

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



# Cisco SSE for Secure Internet Access

The Goldilocks Solution

Jaki Hasan - Solutions Engineer  
BRKSEC-2580

CISCO *Live!*

#CiscoLiveAPJC

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.

**CISCO** *Live!*

<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2580>



# Agenda

- Introduction
- Why Cisco SSE?
- DNS! DNS! DNS!
- May the proxy be with you!
- What can the proxy do for me?
- Firewall in the cloud.

# Introduction (Why?)

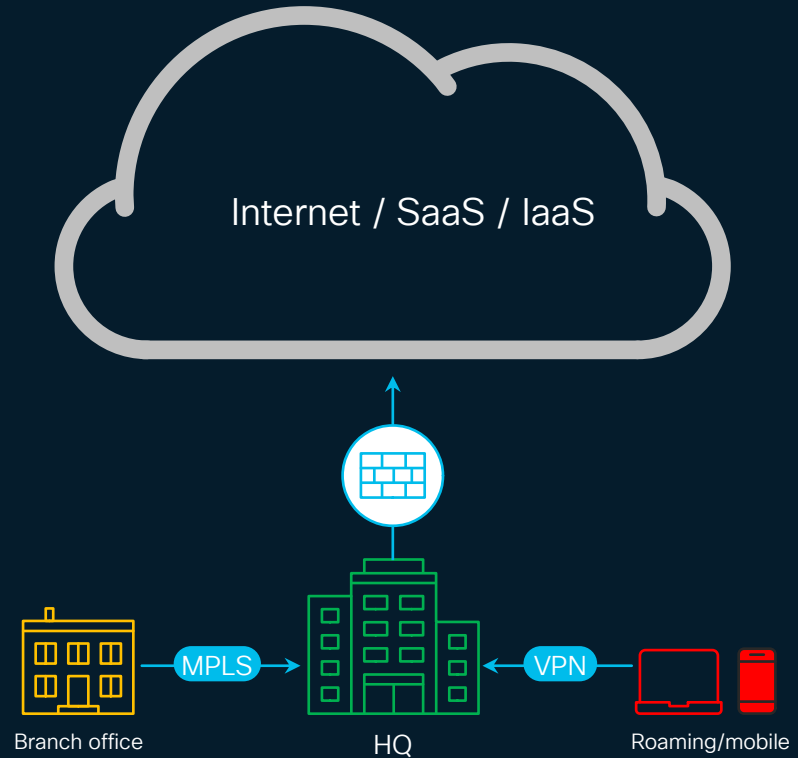
# Traffic flow in the historical times

## Network

Centralised

## Security

Single place to enforce policies and protection



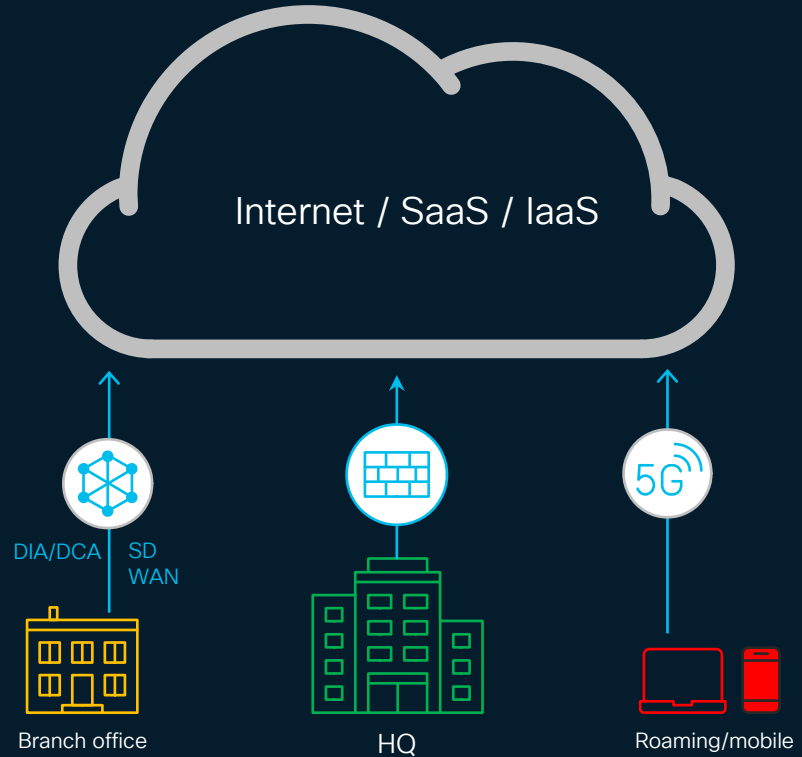
# Traffic flow in the modern times

## Network

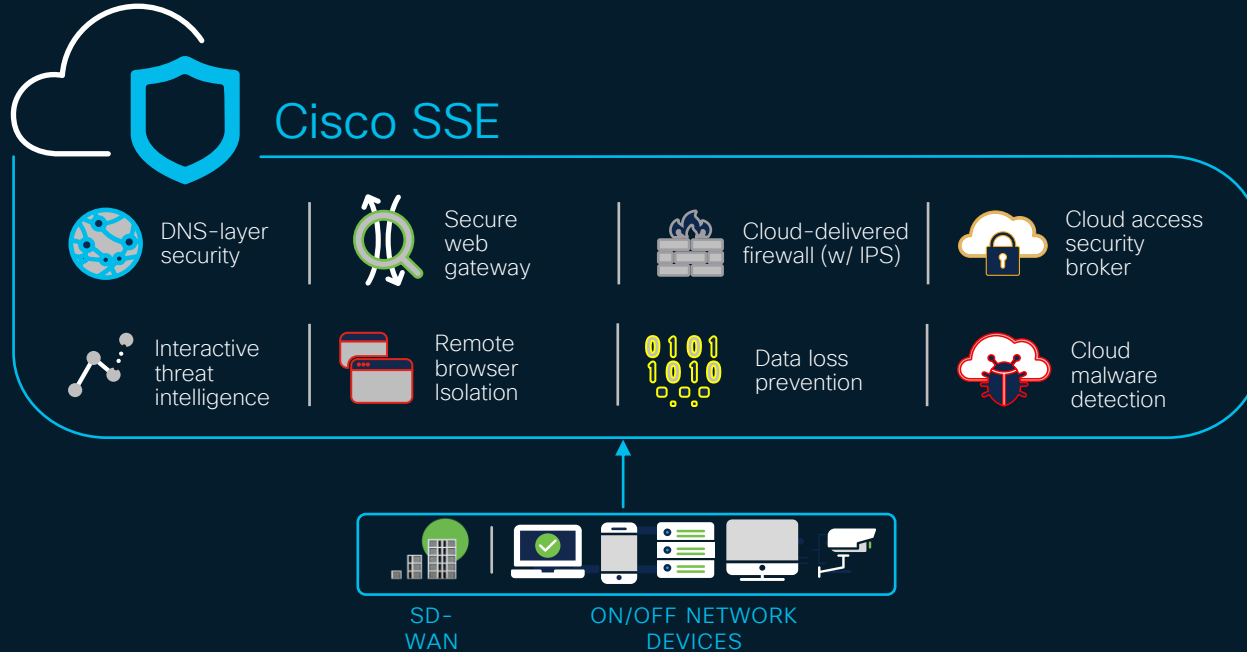
Decentralised

## Security

Protect at data centre, cloud, and branch edge



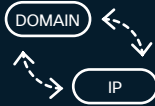
# Why Cisco SSE for Secure Internet Access?














# Why Cisco SSE for Secure Internet Access?

- Single dashboard to rule them.
- Easy to deploy, adopt and protect.
- Threat detection efficacy.
- End to end visibility and protection.

# Multi-faceted Threat Intelligence



-  1. Lexical  
Live DGA prediction
-  2. Anomaly detection  
Newly seen domains
-  3. DNS tunnelling
-  4. Graph-based  
Co-occurrence model

-  Botnet 1 | 2 | 4
-  Crimeware 3 | 4
-  Exploit Kit 2 | 4
-  Phishing 1 | 2 | 4
-  Ransomware 2 | 4
-  Spam 2 | 4
-  Trojan 2 | 3 | 4

Secure  
Access



Investigate



# Theme of this session

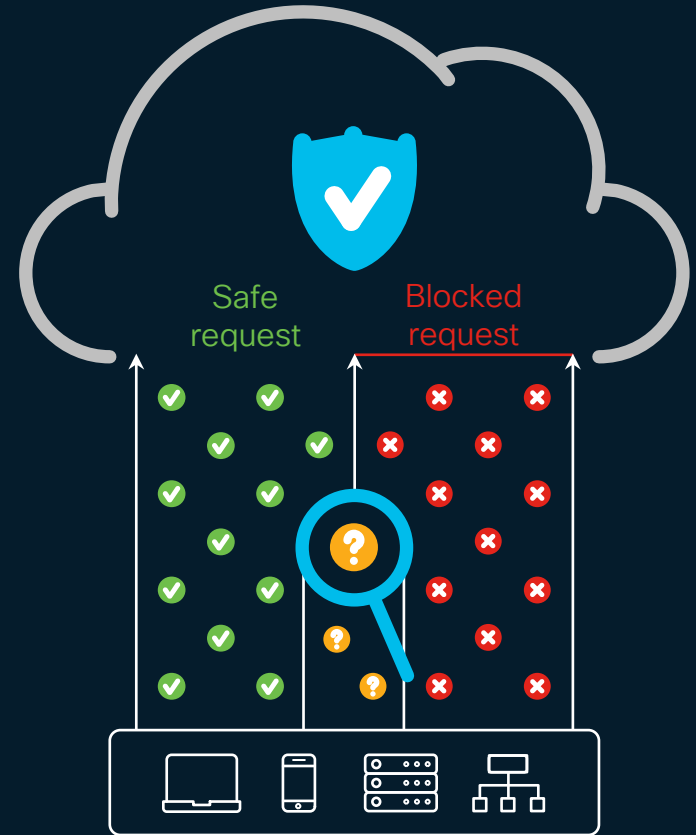
- Ease of deployment, adoption and protection.

DNS! DNS! DNS!



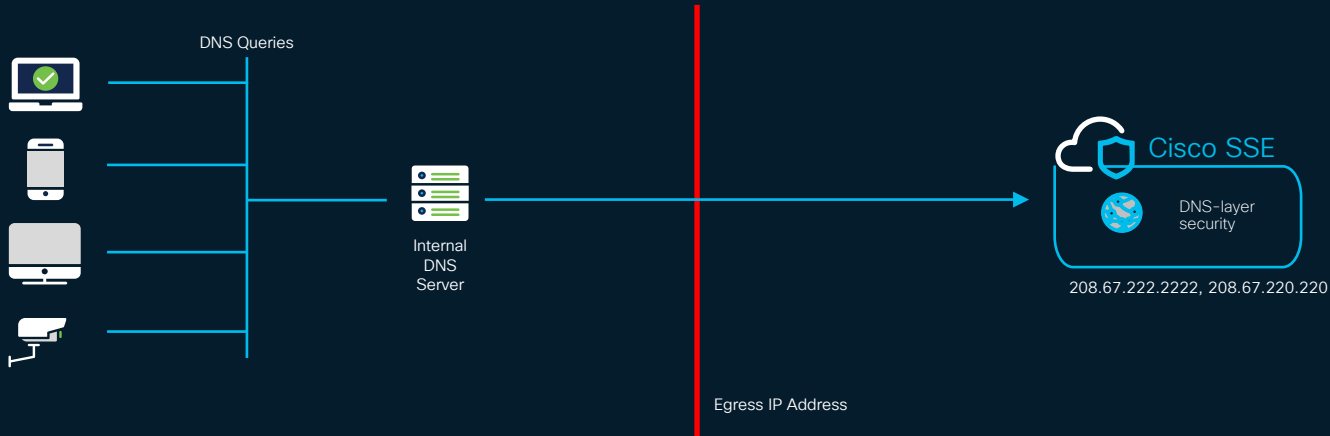
# DNS is simple, but effective!

- Everything uses DNS, web and non-web.
- Extends protection to areas where it may not be easy to inject:
  - a proxy
  - a firewall
- Network segment reachability.
  - Security Cameras, Sensors, Badge Scanners.
- Cleans the pipe.
  - Block unwanted traffic like advertisement.



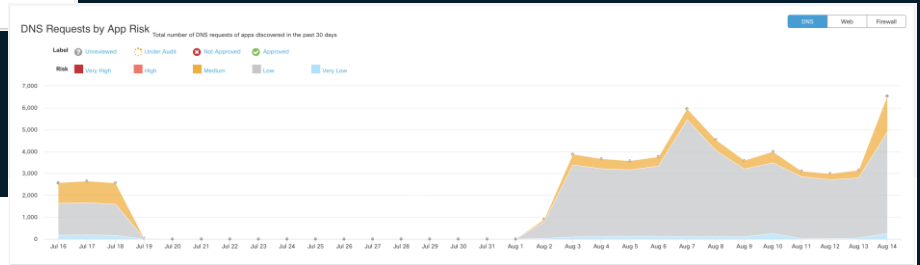
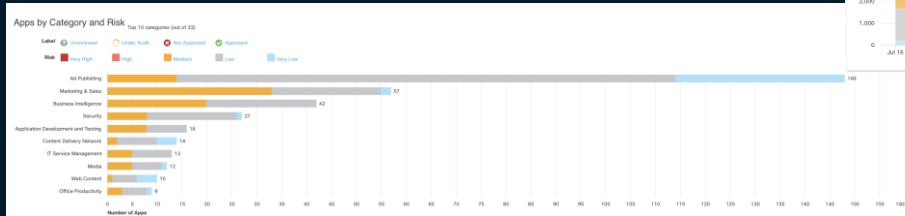
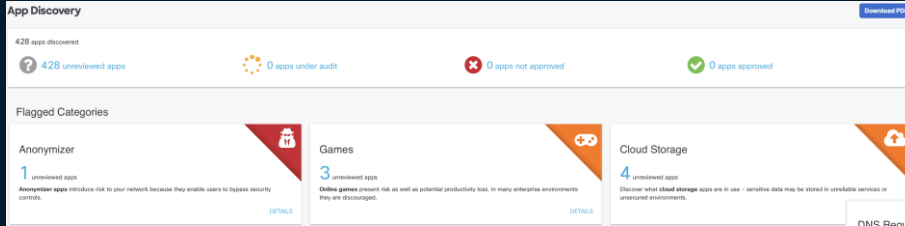
# Deploy, adopt and protect

- 2 steps to deploy, adopt and protect your network.
  - Register egress public IP address in SSE.
  - Point internal devices to SSE DNS servers, 208.67.222.222 and 208.67.220.220.



# Shadow IT detection, is it really CASB thing?

- Do you really need a CASB to detect risky applications?



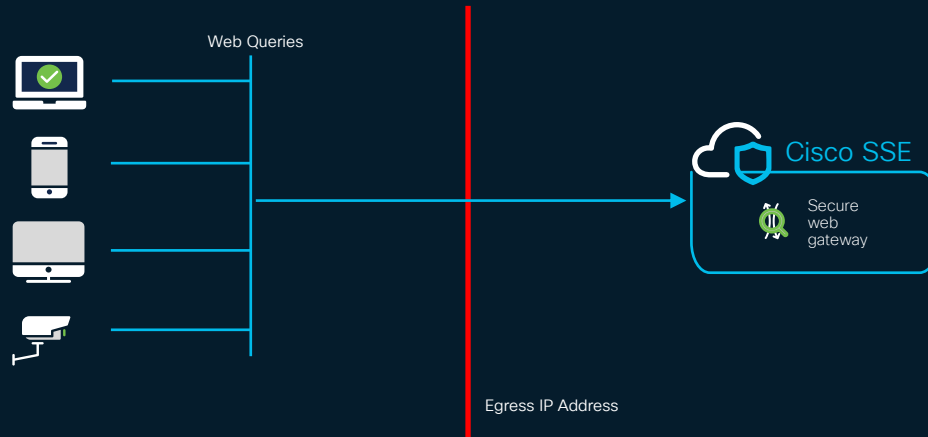
May the proxy be with  
you!

# A true proxy in the cloud

- Proxy designed for the cloud.
- With extensive granular features.
  - Anti-Virus and Anti-Malware scans.
  - Sandboxing to detect zero-day vulnerabilities.
  - Data Loss Prevention built in.
  - Remote Browser Isolation.
  - Application Visibility with granular Control.

# Deploy, Adopt and protect

- 2 steps to deploy, adopt and protect your network.
  - Register egress public IP address in SSE.
  - Point internal devices to SSE proxy.



What can the proxy do for me?



# Malware Sandboxing

- Ability to detect hidden threats in files that are being downloaded
- A set of new or higher risk files are placed in a sandbox environment and checked for malicious activity/content
  - Alerts posted on files that show bad activity
  - Secure Access threat intelligence is updated for that file

**File Analysis**  
Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

**File Inspection**  
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

**Threat Grid Malware Analysis**  
Analyze files for malicious behavior using advanced sandboxing with static and dynamic threat intelligence

Sandbox Region: Europe

CANCEL SET & RETURN

**File Retrospective**

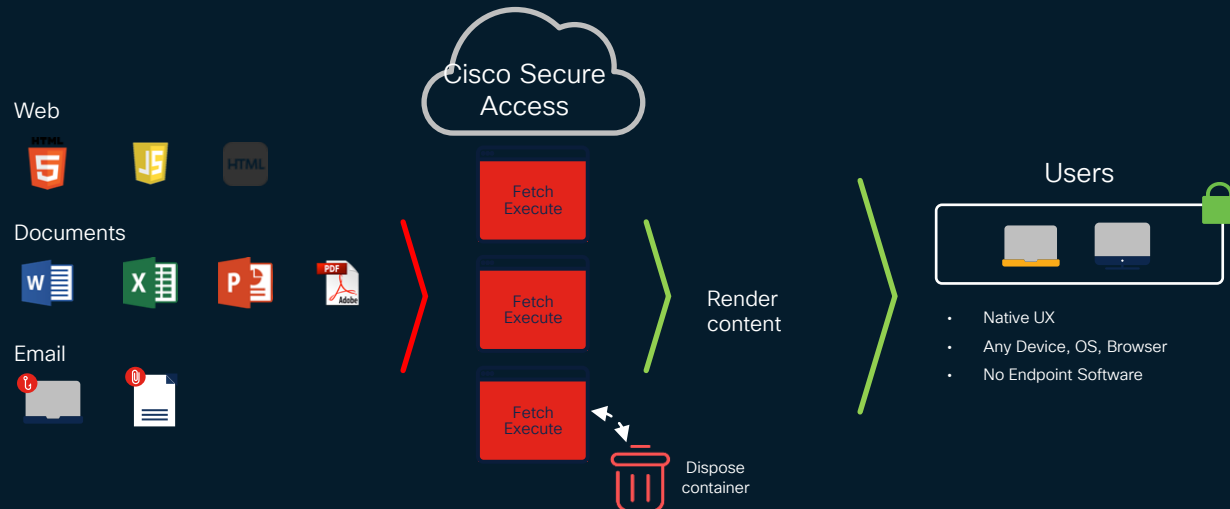
Recent Retrospective Events

SHA256	Threat Score	Malware Name	Date Detected
7638fd4a9cd3ea5fa88f9958da6e6e745b2931b96ceca...	100	W32.7638F6D4A9-100.SBX.TG	Jul 30, 2019 at 3:22 AM
526b2cad716f7dc1e568d5e68b8a251d19e129308006b...	100	W32.526B2CAD71-100.SBX.TG	Jul 27, 2019 at 3:23 AM
1a27fd68d61964ddc13a62a75b15b7c94978def0b014...	100	W32.1A27FDF68D-100.SBX.TG	Jul 26, 2019 at 3:24 AM
49ade947bb9de7ce36f9735f90758d8425f939c2ce84b6...	100	W32.49ADE947BB-100.SBX.TG	Jul 25, 2019 at 4:31 AM
f9f23288188bc1a959e890084cc685db4ff9c50b95a52a...	100	W32.F9F2328818-100.SBX.TG	Jul 24, 2019 at 3:26 AM

1 - 5 of 32

# Remote Browser Isolation (RBI)

- Spins up browsers in containers, in the cloud.
- Web contents are inspected in the cloud.
- Web contents do not get to the endpoint



# Tenant Control



Select the instance(s) of core SaaS applications that can be accessed by all users or by specific groups/individuals

Global Allowed Enterprise Apps

Select the cloud app or suite you wish to approve:

- Microsoft Office365  
OneDrive, Word, PowerPoint, Excel, Outlook, and more
- Google G Suite  
Gmail, Hangouts, Calendar, Drive, Docs, Sheets, and more
- Slack  
Slack for Enterprise

- cisco.com  
Corporate instance
- Deb Smith  
Personal instance
- Bob Jones  
Personal instance

## Key use cases

### Security

Ensure, sensitive data is created and stored in approved instances of cloud apps

### Productivity

Only provide access to corporate instances of core SaaS apps

# Granular SaaS Application Control

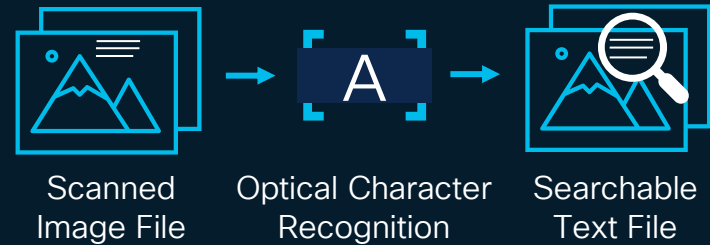
- Block posts/shares to social media apps
- Block attachments to webmail apps
- Block uploads to cloud storage, collaboration, office productivity, content management, and media apps



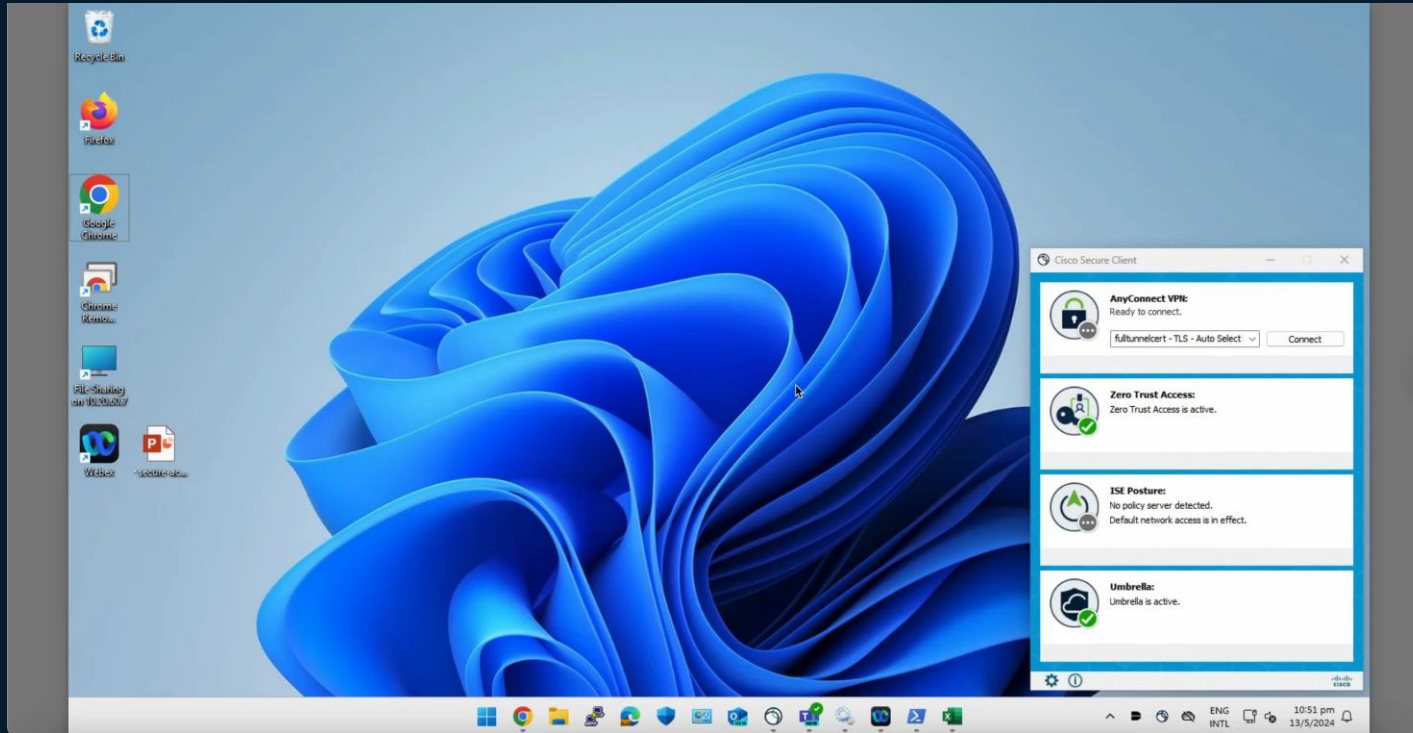
# Optical Character Recognition

OCR scans text contained in image files, or within embedded images in documents, to prevent exfiltration of sensitive data.

- Enabled for all Umbrella DLP customers and applies to all DLP rules by default, at no extra cost
- Automatically extracts text from images and searches for DLP violations per DLP rules.
- Supports JPEG, JPG, PNG, GIF, TIFF and EMF file types
- Applies to data-in-motion using Real Time DLP and data-at-rest using SaaS API DLP



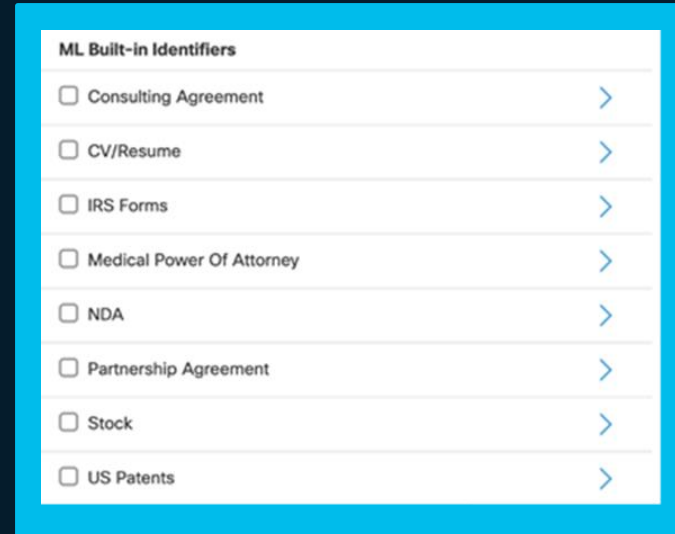
# Optical Character Recognition – Demo



# Machine Learning based Document Classification

**ML-based Document Classification** allows users to select from predefined, pre-trained document types instead of building complex data classifications from scratch.

- Enabled for all Umbrella DLP customers at no extra cost
- Available in new “ML Built-in Identifiers” section (see image →)
- Supports numerous types of documents, such as consulting agreements, resumes, IRS forms, medical powers of attorney, non-disclosure agreements, partnership agreements, stocks, and US patents
- Applies to data-in-motion using Real Time DLP and data-at-rest using SaaS API DLP



# Data Loss Protection (DLP) modes

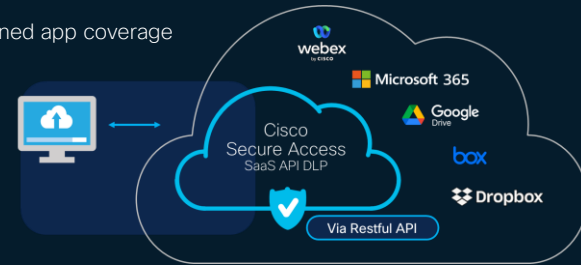
## Real Time DLP

- Works via Umbrella Secure Web Gateway (SWG) proxy.
- Scans web traffic **inline** for real-time enforcement.
- All application coverage: sanctioned and unsanctioned.



## SaaS API DLP

- via cloud APIs for data at rest, without SWG proxy
- Scans web traffic **out-of-band** with near real-time enforcement
- Sanctioned app coverage



One management interface

Many crossover capabilities:

Exact Data Matching (EDM) · Indexed Document Matching (IDM) · Dictionary and Pattern Matching  
Optical Character Recognition (OCR) · Machine Learning-based Document Classification  
Policy Inclusion and Exclusion · Scheduled Reporting and Ad-hoc Reporting · Built-in Identifiers and Classifications

# In-Line DLP

- Data Loss Protection for a distributed workforce.
- 1,200 built-in data classifiers.
- 13 AI powered classifiers.
- Custom data classifier, with regex support.
- OCR support.
- Exact Data Matching (EDM)
- Indexed Document Matching (IDM)



Reporting / Additional Reports  
Data Loss Prevention

FILTERS Search... Advanced

89 Total Events

Detected	Identity	File Name	Destination	Data Classification	Action	Type	Size	File Name	Content
Jun 2, 2021 at 10:01 AM	sig1-ec2-east-1b	Content	Dropbox	4 Matches Shaun DLP	Block	text/plain	31.0 B	Detected	
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	Destination URL	dl-web.dropbox.com
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	Rule Triggered	Shaun DLP Demo
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	Application	Dropbox
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	Classification	
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	1 Match	Social Security Number (US) - Lenient XXXXXXXX-4264
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	1 Match	Credit Card Number - Lenient XXXXXXXXXXXXXXXX068
Jun 2, 2021 at 9:23 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	1 Match	Social Security Number (US) - Moderate XXXXXXXX-4264
Jun 2, 2021 at 9:22 AM	sig1-ec2-east-1b	Content	WeTransfer	4 Matches Shaun DLP	Block	text/plain	31.0 B	1 Match	Credit Card Number - Moderate XXXXXXXXXXXXXXXX068
Jun 2, 2021 at 9:21 AM	sig1-ec2-east-1b	Content	Salesforce Lightning	2 Matches Shaun DLP	Block	text/plain	11.0 B		

# SaaS API DLP

- Same as In-Line DLP but using API.
  - Data Loss Protection for a distributed workforce.
  - 1,200 built-in data classifiers.
  - 13 AI powered classifiers.
  - Custom data classifier, with regex support.
  - OCR support.
  - Exact Data Matching (EDM).
  - Indexed Document Matching (IDM).
- Detect AND Remediate.



# Exact Data Matching (EDM)

- This is for structured data.
- Generates a fingerprint of the structured data.



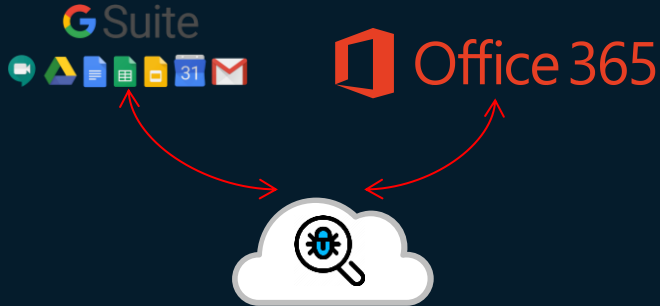
# Index Document Matching (IDM)

- This is for unstructured data.
- Generates a fingerprint of the document.



# Cloud Malware

- Takes the concept of SaaS API DLP, but:
  - Instead of checking for data violation, it checks for malicious files.
- Detect AND Remediate.



The screenshot displays the Cisco Cloud Malware reporting interface. At the top, it shows 'Reporting / Additional Reports' and 'Cloud Malware'. The dashboard provides a summary of scan results:

- Total files scanned: 63,916 (Scan complete.)
- Platforms: Box
- Malware found: 268
- Users with malware: 17

Below the summary, there are filters for Platform (Dropbox, Box, Webex Teams), Severity (High, Medium), Exposure (Public, Organization, Domain, Group, Private), and Status. A search bar for file names is also present.

The main section, titled 'Malicious Files', contains a table with the following data:

Platform	File Name	Severity	Detected	Exposure	Status	De:
Box	527KBFile.zip	high	Aug 14, 2019 at 8:40 AM	Private	Quarantine in progress	PUA
Box	jptrmpd.exe	high	Aug 14, 2019 at 8:40 AM	Private	New	See Full Details Quarantine
Box	eicar.txt	high	Aug 14, 2019 at 8:40 AM	Private	New	Win
Box	java_bad5	high	Aug 14, 2019 at 8:40 AM	Private	New	Silv
Box	silverlight_bad3	high	Aug 14, 2019 at 8:40 AM	Private	New	W3
Box	donk001-01.exe	high	Aug 14, 2019 at 8:40 AM	Private	New	

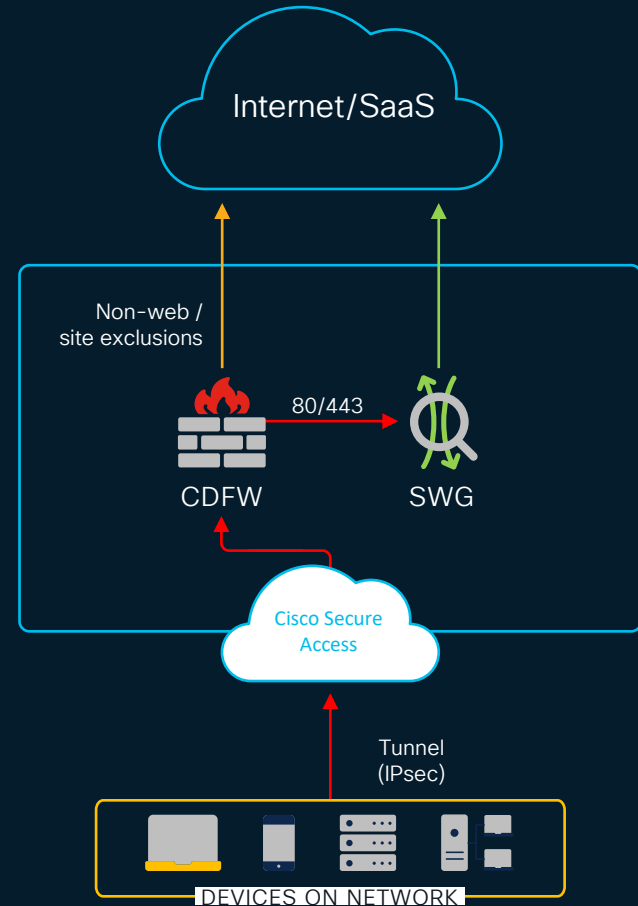
# Firewall in the cloud

CISCO *Live!*



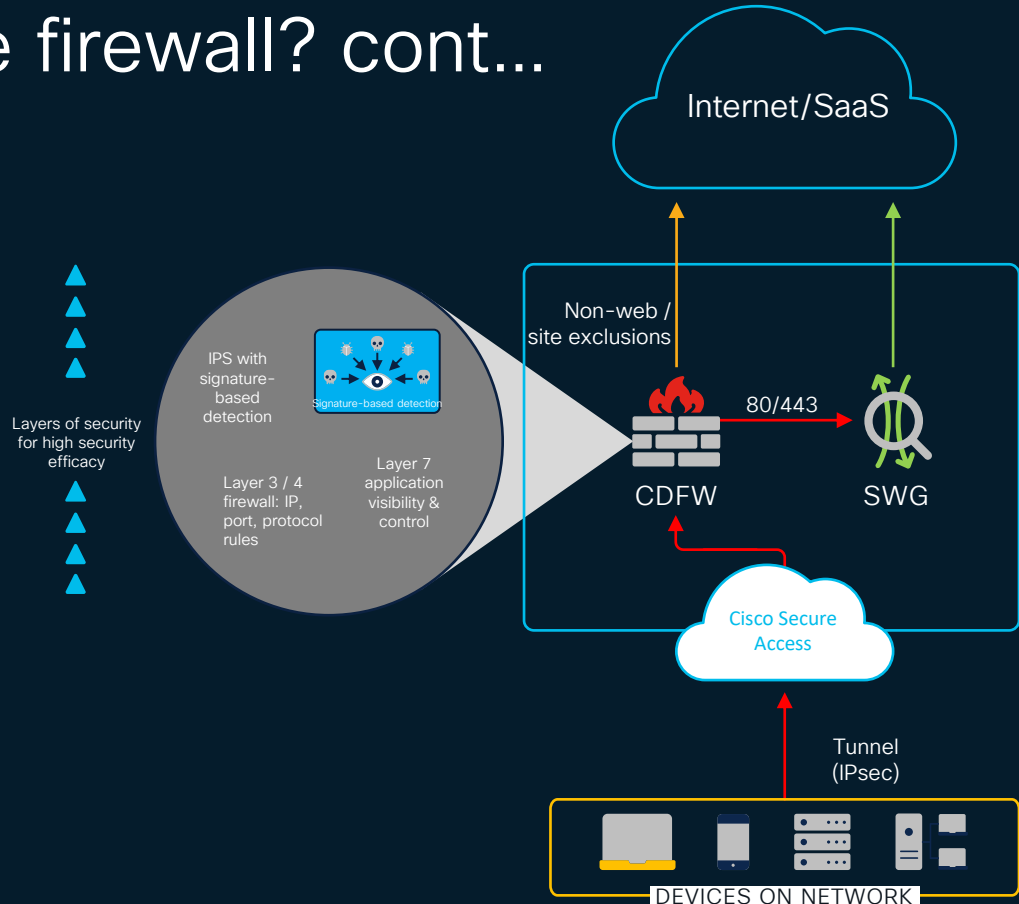
# Why do I need the firewall?

- L3-4 protection.
- Block non-web access to the internet.
- IPS/IDS.



# Why do I need the firewall? cont...

- L7 and IPS protection.
- Application control.
- Applications are sneaky.
- Connection flow:
  - Application tries to resolve application server FQDN
    - DNS blocks it.
  - Application then falls back to IP address on port 80/443
    - SWG blocks it.
  - Application then attempts to connect using IP address and random port
    - CDFW is to the rescue.



# IPS/IDS

- Powered by the Snort engine.
- 50K+ signatures included.
- Option to run in detection mode or prevention mode.
- Decrypt traffic for inspection.
- Dynamic inspection of web traffic

Connectivity Over Security	Prevention	477 Block	112 Log Only	50109 Ignore
Balanced Security and Connectivity Default IPS Profile	Prevention	9380 Block	488 Log Only	40830 Ignore
Security Over Connectivity	Prevention	22008 Block	760 Log Only	27930 Ignore
Maximum Detection	Prevention	39661 Block	1366 Log Only	9671 Ignore

Intrusion Prevention (IPS) Rule Defaults Enabled

Traffic will be decrypted and inspected based on the selected IPS profile. Transactions involving destinations on the [Do Not Decrypt List](#) will not be decrypted. [Help](#)

Profile: **Balanced Security and Connectivity** | Intrusion System Mode: **prevention** | Signatures: 9380 Block 488 Log Only 40830 Ignore

# Summary

- Multiple products with a **single dashboard**.
- **DNS** can reach network segments where it is **difficult to inject** a proxy or a firewall.
- **Granular internet access** control using the **proxy**.
- Control **non web internet traffic** using the **Cloud Delivered Firewall (CDFW)**.

# Keynote Deep Dives

Wednesday

10:30am - 11:30am



Experiences Amplified:  
How AI Can Fuel Better Employee and Customer Experiences

**Level 1**  
**Room 106**



Smart, Secure, Seamless:  
Transforming Experiences with Next-Generation Networking

**Level 2**  
**Room 204**



Harness a Bold New Era:  
Transform Data Centre and Service Provider Connectivity

**Level 2**  
**Room 203**



Securing User to Application and Everything in Between

**Level 2**  
**Melbourne Room 2**



Unlocking Digital Resilience through Unified Observability

**The HUB**  
**Centre Stage**

# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

---



Complete your surveys in the **Cisco Live mobile app**.

---



# Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC