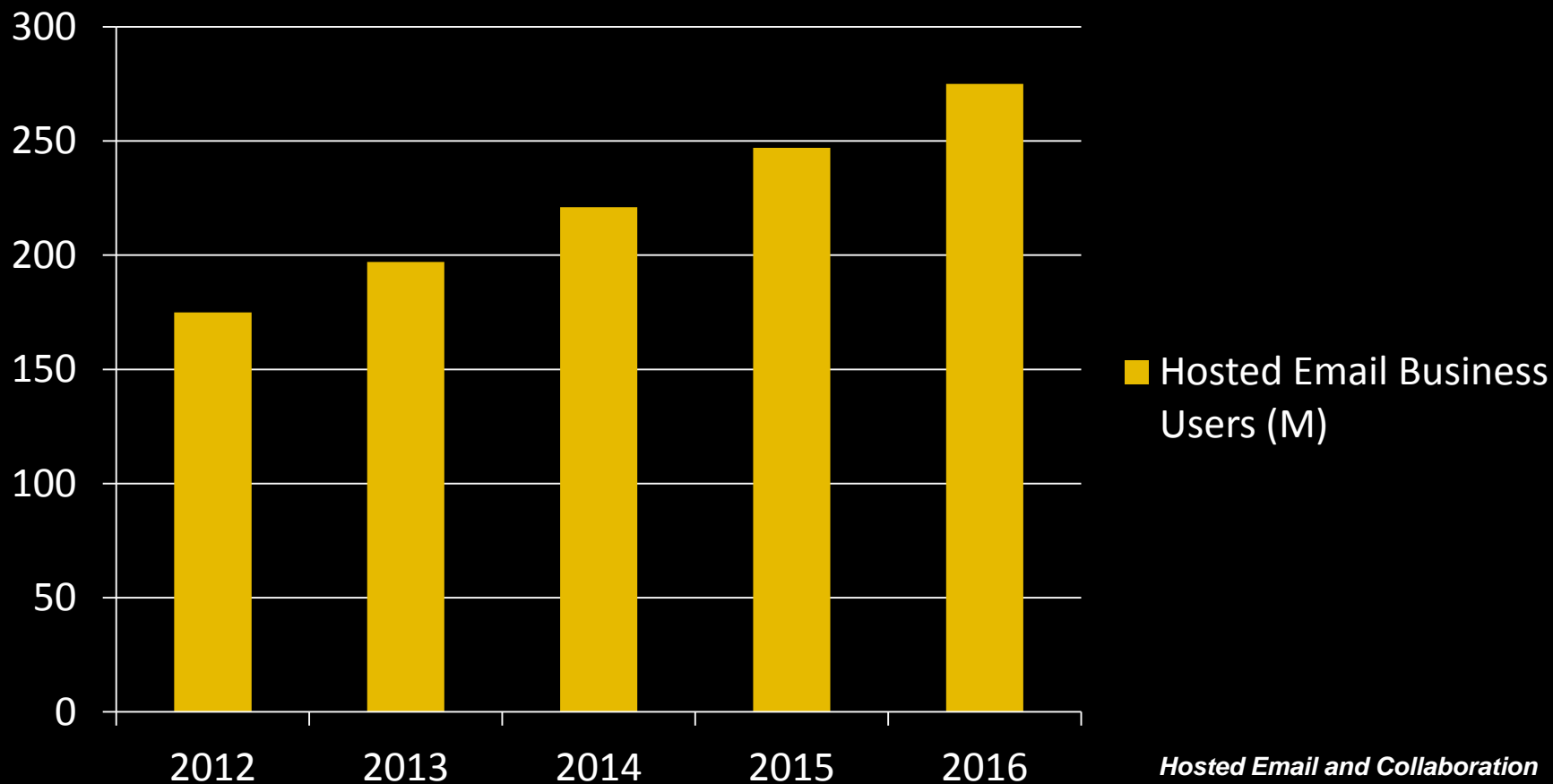
vision



Support for hosted email platforms

Growth of Hosted Email Providers

Hosted Email Business Users (M)



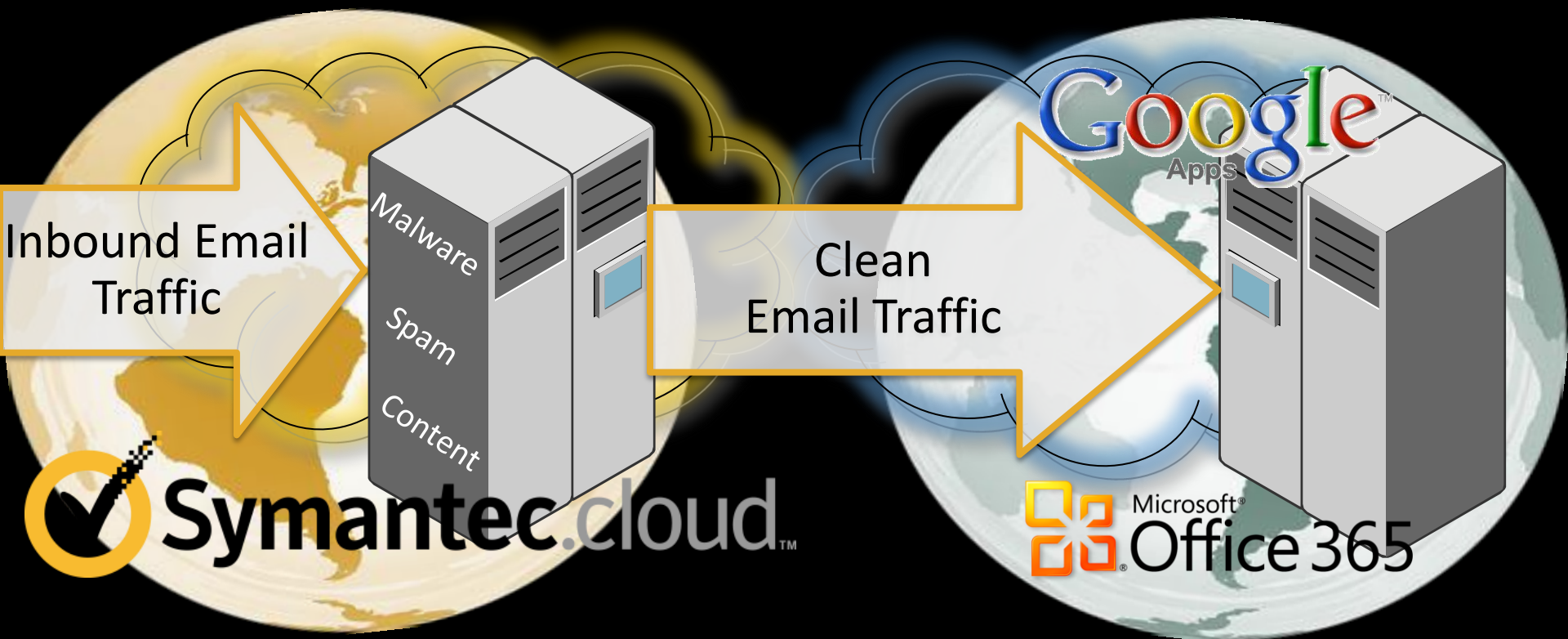
Hosted Email and Collaboration Market, 2012-2016 Radicati Group

The Gartner logo is displayed in white text on a blue rounded square background.

“ By the end of the decade we believe cloud email adoption will comprise about 65% of the enterprise email market.”

*Matthew W. Cain, Tom Austin
Gartner Group*

What have we been able to do in the past?

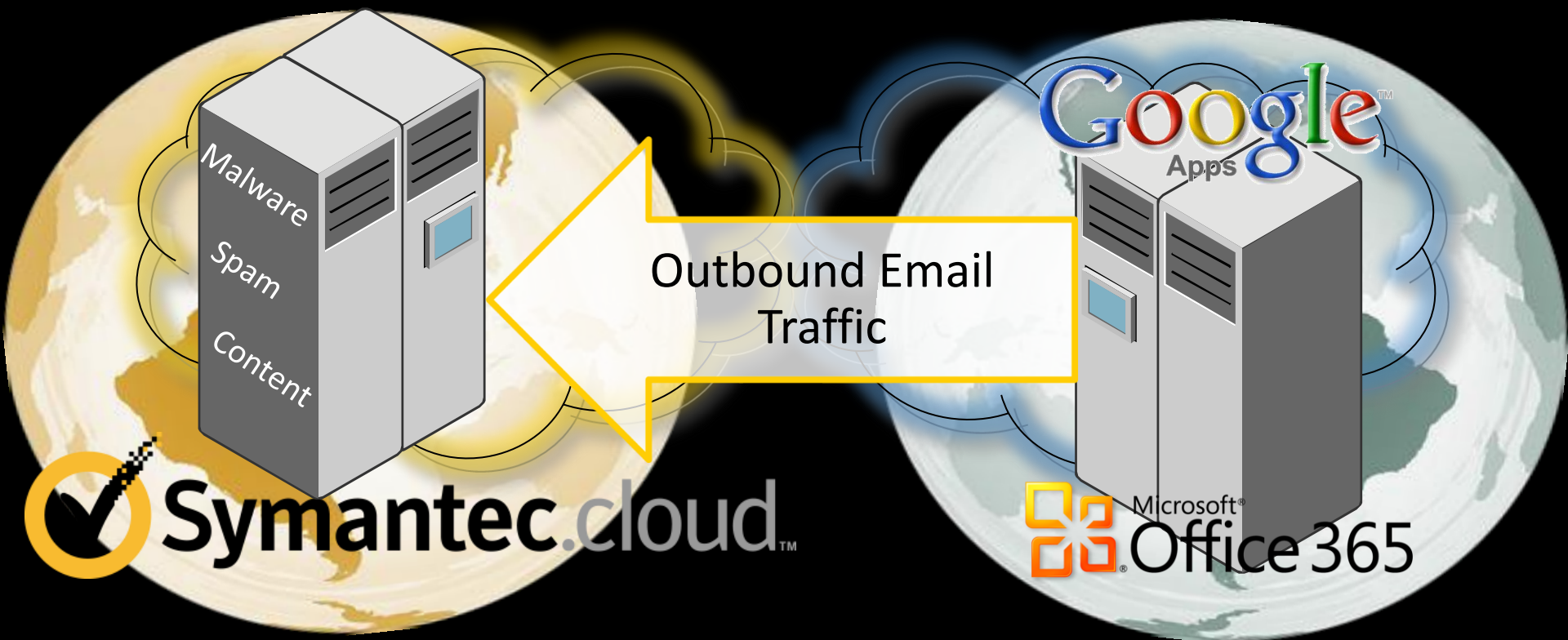


What was missing?

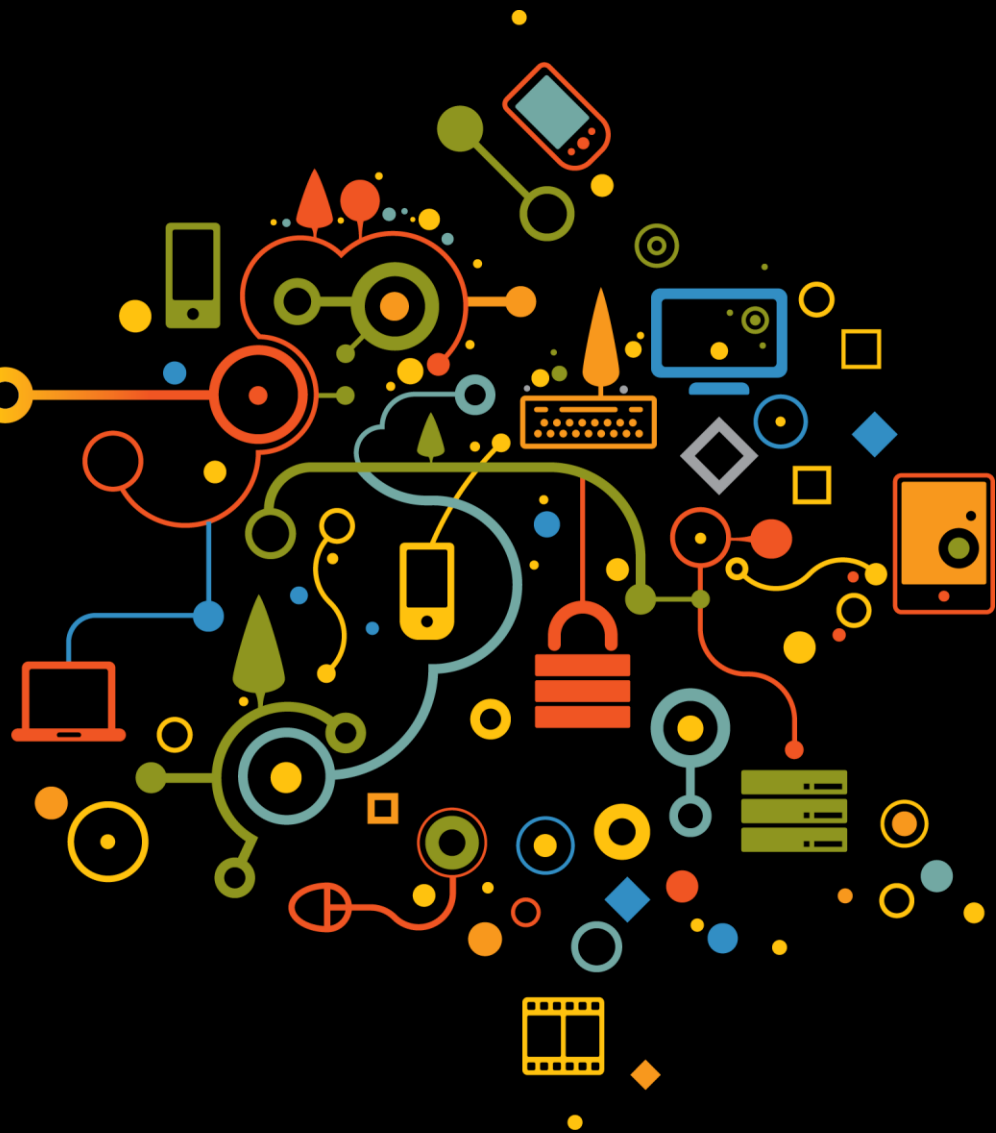
- Scanning of outbound email for viruses and spam.
- Controlling and/or monitoring outbound email.
- Preventing information leaks through data loss prevention.
- Scanning outbound emails for offensive images.
- Scanning outbound emails for malware.



Scanning of Outbound Email from Hosted Email Providers



vision

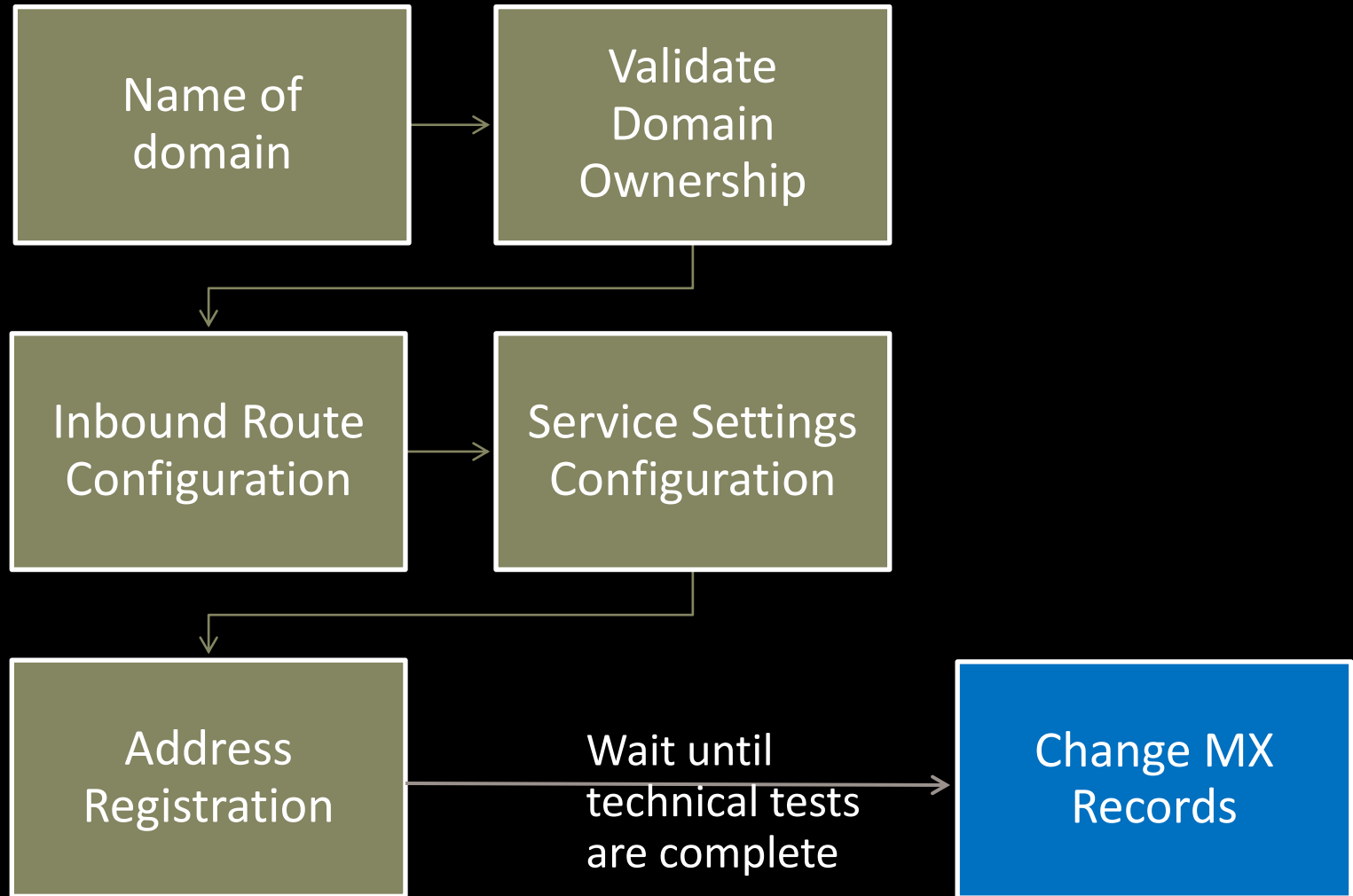


Self-serve Domains

Adding new domains with the Symantec.cloud Management Portal

- In the past new domains could only be added by the Symantec.cloud Provisioning Team.
- Now you can add domains using the Symantec.cloud Management Portal.
- For each domain we still need to confirm:
 - That you own the domain
 - That the Internet mail infrastructure passes various technical tests
- From later this quarter you should be able to remove domains from scanning using the Delete Domain wizard.

Process Overview

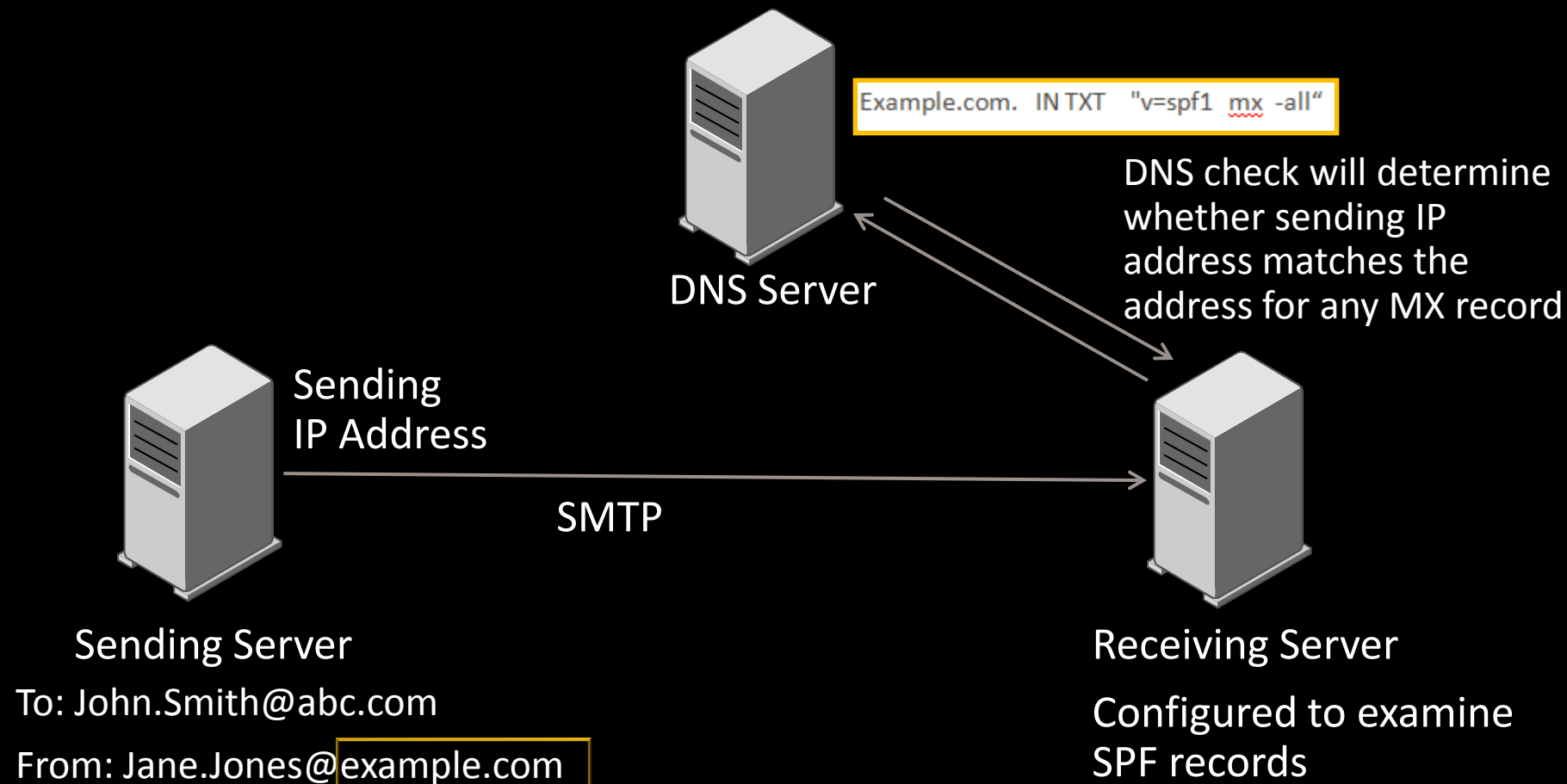


vision



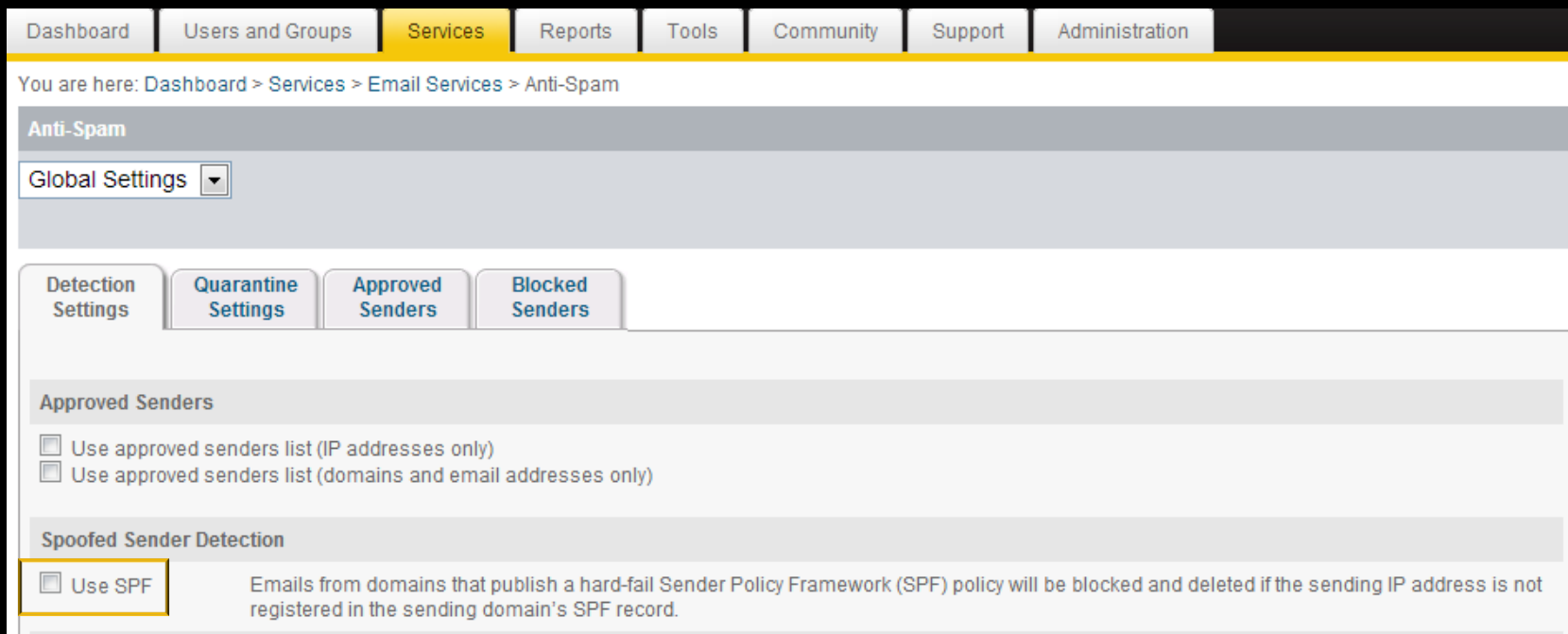
Support for Sender Policy Framework

What is Sender Policy Framework?



How to configure Spoofed Sender Detection

- Configured as part of the anti-spam settings in the Management portal.
- Will block emails if a domain publishes a hard-fail Sender Policy Framework policy.



The screenshot shows the Symantec Management Portal interface. The navigation bar includes 'Dashboard', 'Users and Groups', 'Services', 'Reports', 'Tools', 'Community', 'Support', and 'Administration'. The breadcrumb trail reads 'You are here: Dashboard > Services > Email Services > Anti-Spam'. The 'Anti-Spam' section has a 'Global Settings' dropdown menu. Below this are four tabs: 'Detection Settings', 'Quarantine Settings', 'Approved Senders', and 'Blocked Senders'. The 'Approved Senders' section contains two checkboxes: 'Use approved senders list (IP addresses only)' and 'Use approved senders list (domains and email addresses only)'. The 'Spoofed Sender Detection' section has a checkbox for 'Use SPF' which is checked and highlighted with a yellow box. To the right of this checkbox is the text: 'Emails from domains that publish a hard-fail Sender Policy Framework (SPF) policy will be blocked and deleted if the sending IP address is not registered in the sending domain's SPF record.'

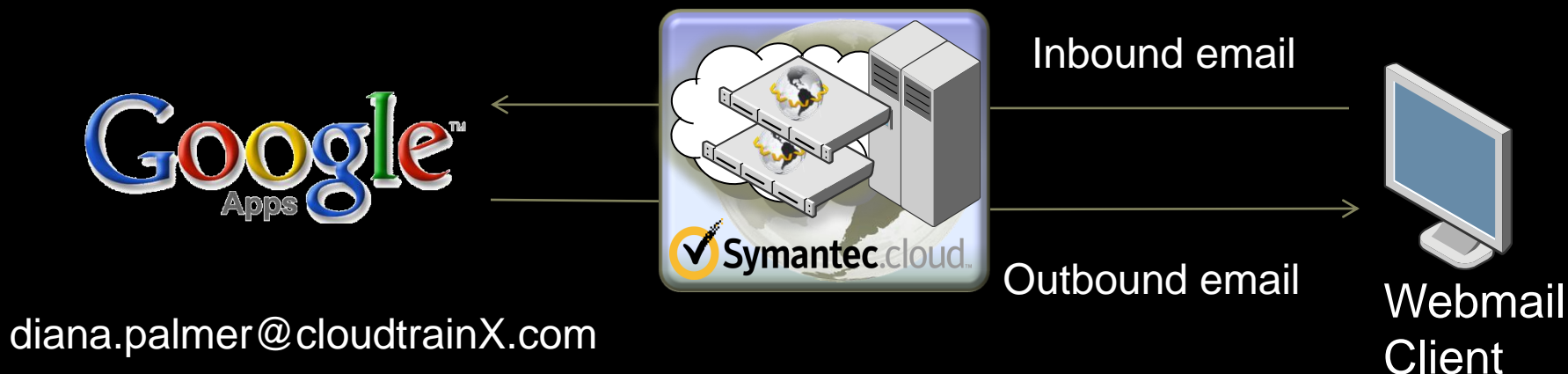
vision



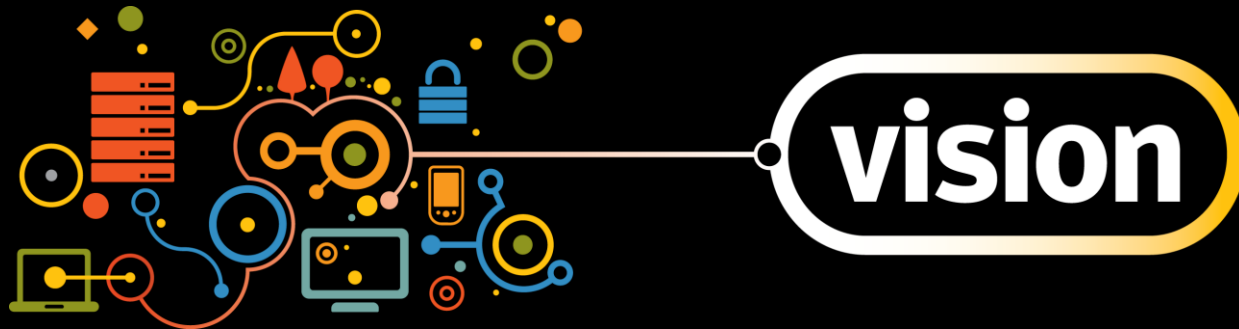
Introduction to the Lab Exercises

Lab Setup

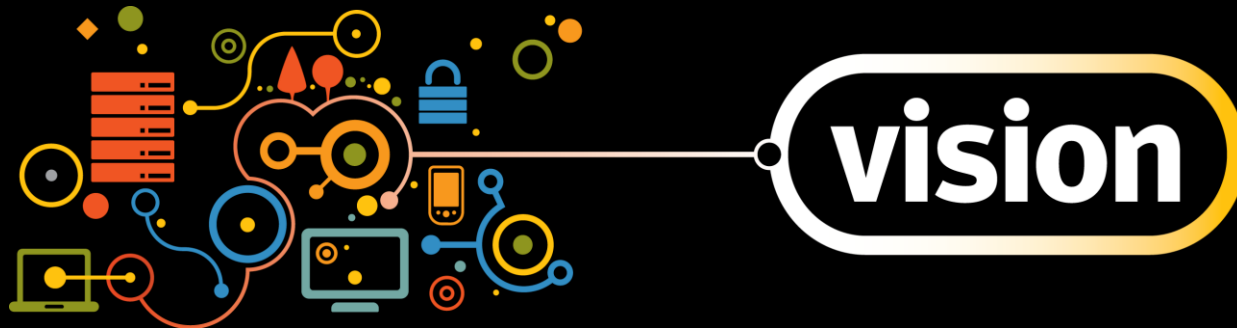
CloudtrainX.com



1. Send some emails from your personal webmail account.
2. Examine the settings for outbound email scanning from hosted email providers.
3. Create some DLP policies.
4. Examine whether the emails sent at the beginning of the lab matched any DLP policies.



Any questions?



Thank you!

Phil Walters

phil_walters@symantec.com

+44 (0)7785456838

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.