

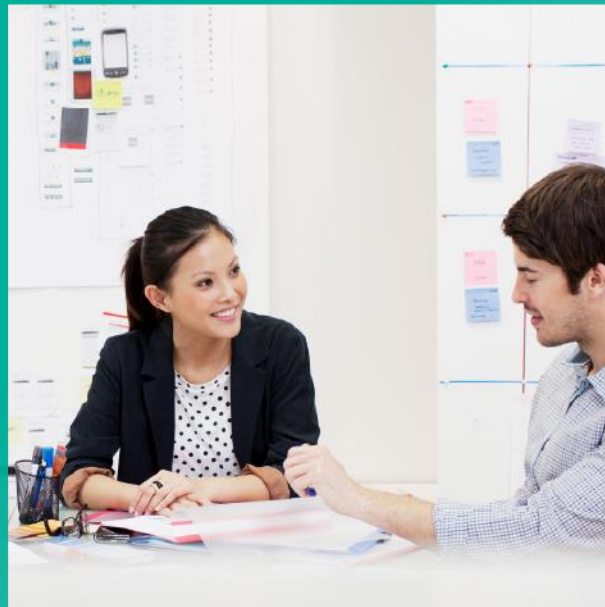
# Tech Update: DLP v8.7.1

## Main Topic: DLP Cloud Applications Inline Proxy

Presenter: Dave Barnett

Director: Edge portfolio

24<sup>th</sup> April 2020



# Agenda

- Refresh on new risks in the cloud
- CASB Deployment Options Review
- DLP Cloud Applications: What is it?
- What's new in Forcepoint DLP v8.7.1

# What are the 5 main cloud risk problems?



Users oversharing sensitive data in file sharing and collaboration apps



Employees and 3<sup>rd</sup> parties accessing cloud apps from their own devices



Admins making mistakes or becoming under attack

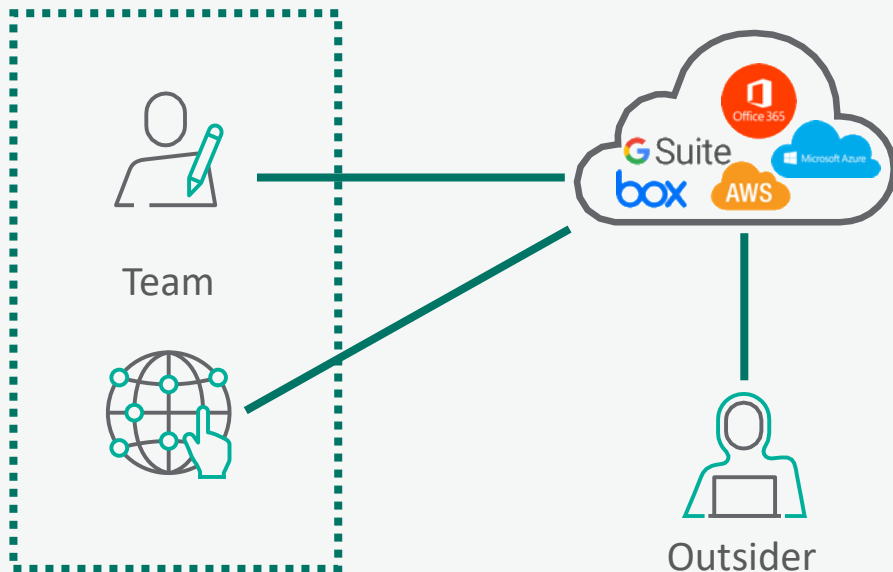


The cloud is the the new attack surface and a lack of governance



Concerns about employees finding and using their own cloud services aka shadow IT

## Scenario – Users Oversharing Data



Collaborate via cloud apps



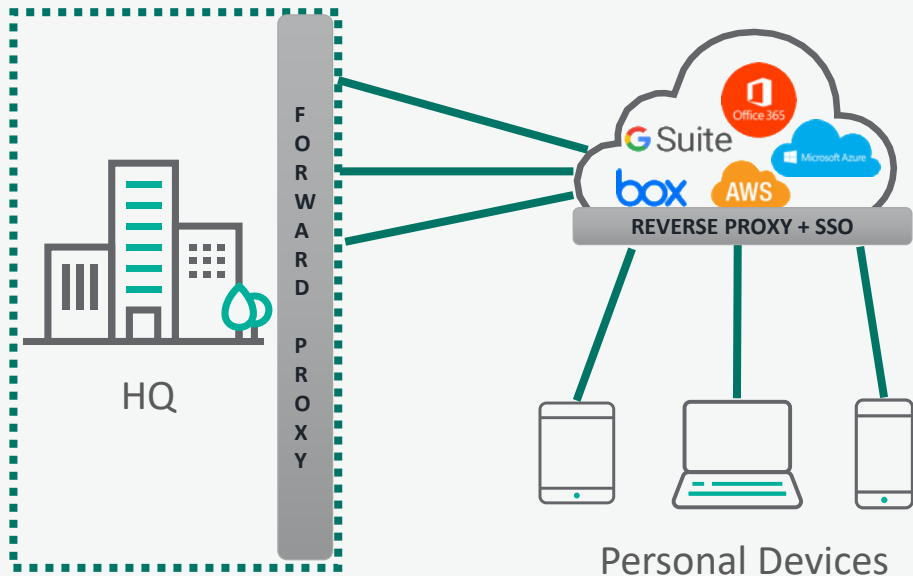
Policy to exclude external users



Geo-location anomaly

We can allow you to collaborate safely within cloud applications

## Scenario – Personal Device use



### Enable BYOD Access



Access apps anywhere



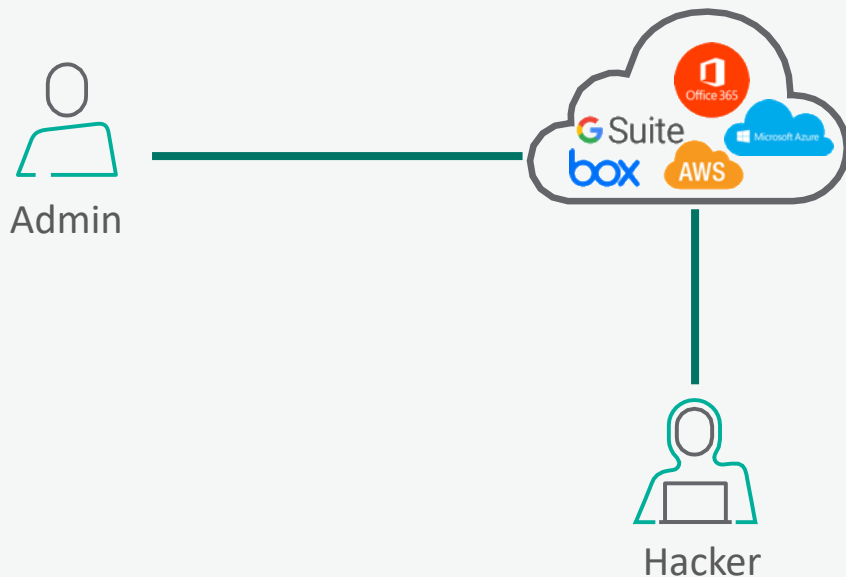
Robust reverse proxy



Seamless SSO  
integration

We can help you use BYOD/HYOD devices.

## Scenario – Admin risk



### Stop Risky Access



Behavioural Analytics



Step up authentication



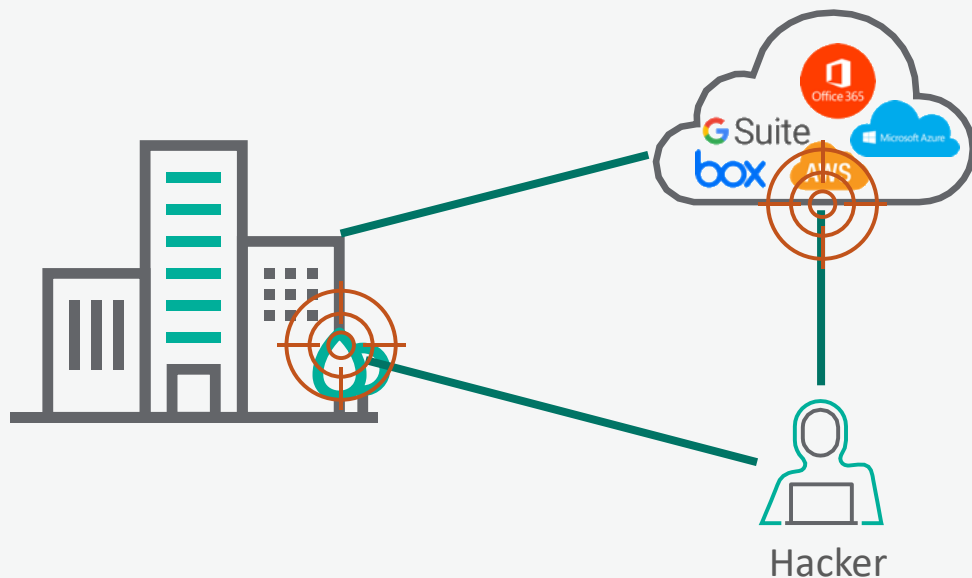
Automatic Policy Enforcement



Cloud compliance

We can monitor and block risky admin actions

## Scenario – Cloud becoming the new attack surface



### Protect against attack



Access policy  
Enforcement



Step-up  
authentication



Block unauthorized  
access

We can tell you exactly who is under attack in real time

## Scenario – Shadow IT risk and opportunity



Gain full visibility into Shadow IT



Visibility into  
unsanctioned apps



Control over both  
unsanctioned and  
sanctioned apps

We can help you say YES to any cloud application

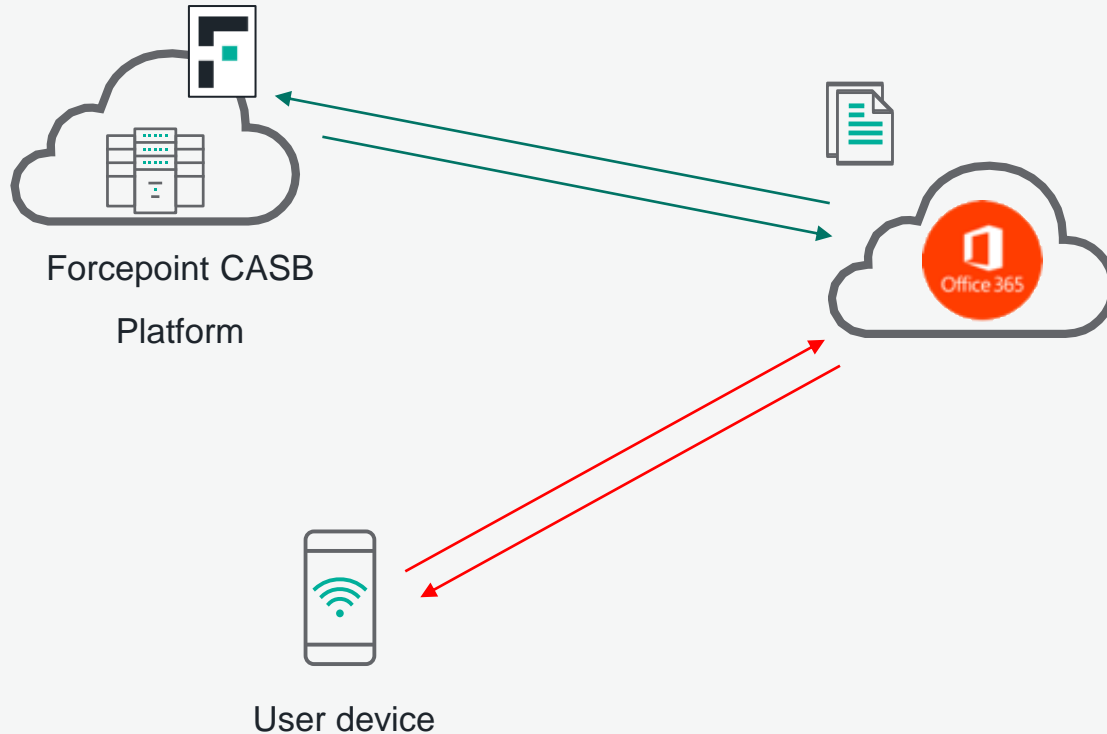
# CASB/DLP Deployment Options Review



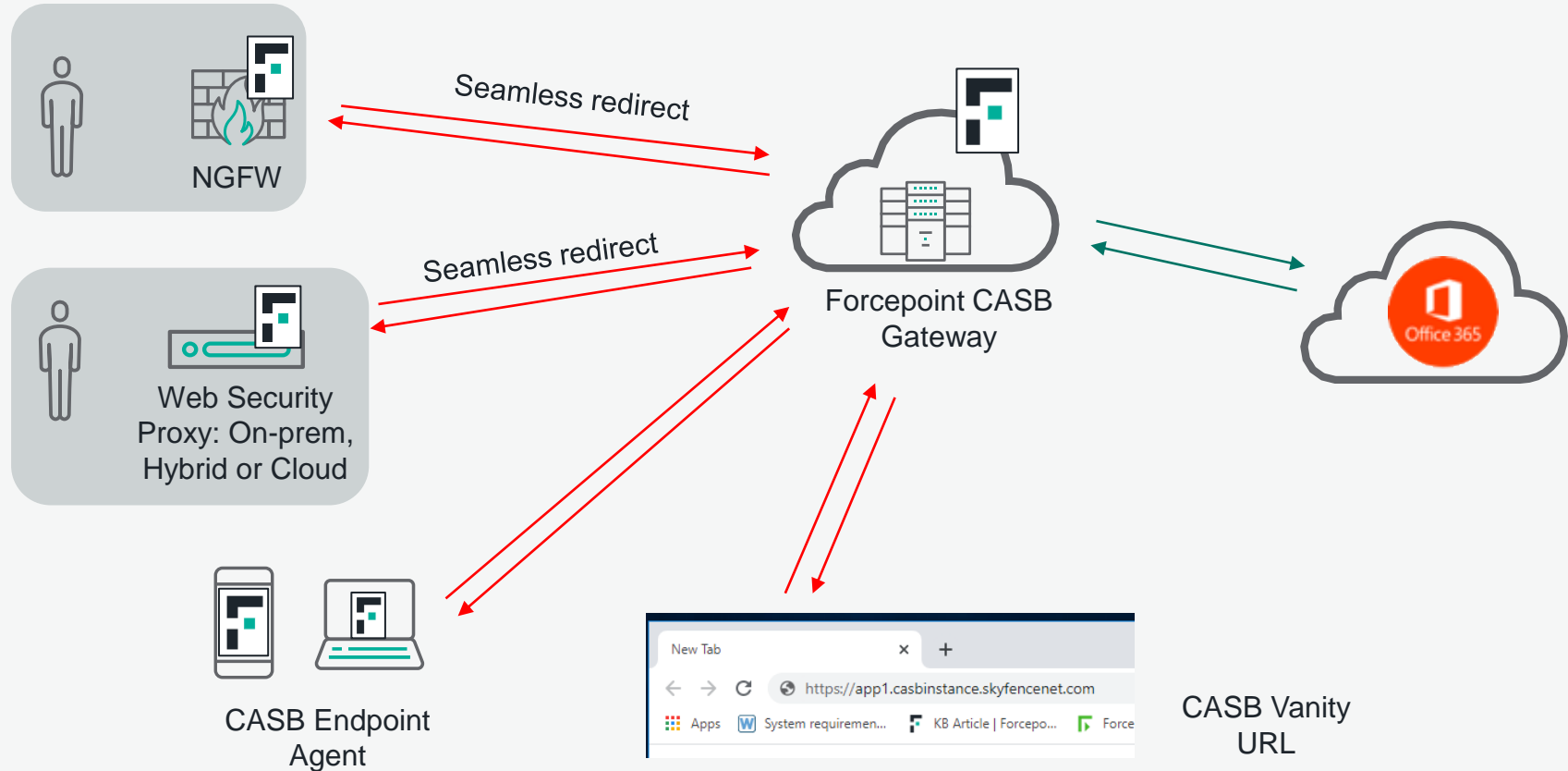
# Deployment Options Review

- API Deployment Type (Tokenisation):
  - Seamless Integration – No impact on Userbase.
  - DLP/CASB connects to Sanctioned Cloud App via API call.
  - DLP/CASB retrieves and reads Sanctioned Cloud App logs to understand User Activities
- Inline Proxy Type (User traverses DLP/CASB Gateway):
  - Full User Activity monitoring
  - Full blocking and alerting
  - Either Reverse Proxy or Forward Proxy Deployment Options available.
- For Realtime DLP Cloud Applications blocking to happen you need to have a CASB licence, and you need to be inline with the CASB Gateway.

# CASB: API Deployment Mode



# CASB: Inline Deployment Mode: Forward Proxy



# CASB: Inline Deployment Mode: Reverse Proxy (SSO)



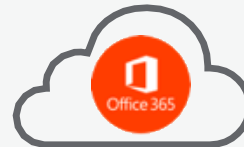
Unmanaged Device



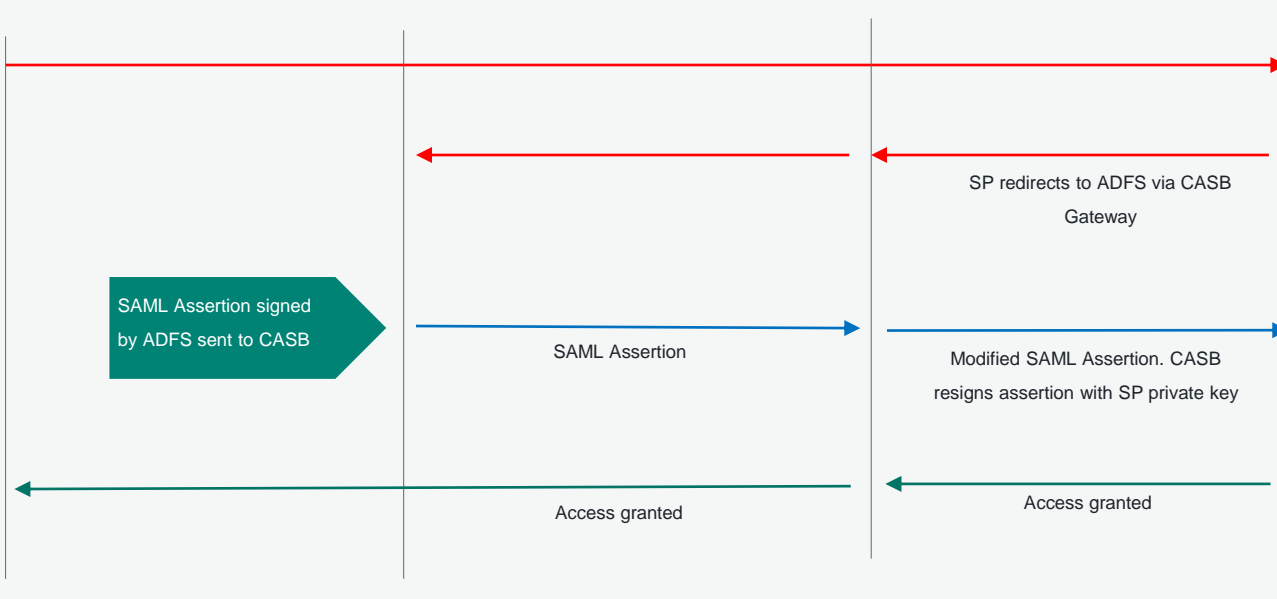
Customer ADFS  
Service



Forcepoint CASB Gateway



User logs into SP  
Direct connection to SP



The background of the slide is an aerial photograph of a fighter jet, possibly an F-35, on a runway. The jet is positioned vertically in the center, facing upwards. The runway has white vertical markings on either side of the jet. In the top right corner, there is a teal-colored square inset. Inside this inset is a smaller, slightly offset square showing a person in a yellow safety vest walking on the runway, casting a long shadow.

# DLP Cloud Applications: What is it?

**Forcepoint**

# The DLP Journey: DLP Suite



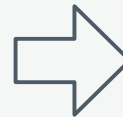
**Monitor**

Non-intrusive



**Notify**

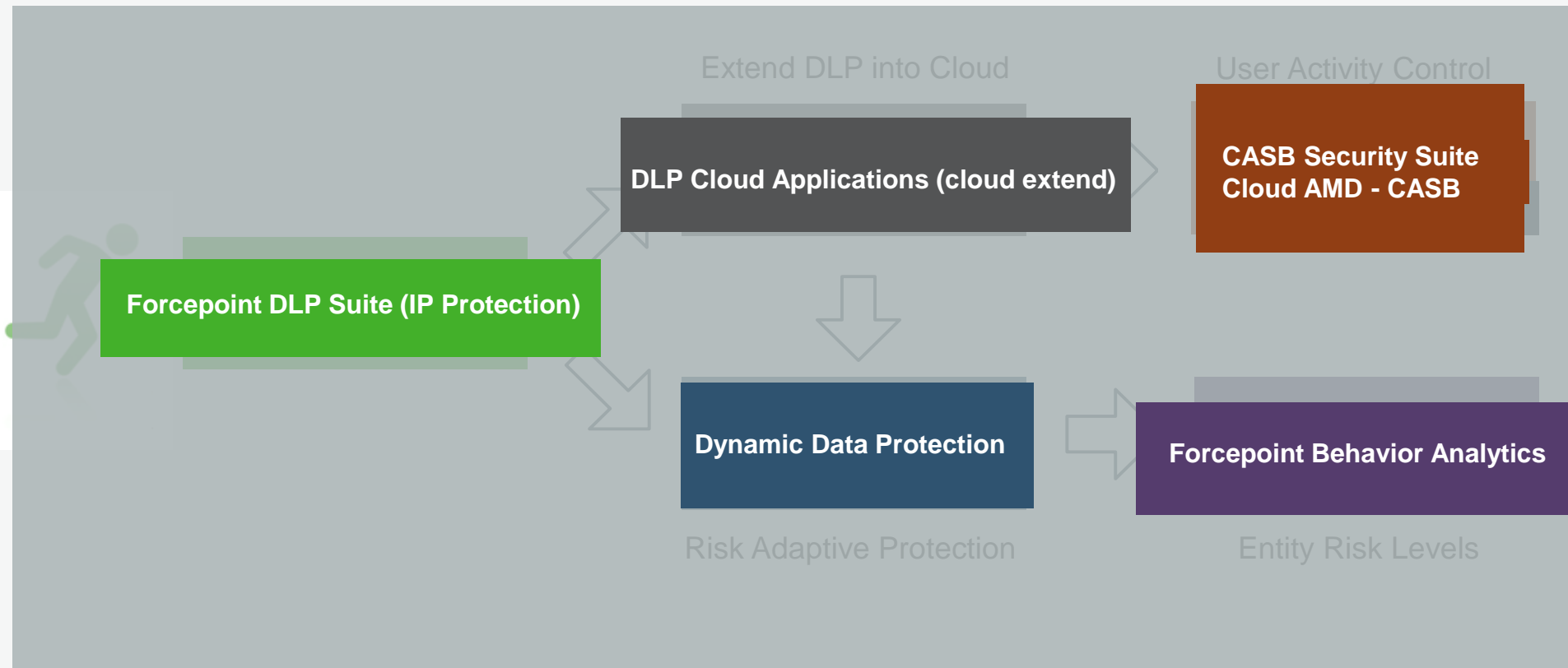
User Education



**Block**

Control

# The DLP Journey: DLP Cloud Apps or FBA?



# Introducing the Forcepoint data protection portfolio

## DLP Discover

Data at Rest

Cloud

## DLP Network

Data in Motion

IM

## DLP Endpoint

Data in Use

IM

## DLP Cloud Apps

Data In Use, in Motion  
& at Rest

Monitor File  
Permissions

Monitor  
Uploads

**DDP:**

*Continuous, adaptive data protection offering automatic policy change for data exfiltration as the risk of user behavior*

Email

Databases

Active  
Sync

FTP

Storage

Printer

**CASB:**

*Continuous, adaptive risk protection offering automatic policy change for user behavior in the cloud*

Storage

Drives

Network  
Printer

Web

Media

Email

Discover  
Cloud Apps

# What is DLP Cloud Applications

- DLP Cloud Applications extends your DLP Ruleset so that it can be used in protecting data residing in Sanctioned Cloud Applications.
- You create your DLP Ruleset on the Forcepoint Security Manager (FSM) WebGUI.
- DLP Cloud Applications is a service/system residing in the Forcepoint AWS space. It shares space with our CASB platform...but see it as a separate system to CASB (think DLP Protector in the Cloud).
- You maintain one DLP Truth:
  - You maintain central DLP rulesets on the FSM.
  - All Logging comes back to the same central FSM WebGUI.
  - All DLP Incidents come back to the same central FSM WebGUI.

# What is DLP Cloud Applications (pre v8.7.1)

- DLP Cloud Applications purchased on it's own can offer:
  - An API connection into your Sanctioned Cloud Application (nothing real-time as DLP Cloud Applications relies on the SP logs to investigate data movement).
  - Visibility into sensitive data being up/downloaded to/from Sanctioned Cloud Applications.
  - Perform unshare (external/Internal/both) of sensitive data incorrectly shared as such.
  - Quarantine or perform Safe Copy of sensitive data.
  - Perform a Data at Rest scan of data residing within your Sanctioned Cloud Application.
  - Support (currently) for six Sanctioned Cloud Applications:
    - Office 365 (includes OneDrive and SharePoint Online).
    - Salesforce
    - Dropbox for Business
    - Box
    - G Suite
    - ServiceNow

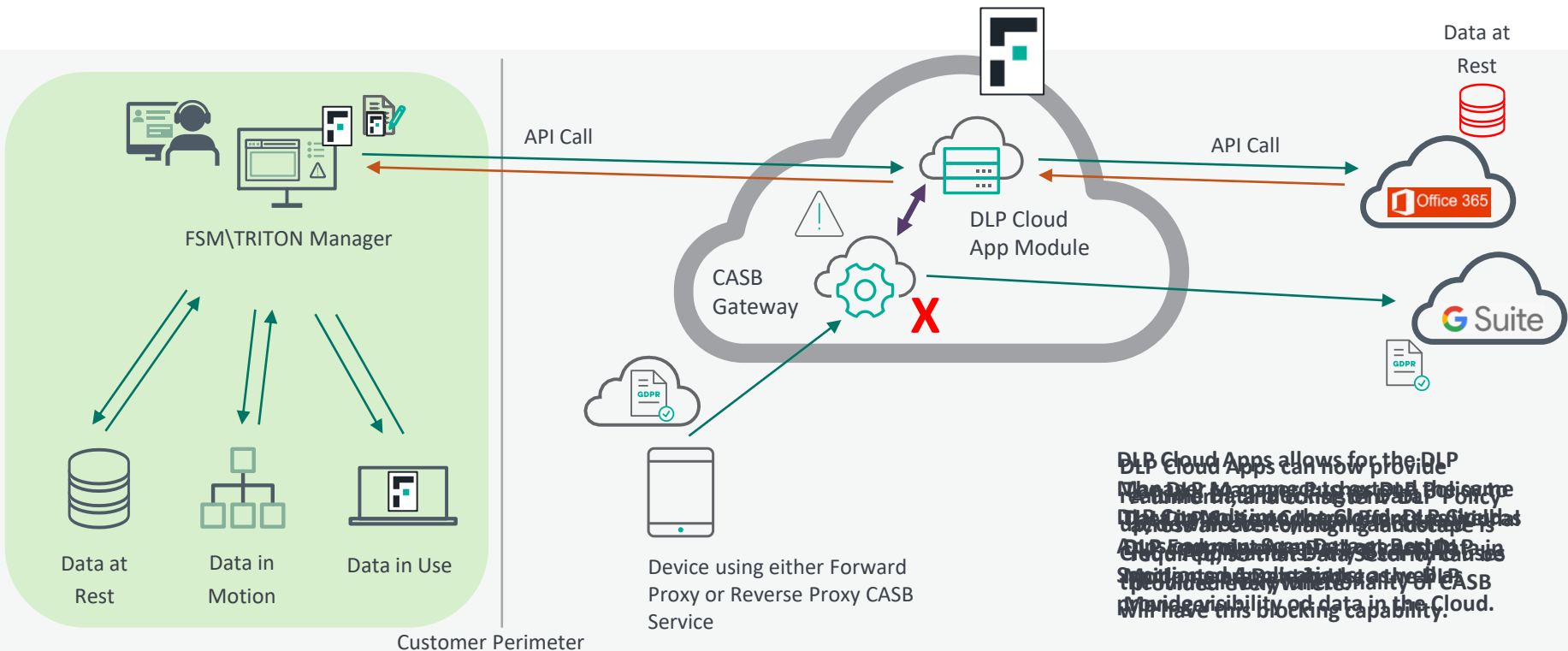
# What is DLP Cloud Applications (v8.7.1)

- DLP Cloud Applications purchased together with CASB (CASB Security Suite or CASB Single App license) can offer:
  - All features mentioned in previous slide
  - All CASB features as per license capabilities
  - Realtime blocking of sensitive data being up/downloaded to/from Sanctioned Cloud Applications irrespective of device (Managed or Unmanaged devices)\*:
    - Inline CASB Proxy deployment types required (Forward and/or Reverse CASB Proxy).
    - No need for a Forcepoint Agent to make this happen.
    - Data Security protection on Unmanaged devices accessing Sanctioned Cloud Applications.
  - \*In DLP v8.7.1 we offer realtime blocking support for the full set of Forcepoint DLP's predefined rulesets. Examples include regulatory compliance sets such as GDPR, PCI, POPI, HIPPA...
  - \*Roadmap\* to offer the addition of realtime blocking support for fingerprinted files later this year.

## What is required for DLP Cloud Applications to offer real-time blocking?

- For DLP Cloud Applications to enforce real-time blocking:
  - CASB Forward Proxy and/or Reverse Proxy is required.
  - Client requires the DLP Cloud Application licence as well as either CASB Security Suite or CASB Single Application license.

# Forcepoint DLP Cloud Applications and CASB Architecture



DLP Cloud Apps allows for the DLP Manager to enforce DLP Policy on Cloud Applications. The CASB Gateway is required for the DLP Cloud Apps to enforce DLP Policy on Cloud Applications. The CASB Gateway is required for the DLP Cloud Apps to enforce DLP Policy on Cloud Applications.

# DLP Cloud Application Inline Proxy Demo





—  
Tell me one thing  
that is new in CASB?



# Business Impact Analysis - what is BIA?

Level	Range	Description
Critical	81-100	Sensitive activities. For example, sensitive administrative actions, modifying or disabling main security controls, bulk data export, mass deletion, bulk sharing.
High	55-80	High impact activities that usually require high level permissions, but do not need to be reviewed by a security department each time they occur. For example, modifying a Price Book in Salesforce, resetting a user password.  Individually, these activities do not need to generate a security alert or a push notification. It is recommended to use additional conditions with these activities to generate an alert.
Medium	31-54	Activities that require common permissions. For example, sharing a file, exporting a report, viewing a lead.  Individually, these activities do not need to generate a security alert or a push notification. It is recommended to use additional conditions with these activities to generate an alert.
Low	0-30	Activities that do not require special roles or permissions. For example, modifying personal profile settings, uploading or downloading content to personal user folder.

Definition:

**Business impact score** is a number in a range of 0-100. This number reflects the potential impact of a single user activity on specific data in a cloud application.

Higher score = higher impact.

The value range is divided into clusters:

**Critical: 81-100**

**High: 55-80**

**Medium: 31-54**

**Low: 0-30**



# Which cloud apps is BIA available for right now?



# Example Rule – Critical Impact Score

Name: [BIA] Critical Activity Alert

Rule Description: A Critical user activity occurred.

Incident Description: \${account\_login\_name} from \${ip\_origin} at locatio...

Recommendations: Critical Impact action occurred. Notify specific Adminis...

on Enabled

Severity: Critical

Activity mitigation matching this rule

Real time based : Audit

API : Audit

## Choose Predicates

- Forcepoint DLP
- ☒ Server IP
- URL
- Target
- Data object ID
- Message
- Properties
- Amount

☒ Impact Score

How

## Choose Operators

AND OR NOT ( )

## Condition

Create your policy by choosing predicates and operators



Summary: Any occurrence of: Impact Score is from: 81 to: 100

[Clear Condition](#)

[Set Occurrences](#) [Incident Settings](#)

# Example Rule – High Impact Score (unusual activity)

Name: [BIA] High Impact from Unusual X

Rule Description: High Impact activity from Unusual Device/Location

Incident Description: \${account\_login\_name} from \${ip\_origin} at locatio...

Recommendations: Block Action

on Enabled

Severity: High

Activity mitigation matching this rule

Real time based : Block Action

API : Audit

## Choose Predicates

Who

What

How

Where

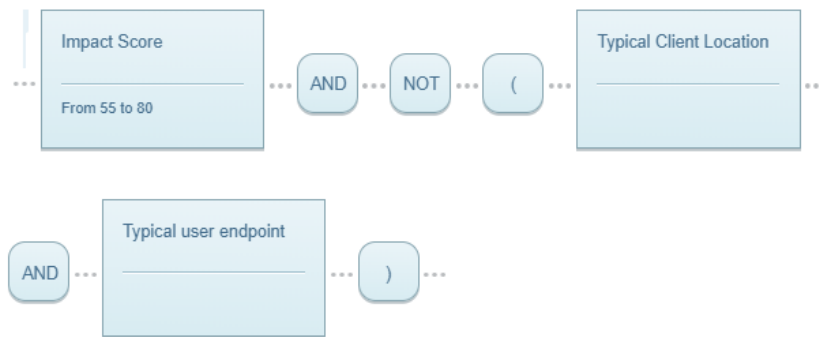
When

## Choose Operators

AND OR NOT ( )

## Condition

Create your policy by choosing predicates and operators




Summary: Any occurrence of: Impact Score is from: 55 to: 80 AND NOT ( Typical Client Locat...

[Clear Condition](#)

[Set Occurrences](#)

[Incident Settings](#)



# Thank You

