FORCEPOINT

POWERED BY Raytheon

COUNTERMEASURE | 2017

Data Security & Office 365—Stop Chasing Data

Paul Da Silva
Sales Engineer , Eastern Canada

AGENDA

✓ **Introduction**

✓ **Architecture**

✓ **CASB Solution and capabilities (Demo)**

✓ **Q & A**

UNIQUE NEW COMPANY, OFFERING A NEW APPROACH

websense® ▶ **Raytheon** ▶ **STONESOFT** ▶ **skyfence**

**Commercial
Agility**
with
Content Security & DLP
Cloud / On-Premise /
Hybrid

**Pioneer on
Cyber Frontlines**
with
Financial Resources
Deep Understanding of Threat Detection

**Networking
Innovator**
with
Advanced Evasion Prevention
Security at Scale

Cloud Management
with
visibility and control over
sanctioned and unsanctioned
cloud apps.

FORCEPOINT
POWERED BY **Raytheon**

DEFEND
DETECT
DECIDE
DEFEAT
USERS, DATA
& NETWORKS

UNIQUE NEW COMPANY, OFFERING A NEW APPROACH

Forcepoint UEBA

The combination of RedOwl UEBA, Forcepoint DLP, Forcepoint Insider Threat and Forcepoint CASB will provide the industry's only comprehensive solution for understanding and responding to the behaviors and intent of people.

BROAD AND DEEP PORTFOLIO
OF ADVANCED SOLUTIONS

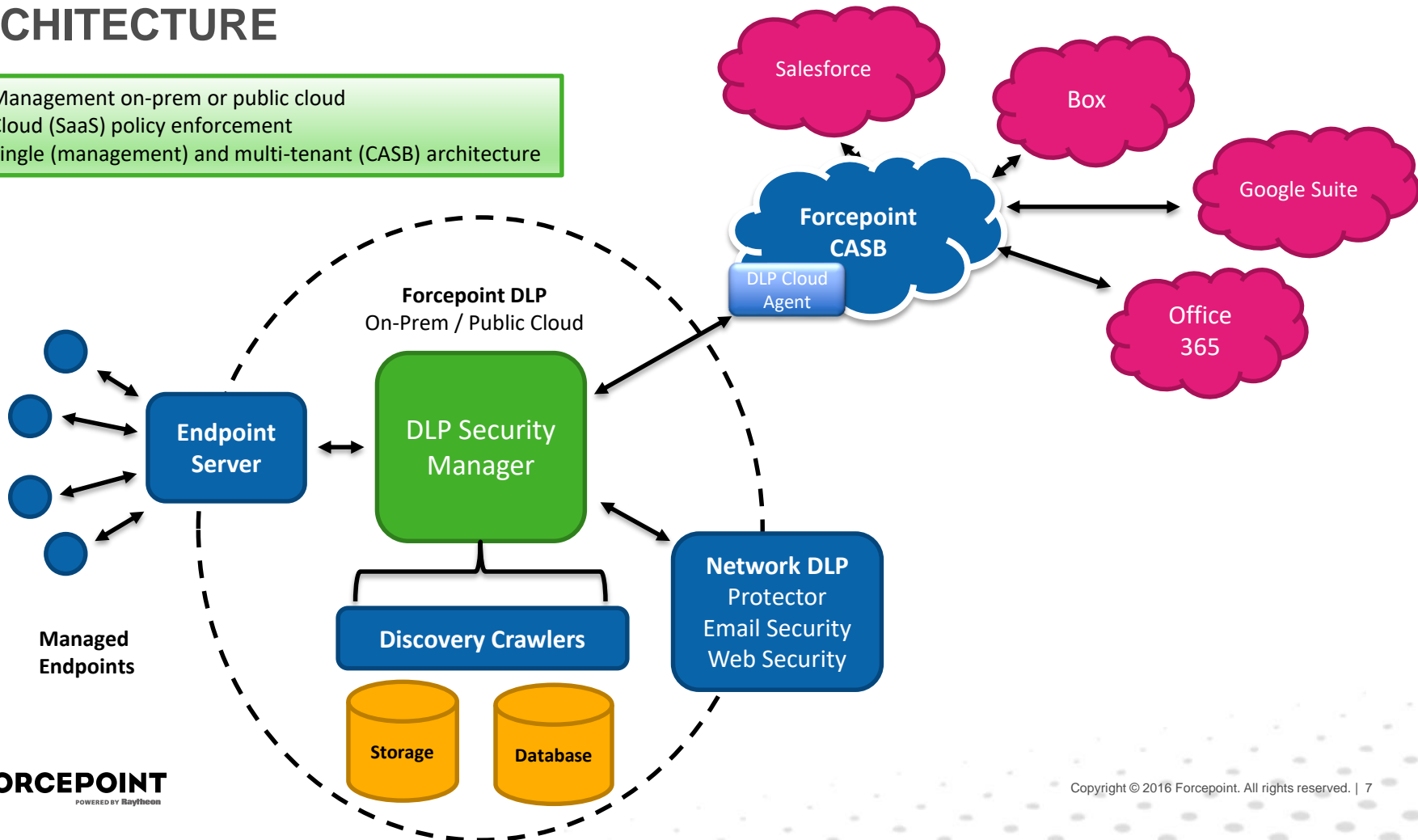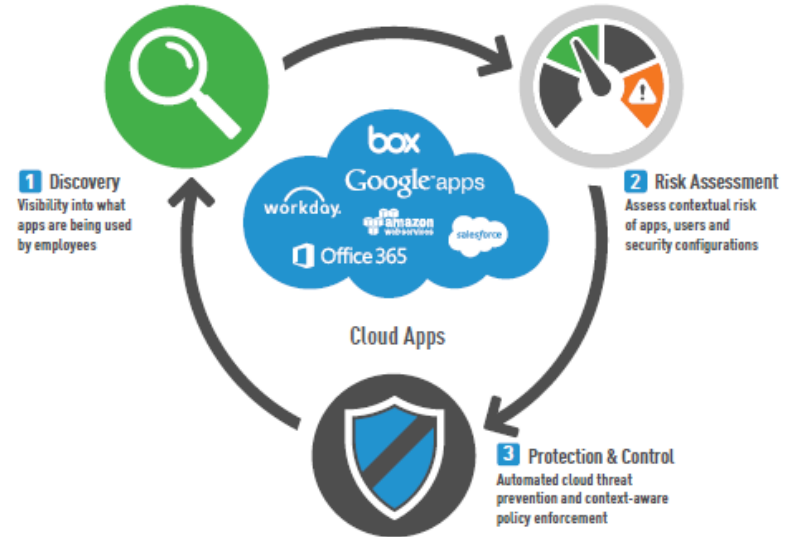| INTEGRATED DEFENSE SYSTEMS	INTELLIGENCE, INFORMATION AND SERVICES	MISSILE SYSTEMS	SPACE AND AIRBORNE SYSTEMS	FORCEPOINT POWERED BY RAYTHEON
C5I™	Cyber	AMRAAM®	Airborne Radars	Web and Email Security
Patriot™	Digital Battlespace	Tomahawk	Electronic Warfare	Next-Generation Firewall
Zumwalt	Space	SM-3®	Space Sensors	Insider Threat Solutions
AN/TPY-2	Intelligent Transportation	Paveway™	Intelligence, Surveillance and Reconnaissance	Data and Intellectual Property Loss Prevention
AMDR	Training	ESSM®	Special Mission Aircraft	Cross Domain Solutions

Architecture

ARCHITECTURE

- Management on-prem or public cloud
- Cloud (SaaS) policy enforcement
- Single (management) and multi-tenant (CASB) architecture

Salesforce

Box

Google Suite

Forcepoint CASB

DLP Cloud Agent

Office 365

Forcepoint DLP
On-Prem / Public Cloud

Endpoint Server

DLP Security Manager

Network DLP
Protector
Email Security
Web Security

Managed Endpoints

Discovery Crawlers

Storage

Database

FORCEPOINT
POWERED BY Raytheon

DLP 8.5: INTEGRATION WITH FORCEPOINT CASB

- DLP Cloud Engine hosted in Forcepoint CASB infrastructure

- DLP policies are pushed into the cloud and enforced using cloud platforms APIs and inline cloud proxies.

- Incidents and forensics stored securely within on-prem / public cloud deployed DLP Security Manager

- New cloud applications added dynamically.

CASB

FORCEPOINT

WHAT IS A CLOUD ACCESS SECURITY BROKER (CASB)?

Users from Anywhere

Cloud App

Cloud Access Security Broker (CASB)

amazon web services™

Dropbox

salesforce

workday.

Google Apps for Work

zendesk

box

Office 365

CUSTOMER SECURITY NEEDS AS THEY ADOPT THE CLOUD

I need visibility into what my users are doing in the cloud in order to understand my risks and protect my users

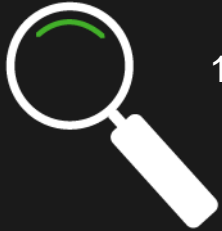**Unsanctioned Cloud Applications / "Shadow IT"**

I need to be able to monitor and control how my users interact with my critical cloud applications

Sanctioned Cloud Applications

I need security that helps me safely embrace the cloud.

SECURITY USE CASES FOR UNSANCTIONED CLOUD APPS

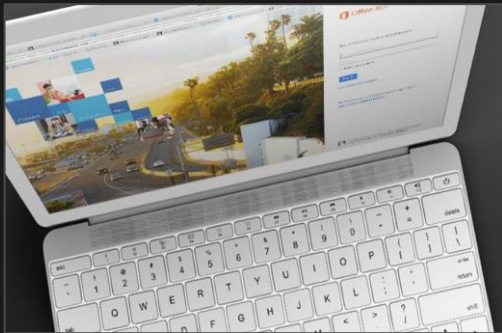1. Visibility into Shadow IT

2. Identify Risky Apps

3. Prevent Risky Usage

4. Identify Users in Risk

SANCTIONED APPS CREATE SECURITY AND COMPLIANCE BLIND SPOTS

Productivity Apps

(Office 365, Google Apps)

File Collaboration Apps

(Box, Dropbox, Google Drive)

Line of Business Apps

(Salesforce, AWS, ServiceNow, NetSuite, etc.)

> **"CASB is a required platform for organizations using Cloud Services."**

Gartner

Market Guide for CASBs, October 2015

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

SECURITY USE CASES

Controls

1. **Prevent Cyber Threats**

2. **Prevent Data Leakage**

3. **Control External File Sharing**

4. **Manage Admins & Privileged Accounts**

5. **Manage BYOD Access**

6. **Monitor All User Activity**

Mail

Financial Apps

CRM

Collaboration

Users

SECURITY USE CASES

**Office365
G Suite**

**Workday
NetSuite**

**Salesforce
MS Dynamics**

**Box
OneDrive**

Forcepoint CASB

1. Prevent Cyber Threats

2. Prevent Data Leakage

3. Control External File Sharing

4. Manage Admins & Privileged Accounts

5. Manage BYOD Access

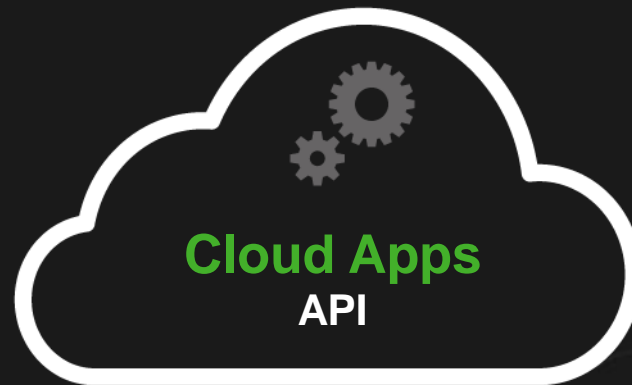**6. Monitor All User Activity**

Users

FLEXIBLE CASB DEPLOYMENT OPTIONS

1. Cloud APIs

Pros

- ▸ Quick time to value
- ▸ No internal politics
- ▸ Certified by provider
- ▸ No end user impact

2. Cloud Proxy

Pros

- ▸ Full user activity monitoring
- ▸ Full blocking and alerting
- ▸ No API dependency

Cloud Apps
API

Cloud Apps
Proxy

FORCEPOINT CASB FOR VISIBILITY AND CONTROL OF CLOUD APPLICATIONS

Corporate Employees, Mobile Workers and Hackers

Google Apps for Work

salesforce

Dropbox

amazon web services

workday

Office 365

Cloud Applications (6000+ apps)

Forcepoint CASB Solution Components

Governance	Audit & Protection	Security Suite
▸ Discover Shadow IT apps & assess risk	▸ Detect behavioral anomalies & prevent attacks in real-time	▸ All capabilities from Governance and Audit & Protection
▸ Discover & manage sensitive data in cloud file sharing apps	▸ Real-time & API-based, comprehensive user activity monitoring	
▸ Identify admins, inactive, external and former employees	▸ Control sensitive data with DLP policies	
▸ Centrally assess data and security configuration settings	▸ Enforce risk-based MFA	
▸ SIEM enablement	▸ Prevent data proliferation to unmanaged devices	

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

CASB CAPABILITIES FOR FORCEPOINT PRODUCTS

- **CASB add-ons for Web Security**

  - Simplified integration for Cloud Access Security (Visibility & Control, UBA, Threat Prevention)
  - BYOD (Device Control) for Web control

- **CASB add-on for NGFW**

  - Unified Visibility & Control, UBA, Threat Prevention)

- **CASB add-on for DLP**

  - Cloud Data at Rest classification & threat mitigation
 - Cloud Data in Motion – content inspection and blocking

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

PROXY-BASED DEPLOYMENT WITH SSO/ IDP SERVICE PROVIDER INITIATED

Deployment steps using a SSO/ IDP products (Ping, CA, OIAM, etc),

1. Client logins to SaaS application
2. Client is redirected by the SaaS to the IDP
3. IDP configured to redirect client POST response to Skyfence Cloud gateway
4. Skyfence Cloud gateway reverse proxies client sessions, implements activity monitoring and policy controls

Benefits

1. Transparent to the user
2. IDP resource can be allocated to select individuals/groups without domain wide deployment
3. Supports all devices

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.
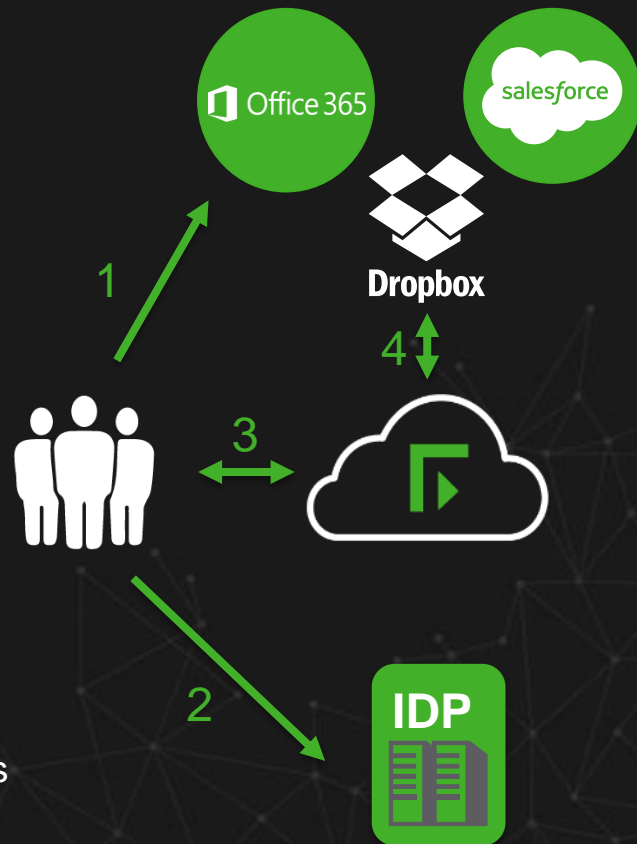
PROXY-BASED DEPLOYMENT WITH SSO/ IDP IDENTIFY PROVIDER INITIATED

Deployment steps using a SSO/ IDP products (Ping, CA, OIAM, etc),

1. Client logins/authenticates to IDP
2. Client selects resource and receives SAML response
3. IDP configured to redirect client POST response to Skyfence Cloud gateway
4. Skyfence Cloud gateway reverse proxies client sessions, implements activity monitoring and policy controls

Benefits

1. Transparent to the user
2. IDP resource can be allocated to select individuals/groups without domain deployment
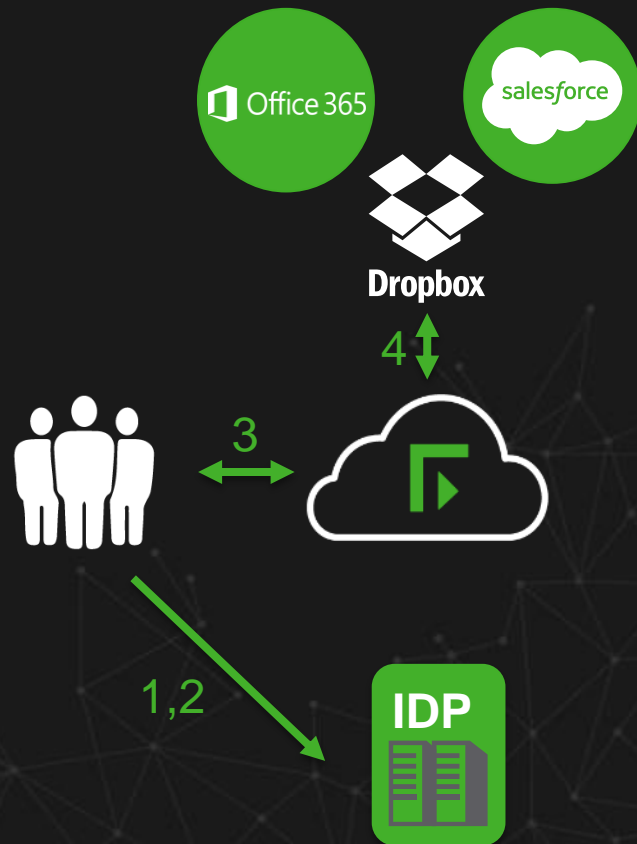3. Supports all devices

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Office 365 DLP & EMAIL can and can't do

Data Loss Prevention	Office 365
DLP integrated into email security	YES
Breadth of built---in DLP policies	NO
	NO
Granular fingerprinting of data within documents and database records	NO
Optical Character Recognition (OCR) for detecting data hidden in images	NO
Data Discovery for SharePoint Online	YES
Data Discovery for OneDrive	YES
Incident management workflow with role---based access controls	NO
Encrypted storage of forensic data	NO
Same DLP policies used throughout Office 365 apps	NO
Same DLP policies used in other Cloud apps	NO
Same DLP policies used in web channels, endpoints, internal servers & networks	NO

FORCEPOINT
POWERED BY Raytheon

Office 365 DLP & EMAIL can and can't do

Security for Office 365 Exchange	Exchange Online Protection
Email Security	
Blocks known spam and viruses	YES
Differentiates spam and phishing to avoid accidental breaches	NO
Integrated protection across web and email communications	NO
Advanced Email Security	Advanced Threat Protection
Leader in APT Protection with deep dynamic and static threat	NO
Blocks click---through of URLs pointing to suspicious content	Basic
Phishing education at the point of click	NO
Advanced Threat Protection against malware, spam, phishing, Zero---Days	Basic
Sandboxing of suspicious attachments in cloud or on-premise	Cloud Only
Management	
Single console for security across Office365 apps	NO
Single console for Exchange Online & Server, SharePoint Online & Server	NO
Built---in library of reports for security, compliance, and operations	NO
Report customization and scheduled delivery	NO

FORCEPOINT
POWERED BY Raytheon

FORCEPOINT

Q&A