Cisco 思科演示云dCloud系列培训

如何使用dCloud 来做思科Cisco Email Security Advanced Phishing Protection v1 的演示

dCloud – 思科的演示云

思科演示云将其产品解决方案架构的软件和硬件虚拟化，让思科与合作伙伴的销售团队在任何地方，任何时间都可以做产品演示.

什么是Cisco dCloud?

服务

思科，合作伙伴，客户

自服务, Managed Service

Instant（实时）, Scheduled（预约）, 企划书

Demo, Lab, 沙盘, POV, Events

可定制化，保持，共享

创建content

平台

5 个数据中心

云，基础架构，自动化，用户 UI

管理员Admin, 开发工具

Cisco on Cisco

内容

超过250 offerings, 所有的架构

预配置有文档提供

虚拟机，硬件，用户设备, licensing

认证，可信

可选的终端l

Operations 和技术支持

24x5* chat, email, web, phone

Self help, event support, metrics

Cisco dCloud – 使用小技巧

- **请随时给我们反馈**
- **共享给你的客户**
- 定制化保存
- 和技术支持联系来Extend sessions
- 超过5个sessions可使用Event scheduling
- 多种 RDP连接的方式
- 将本地应用和云服务加入demo
- 使用多个数据中心来 capacity/redundancy

dCloud 满足你的要求

http://dcloud.cisco.com

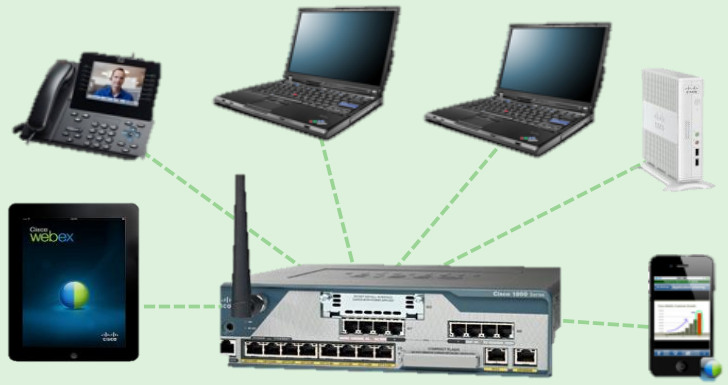
As Easy As…

- 思科员工和合作伙伴
- 完整脚本
- 定制化，本地化，共享
- 可选的终端 (BYOD)
- 可使用你自己的设备

dCloud
Data Centers

US East
US West
EMEAR
APJ
GC

As Complete As…



- Virtual desktops
- Local clients on laptops
- Room based configuration
- 可添加你本地的服务器
- 多种使用案例

思科Cisco Email Security Advanced Phishing Protection v1 的演示

- **现在就让我们和思科安全架构的专家 Zhou Yiwei一起开始吧：**
  - 转去dcloud.cisco.com
  - 使用CCO帐户SSO登陆
  - 选择大中华区GC数据中心
  - 马上就跟随Zhou Yiwei开始学习吧，你可以随时提问题

思科邮件安全高级钓鱼防护

Cisco Email Security Advanced Phishing Protection

Yiwei Zhou
Global Virtual Engineering
yiwzhou@cisco.com

议程 (Agenda)

- 思科邮件安全高级网络钓鱼保护基础介绍
- 使用dCloud平台演示思科邮件安全高级网络钓鱼保护

思科邮件安全高级网络钓鱼保护基础

躲不过的钓鱼邮件

网络攻击者不断寻找新的方法来渗透你的网络. “商业电子邮件诈骗”（BEC）和其他基于身份欺骗的威胁是攻击者成功破坏组织的新方式. “商业电子邮件欺诈”在全球范围内耗资（消耗掉）53亿美元根据FBI1.组织需要更多层保护来保护用户免受欺诈性发件人的侵害。

高级邮件钓鱼防护功能

Cisco Advanced Phishing Protection——CAPP

思科在邮件安全里增加了高级网络钓鱼防护，这个功能进一步增强了发件人认证和“商业电子邮件欺诈”检测功能.

高级邮件钓鱼防护功能
Cisco Advanced Phishing Protection

CAPP支持对复杂的基于身份的电子邮件攻击提供防护，通过将全球Cisco Talos威胁情报与本地电子邮件智能和先进的机器学习技术相结合，在组织内部和个人之间对互联网上的可信电子邮件行为进行建模，从而停止基于身份欺骗的攻击，例如社交工程，冒名顶替者和BEC“商业电子邮件欺诈”.

高级邮件钓鱼防护功能
Cisco Advanced Phishing Protection

从应用场景来看CAPP能做些什么.

- 从用户的收件箱中删除恶意电子邮件以防止电汇欺诈或其他高级攻击
- 详细了解电子邮件攻击活动，包括安全邮件总数和防止攻击
- 在ESA中增加对网络钓鱼和“商业电子邮件欺诈”的检测和阻止功能

高级邮件钓鱼防护功能部署方式

Cisco Advanced Phishing Protection Sensors
Cloud（hosted）
On-premises本地部署

高级邮件钓鱼防护功能部署

Virtual machine hardware requirements for Cisco Advanced Phishing Protection on-premises sensor deployment

Operating system	CPU	Memory	Disk	Network
Modern, 64-bit Linux: ● Red Hat Enterprise Linux 7.2 or later ● CentOS 7.2 or later ● Ubuntu 14.04 or later	Intel or AMD x 86_64 2 cores minimum 4 cores recommended	16 GB minimum 32 GB recommended	5 GB minimum 100 GB+ if anticipated email volume is high	1 Gbit/sec recommended

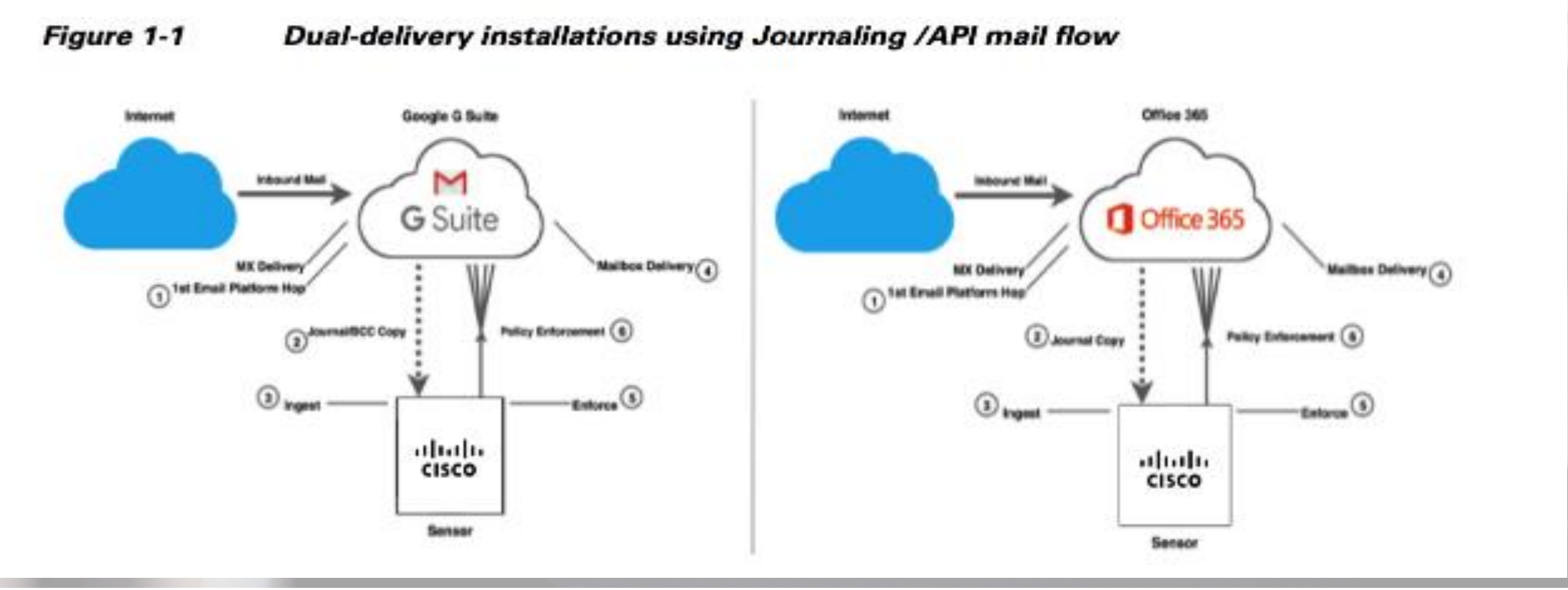
高级邮件钓鱼防护功能部署方式

Dual-delivery
In dual-delivery mode, the sensor accepts copies of email messages over Simple Mail Transfer Protocol (SMTP) and extracts metadata in a streaming fashion

In-line modes
In an in-line configuration, the sensor acts as an Mail Transfer Agent (MTA): it takes responsibility for accepting the message and delivering it to the next hop (usually another internal MTA).

高级邮件钓鱼防护功能部署方式

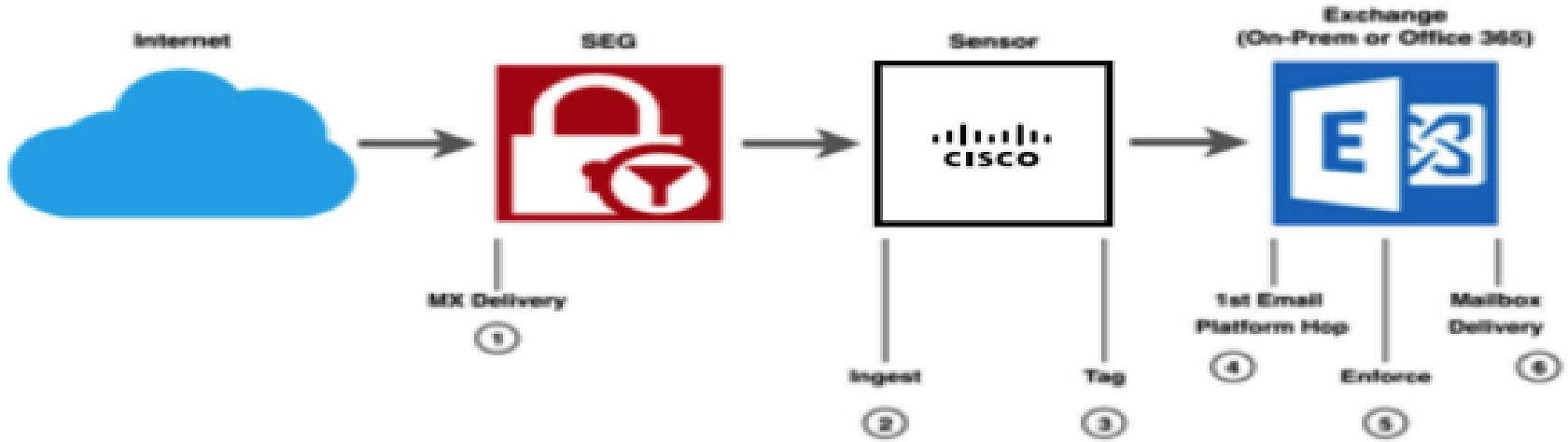
Dual-delivery is typically used for hosted email architectures like Office365 and G Suite.



高级邮件钓鱼防护功能部署方式

In-line sensor installations are primarily used when the client mailboxes have not been migrated to either Office 365 or Google G Suite

Figure 1-2 Inline Installations Mail Flow



高级邮件钓鱼防护功能订购

Offerings	Description	Top-Level SKU
Cisco Advanced Phishing Protection On-prem (with on-prem sensor)	This is for customers particular about content of email not leaving customer premise while only metadata is sent to cloud	L-ESA-APP-LIC=
Cisco Advanced Phishing Protection On-prem (with cloud sensor)	This is for customers having on-prem email gateway/mailbox but not concerned with email going to cloud for Advanced Phishing Protection	L-ESA-APPC-LIC=
Cisco Advanced Phishing Protection Cloud (with cloud sensor)	This is for customers preferring email analysis on cloud	L-CES-APPC-LIC=

Demo

Call to Action

- Go to: dcloud.cisco.com
- dCloud for demo, lab, PoC, etc.
- Live support 24x5… chat, email, Phone