



# Cisco Email a Cloud Security

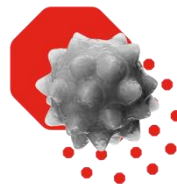
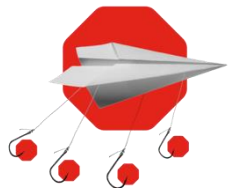
Layered Defenses For Comprehensive Protection

Milan Habrcetl, Cisco CyberSecurity Specialist  
mhabrcet@cisco.com  
9<sup>th</sup> March, 2021





Email is **still** the #1 threat vector



# Attackers use **multiple ways** to get in



## Business Email Compromise (BEC)

Estimated exposed losses due to BEC between 2016 and 2019 totaled \$26 billion.<sup>1</sup>



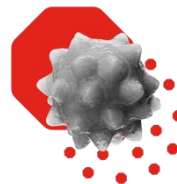
## Ransomware

Predicted to hit \$20 billion in 2021<sup>2</sup>



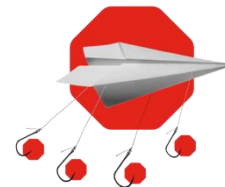
## Domain Compromise

54% of legitimate domains used in phishing campaigns<sup>3</sup>



## Malware

10.52 billion malware attacks in 2018<sup>4</sup>



## Phishing

27% of data breaches in 2019 involved the theft of credentials such as logins or encryption keys<sup>5</sup>

1. [Business email Compromise The \\$26 Billion Scam](#), Public Service announcement, Federal Bureau of investigation, September 10, 2019

2. [2019 Cybersecurity Almanac](#)

3. [Cisco 2018 Annual Cybersecurity Report](#)

4. [2019 SonicWall Cyber Threat Report](#)

5. "Forrester @ Best Practices for Phishing Prevention, September 30, 2019

Email threats cost organizations time and money. Organizations need complete coverage and should assess if their SaaS email providers have left them exposed.

Customers say an effective email security solution should include:



Malware Protection



Data Encryption



Phishing Protection



Email Authentication



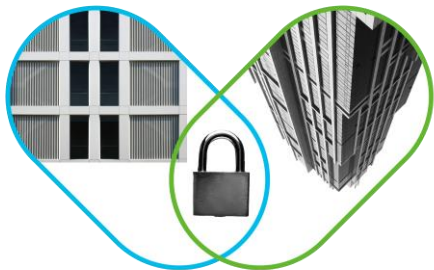
Continuous Monitoring



Threat Intelligence

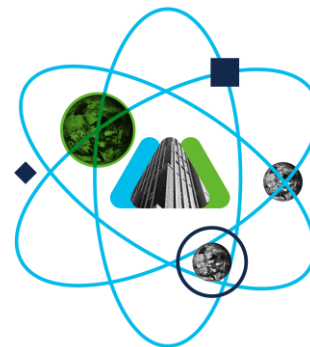
(<https://www.cisco.com/c/dam/en/us/products/se/2018/11/Collateral/esg-info-email-security.pdf>)

# Cisco Email Security



## Inbound

- Cisco Email Security with Advanced Malware Protection and Threat Grid
- Cisco Advanced Phishing Protection



## Outbound

- Cisco Email Security with Data Loss Prevention and Encryption
- Cisco Domain Protection

# SecureX threat response and Email Security

## Email Security integration



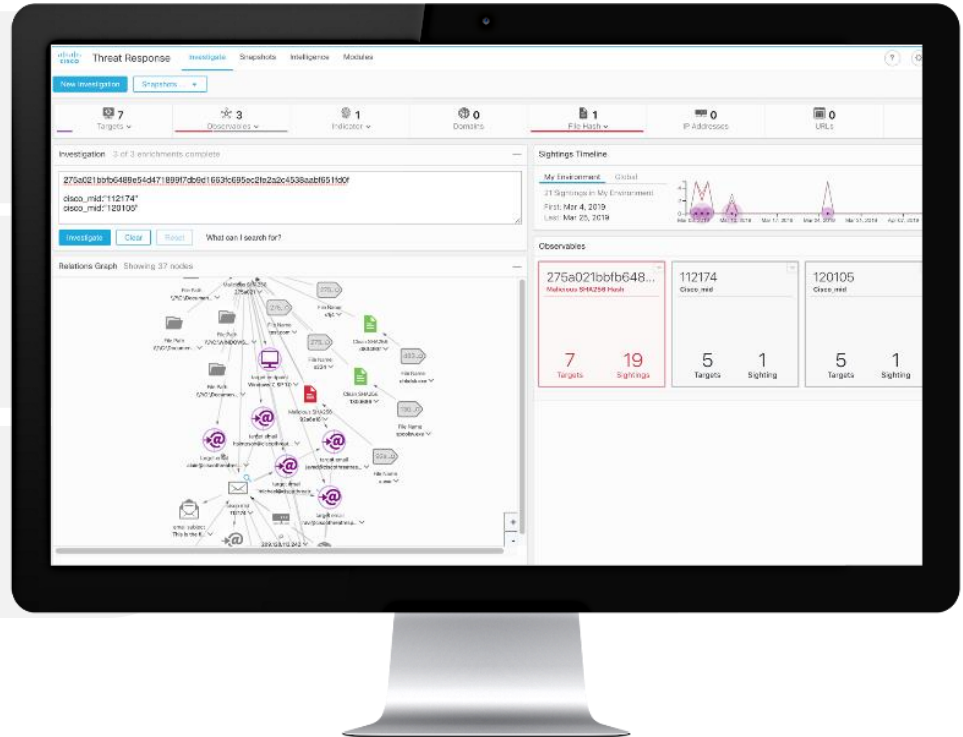
Understand email as a threat vector by visualizing message, sender, and target relationships in the context of a threat



Search for multiple email addresses, subject lines, attachments at once to understand how a threat has spread



Expand visibility for your SOC into email and other threat artifacts



# Cisco Email Security is the leader because...

## Spam and threat filtering

- IP Reputation Filtering
- Sender Domain Reputation Filtering
- Connection Controls
- External Threat Feeds
- Anti-Spam

## Malware and attachment control

- Antivirus
- Macro and File Type filtering
- Bad URL document scanning
- Safe Print
- Outbreak Filters

## Anti-spoofing

- DMARC, DKIM, SPF analysis
- DANE support
- Forged Email Detection
- Domain Protection

## Advanced Malware Protection (AMP)

- File Reputation
- File Sandboxing
- File Retrospection
- File Remediation

## Anti-phishing and malicious URL detection

- URL Filtering
- Content Filters
- Outbreak Filters
- Web Interaction Tracking
- Advanced Phishing Protection

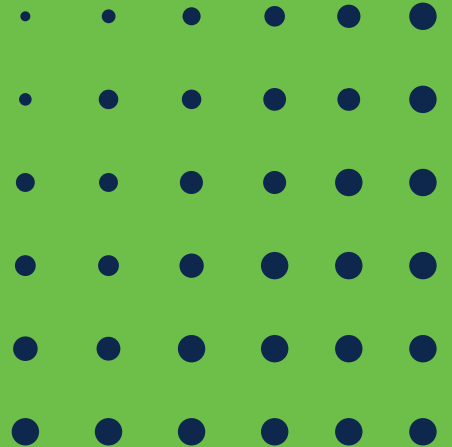
## Threat visibility and investigation

- Secure X Cisco Threat Response integration

## Outbound control

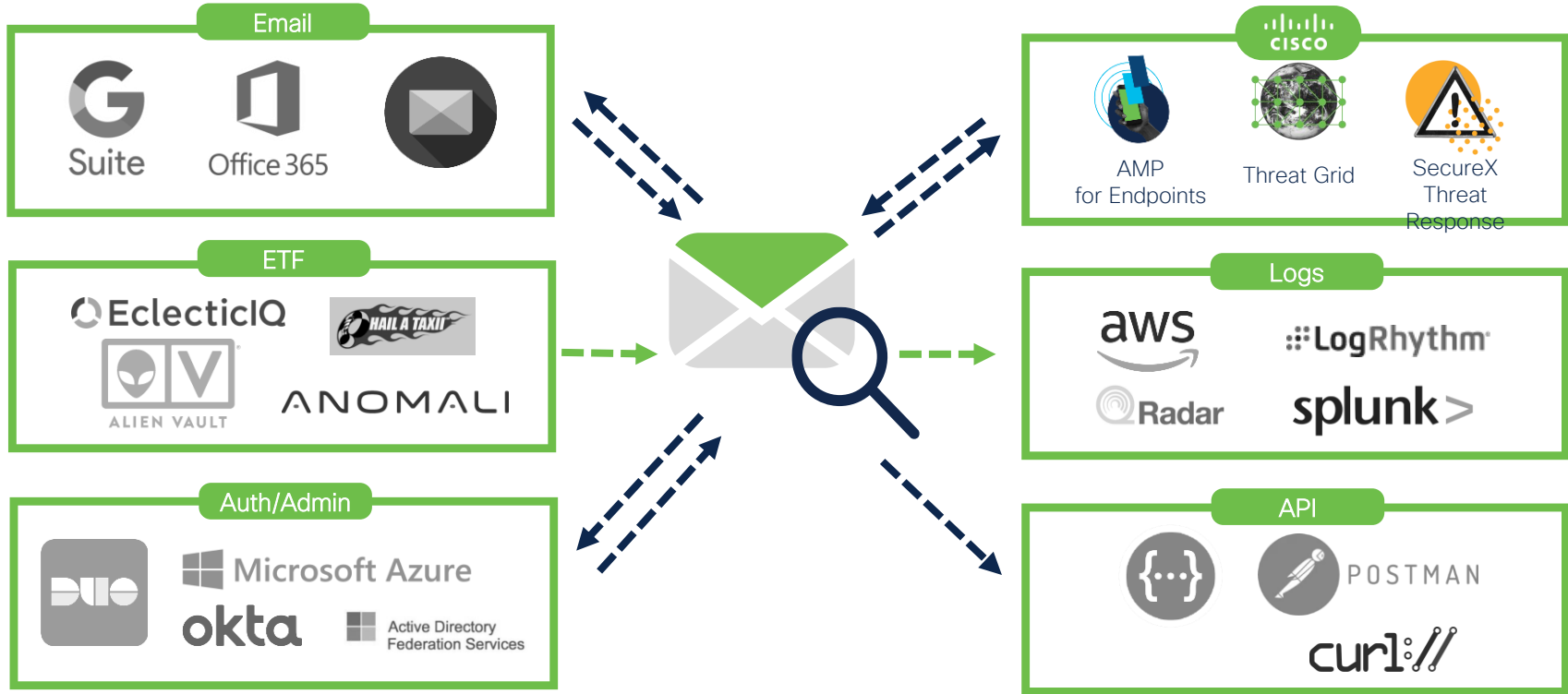
- Data Loss Prevention
- Encryption
- Rate Limiting

# Integrations





# Cisco Email Security and integrations



# Cisco Email Security and Cisco integrations



AMP for Endpoints



Threat Grid



SecureX Threat Response

AMP for Endpoints Dashboard

**New AMP for Endpoints Windows Connector**  
Version 3.0.5.7.403 is now available. Learn more in the Official Release Notes

**Computers**

- 9 Computers
- 2 Not Seen in Over 7 Days
- 0 Need An Update
- 3 Need Connector Update
- 0 Computers With Faults

Filters: No filters applied

Name	Type	Started	VM	Threat score	Tags	User	State	Matched on...
2019100102.pdf	pdf	10/1/2019 4:03	win7-ad4	100		asa-0w0c0-20030ad-377-4303-378a-614c20302c4d0		analysis.artifact...

Threat Grid Dashboard

Query: 7ba820-684029e054701e464b-436a35a7a3d8a4641d

Match By: SHA-256

Date Range: Last 30 Days

Scope: All samples

Access: All, Private, Public

Regularity: low

UPLs

Name	Type	Started	VM	Threat score	Tags	User	State	Matched on...
2019100102.pdf	pdf	10/1/2019 4:03	win7-ad4	100		asa-0w0c0-20030ad-377-4303-378a-614c20302c4d0		analysis.artifact...

Threat Response Investigate

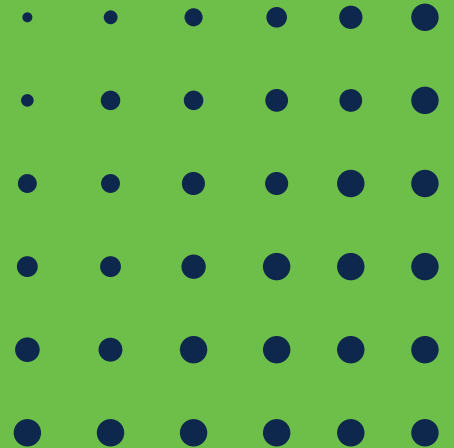
Investigation: 1 of 1 enrichments complete

aha256-7ba820-684029e054701e464b-436a35a7a3d8a4641d

Resolution Graph: Showing 12 nodes

```
graph TD
    Root[aha256-7ba820-684029e054701e464b-436a35a7a3d8a4641d] --> Node1[...]
    Node1 --> Node2[...]
    Node2 --> Node3[...]
```

# Deploying Cisco Email Security



# Cisco Email Security: deployment options

<http://cs.co/9009DdIRN>



## Cloud

Dedicated email security deployments in multiple resilient Cisco data centers provide the highest levels of service availability and data protection



## On-premises

The Cisco Email Security Appliance is a gateway typically deployed in a network edge outside the firewall (the so - called demilitarized zone)



## Virtual

A software version of the physical appliance runs on top of a VMware ESXi hypervisor and Cisco Unified Computing System™ (Cisco UCS®) servers



## Hybrid

With Cisco Email Security in the cloud Run on-premises and virtual Cisco Email Security in the same deployment

# Cloud Email Security (CES) datacenters



# New x95 hardware for ESA/SMA

 30%  
Performance Gain

C/M195 & C/M395 (1 RU Appliance)



<http://cs.co/C220M5>

ESA default AsyncOS release: 11-5-0-066

C/M695 & C/M695F (2RU Appliance)



<http://cs.co/C240M5>

SMA default AsyncOS release: 11-1-0-083

# Cisco Secure Web Appliance

Top-of-the-line defense for  
threats on the Internet

Jiří Tesař

Technical Security Architect



# Cisco Umbrella

Accelerate Secure Cloud Adoption



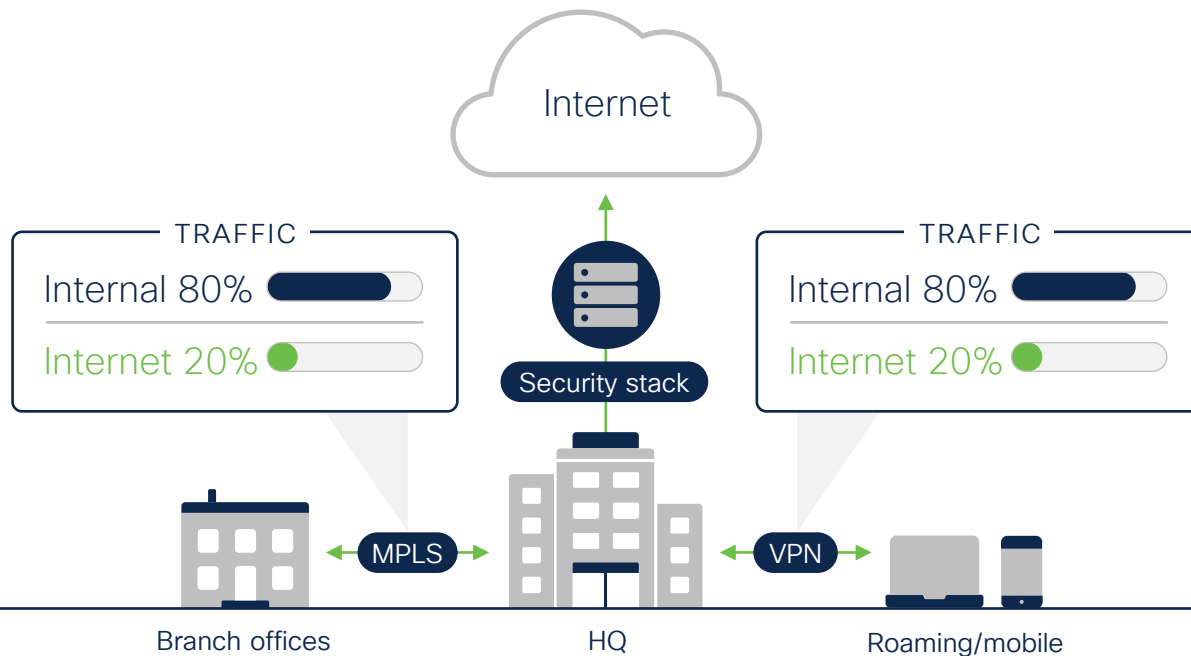


# Historic traffic flows

Led to the age of perimeter-based security and networking

**Network:**  
Centralized

**Security:**  
Single, on-premise  
security stack

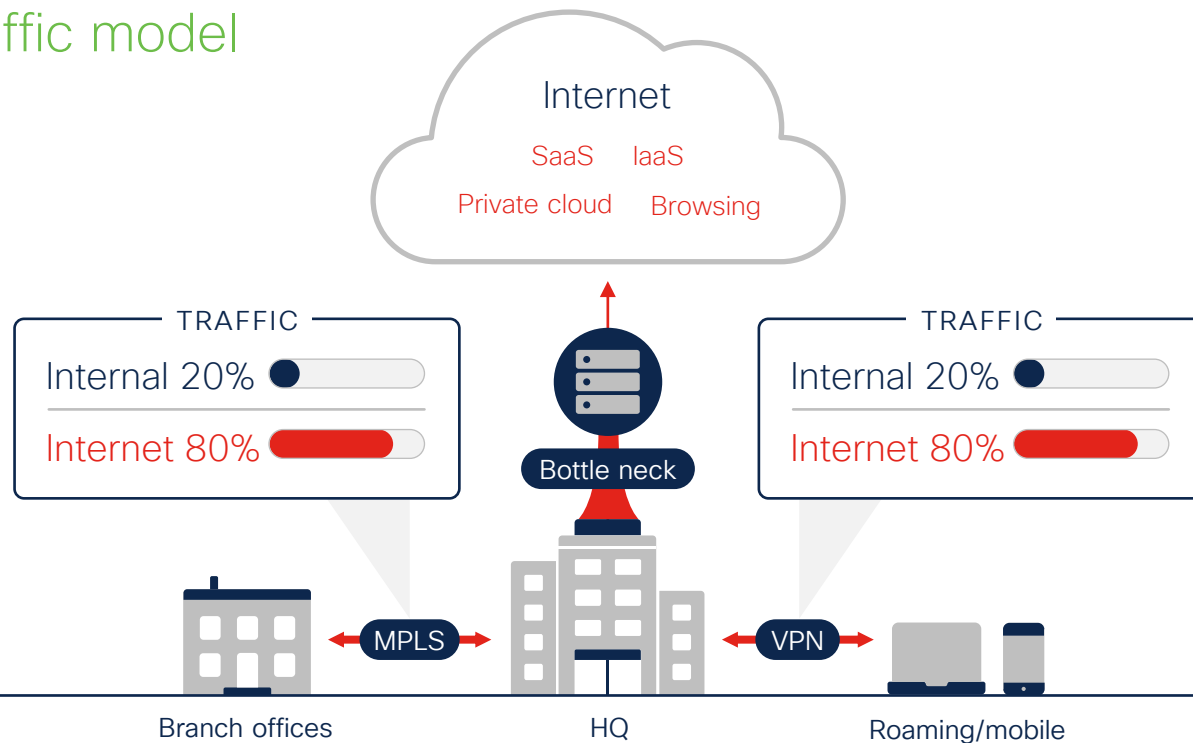


# Changes in the types of traffic and destinations

Have inverted the traffic model

## Problems:

- Costs
- Performance
- # Tools/vendors
- Integrations
- Maintenance



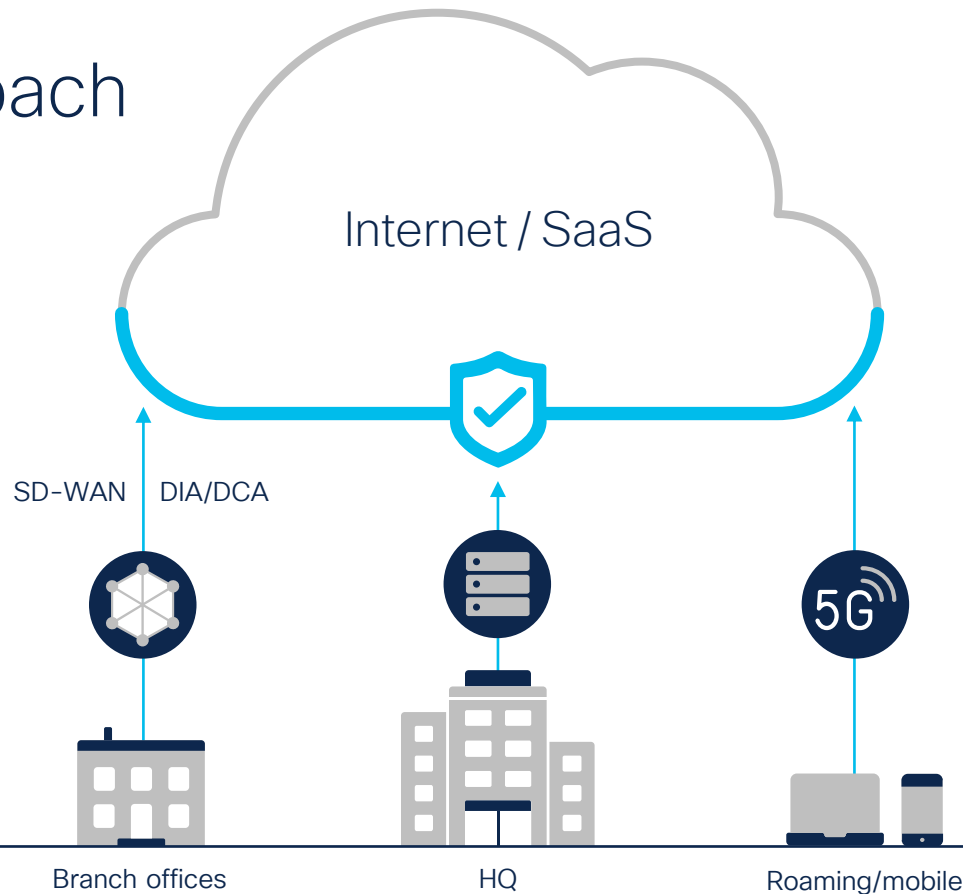
# A more modern approach

## Security:

Enforced at the cloud edge

## Network:

Optimized routing from anywhere to the cloud



# Cloud and network evolution

 Today's networks are decentralized

 Users and Apps have adopted the Cloud

 Security and networking are moving to the cloud too

80%

of orgs are shifting  
to direct internet  
access (DIA)

76%

of orgs use SD-  
WAN extensively  
or selectively

42%

of branch office  
security deployments  
take over a month

68%

of branch offices  
and roaming users  
were the source  
of compromise  
in recent attacks

# The typical first step to address these issues is to combine cloud-delivered security services

93%

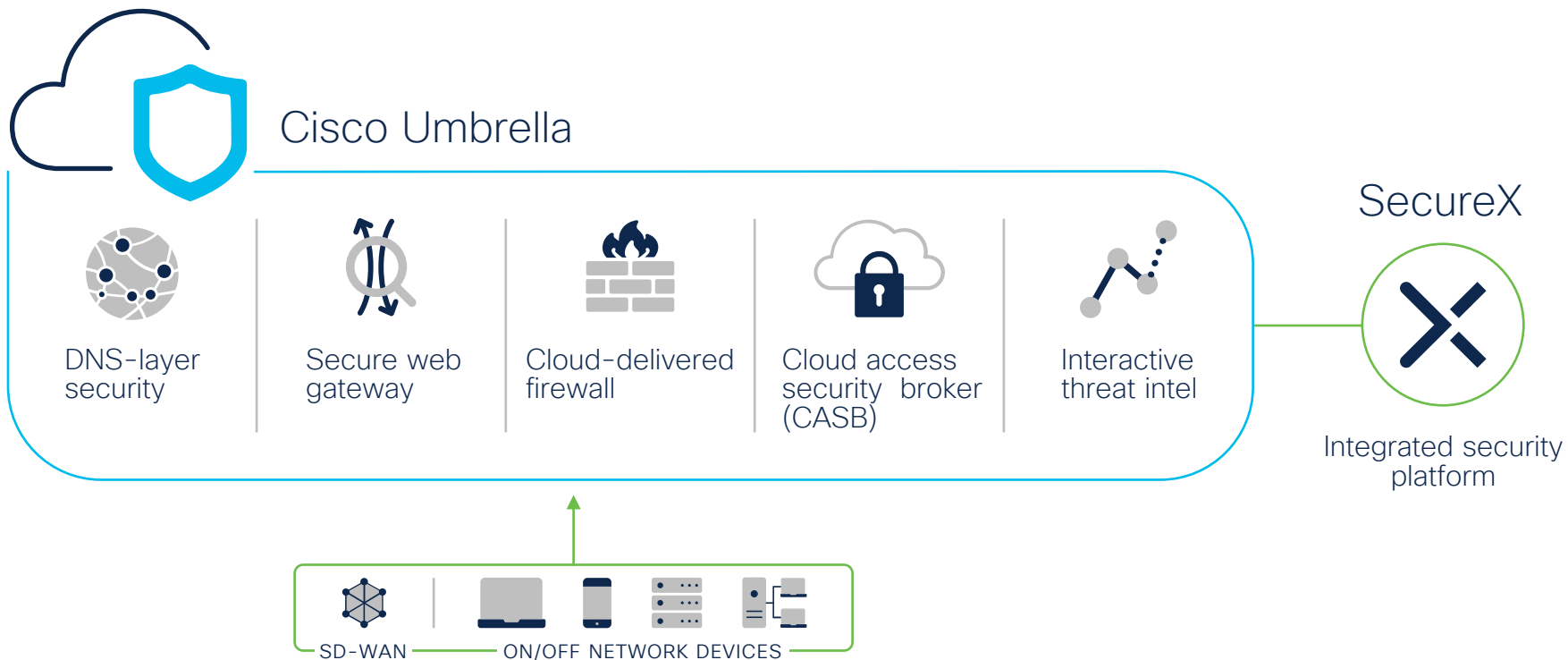
of orgs agree that moving security to the cloud has increased efficiency



76%

of orgs are looking for multi-function cloud security services

# The Umbrella multi-function security solution



# Cisco Umbrella: key capabilities

Secure onramp to the internet, everywhere



## Visibility

- On & off corporate network
- All internet & web traffic
- All apps
- All devices
- SSL decryption
- Shadow IT

## Protection

- DNS-layer security
- Web inspection
- File inspection
- Threat intel access
- Sandboxing
- Non-web traffic inspection

## Control

- URL block/allow lists
- Port & protocol rules
- Granular app controls
- Content filtering
- App blocking
- Tenant controls

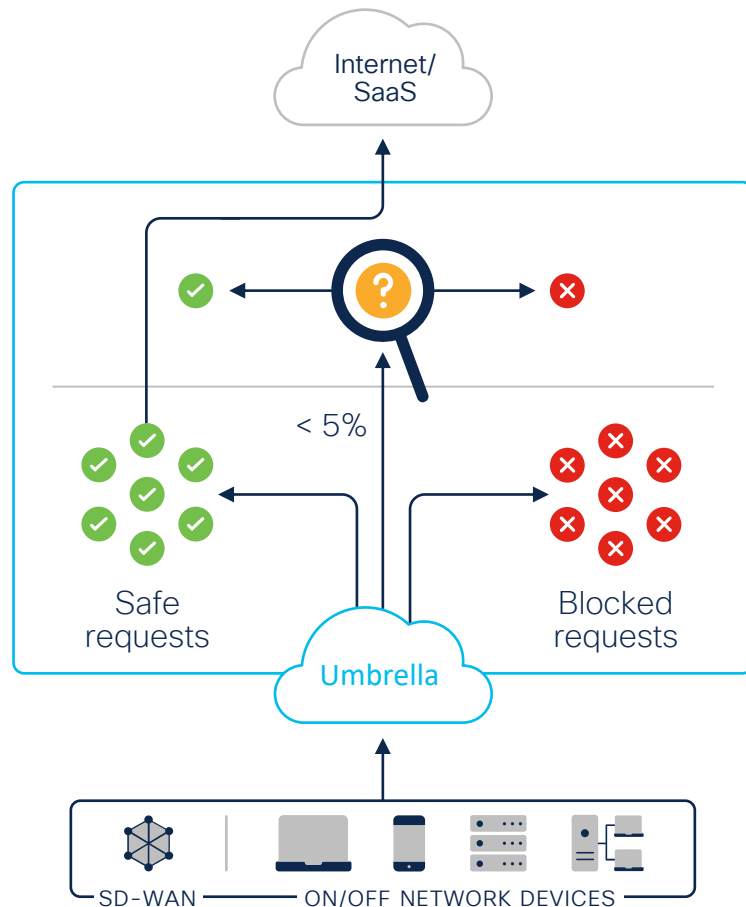


Built-in platform with Cisco SecureX and threat intelligence by Cisco Talos

# DNS-layer security

## First line of defense

- Deploy enterprise wide in minutes
- Block domains associated with malware, phishing, command and control callbacks anywhere
- Stop threats at the earliest point and contain malware if already inside
- Accelerate threat response with an integrated security platform
- Amazing user experience – faster internet access; only proxy risky domains





# Secure web gateway: full web proxy

## Deep inspection and control of web traffic

- ▶ Gain additional visibility via full URL logging and cloud app discovery
- ▶ Enforce acceptable use policy via app controls, content filtering, and URL block/allow lists



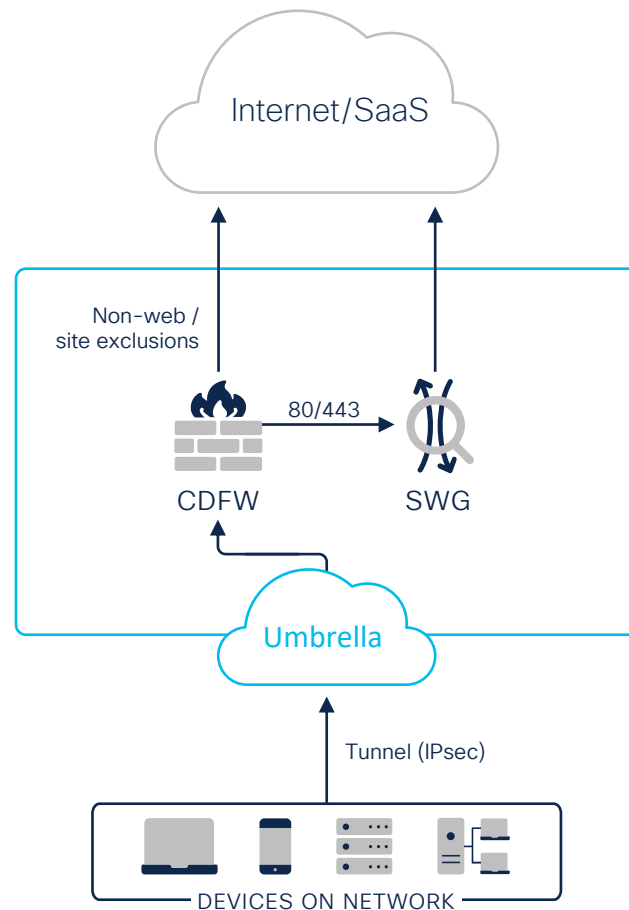
Full web proxy

- ▶ Extend protection against malware via SSL decryption and file inspection
- ▶ Enrich file inspection (with retrospective alerts) via malware defense and analytics

# Cloud-delivered firewall

## Firewall for the cloud edge

- Tunnel all outbound traffic to Umbrella
- Block high risk, non-web applications
- Centrally manage IP, port, protocol and application rules (layer 3, 4, and 7)
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination



# Enforcement that works together

Improved responsiveness  
and performance

## 1. DNS-layer security

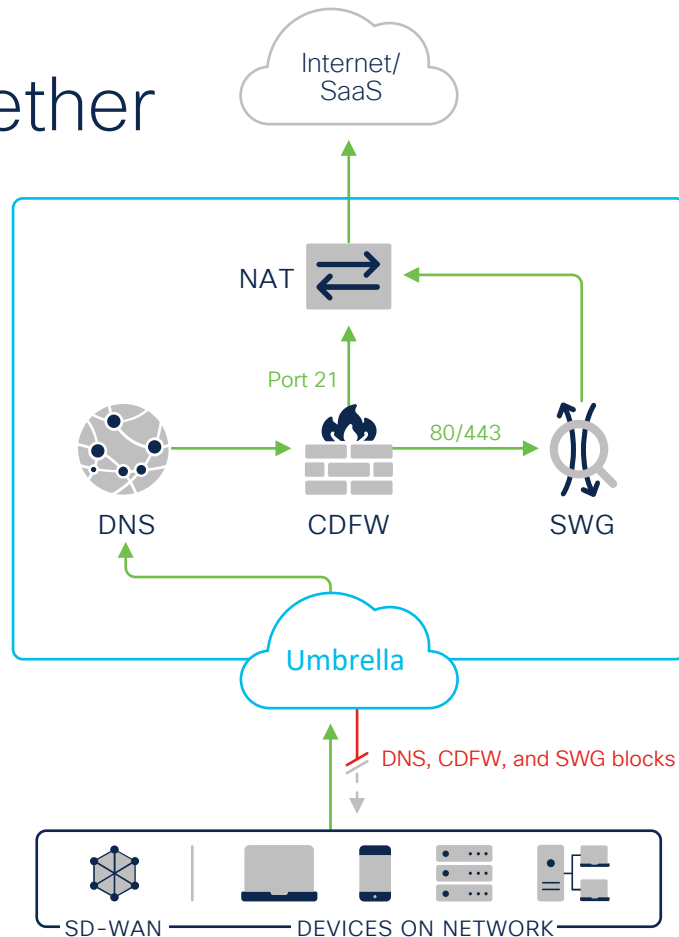
First check for domains associated with malware

## 2. Cloud-delivered firewall (CDFW)

Next check for IP, port, protocol and application rules

## 3. Secure web gateway (SWG)

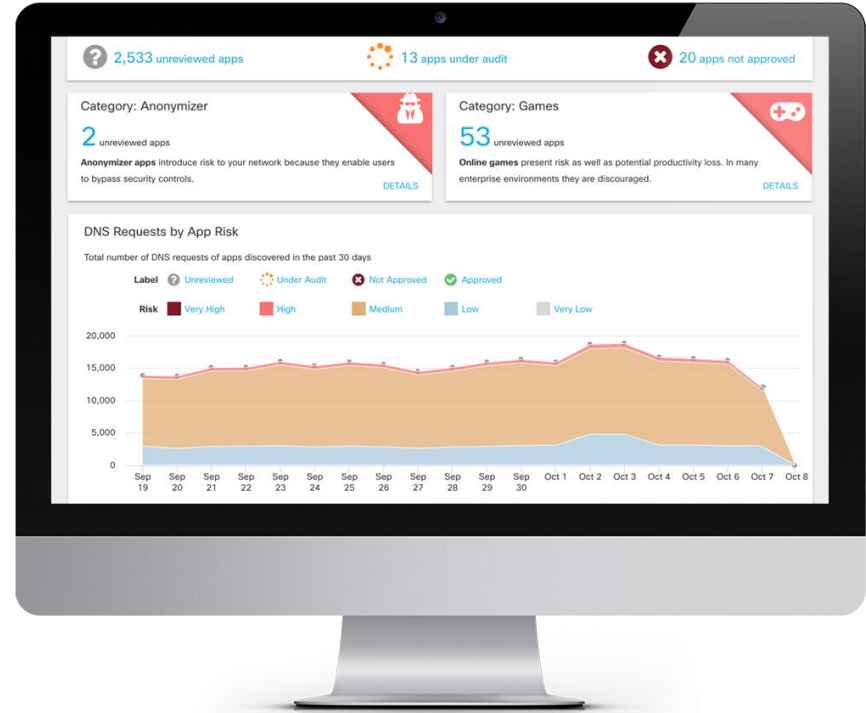
Final check of all web traffic for malware and policy violations



# CASB functionality

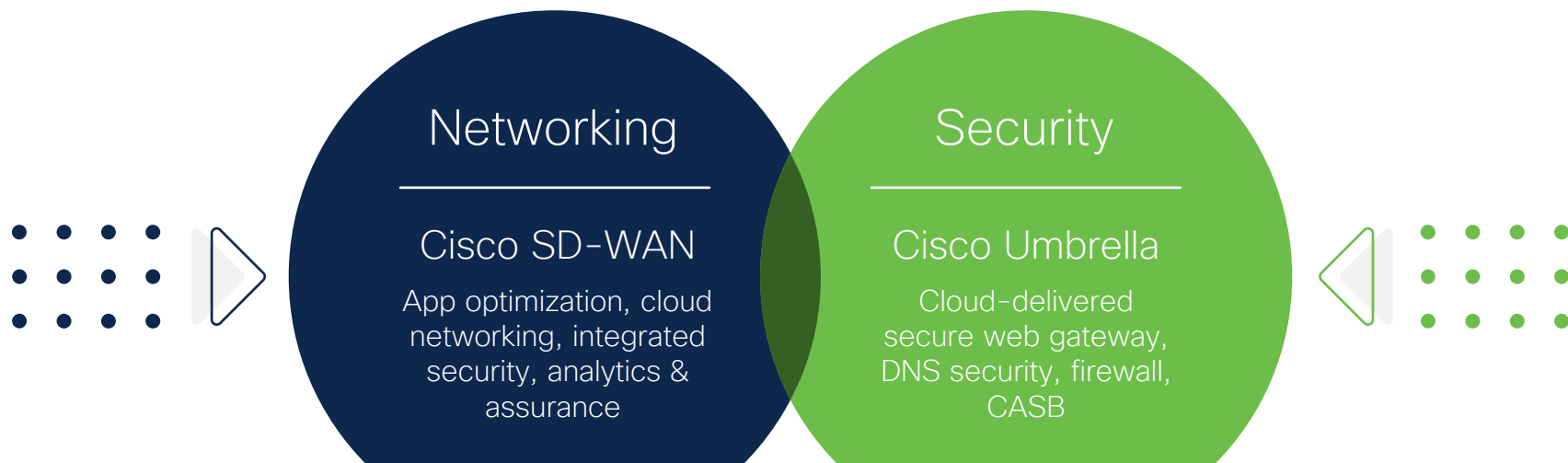
## Visibility control and protection

- A dashboard that highlights risky apps and activity trends
- Deeper visibility into cloud app usage
- Content and app control including specific app/URL block or allow policies
- Activity controls for popular SaaS apps (uploads/attachments/post/share)
- SecureX unifies visibility of security metrics related to cloud app usage
- Cloud malware detection for data at rest in core SaaS apps



# Cisco breaks new ground in SASE convergence

Unifying cloud security and networking with SD-WAN automation

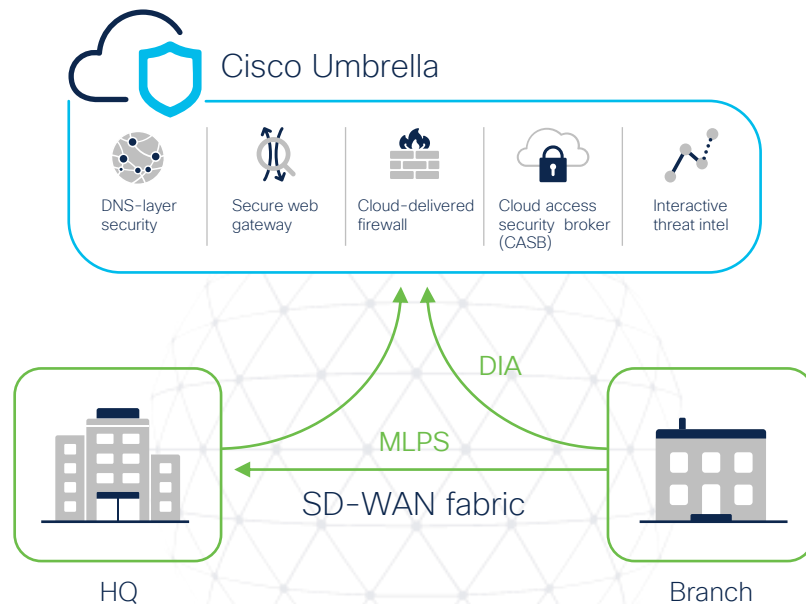


Highly available global cloud infrastructure | API-based, programmable architecture  
SecureX | Threat intelligence powered by Cisco Talos | 3<sup>rd</sup> party ecosystem

# Umbrella for Cisco SD-WAN

## Fast forward time to value with automated security

- **Hands-off automation:** deploy cloud security across thousands of branches in minutes
- **Top notch protection:** defend against threats at the branch with the leader in security efficacy
- **Simplified management:** single pane of glass across all offices and users
- **Deeper inspection & controls:** SWG and cloud-delivered firewall with IPsec tunnels

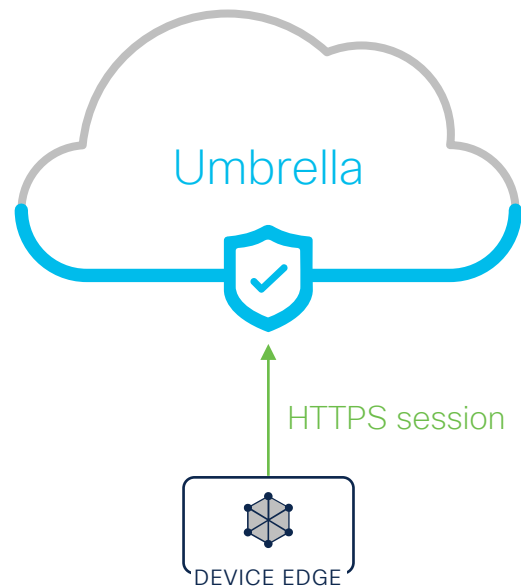


# Rapid onboarding: accelerates security and ROI

## Umbrella for Cisco SD-WAN

Deploying Secure SD-WAN now takes minutes not months:

- SD-WAN Edge devices are automatically registered to Umbrella
- No need to manually enter API keys
- Secure API key is automatically provisioned on the edge device via an HTTPS session



New DNA-Premier package

# Cisco Talos: the largest non-government threat intelligence organization on the planet

- ▶ **250+** full-time threat researchers and data scientists
- ▶ Analyzing **1.5 million** unique malware samples daily
- ▶ Blocking **20 billion** threats daily. More than **20x** any other vendor.

We **see more** so you can **block more** and **respond faster** to threats.





# Cisco SecureX

Praktická ukázka ESA-WSA-Umbrella

Jiří Tesař





# Cisco Tech Club Days



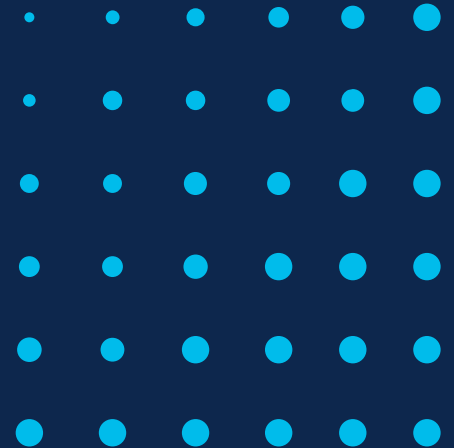
## Web Security

Jiří Tesař

Technical Solution Architect - Security

8.3. 2021

# Customer Challenges



# Web Page Consumption

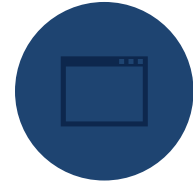
## Potential Threats



JAVA



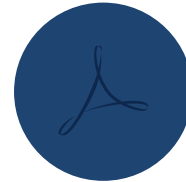
JPG



EXE



FLASH

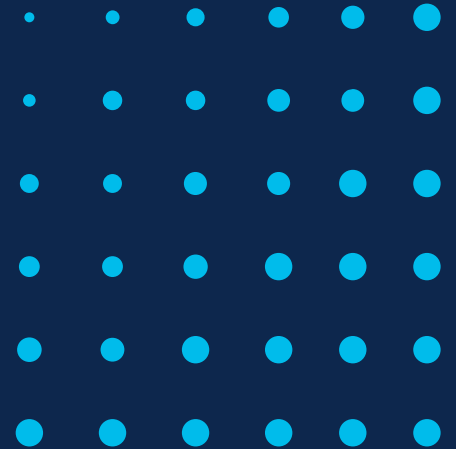


PDF

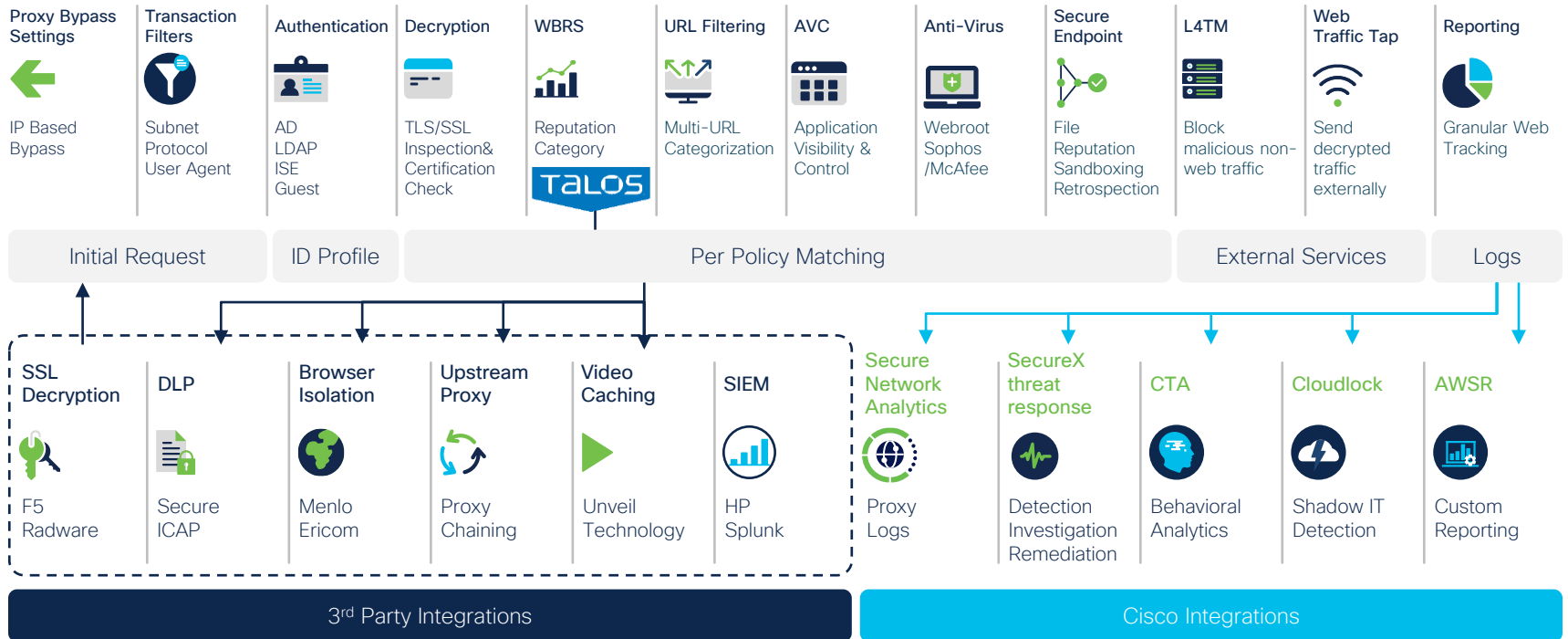


SCRIPT

# Web Security Solution



# Cisco Secure Web Appliance Pipeline



# WSA Priorities



## Simple and Flexible

- Enhance User Interface Flows to enable ease of use
- Provide seamless user experience



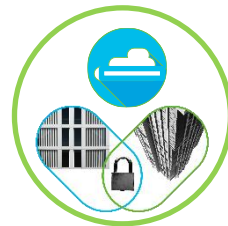
## Web Standards and Performance

- Support latest web standards



## Integrations

- Integration with other security products to offer overall security architecture
- Ease of deployment



## Virtual Strategy

- Enable usage in public, private data centers
- Provide customers with choice of VM's



## Threat Focus

- Provide excellent web security
- Continuous improvements in HTTP/HTTPS security

Provide Top-of-the-line defense for threats on the Internet for our customers



Header Modification

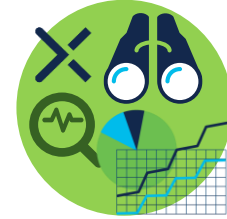


Header Consumption



HTTP 2.0

# 14.0 Highlights



SecureX Integration



System Health  
Dashboard in  
SMA/WSA



Rest API Support



What is common here?

Google YAHOO!



# HTTP2.0

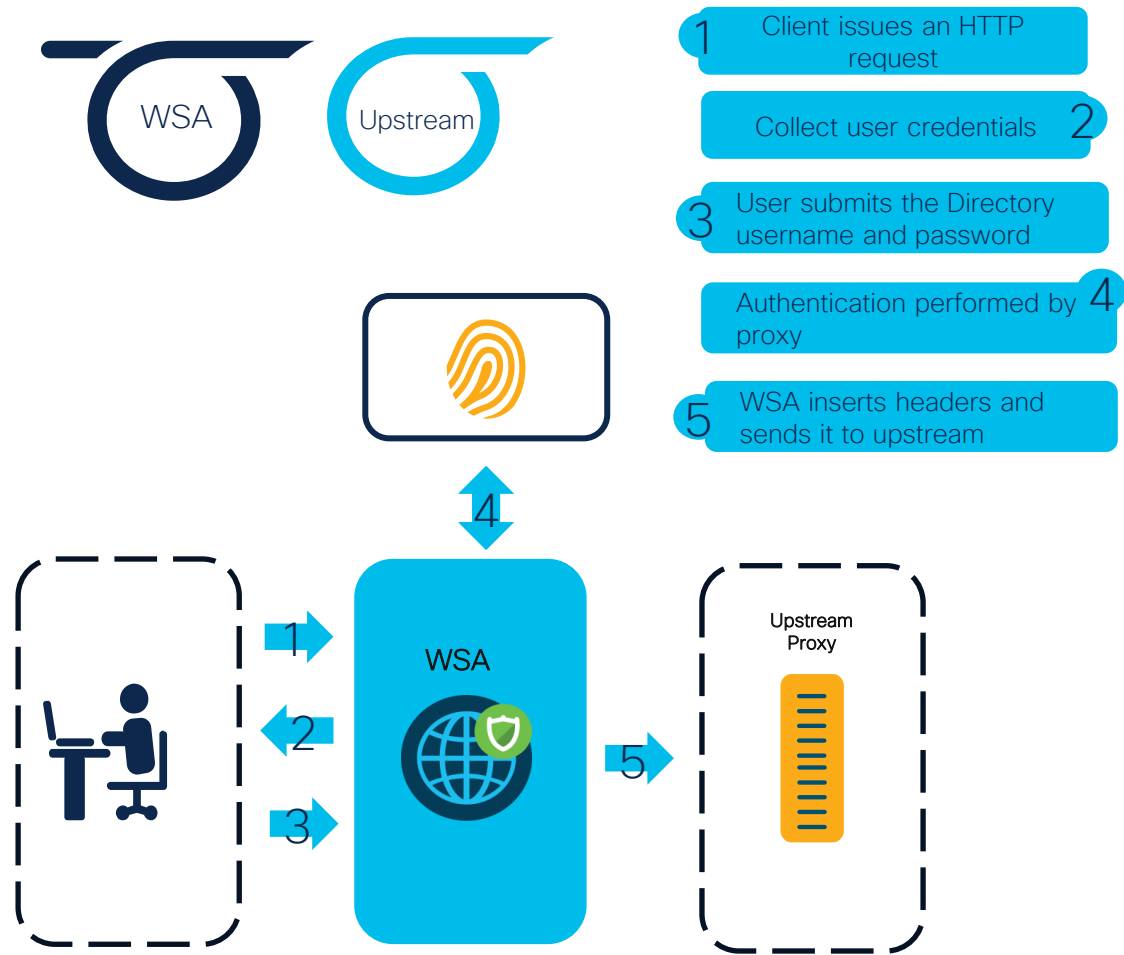
A critical value proposition in HTTP/2 vs HTTP1 - Low overhead in parsing data

What makes HTTP2 better?



HTTP/2 is used by 49.4% of all the websites!

# WSA Header Rewrite



# Header Rewrite: How-To-Configure

reporting web security manager Security Services network system Administration

## Access Policies

Success — Settings have been saved.

Policies

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Delete
1	<b>Client network 1 Access</b> Identification Profile: Client Network 1 6 groups (AD\W2016-02\Domain Admins...)	(global policy)	Block: 27 Warn: 24 Monitor: 34	(global policy)	(global policy)	(global policy)	my profile 1	
2	<b>Client network 2 Access</b> Identification Profile: Client Network 2 All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	<b>Global Policy</b> Identification Profile: All	No blocked items	Monitor: 85	Monitor: 356	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	<a href="#">delete_profile</a>	

Edit Policy Order...

Copyright © 2003-2020 Cisco Systems, Inc. All rights reserved. | Privacy Statement

- ✓ Create HTTP Header Profile
- ✓ Add HTTP Request Header
- ✓ Add Header Name, Value, formatting & encoding
- ✓ Add/Copy/Delete Row
- ✓ Request Header Profiles
- ✓ X-Auth Header Global Settings
- ✓ View allowed format for groups
- ✓ Associate Header ReWrite Profile to Access Policies.

**Note:** Null / empty header values are allowed. Such headers will be ignored and won't be added in the transactions.

**Ex:** Via and Proxy Connection in this case. 44

# WSA X-auth Header Consumption

Use Case:

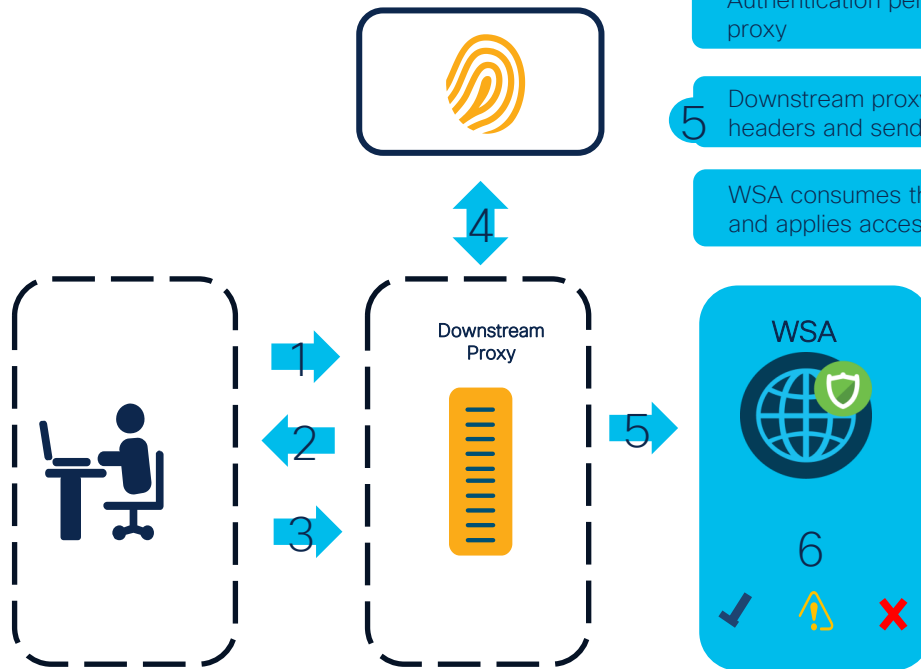
“Administrator wants to authenticate users against a downstream proxy and send user information to the WSA via authentication headers, so it can help WSA recognize the user by using the information in header with out requesting for authentication again and apply corresponding policies”

Scenarios:

- A Load balancer, before sending the traffic to proxies, it authenticates the users and inserts the headers in http and sends it to the proxy
- A SSL Orchestrator performs authentication of users and sends the traffic in service chaining manner to multiple devices in the chain before sending the traffic out to internet.



- 1 Client issues an HTTP request
- 2 Collect user credentials
- 3 User submits the Directory username and password
- 4 Authentication performed by proxy
- 5 Downstream proxy inserts headers and sends it to WSA
- 6 WSA consumes the headers and applies access policies



# WSA X-auth Header Consumption: How-To-Configure

**Access Policy: AP1**

**Policy Settings**

**Enable Policy**

Policy Name:   
(e.g. my IT policy)

Description:

Insert Above Policy:

Policy Expires:

Set Expiration for Policy

On Date:

At Time:

**Policy Member Definition**

*Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.*

Identification Profiles and Users:

Identification Profile:

Authorized Users and Groups:

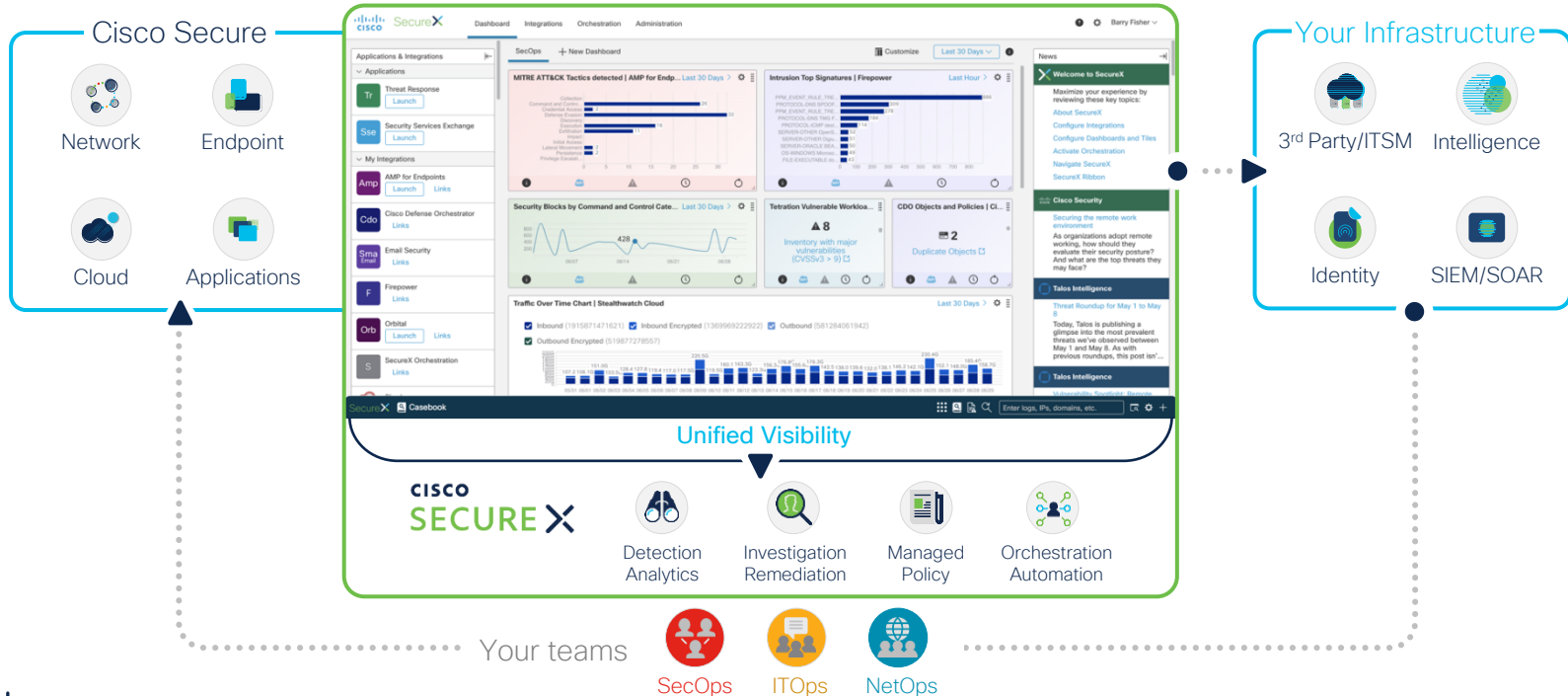
All Authenticated Users

Selected Groups and Users ?  
Groups: No groups entered  
Users: No users entered

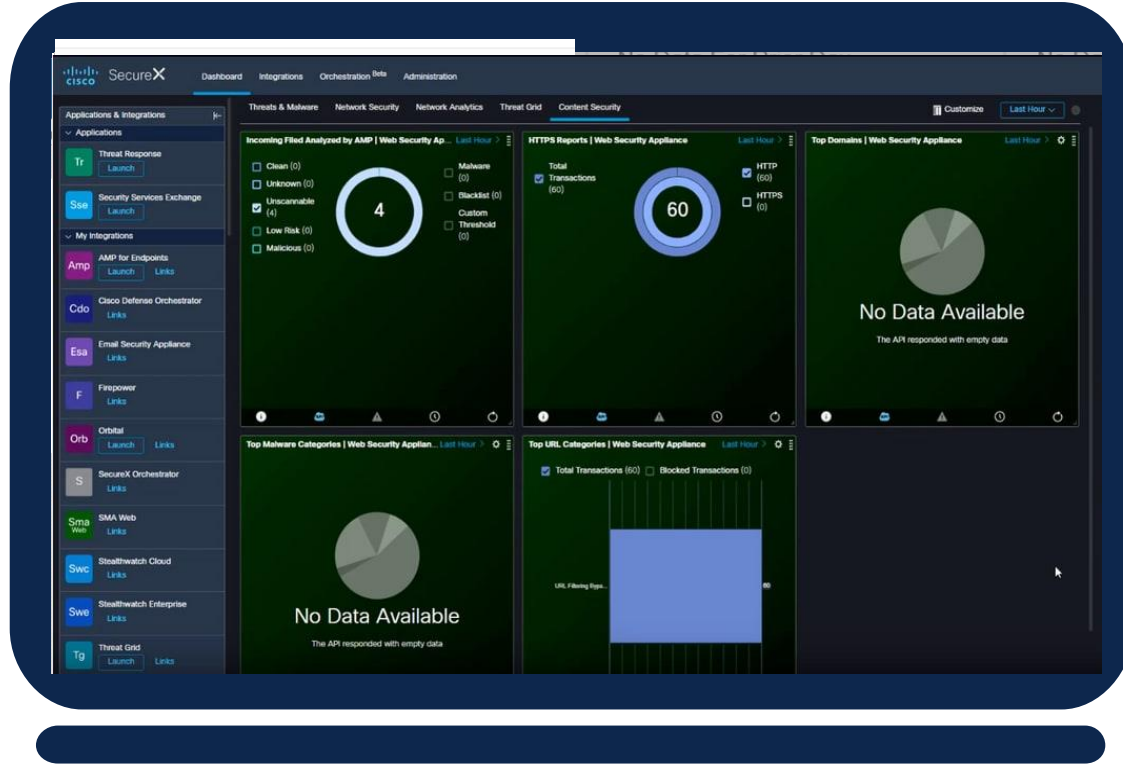
All the configurations could be done from GUI only, there are no new CLI commands added for this feature

# SecureX

A cloud-native, **built-in platform** experience within our portfolio



# SecureX Integration : How-To



- ✓ New SecureX ribbon
- ✓ SecureX WSA Tile
- ✓ Register WSA on SSE Portal
- ✓ Generate client ID and Client Secret.
- ✓ Copy client ID and Password
- ✓ Enter details back on WSA
- ✓ SecureX Pivot menus
- ✓ Reports on SecureX Portal



# Rest APIs supported in 12.5

## Rest API support for configuration

“Automate WSA configuration through scripts and integrate with third party solutions”



Helpful for automation of WSA configurations

Easy integration with 3<sup>rd</sup> party solutions

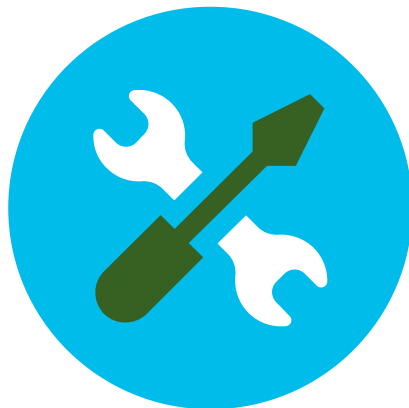
## 64 APIs available for configuration

- System Time
- Certificate Management
- Routes
- SMTP
- Feature Keys
- Custom and external URL Category
- Appliance Certificate
- DNS
- Proxy Bypass
- Interface

# Rest APIs supported in 14.0

## Rest API support for configuration

“Automate WSA configuration through scripts and integrate with third party solutions”



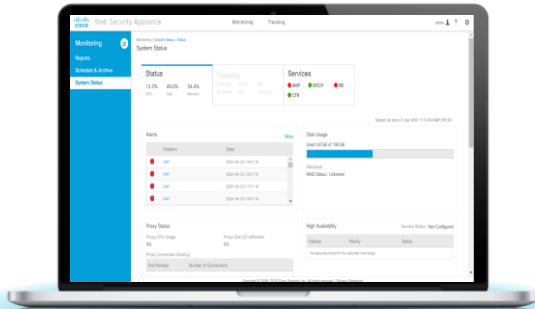
New APIs available for configuration

# Why SHD?

## Visibility to System Health of WSA in a single pane of glass



System Health Dashboard

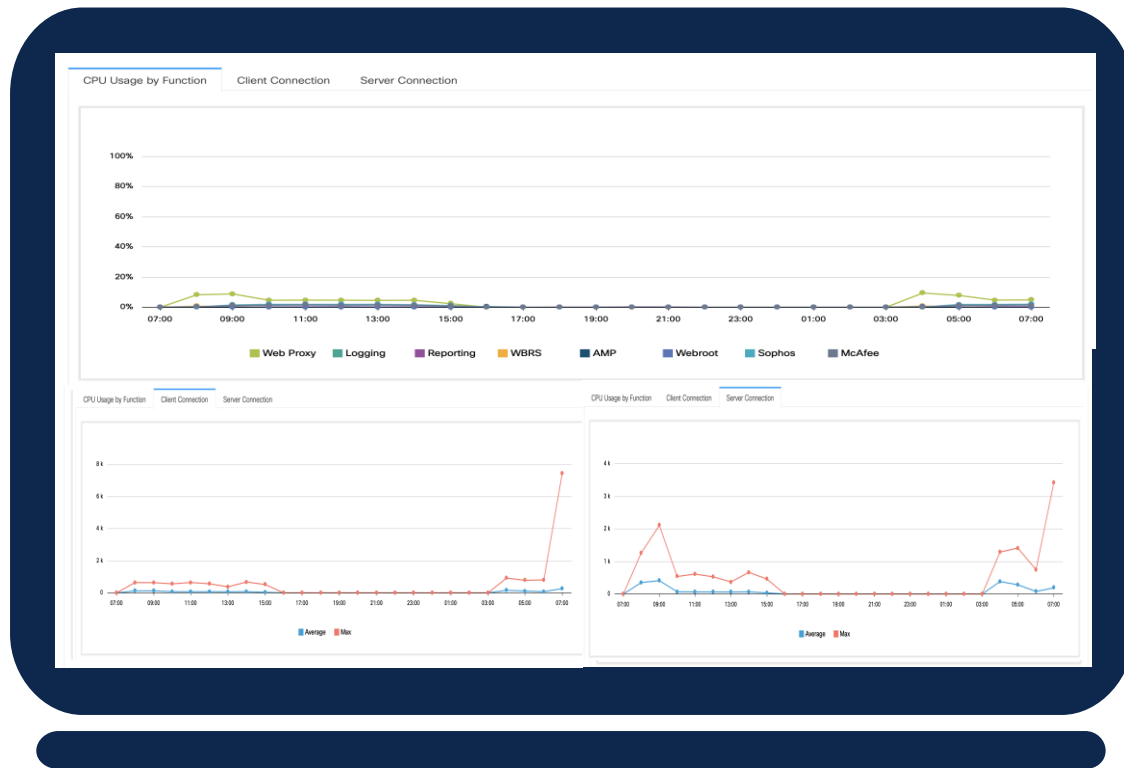


“Admin is logged in to WSA. He goes for coffee and come back to see if anything is wrong with any of his WSA or he is occupied with some other work and wants to check if the health of his WSA device looks good”

“Admin gets a complaint saying there are some issues with his WSA in his network. He can drill down deeper in to the issues using SHD”

# System Health - Capacity Tab (Phase 2)

14.0



## Capacity

- ..... CPU Usage
- ..... Memory Usage
- ..... Disk
- ..... RPS
- ..... Bandwidth
- ..... CPU Usage
- ..... Client Connections
- ..... Server Connections

# Advance Web Security Reporting (AWSR)



## Latest Release 7.5

- Splunk Engine update 7.3.3
- AD Group Details

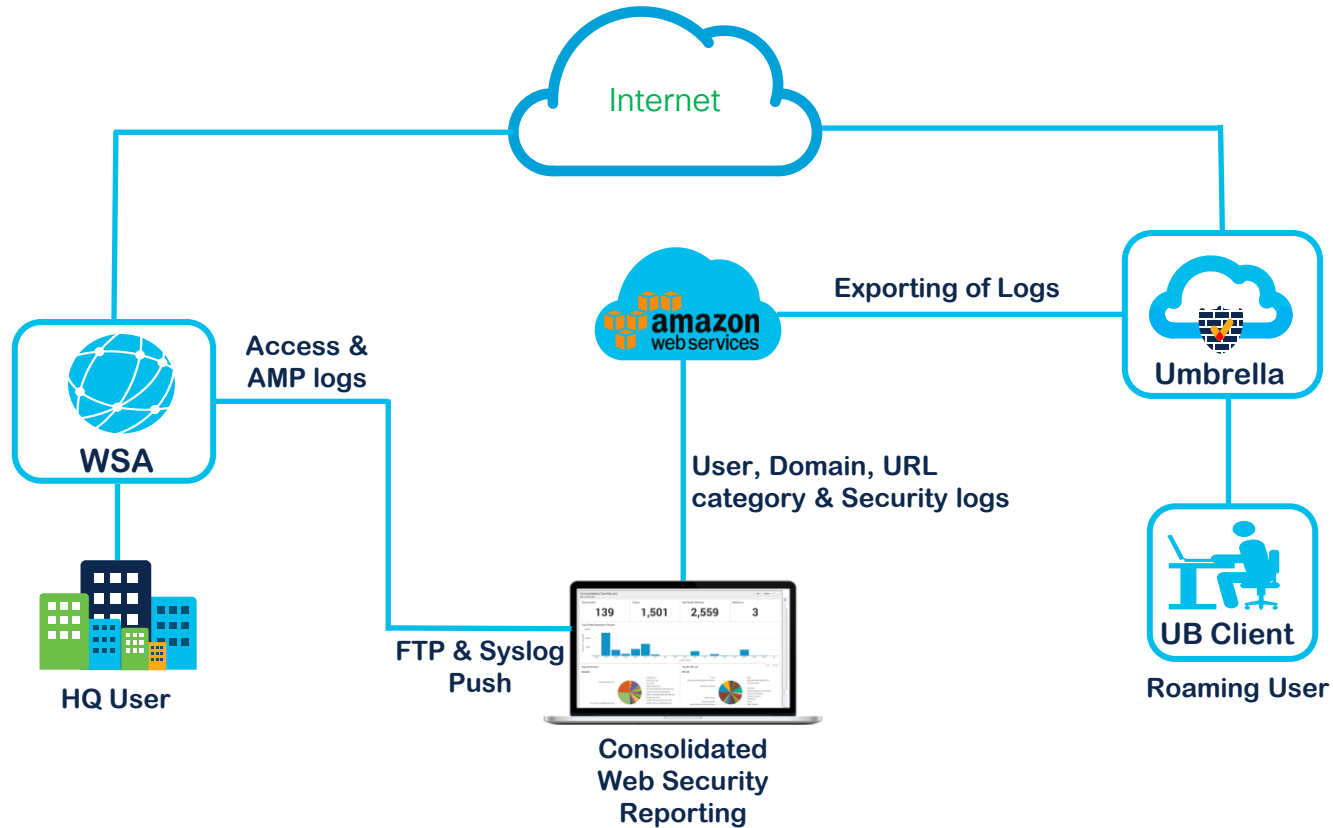


## Distributed Deployment

Need Reporting for more users

Link: [WSA Wiki](#)

# Advance Web Security Reporting v7.5 (WSA + Umbrella)



# Cisco Web Security Integrations & Technical Collaborations

## Data Loss Prevention



## Threat Detection & Isolation



Secure Endpoint



Secure Malware Analytics



Umbrella



Isolation

## Logs



## Web Log Analysis



SecureX



CTA



Secure Network Analytics



Cloudlock

## Video Caching & Isolation



## Identity & SSL Visibility



ISE



CDA



# ISE Integration on Cisco Secure Web Appliance

Secure Web Appliance 8.7	Secure Web Appliance 11.7 (1 <sup>st</sup> )	Secure Web Appliance 11.7 (2 <sup>nd</sup> )	Secure Web Appliance 11.8 (1 <sup>st</sup> )	Secure Web Appliance 11.8 (2 <sup>nd</sup> )
--------------------------	--	--	--	--

## ISE

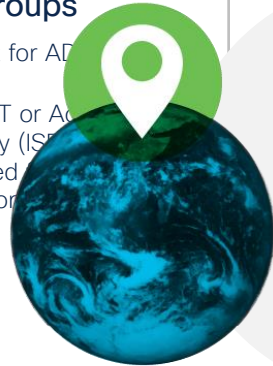
Secure Web Appliance and ISE integration

Support for Secure Group Tags(SGT), retrieved from ISE for Secure Web Appliance Policy creation

## AD Groups

Support for AD

Use SGT or Active directory (ISE) retrieved (AND) for



## SGT OR AD Group

Fallback to AD group

Fallback to Active directory group for policy control



## VDI Support

Proxy Auth for VDI clients

Support for Citrix & Microsoft terminal services clients

Identification Profile	Authorized Users and Groups
ISE	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: No tags entered Users: no users entered <input type="radio"/> Guests (users failing authentication)

Identification Profile	Authorized Users and Groups
ISEUsers	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered <input type="radio"/> Guests (users failing authentication)

11.7

Identification Profile	Authorized Users and Groups
Isefallback	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Configuration ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered Fallback Configuration Groups and Users by Realm Groups: No groups entered Users: No users entered <input checked="" type="radio"/> Guests (users failing authentication)

11.8



# WSA - License Model



WSA Essentials

- Web (URL) Filtering
- Web Reputation
- Application Visibility & Control

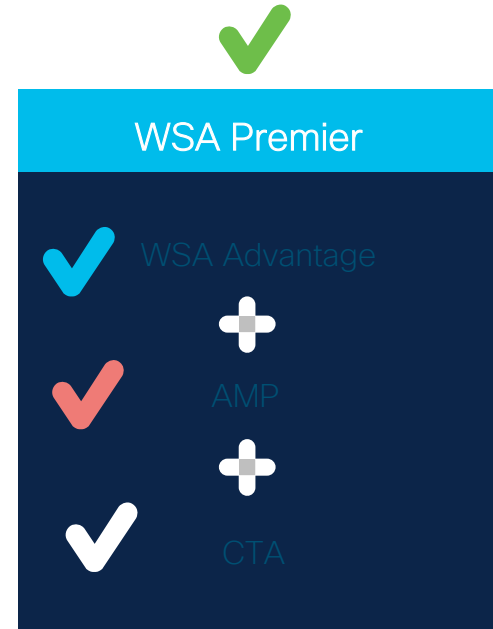
The diagram shows a blue box with an orange header labeled 'WSA Essentials'. An orange checkmark is positioned above the box. The main body of the box is dark blue and contains a list of three features: Web (URL) Filtering, Web Reputation, and Application Visibility & Control.



WSA Advantage Bundle

- WSA Essentials
- Sophos + Webroot

The diagram shows a blue box with a green header labeled 'WSA Advantage Bundle'. A blue checkmark is positioned above the box. The main body of the box is dark blue and contains two items: 'WSA Essentials' with an orange checkmark and 'Sophos + Webroot' with a red checkmark. A white plus sign is centered between the two items.



WSA Premier

- WSA Advantage
- AMP
- CTA

The diagram shows a blue box with a light blue header labeled 'WSA Premier'. A green checkmark is positioned above the box. The main body of the box is dark blue and contains three items: 'WSA Advantage' with a blue checkmark, 'AMP' with a red checkmark, and 'CTA' with a white checkmark. White plus signs are centered between the items.

## A La Carte Options





**cisco** Secure