

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, pink, purple, blue, and green. Overlaid on this are large, soft, wavy shapes in shades of orange, red, and yellow, giving the impression of clouds or flowing liquid. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Using the Cisco Secure Firewall with the Encrypted Visibility Engine

Application Visibility Insights

Costas Kleopa, Senior Engineering Manager

@costaskleopa

BRKSEC-2099

CISCO *Live!*

#CiscoLive

Cisco Webex App

Questions?

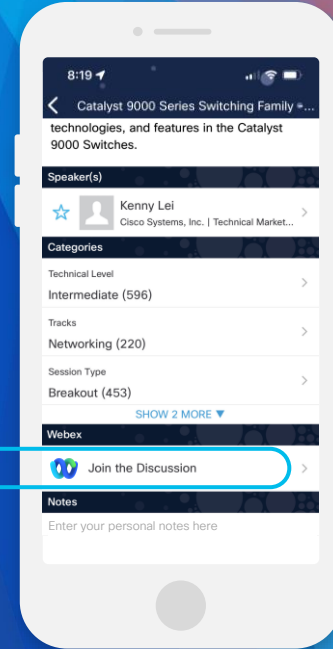
Use Cisco Webex App to chat with the speaker after the session

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 June 9, 2023.

BRKSEC-2099



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2099>

About me

- Part of the Cisco Family since 2012
- Cisco Secure Firewall Unit
- Engineering Manager
 - Snort
 - Application Detection

Patents (8)

- Encrypted Visibility Engine (EVE)
- Encrypted Traffic Analytics (ETA)

Other

- Based in Fulton Maryland, originally from Cyprus
- Father of 4



Agenda

- Problem Statement
- Encrypted Visibility Engine
- Application Detection
- Threat Detection
- Conclusion

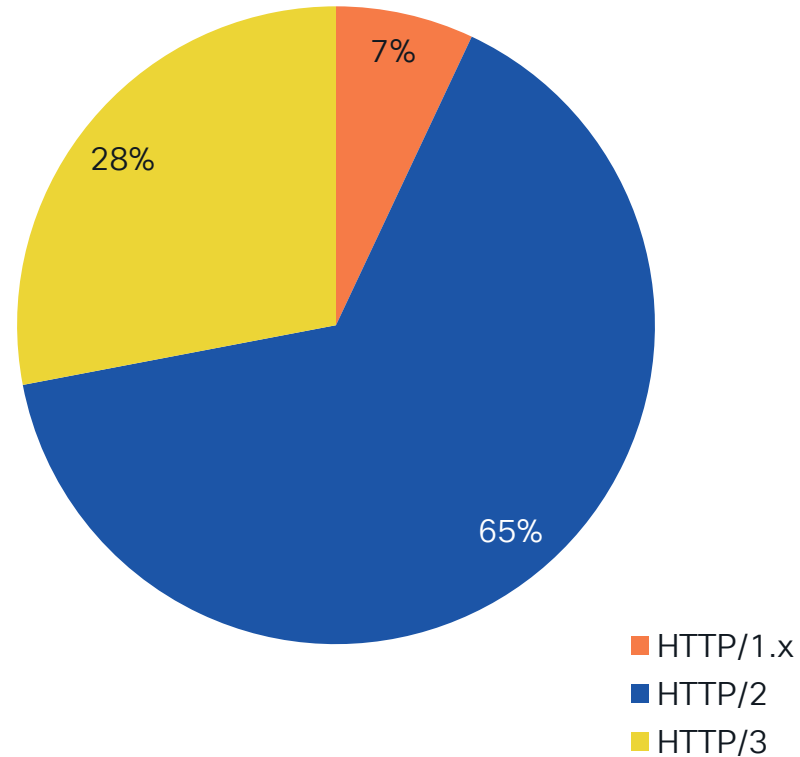
Cisco Secure Firewall & Firepower Threat Defense

1000 Series
2100 Series
3100 Series
4100 Series
9300 Series
Virtual



2023: Your Network, Encrypted

CISCO *Live!*





Summary Dashboard [\(switch dashboard\)](#)

Provides a summary of activity on the appliance

Network

Threats

Intrusion Events

Status

Geolocation

QoS

Zero Trust

+

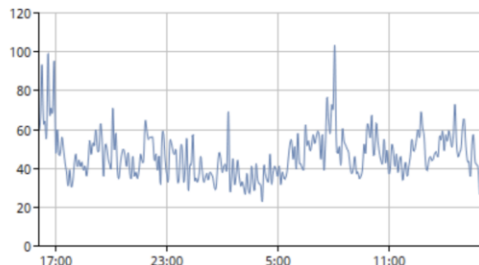
Show the Last

1 day



Add Widgets

Unique Applications over Time



Last updated less than a minute ago

Traffic by Application Risk

Risk	Total Bytes (KB)
Medium	54,074,698.45
Low	16,694,066.81
Very Low	16,027,433.34
High	7,947,800.71
Very High	3,676.11

Last updated less than a minute ago

Top Web Applications Seen

Application	Total Bytes (KB)
Apple TV Plus	3,736,281.37
iCloud	3,177,531.34
Disney Plus	3,035,875.45
Apple Update	2,220,990.61
YouTube	1,770,604.47
Instagram Media	1,451,025.81
QUIC	1,283,358.99
SurfEasy VPN	1,063,667.26
Facebook	569,321.61
BlueStacks	563,835.21
Google APIs	425,624.78
TwitPic	411,965.76
iTunes	273,411.44
Exchange Online	166,622.01
Apple sites	143,260.27

Last updated less than a minute ago

Top Server Applications Seen

Vendor	Count
vsFTPD	99
nginx	89

Top Client Applications Seen

Application	Total Bytes (KB)
SSL client	25,780,414.07
Mac App Store	11,457,461.63
Apple Update	2,220,990.61
YouTube	1,770,604.47
QUIC	1,283,358.99
Facebook	569,321.61
BlueStacks	563,835.21
iTunes	273,411.44
iCloud Private Relay	142,111.15
Chrome	141,959.89
Amazon Web Services	138,595.53
Webex Teams	106,375.91
Marco Polo	65,361.33
Apple Maps	63,618.00
Yahoo!	11,393.55

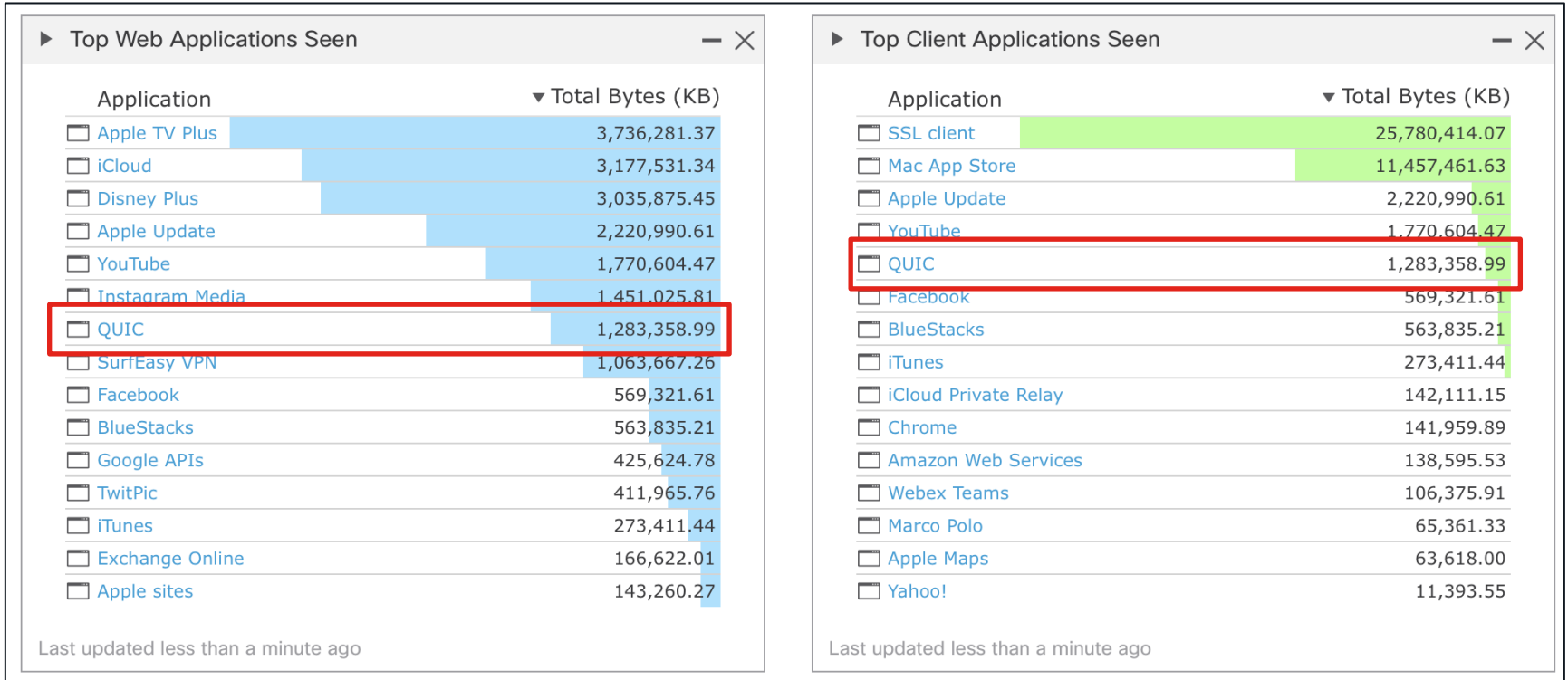
Last updated less than a minute ago

Top Operating Systems Seen

OS Name	Count
Linux	449
Enterprise Linux	149

Application Visibility Dashboards

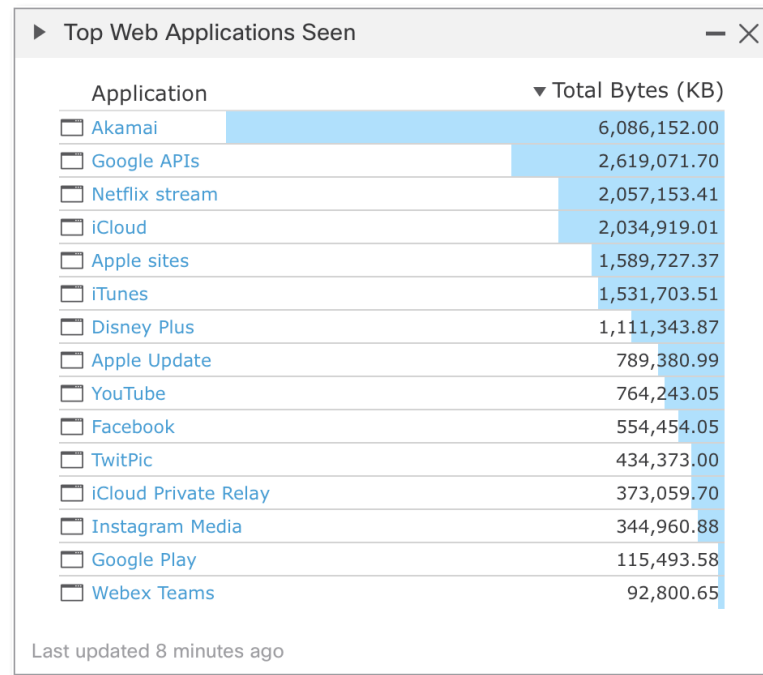
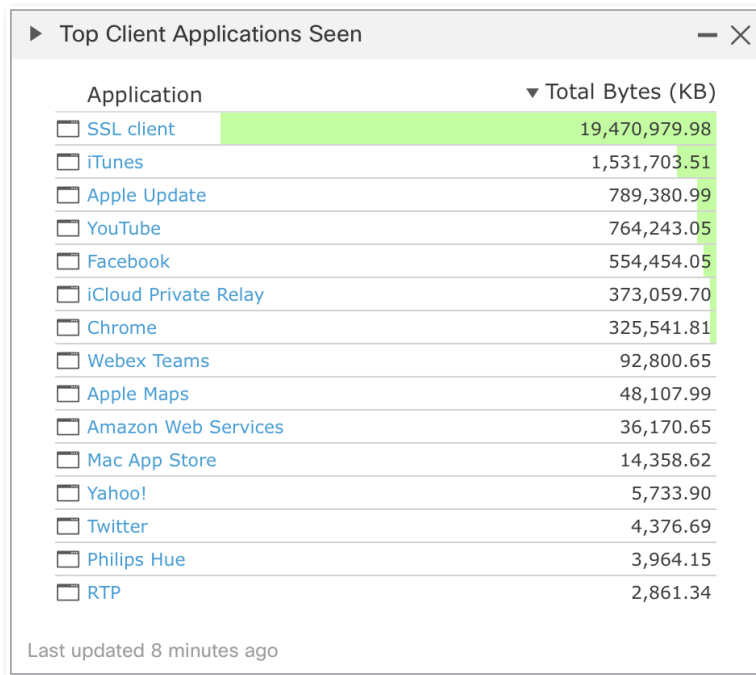
Encrypted Visibility Engine: OFF



Application Visibility Dashboards

Encrypted Visibility Engine: ON

- QUIC protocol identified under their respective Applications



What is QUIC

Transport Layer Protocol	Request/Response	Description	Protocol
HTTP	HTTP/1.x	Your web traffic in Clear Text	TCP
HTTPS	HTTP/1.1	Your web traffic Encrypted	TCP
HTTPS	HTTP/2	Your traffic broken into multiple-streams in same session, encrypted	TCP
QUIC	HTTP/3	Your web traffic broken into multiple-streams & encrypted	UDP

- Encrypted Visibility Engine can decode QUIC handshakes and report the protocols used in encrypted packets

What is QUIC – Packet View

```
QUIC IETF
  QUIC Connection information
  Packet Number: 1
  CRYPTO
    Frame Type: CRYPTO (0x0000000000000006)
    Crypto Data
      TLSv1.3 Record Layer: Handshake Protocol: Client Hello
        Handshake Protocol: Client Hello
          Handshake Type: Client Hello (1)
          Version: TLS 1.2 (0x0303)
          Extension: server_name (len=19)
            Type: server_name (0)
            Server Name Indication extension
              Server Name: www.google.com
          Extension: application_layer_protocol_negotiation (len=8)
            Type: application_layer_protocol_negotiation (16)
            ALPN Protocol
              ALPN Next Protocol: h3-29
```

What's in my network: Filtering: QUIC -> HTTP/3

☐	Application Protocol X	Client X	Web Application X	URL X	↓ Count
☐					20,499
☐	☐ HTTP/3	☐ Office 365	☐ Exchange Online	https://outlook.office365.com	16,209
☐	☐ HTTP/3	☐ HTTP/3 client	☐ iCloud Private Relay	https://mask.icloud.com	6,469
☐	☐ HTTP/3	☐ Chrome	☐ Google	https://ccp-lh.googleusercontent.com	814
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Firebase Crashlytics	https://app-measurement.com	763
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Google Calendar	https://calendar.google.com	343
☐	☐ HTTP/3	☐ Chrome	☐ Google	https://clients4.google.com	321
☐	☐ HTTP/3	☐ Chrome	☐ Google APIs	https://optimizationguide-pa.googleapis.com	300
☐	☐ HTTP/3	☐ Chrome	☐ Google	https://clients3.google.com	295
☐	☐ HTTP/3	☐ HTTP/3 client	☐ YouTube	https://youtubei.googleapis.com	274
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Google	https://google.com	271
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Google	https://www.google.com	217
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Gmail	https://mail.google.com	170
☐	☐ HTTP/3	☐ HTTP/3 client	☐ YouTube	https://s.youtube.com	148
☐	☐ Unknown				145
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Facebook for Developers	https://graph.facebook.com	120
☐	☐ HTTP/3	☐ HTTP/3 client	☐ YouTube	https://i.ytimg.com	116
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Airbnb	https://api.airbnb.com	113
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Google APIs	https://www.googleapis.com	111
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Sentry	https://o55978.ingest.sentry.io	103
☐	☐ HTTP/3	☐ HTTP/3 client	☐ Google APIs	https://firebase logging-pa.googleapis.com	97

Traffic moving to HTTP/3

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Q

Encrypted Visibility Process Name

microsoft office

+

Application Protocol

HTTP/3

x

+

Showing all 4,975 events (4,975)

	Time	Port /	Application Protocol	Client Application	Web Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility...	Encrypted Visibility Process...	Detection Type
>	2023-04-05 11:59:40	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 11:59:40	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 10:30:33	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 09:46:04	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 09:21:29	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 09:01:22	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 08:55:07	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office.com	🔒 quic/(00000001)(C	99%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:44	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:44	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:44	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:44	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:42	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:42	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:42	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:42	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:42	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:41	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:41	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility
>	2023-04-05 07:26:41	/ udp	HTTP/3	Office 365	Exchange Online	https://outlook.office365.com	🔒 quic/(00000001)(C	98%	microsoft office	Encrypted Visibility

Filtering on specific fingerprints of: “microsoft office”

Firewall Management Center										
Analysis / Unified Events										
Overview Analysis Policies Devices Objects Integration										
X Encrypted Visibility Process Name microsoft office X X Encrypted Visibility Fingerprint tls/1/(0303)(0a0a130113021303... X										
Showing all 30 events (30) ↓										
Time	Port /	Application Protocol	Client Application	Web Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility...	Encrypted Visibility Process...	Detection Type	
2023-04-05 08:45:01	/ tcp	HTTPS	SSL client	Office 365	https://mamservice.manage.microsoft.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 08:45:01	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office365.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 08:45:00	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office365.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 08:45:00	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 08:45:00	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 08:42:35	/ tcp	HTTPS	Office 365	Azure cloud portal	https://officeci-mauservice.azurewebsites.net	tls/1/(0303)(0a0a130113021303...	99%	microsoft office	Encrypted Visibility	
2023-04-05 08:11:10	/ tcp	HTTPS	Office 365	Microsoft Teams	https://self.events.data.microsoft.com	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	
2023-04-05 06:40:46	/ tcp	HTTPS	Office 365	Microsoft Teams	https://self.events.data.microsoft.com	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	
2023-04-05 01:37:25	/ tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	
2023-04-05 01:37:23	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office365.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 01:37:21	/ tcp	HTTPS	SSL client	Office Mobile	https://roaming.officeapps.live.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 01:37:20	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office365.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 01:37:20	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 01:37:20	/ tcp	HTTPS	SSL client	Exchange Online	https://clients.config.office.net	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 01:37:20	/ tcp	HTTPS	SSL client	Exchange Online	https://outlook.office365.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-05 01:37:19	/ tcp	HTTPS	SSL client	Office 365	https://mamservice.manage.microsoft.com	tls/1/(0303)(0a0a130113021303...	26%	microsoft office	AppID	
2023-04-04 22:47:48	/ tcp	HTTPS	Office 365	Microsoft Teams	https://self.events.data.microsoft.com	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	
2023-04-04 21:30:35	/ tcp	HTTPS	Office 365	Microsoft Teams	https://self.events.data.microsoft.com	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	
2023-04-04 21:20:19	/ tcp	HTTPS	Office 365	Azure cloud portal	https://officeci-mauservice.azurewebsites.net	tls/1/(0303)(0a0a130113021303...	99%	microsoft office	Encrypted Visibility	
2023-04-04 20:44:58	/ tcp	HTTPS	Office 365	Microsoft Teams	https://self.events.data.microsoft.com	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	
2023-04-04 20:44:58	/ tcp	HTTPS	Office 365	Microsoft Teams	https://self.events.data.microsoft.com	tls/1/(0303)(0a0a130113021303...	98%	microsoft office	Encrypted Visibility	

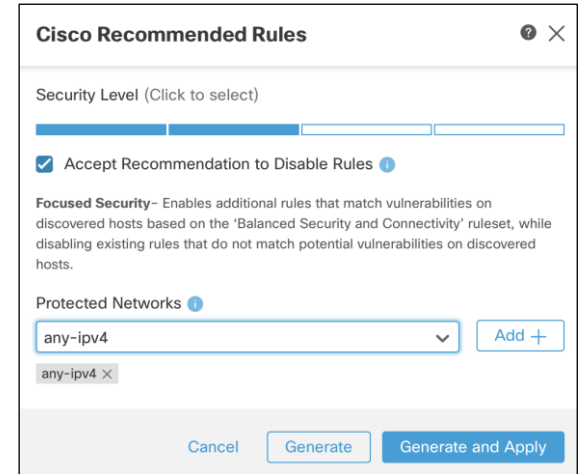
Missing Web Application Coverage

In what other
ways can it help
our customers?



Operating System Improvements

- Without EVE:
 - Depends on a set of 7 types of fingerprints need to be manually updated.
- With EVE:
 - 2+ additional types of fingerprints that are automatically updated by our infrastructure.
- End-Result:
 - Much richer coverage with most accurate readings.
 - Better classification for your Firepower Recommended Rules policies.



The screenshot shows the 'Cisco Recommended Rules' configuration window. At the top, there's a title bar with a question mark icon and a close button. Below the title, the 'Security Level' section has a label '(Click to select)' and a progress bar with four segments, the first two of which are filled. A checkbox labeled 'Accept Recommendation to Disable Rules' is checked. Below this, a text block explains 'Focused Security' as enabling additional rules that match vulnerabilities on discovered hosts while disabling existing rules that do not match potential vulnerabilities. The 'Protected Networks' section features a dropdown menu currently showing 'any-ipv4' and an 'Add +' button. Below the dropdown, a tag 'any-ipv4' with a close icon is visible. At the bottom of the window, there are three buttons: 'Cancel', 'Generate', and 'Generate and Apply'.

Analysis -> Discovery Events -> Table View

Encrypted Visibility Engine: OFF

IP Address ×	↓ Description ×
 192.168.1.167	OS Ubuntu or CentOS Linux or Linux Linux 11.04, 11.10, 12.04, 13.04 or Linux 6.3, 6.4
 192.168.1.167	OS Ubuntu Linux Linux 11.04, 11.10, 12.04, 12.10, 13.04
 192.168.1.252	OS Ubuntu Linux Linux 11.04, 11.10, 12.04, 12.10, 13.04
 192.168.1.72	OS Google or Ubuntu or CentOS or Red Hat or Cisco Android or CrOS or Linux or Linux or Enterprise Linux or Cisco Android 2.2,2.3,3.2,4.0,4.1,4.
 192.168.1.2	OS Apple Mac OSX or iOS Mac_OSX 10.5,10.6,10.10,10.11,10.12,10.13 or iOS 8.0,8.1,8.2,8.3,8.4,9.0,9.1,9.2,9.3,10.0,10.1,10.2,10.3
 192.168.1.29	OS Apple Mac OSX or iOS Mac_OSX 10.5,10.6,10.10,10.11,10.12,10.13 or iOS 8.0,8.1,8.2,8.3,8.4,9.0,9.1,9.2,9.3,10.0,10.1,10.2,10.3
 192.168.1.52	OS Apple Mac OSX or iOS Mac_OSX 10.5,10.6,10.10,10.11,10.12,10.13 or iOS 8.0,8.1,8.2,8.3,8.4,9.0,9.1,9.2,9.3,10.0,10.1,10.2,10.3
 192.168.1.20	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
 192.168.1.61	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
 192.168.1.217	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
 192.168.1.254	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
 192.168.1.61	OS Apple Mac OSX Mac_OSX 10.5, 10.6, 10.14
 192.168.1.98	OS Apple Mac OSX Mac_OSX 10.5, 10.6, 10.10, 10.11, 10.12, 10.13

Analysis -> Discovery Events -> Table View

Encrypted Visibility Engine: ON

↓ IP Address ×	Description ×
192.168.1.217	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.217	Apple Mac OSX 10.14.6, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6; Microsoft Windows 10 21h2.x
192.168.1.217	Apple Mac OSX 10.15.7; Apple MacOS 12.3.1, 12.4, 12.6
192.168.1.217	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
192.168.1.215	OS Linux or Google Linux kernel or Android Linux kernel 2.6 or Android 2.2, 2.3
192.168.1.204	Microsoft Windows 10 21h2.x
192.168.1.72	OS Google or Ubuntu or CentOS or Red Hat or Cisco Android or CrOS or Linux or Linux or Enterprise Linux or Cisco Android 2.2,2.3,3.2,4.0,4.1,4.2,4.3,4.4,5.0,5.1,7.0 or Linux 11.04,12.10,
192.168.1.61	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.61	Apple Mac OSX 10.15.7; Apple MacOS 12.3.1, 12.4, 12.6
192.168.1.61	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
192.168.1.53	OS Apple Mac OSX Mac_OSX 10.5, 10.6, 10.10, 10.11, 10.12, 10.13
192.168.1.52	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.29	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.2, 10.15.7; Apple MacOS 11.6.5, 11.6.8, 11.7, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 12.6
192.168.1.20	Apple MacOS 11.6.8, 11.7.1, 12.0.1, 12.3.1, 12.4, 12.5, 12.6
192.168.1.20	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1

Analysis -> Discovery Events -> Table View – IP Filtering

Encrypted Visibility Engine: ON

IP Address ×	↓ Description ×
192.168.1.20	OS Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.14 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1
192.168.1.20	OS Apple Mac OSX Mac_OSX 10.5, 10.6, 10.14
192.168.1.20	Apple MacOS 11.7.1, 12.2.1, 12.3.1, 12.4, 12.5, 12.6
192.168.1.20	Apple MacOS 11.6.8, 11.7.1, 12.0.1, 12.3.1, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 12.3.1, 12.4, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 12.2.1, 12.3.1, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 11.7.1, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 11.7.1, 12.2.1, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 11.6.6, 11.6.8, 11.7, 12.2.1, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.7; Apple MacOS 11.6.5, 12.3.1, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.2, 10.15.7; Apple MacOS 11.6.5, 11.6.8, 11.7, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.15.2, 10.15.7; Apple MacOS 11.2.2, 11.2.3, 11.6.5, 11.6.6, 11.6.7, 11.6.8, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.14.6, 10.15.7; Apple MacOS 11.6.5, 11.6.6, 11.6.7, 11.6.8, 11.7, 12.0.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.14.6, 10.15.7; Apple MacOS 11.2.3, 11.6, 11.7, 12.0.1, 12.2.1, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6; Microsoft Windows 10 21h2.x
192.168.1.20	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6
192.168.1.20	Apple Mac OSX 10.14.6, 10.15.2, 10.15.7; Apple MacOS 11.1, 11.2.2, 11.2.3, 11.4, 11.6, 11.7, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6

Network Map – Host Profile

Encrypted Visibility Engine: OFF

Host Profile

[Scan Host](#)[Generate Allow List Profile](#)

IP Addresses 192.168.1.20 (ip-192-168-1-20.ec2.internal)

NetBIOS Name

Device (Hops) 192.168.1.178 (1)

MAC Addresses (TTL) 72:CD:D6:AD:E0:56 (255)

Host Type Host

Last Seen 2023-03-13 11:12:12

Current User

View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (0)

[Edit Rule States](#)

▼ Operating Systems (2)

[Edit Operating System](#)[View Operating Systems](#)

Vendor	Product	Version	Source
Apple	iOS	11.0, 11.1, 11.2, 11.3, 11.4, 12.0, 12.4, 13.1	Firepower
Apple	Mac OSX	10.5, 10.6, 10.14, Server 10.5, Server 10.6, Server 10.14	Firepower

Network Map – Host Profile

Encrypted Visibility Engine: ON

Host Profile

[Scan Host](#)[Generate Allow List Profile](#)

IP Addresses 192.168.1.20 (ip-192-168-1-20.ec2.internal)

NetBIOS Name

Device (Hops) 192.168.1.178 (1)

MAC Addresses (TTL) 72:CD:D6:AD:E0:56 (255)

Host Type Host

Last Seen 2023-03-13 11:12:12

Current User

View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Indications of Compromise (0)

[Edit Rule States](#)

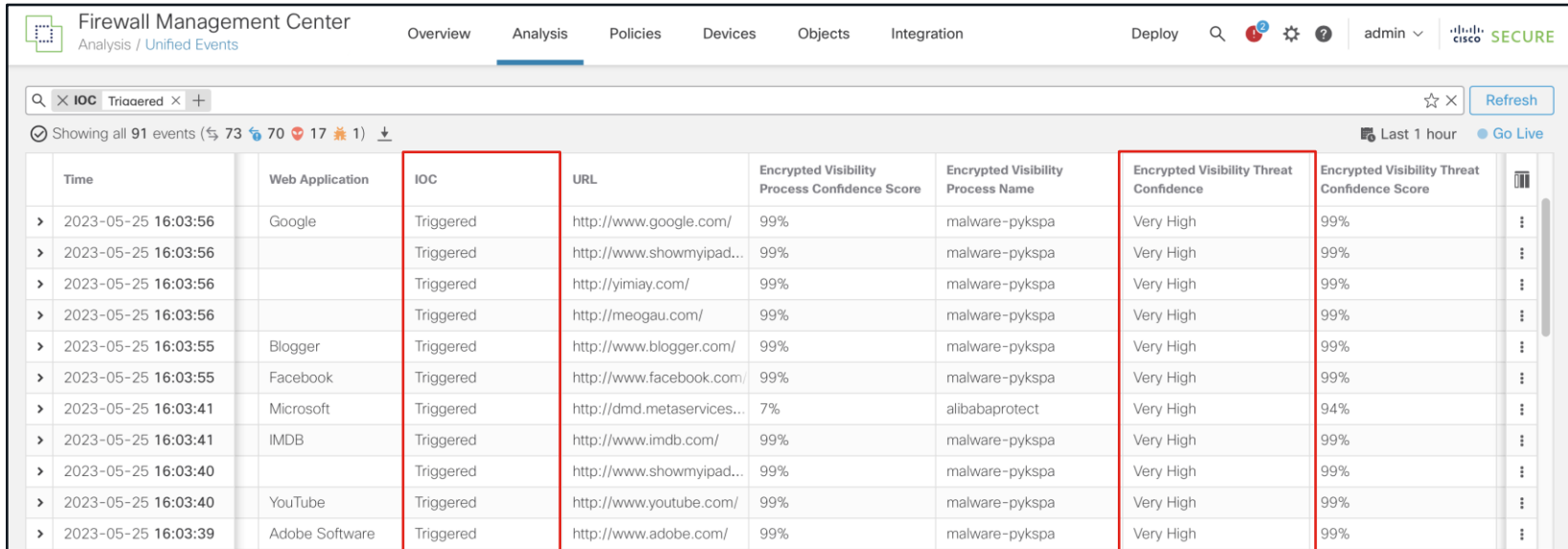
▼ Operating System

[Edit Operating System](#)

Vendor	Product	Version	Source
Apple	Macos	12.3.1, 12.4, 12.5, 12.6	Firepower

Indicators of Compromise: Unified Event View

- The IoC column presents the triggered an IoC events.
- IoC Trigger for Encrypted Visibility Engine
 - Encrypted Visibility Threat Confidence = 'Very High'.



Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 2 ⚙️ ? admin ✖️ cisco SECURE

🔍 X IOC Triggered X + ☆ ✖️ Refresh

☑ Showing all 91 events (📅 73 📊 70 📈 17 📉 1) ⬇️ 🕒 Last 1 hour 🟢 Go Live

Time	Web Application	IOC	URL	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score	
2023-05-25 16:03:56	Google	Triggered	http://www.google.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:56		Triggered	http://www.showmyipad...	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:56		Triggered	http://yimiay.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:56		Triggered	http://meogau.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:55	Blogger	Triggered	http://www.blogger.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:55	Facebook	Triggered	http://www.facebook.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:41	Microsoft	Triggered	http://dmd.metaservices...	7%	alibabaprotect	Very High	94%	⋮
2023-05-25 16:03:41	IMDB	Triggered	http://www.imdb.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:40		Triggered	http://www.showmyipad...	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:40	YouTube	Triggered	http://www.youtube.com/	99%	malware-pykspa	Very High	99%	⋮
2023-05-25 16:03:39	Adobe Software	Triggered	http://www.adobe.com/	99%	malware-pykspa	Very High	99%	⋮

Indicators of Compromise: Network Map

 **Firewall Management Center**
Analysis / Hosts / Network Map / Indications of Compromise

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 4 ⚙️ ? admin ▾ 

HostsNetwork DevicesMobile DevicesIndications of CompromiseApplication ProtocolsVulnerabilitiesHost Attributes

Filter by IP and MAC addresses ✕

Indications of Compromise

▼ Suspicious Activity (2)

▶ 162 (1)

▼ 192 (1)

▼ 192.168 (1)

▼ 192.168.1 (1)

▶ [192.168.1.192](#)

Select required Host IP address from the list of hosts that generated suspicious activity

Host Profile

Scan HostGenerate Allow List Profile

IP Addresses192.168.1.192

NetBIOS Name

Device (Hops)10.10.8.73 (0)

MAC Addresses (TTL)00:50:AE:1B:54:61 (FDK Co., Ltd) (128)

Host TypeHost

Last Seen2022-07-21 11:29:51

Current User

ViewContext Explorer | Connection Events | Intrusion Events | File Events | Malware Events

▼ Indications of Compromise (1)

Edit Rule StatesMark All Resolved

Category	Event Type	Description	First Seen	Last Seen	
Suspicious Activity	Encrypted Visibility Engine	Probable Malware Communication	👁 2022-07-21 11:29:51	👁 2022-07-21 11:56:57	🗑

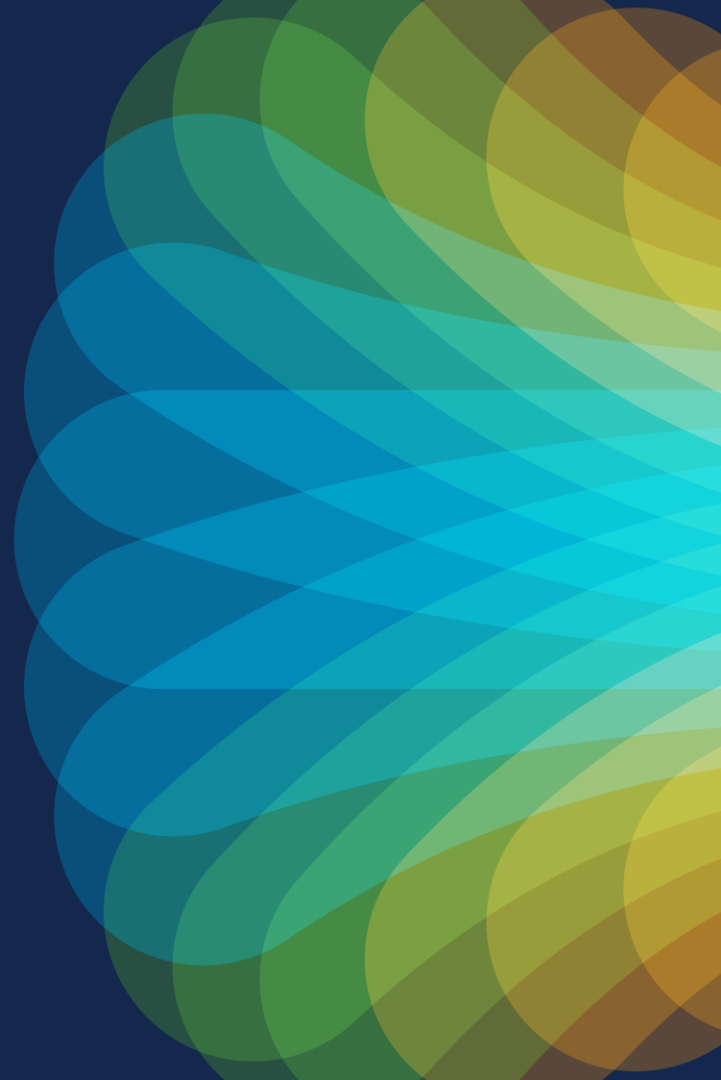
▼ Operating System

Edit Operating System

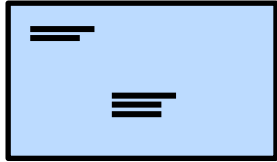
Vendor	Product	Version	Source
Microsoft	Windows	Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8, Server 2012, 10, Server 2016	Firepower

Users (no user history available)

How does this work?



Encrypted Visibility Engine (EVE)



Analyzes Session
Metadata
Without Decryption



Fingerprints Client
Application



Machine Learning Driven
Threat Detection

Encrypted Visibility without Decryption

TLS Client Hello



TCP/TLS 192.168.2.110/34624->172.16.45.200/443

TCP/TLS 192.168.2.110/21013->203.0.113.154/443

TLS Client Hello

▼ Cipher Suites (18 suites)

```
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc03c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03d)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

Confidence: 99.94%
Process: [firefox.exe](#)
Version: 76.0.1
Category: **browser**
OS: [Windows 10 19041.329](#)
Destination FQDN: [cisco.com](#)

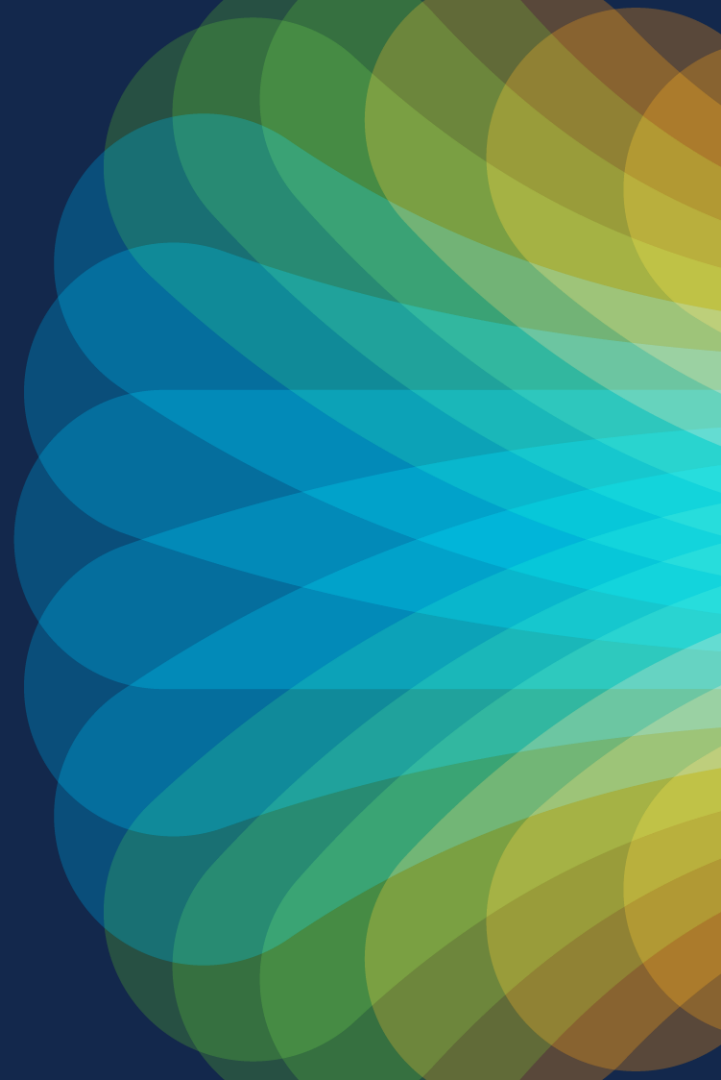
Encrypted Visibility Engine (EVE): Generates unique fingerprints for client applications based on outer packet fields, and use for policy matching and context enrichment

▼ Cipher Suites (19 suites)

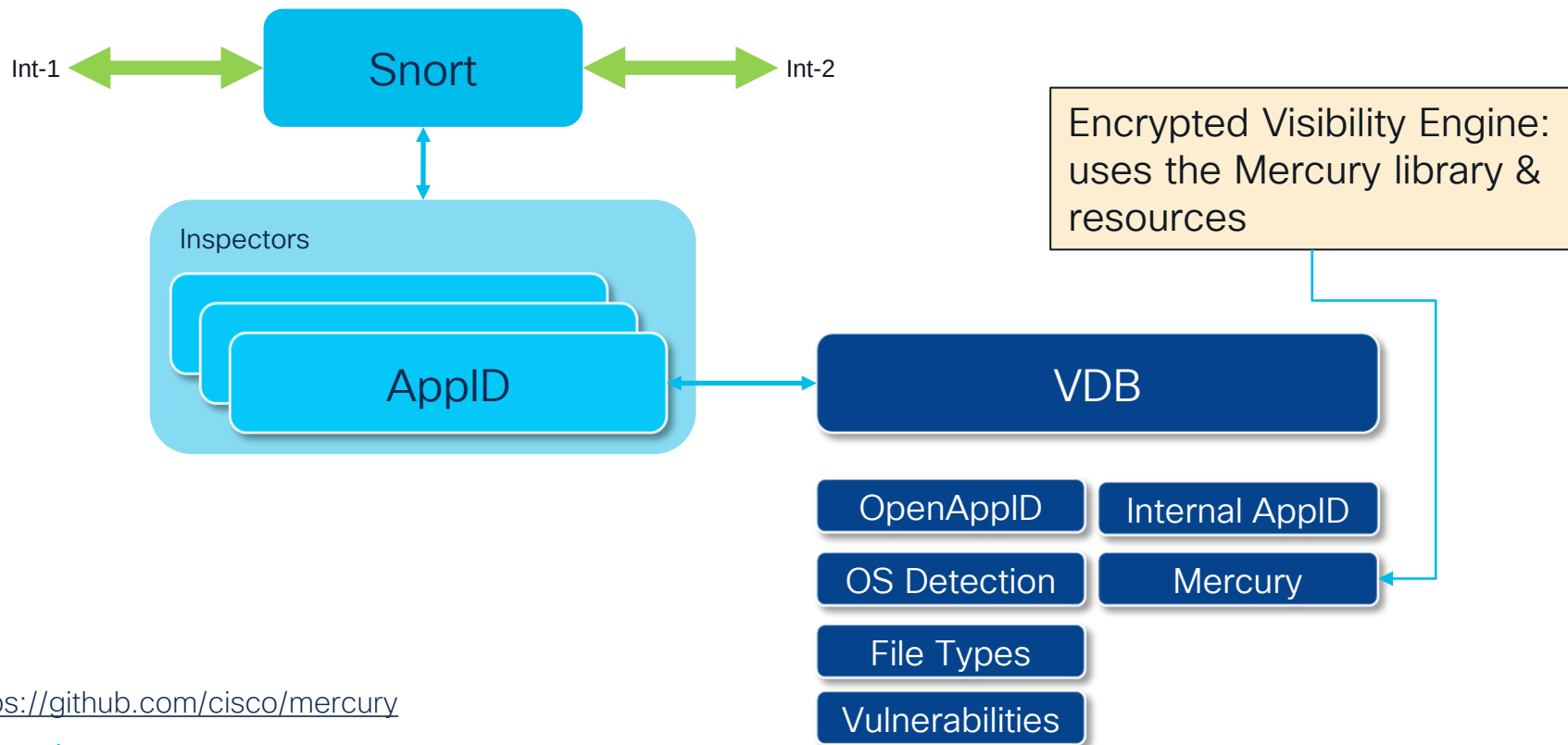
```
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc03c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03d)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc03e)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc03f)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
```

Confidence: 100%
Process: [tor.exe](#)
Version: 9.0.2
Category: **anonymizer**
OS: [Windows 10 19041.329](#)
Destination FQDN: [nksdilkoup.me](#)

Platform Architecture

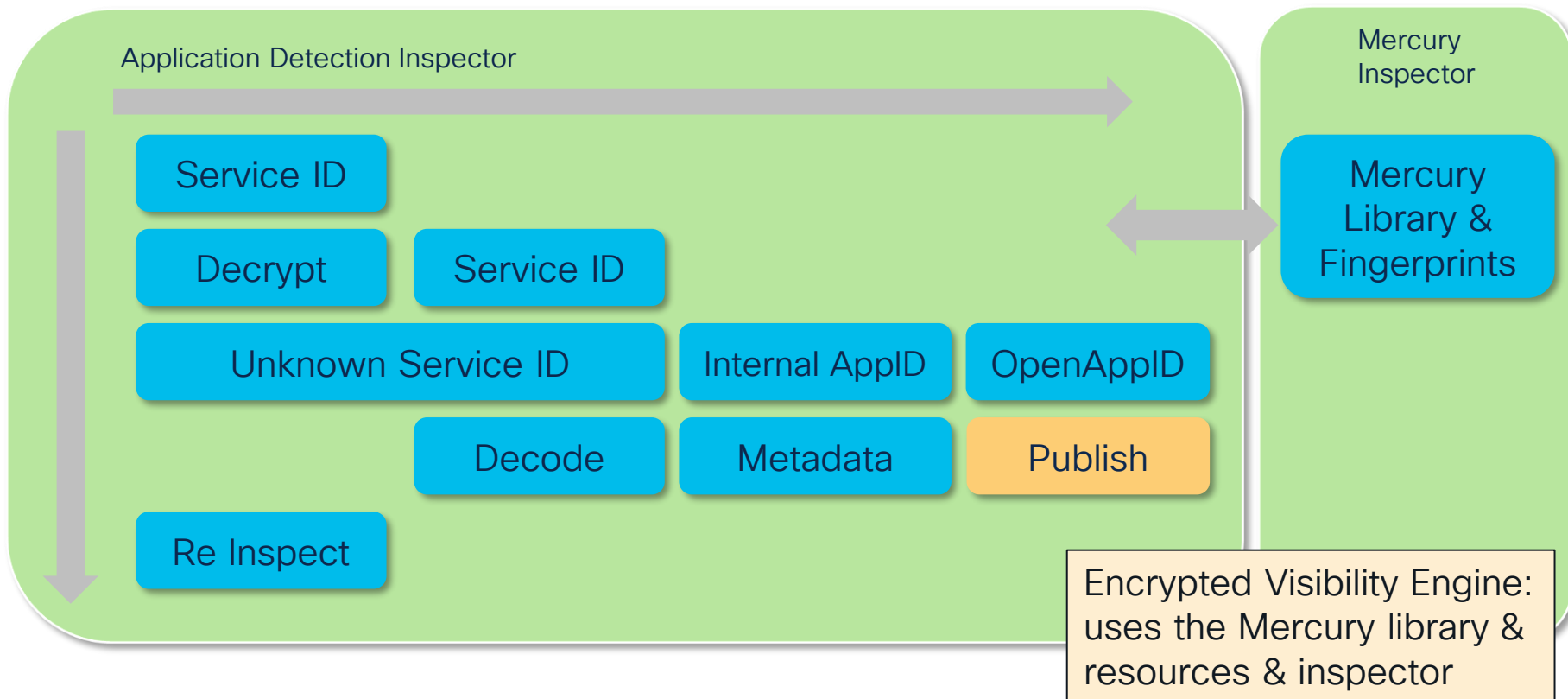


Overall Architecture Diagram: Content Package



<https://github.com/cisco/mercury>

Overall Architecture Diagram: Inspectors



Features and Roadmap

Encrypted Visibility Capabilities

Feature Journey

Cisco Secure
Firewall

7.1: Visibility	7.2: Control	7.3: Warning
• Process Names • Threat Score • Dashboards • Telemetry	• Process -> Client Apps • Operating System Detection • QUIC/Client Hello->Server Name • Server Name->Web Apps	• Indicator of Compromise Integration • QUIC Process Names • QUIC/ALPN Extraction • QUIC/User-Agent

VDB

348	350	353	354	361
• Initial Update • TLS Protocol	• 150 Client/Process	• QUIC Protocol • QUIC: Server Name	• QUIC Fingerprints	• HTTP Protocol for telemetry • 303 Client/Process

Architectural Comparisons

ETA or EVE

- Both technologies serve their own purpose
- There is value when being able to have 1 pass vs multiple at a later time

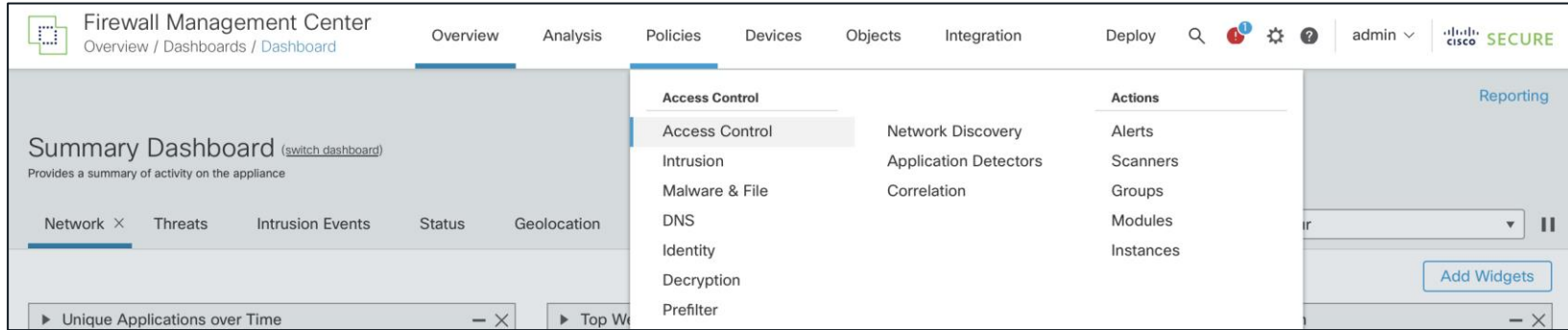
Encrypted Traffic Analytics	Encrypted Visibility Engine
Introduced in 2017 (Network Intuitive launch)	Introduced 2021 (Cisco Secure Firewall)
Initial Data Packet Analysis: Later	Initial Data Packet: Now.
Deeper Analysis on multiple views	Results can be provided at the Firewall
Networking and Secure Network Analytics Solution	Self Contained Solution (Firewall)
	Support for Multiple Types of Fingerprints

EVE vs JA3

Feature	EVE	JA3
Fingerprint string computed from packet fields	✓	✓
Analyze ports	✓	✗
Consider DNS top level domains	✓	✗
Data-driven, continuously trained	✓	✗
Destination context	✓	✗
TLS support	✓	✓
QUIC, HTTP support and more	✓	✗
Normalized evasive randomized fingerprints	✓	✗

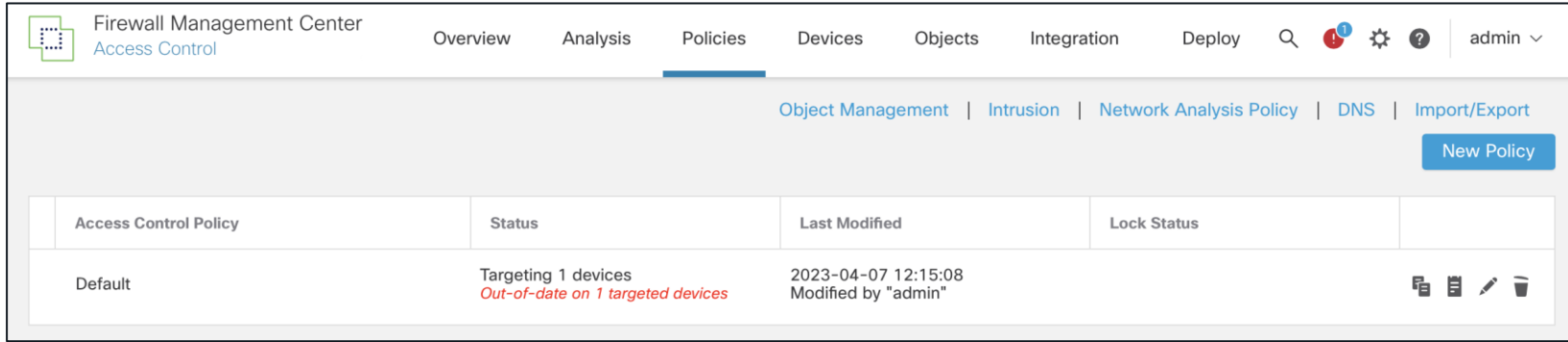
How to enable the Encrypted Visibility Engine

Access Control Policy



How to enable the Encrypted Visibility Engine

Edit or Create a New Policy



Firewall Management Center
Access Control

Overview Analysis **Policies** Devices Objects Integration Deploy 🔍 ⚙️ ? admin ▾

[Object Management](#) | [Intrusion](#) | [Network Analysis Policy](#) | [DNS](#) | [Import/Export](#)

[New Policy](#)

Access Control Policy	Status	Last Modified	Lock Status	
Default	Targeting 1 devices <i>Out-of-date on 1 targeted devices</i>	2023-04-07 12:15:08 Modified by "admin"		   

How to enable the Encrypted Visibility Engine

More -> Advanced Settings

The screenshot displays the Cisco Firewall Management Center (FMC) Policy Editor interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, Integration, and Deploy. A search icon, a notification bell with a '1', a settings gear, and a user profile 'admin' are on the right. Below the navigation bar, a breadcrumb trail shows the path: Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control (selected). A 'More' dropdown menu is open, showing options: Advanced Settings, HTTP Responses, Inheritance Settings, and Logging. The 'Advanced Settings' option is highlighted. The main content area shows a table with columns: Name, Action, Sources, and Dest. The first row is labeled 'Mandatory (1 - 6)'. On the right side of the interface, there are buttons for 'Analyze', 'Discard', and 'Save', along with a 'Switch to Legacy UI' toggle and a 'Targeted: 1 device' indicator.

How to enable the Encrypted Visibility Engine

Encrypted Visibility Engine Section

Firewall Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ **SECURE**

Return to Access Control Policy Management

Default ✎

⏏ Packets → ☒ Prefilter Rules → ☐ Decryption → ☒ Security Intelligence → ☐ Identity → ☒ Access Control

Advanced Settings

Switch to Legacy UI

Analyze ▾ Discard Save

Targeted: 1 device

General Settings ✎		Threat Detection ✎	
Maximum URL characters to store in connection events	1024	Portscan Mode	Disabled
Allow an Interactive Block to bypass blocking for (seconds)	600	Elephant Flow Settings ✎	
Retry URL cache miss lookup	Yes	Generate Elephant Flow Events	Enabled
Enable Threat Intelligence Director	Yes	Intelligent Application Bypass Settings ✎	
Enable reputation enforcement on DNS traffic	Yes	Intelligent Application Bypass Settings	Off
Inspect traffic during policy apply	Yes	Total Apps and Filters Configured	All applications including unidentified applications
Identity Policy Settings ✎		Transport/Network Layer Preprocessor Settings ✎	
Identity Policy	None	Ignore the VLAN header when tracking connections	No
Decryption Policy Settings ✎		Detection Enhancement Settings ✎	
Decryption Policy to use for inspecting encrypted connections	None		

Application Visibility Dashboards

Encrypted Visibility Engine: ON

Prefilter Policy Settings			Performance Settings		
Prefilter Policy used before access control	Default Prefilter Policy		Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet		5
Network Analysis and Intrusion Policies			Performance Statistics - Sample Time (seconds)		300
Intrusion Policy used before Access Control rule is determined	Balanced Security and Connectivity		Regular Expression - Limit	Default Value	
Intrusion Policy Variable Set	Default-Set		Regular Expression - Recursion Limit	Default Value	
Default Network Analysis Policy	Balanced Security and Connectivity		Intrusion Event Logging Limits - Max Events Stored Per Packet		8
Threat Defense Service Policy			Latency-Based Performance Settings		
Threat Defense Service Rule(s)	0		Applied from Installed Rule Update	true	
Files and Malware Settings			Packet Handling	Disabled	
Limit the number of bytes inspected when doing file type detection	1460		Rule Handling	Enabled	
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2		Rule Handling - Threshold (microseconds)	512	
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760		Rule Handling - Consecutive Threshold Violations Before Suspending Rule	3	
Minimum file size for advanced file inspection and storage (bytes)	6144		Rule Handling - Suspension Time (seconds)	10	
Encrypted Visibility Engine			Encrypted Visibility Engine		
			Encrypted Visibility Engine	Disabled	

How to enable the Encrypted Visibility Engine

Encrypted Visibility Engine: ON

The screenshot displays the Cisco Secure Manager configuration interface. On the left, a sidebar lists various settings categories: Prefilter Policy Settings, Network Analysis and Intrusion Policies, Threat Defense Service Policy, and Files and Malware Settings. The main area shows the 'Encrypted Visibility Engine' configuration window, which is currently open. This window contains a blue information box with instructions for Snort 3 devices, a section titled 'About Encrypted Visibility Engine' explaining its machine learning capabilities, and a list of prerequisites for improved efficacy. At the bottom of the window, the 'Encrypted Visibility Engine (EVE)' toggle switch is shown in the 'ON' position. The background interface shows various other settings, including 'Pattern Matching Limits' and 'Encrypted Visibility Engine' status, which is currently 'Disabled'.

Encrypted Visibility Engine

For Snort 3 devices 7.4.0 onwards, use this window to configure the following:

- **Assign Client Applications to EVE-detected Processes** (disabling this feature is not applicable for Snort 3 devices 7.3.0 and earlier)
- **Enable Enhanced Analytics**
- **Block Traffic Based on EVE Score**

About Encrypted Visibility Engine

This feature uses machine learning on session metadata to provide insights, such as the name of the process that initiated a connection and whether that process is associated with malware, into encrypted traffic without needing to perform decryption. A valid IPS license is required to use this feature.

For improving efficacy of this feature, ensure that you have enabled:

1. Automatic updates for future Cisco vulnerability database (VDB) releases (Use System > Tools > Scheduling).
2. Cisco Success Network (Use Integration > SecureX > Enable Cisco Success Network).

Encrypted Visibility Engine (EVE) ☒

How to enable the Encrypted Visibility Engine

Save Policy

Firewall Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⓘ ⚙️ ? admin ▾ cisco SECURE

↩️ [Return to Access Control Policy Management](#)

🔒 Default ✎

📁 Packets → ✔️ Prefilter Rules → ○ Decryption → ✔️ Security Intelligence → ○ Identity → ✔️ Access Control

⌵ Advanced Settings

Switch to Legacy UI

🔍 Analyze ▾ Discard Save

Targeted: 1 device

General Settings ✎		Threat Detection ✎	
Maximum URL characters to store in connection events	1024	Portscan Mode	Disabled
Allow an Interactive Block to bypass blocking for (seconds)	600	Elephant Flow Settings ✎	
Retry URL cache miss lookup	Yes	Generate Elephant Flow Events	Enabled
Enable Threat Intelligence Director	Yes	Intelligent Application Bypass Settings ✎	
Enable reputation enforcement on DNS traffic	Yes	Intelligent Application Bypass Settings	Off
Inspect traffic during policy apply	Yes	Total Apps and Filters Configured	All applications including unidentified applications
Identity Policy Settings ✎		Transport/Network Layer Preprocessor Settings ✎	
Identity Policy	None	Ignore the VLAN header when tracking connections	No
Decryption Policy Settings ✎		Detection Enhancement Settings ✎	
Decryption Policy to use for inspecting encrypted connections	None		

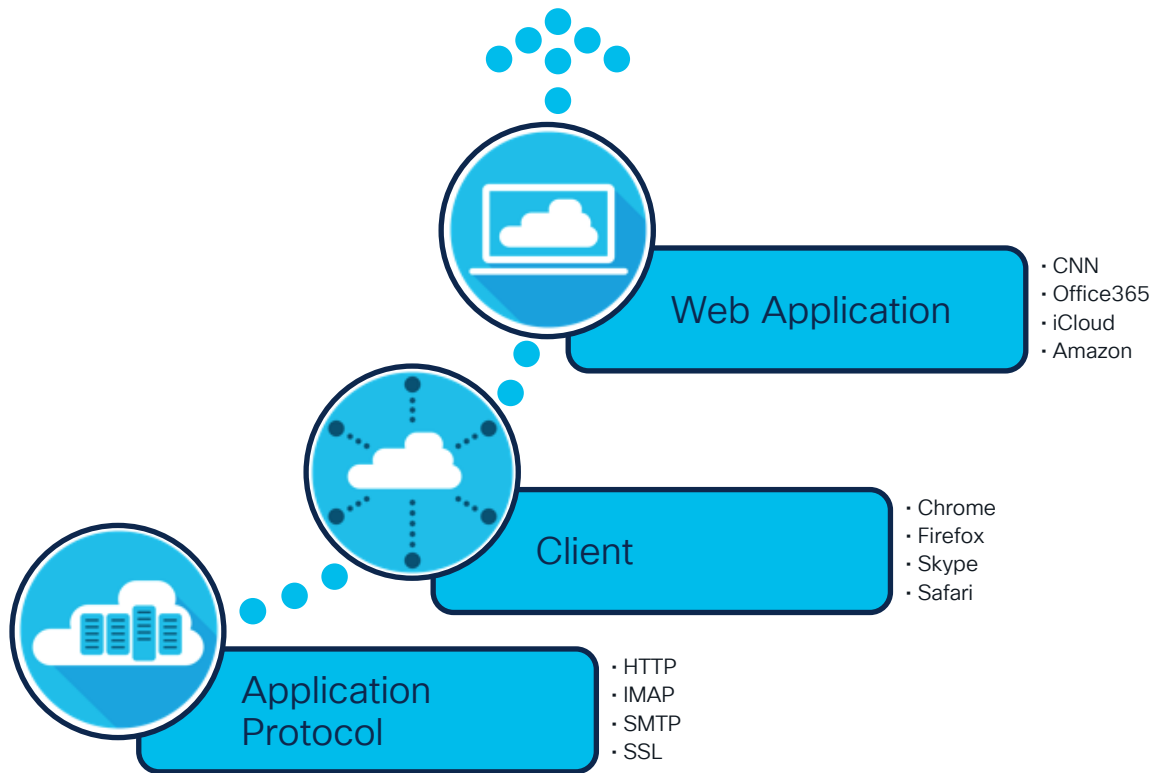
How to enable the Encrypted Visibility Engine

Deploy Changes

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Policies' tab is active, and the 'Policy Editor' is open for the 'Default' policy. The breadcrumb trail shows: Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → Advanced Settings. The 'Advanced Settings' section is expanded, showing various configuration options. A 'Deploy' button is visible in the top right corner. A modal window titled 'Advanced Deploy' is open, showing a search bar with the IP address '192.168.1.178' and a 'Ready for Deployment' status. A message at the bottom of the modal states '1 device is available for deployment'. The background interface shows the 'General Settings' section with various configuration options like 'Maximum URL characters to store in connection events' (1024), 'Allow an Interactive Block to bypass blocking for (seconds)' (600), 'Retry URL cache miss lookup' (Yes), 'Enable Threat Intelligence Director' (Yes), 'Enable reputation enforcement on DNS traffic' (Yes), and 'Inspect traffic during policy apply' (Yes). The 'Identity Policy Settings' section shows 'Identity Policy' set to 'None'. The 'Decryption Policy Settings' section shows 'Decryption Policy to use for inspecting encrypted connections' set to 'None'. The 'Threat Detection Settings' section shows 'Portscan Mitigation' (disabled), 'Elephant Flow Detection' (disabled), 'Intelligent Application Detection' (Off), and 'Total Apps and Filters Configured' (All applications including unidentified applications). The 'Transport/Network Layer Preprocessor Settings' section shows 'Ignore the VLAN header when tracking connections' set to 'No'. The 'Detection Enhancement Settings' section is also visible.

What about the rest of
the visibility capabilities
of our platform

Type of Detectors



Application Visibility Description

What Protocol (HTTP/HTTPS/QUIC) was used to send information for this connection

What Application was running from the “Client’s” side of the traffic to generate this traffic

Where on the Web did this this Application get its content

EVE Process Confidence Score

Time	Application Protocol	Client Application	Web Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility ...	Encrypted Visibility Process Name	Detection Type
2023-03-06 15:44:50	HTTPS	SSL client	Sharepoint Online	https://cisco.sharepoint.com	🔒 tls/1/(0303)(0a0a1301130	62%	microsoft office	ApplD
2023-03-06 15:44:50	HTTPS	SSL client	Sharepoint Online	https://cisco-my.sharepoint.com	🔒 tls/1/(0303)(0a0a1301130	62%	microsoft office	ApplD
2023-03-06 15:44:43	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	🔒 tls/1/(0303)(0a0a1301130	99%	microsoft office	Encrypted Visibility
2023-03-06 15:44:42	ICMP	ICMP client						ApplD
2023-03-06 15:44:42	HTTPS	SSL client	Sharepoint Online	https://cisco.sharepoint.com	🔒 tls/1/(0303)(0a0a1301130	62%	microsoft office	ApplD
2023-03-06 15:44:42	HTTPS	SSL client	Sharepoint Online	https://cisco-my.sharepoint.com	🔒 tls/1/(0303)(0a0a1301130	62%	microsoft office	ApplD

If confidence > 90% use matched ApplD for Client.

EVE Detects “microsoft office”
Assigns Client App “Office 365”

AppID Portal

appid.cisco.com

- Provides details about each application supported for the Cisco Secure Firewall
- Release Notes for each update
- Support Tools for:
 - Current Detectors
 - New Detector Requests
 - Encrypted Visibility Engine
- Additional Documentation and Training Resources

The screenshot displays the Cisco AppID Portal interface. At the top, there's a navigation bar with the Cisco logo, 'Secure Firewall Application Detectors', and links for Home, Release Notes, Support, Documentation, and Resources. A search bar is located below the navigation bar. The main content area is divided into several sections:

- Risk and Business Relevance Summary:** A table showing counts for different risk levels and business relevance categories.
- Tags:** A list of tags with their respective counts.
- Categories:** A list of categories with their respective counts.
- Application Details (5,967):** A table listing individual applications with columns for Application Name, Description, Risk, and Business Relevance.

Risk	Business Relevance
Very Low	1,419
Low	908
Medium	1,360
High	1,641
Very High	639

Tags	Count
allows remote connect	90
allows remote control	52
antivirus	13
autostarts/stays resident	25
bittorrent	19

Categories	Count
active directory	8
ad portal	408
anonymizer/proxy	103
application development and testing	31
backup and recovery	9

Application Name	Description	Risk	Business Relevance
050plus	VoIP smartphone app.	Medium	Medium
1&1 Internet	Internet and Domain name service provider.	Very Low	Low
1-800-Flowers	Online retailer of flowers and other gifts.	Low	Very Low
1.1.1.1 App	Offers a free app for mobile that makes internet private, safer and prevents anyone from snooping on the user.	High	High
1000mercis	Advertising and analytics site.	Low	Very Low
1001.com	Provides online games.	High	Low
100Bao	A Chinese P2P file sharing program.	Very High	Very Low
1010i	Provides a puzzle gaming platform.	High	Low
115Tech	Offers online storage client software.	High	High
12178 Game center	Provides online multiplayer gaming services for payment.	Medium	Medium
12306.cn	China Railway online customer service.	Very Low	High
123Movies	Online movie site.	Medium	Very Low
123RF	Online microstock photography library that hosts stock photographs, vector illustrations, footages, and logos.	High	Medium
126.com	Free webmail system.	Very Low	High
17173.com	Chinese social networking site.	Medium	Very Low

2022 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Demo: Custom Detectors

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center										
Analysis / Unified Events		Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	admin	SECURE
Encrypted Visibility Process Name microsoft office Web Application Web Browsing URL *appcenter.ms										
Showing all 198 events (198)										
2023-03-29 20:04:50 EDT → 2023-04-10 20:04:50 EDT 1w 5d										
Time	Destination Port / ICMP Code	Application Protocol	Client Application	Web Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility...	Encrypted Visibility Process...	Detection Type	
2023-04-10 20:04:18	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 19:03:11	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://codepush.appcenter...	tls/1/(0303)(0a0a130113	58%	microsoft office	ApplID	
2023-04-10 17:13:43	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:13:11	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:12:41	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:12:10	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:11:39	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:11:08	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:09:25	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:07:26	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:06:57	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:06:26	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:04:33	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:03:31	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:02:33	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:01:40	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 17:00:44	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 16:58:45	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	
2023-04-10 16:58:14	443 (https) / tcp	HTTPS	Office 365	Web Browsing	https://in.appcenter.ms	tls/1/(0303)(0a0a130113	98%	microsoft office	Encrypted Visi...	

Custom Detectors and Encrypted Visibility Engine

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Policies' tab is selected, and a dropdown menu is open, showing options like Access Control, Network Discovery, Application Detectors, and Zero Trust Application. The main content area shows a list of events under the 'Encrypted Visibility Process Name' filter. The table below shows the first 10 events.

Time	Destination Port / ICMP Code	Application Protocol	Client Application
2023-04-10 20:04:18	443 (https) / tcp	HTTPS	Office 365
2023-04-10 19:03:11	443 (https) / tcp	HTTPS	SSL client
2023-04-10 17:13:43	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:13:11	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:12:41	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:12:10	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:11:39	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:11:08	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:09:25	443 (https) / tcp	HTTPS	Office 365
2023-04-10 17:07:26	443 (https) / tcp	HTTPS	Office 365

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center
Policies / Application Detectors

Overview Analysis **Policies** Devices Objects Integration

Deploy 🔍 2 ⚙️ ⓘ admin ▾ CISCO SECURE

Import/Export | Custom Product Mappings | User Third-Party Mappings

Create Custom Detector

▼ Name (0)

► Custom Filter (0)

► Author (0)

► State (0)

► Protocol (0)

► Category (0)

► Tag (0)

► Risk (0)

► Business Relevance (0)

Name	Detection Type	Details	Port(s)	Type	State
050plus VoIP smartphone app.	TCP	050plus		Basic	☐
1&1 Internet Internet and Domain name service provider.	TCP	1&1 Internet		Basic	☐
1-800-Flowers Online retailer of flowers and other gifts.	TCP	1-800-Flowers		Basic	☐
1.1.1.1 App Offers a free app for mobile that makes internet private, safer and prevents anyone from snooping on the user.	TCP	1.1.1.1 App		Basic	☐
1000mercis Advertising and analytics site.	TCP	1000mercis		Basic	☐
1001.com Provides online games.	TCP	1001.com		Basic	☐
100Bao A Chinese P2P file sharing program.	TCP	100Bao		Basic	☒
1010! Provides a puzzle gaming platform.	TCP	1010!		Basic	☐

Displaying 1 - 50 of 6347 Detectors |< < Page 1 of 127 > >| C

Custom Detectors and Encrypted Visibility Engine

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The main navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Policies' tab is active, and the 'Application Detectors' section is selected. A 'Create Custom Detector' button is visible in the top right. A modal dialog box titled 'Create A Custom Application Detector' is open in the center. The dialog contains the following fields and options:

- Name:** Office365_Supplemental
- Description:** Additional Patterns for O365
- Application:** Office 365 (with a dropdown arrow and a plus sign)
- Detector Type:** ☒ Basic ☐ Advanced

At the bottom of the dialog are 'Cancel' and 'OK' buttons. The background shows a table of existing application detectors with columns for Name, Detection Type, Details, Port(s), Type, and State. The table lists various applications like 050plus, 1&1 Internet, 1-800-Flowers, 1.1.1.1 App, 1000mercis, 1001.com, 100Bao, and 1010!. The bottom status bar indicates 'Displaying 1 - 50 of 6347 Detectors' and 'Page 1 of 127'.

Custom Detectors and Encrypted Visibility Engine

 Firewall Management Center

Policies / Create Detector

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 2 ⚙️ ⓘ admin ▾ 

Office365_Supplemental

SaveSave as NewCancel

Additional Patterns for O365

Detector Information

Author admin

Application

Office 365 ▾

 +

State Inactive

Type Application: Pattern

Do not upload .lua files from untrusted sources

Detection Patterns

Add

Detection Type	Pattern Type	Pattern	Offset	Port(s)	Min Process Confidence	
There are no patterns. Click "Add" to add a pattern.						

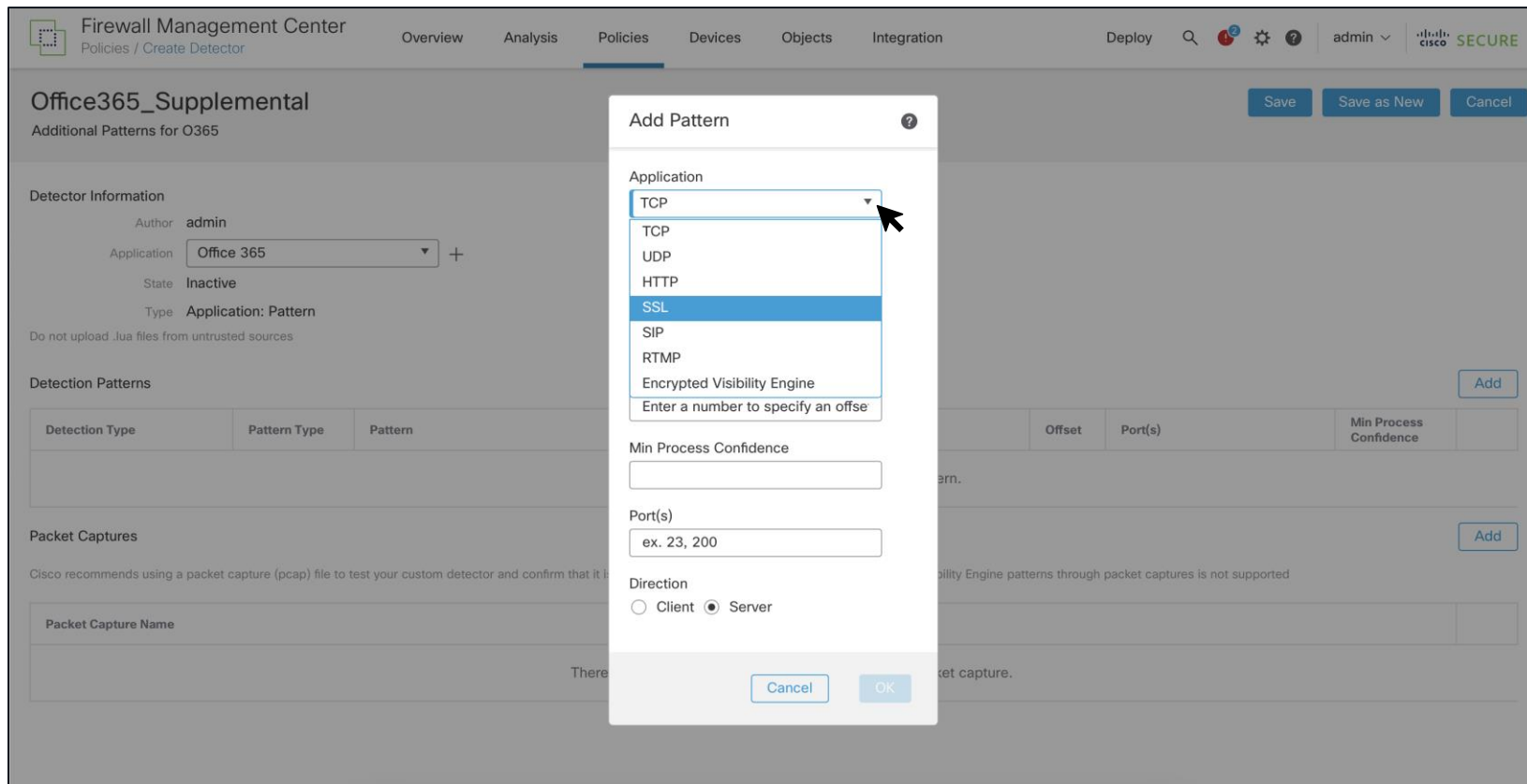
Packet Captures

Add

Cisco recommends using a packet capture (pcap) file to test your custom detector and confirm that it is compatible with your deployment. Testing Encrypted Visibility Engine patterns through packet captures is not supported

Packet Capture Name	
There are no packet captures. Click "Add" to add a packet capture.	

Custom Detectors and Encrypted Visibility Engine



Firewall Management Center
Policies / Create Detector

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ✓ CISCO SECURE

Office365_Supplemental

Additional Patterns for O365

Save Save as New Cancel

Detector Information

Author: admin

Application: Office 365 +

State: Inactive

Type: Application: Pattern

Do not upload .lua files from untrusted sources

Detection Patterns

Detection Type	Pattern Type	Pattern
----------------	--------------	---------

Packet Captures

Cisco recommends using a packet capture (pcap) file to test your custom detector and confirm that it is working as expected.

Packet Capture Name

There is no support for Encrypted Visibility Engine patterns through packet captures

Packet capture.

Add Pattern

Application

- TCP
- UDP
- HTTP
- SSL
- SIP
- RTMP
- Encrypted Visibility Engine
- Enter a number to specify an offset

Min Process Confidence

Port(s)
ex. 23, 200

Direction
☐ Client ☒ Server

Cancel OK

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center
Policies / Create Detector

Overview Analysis **Policies** Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ✓ CISCO SECURE

Office365_Supplemental

Additional Patterns for O365

Detector Information

Author: admin

Application: Office 365 +

State: Inactive

Type: Application: Pattern

Do not upload .lua files from untrusted sources

Detection Patterns

Detection Type	Pattern Type	Pattern	Offset	Port(s)	Min Process Confidence
There are no patterns. Click "Add" to add a pattern.					

Packet Captures

Cisco recommends using a packet capture (pcap) file to test your custom detector and confirm that it is compatible with your deployment. Testing Encrypted Visibility Engine patterns through packet captures is not supported.

Packet Capture Name

There are no packet captures. Click "Add" to add a packet capture.

Add Pattern

Application: SSL

Type: SSL Host

Pattern *: appcenter.ms

Cancel OK

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center

Policies / Create Detector

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 2 ⚙️ ⓘ admin ▾

SECURE

Office365_Supplemental

Additional Patterns for O365

You have unsaved changes Save Save as New Cancel

Detector Information

Author admin

Application Office 365 +

State Inactive

Type Application: Pattern

Do not upload .lua files from untrusted sources

Detection Patterns

Add

Detection Type	Pattern Type	Pattern	Offset	Port(s)	Min Process Confidence	
SSL	SSL Host	appcenter.ms	n/a	n/a	n/a	

Packet Captures

Add

Cisco recommends using a packet capture (pcap) file to test your custom detector and confirm that it is compatible with your deployment. Testing Encrypted Visibility Engine patterns through packet captures is not supported

Packet Capture Name

There are no packet captures. Click "Add" to add a packet capture.

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center
Policies / Create Detector

Overview Analysis **Policies** Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ **SECURE**

Office365_Supplemental
Additional Patterns for O365

You have unsaved changes **Save** **Save as New** **Cancel**

Detector Information

Author: admin

Application: Office 365 +

State: Inactive

Type: Application: Pattern

Do not upload .lua files from untrusted sources

Detection Patterns

Detection Type	Pattern Type	Pattern	Offset	Port(s)	Min Process Confidence	
SSL	SSL Host	appcenter.ms	n/a	n/a	n/a	 

Packet Captures

Cisco recommends using a packet capture (pcap) file to test your custom detector and confirm that it is compatible with your deployment. Testing Encrypted Visibility Engine patterns through packet captures is not supported

Packet Capture Name

There are no packet captures. Click "Add" to add a packet capture.

Add Pattern ⓘ

Application: Encrypted Visibility Engine

Process Name: microsoft office

Min Process Confidence: 60

Cancel **OK**

Custom Detectors and Encrypted Visibility Engine

 Firewall Management Center

Policies / Create Detector

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 2 ⚙️ ⓘ admin ▾ 

Office365_Supplemental

Additional Patterns for O365

You have unsaved changes Save Save as New Cancel

Detector Information

Author admin

Application Office 365 +

State Inactive

Type Application: Pattern

Do not upload .lua files from untrusted sources

Detection Patterns

Detection Type	Pattern Type	Pattern	Offset	Port(s)	Min Process Confidence	
SSL	SSL Host	appcenter.ms	n/a	n/a	n/a	 
Encrypted Visibility Engine	Process Name	microsoft office	n/a	n/a	60	 

Add

Packet Captures

Cisco recommends using a packet capture (pcap) file to test your custom detector and confirm that it is compatible with your deployment. Testing Encrypted Visibility Engine patterns through packet captures is not supported

Packet Capture Name

There are no packet captures. Click "Add" to add a packet capture.

Add

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center
Policies / Application Detectors

Overview Analysis **Policies** Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ **SECURE**

[Import/Export](#) | [Custom Product Mappings](#) | [User Third-Party Mappings](#)

Filters:

Name: ✕ [Create Custom Detector](#)

▼ Name (1)

☒

☐

► Custom Filter (0)

► Author (0)

► State (0)

► Protocol (0)

► Category (0)

► Tag (0)

► Risk (0)

► Business Relevance (0)

Name	Detection Type	Details	Port(s)	Type	State	
Office365_Supplemental Additional Patterns for O365	MULTIPLE	Office 365		Basic	☒	✎ ✕ 🗑️

Displaying 1 - 1 of 1 Detectors matching the filter |< < Page 1 of 1 >| ↻

Custom Detectors and Encrypted Visibility Engine

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, and Integration. The breadcrumb trail is Policies / Application Detectors. The main content area displays a table of custom detectors. A filter is applied to the 'Name' column with the value 'supplemental'. The table lists one detector: 'Office365_Supplemental' with a detection type of 'MULTIPLE' and a state of 'Basic'. A success dialog box is overlaid on the table, stating 'Success' and 'Successfully activated 1 detector(s)'. The dialog has an 'OK' button. The bottom of the interface shows a pagination bar indicating 'Displaying 1 - 1 of 1 Detectors matching the filter'.

Name	Detection Type	Details	Port(s)	Type	State
Office365_Supplemental Additional Patterns for O365	MULTIPLE	Office 365		Basic	☒

Success

Successfully activated 1 detector(s).

OK

Custom Detectors and Encrypted Visibility Engine

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

URL

*appcenter.ms

<

AppID relation with EVE Processes

Applications with the Tag: [encrypted visibility engine](#) are supported with EVE.

For any application related need, checkout:
Secure Firewall Application Detectors portal at
appid.cisco.com



CISCO Secure Firewall Application Detectors Home Release Notes Support Documentation Resources Feedback

Tags: encrypted visibility engine X Search

Risk	Business Relevance	Tags	Categories
Very Low	1,419	encrypted visibility engine	active directory
Low	908	encrypts communications	ad portal
Medium	1,360	evasive	anonymizer/proxy
High	1,641	facebook	application development and testing
Very High	639	facebook game	backup and recovery

Application Details (303)

Application Name	Description	Risk	Business Relevance
1Password	Password management application.	Medium	Medium
2048 Game	Online game.	High	Low
AccuWeather	Weather forecasting website.	Very Low	Low
Adobe Connect	Online meeting and collaboration system.	Low	High
ADrive	Online file storage and backup.	Very Low	High
Aircall	Provides cloud based call center software and business phone system.	Very High	Medium
Airtable	Airtable is a collaboration software which provides a way to create your own organizational databases.	High	High
Amazon	Online retailer of books and most other goods.		
- Amazon Web Services	Online cloud computing service.	Medium	High

What's New in 7.4

- Access Control Policy Driven Options
- New Feedback UI based feedback and troubleshooting mechanism
- New Protocol Coverage

Access Control Policy -> Advanced Settings

- New Options:
 - Control for Applications
 - Enhanced Analytics
 - Blocking traffic based on Encrypted Visibility Threat Score

Encrypted Visibility Engine ?

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. [Learn more](#)

Recommended Settings ▼

- [Enable](#) automatic updates for future Cisco Vulnerability Database (VDB) releases.
- [Enable](#) Cisco Success Network.

Encrypted Visibility Engine (EVE) ☑

Use EVE for Application Detection ☑

Allow EVE to assign client applications to processes.

EVE Enhanced Analytics ☑

Add EVE's fingerprint information in the connection events.

Block Traffic Based on EVE Score ☑

i Customize your threshold for blocking traffic based on the EVE scores.

i **Advanced Mode** ☐ — Block

Very Low Low Medium High Very High

Encrypted Visibility Fingerprint

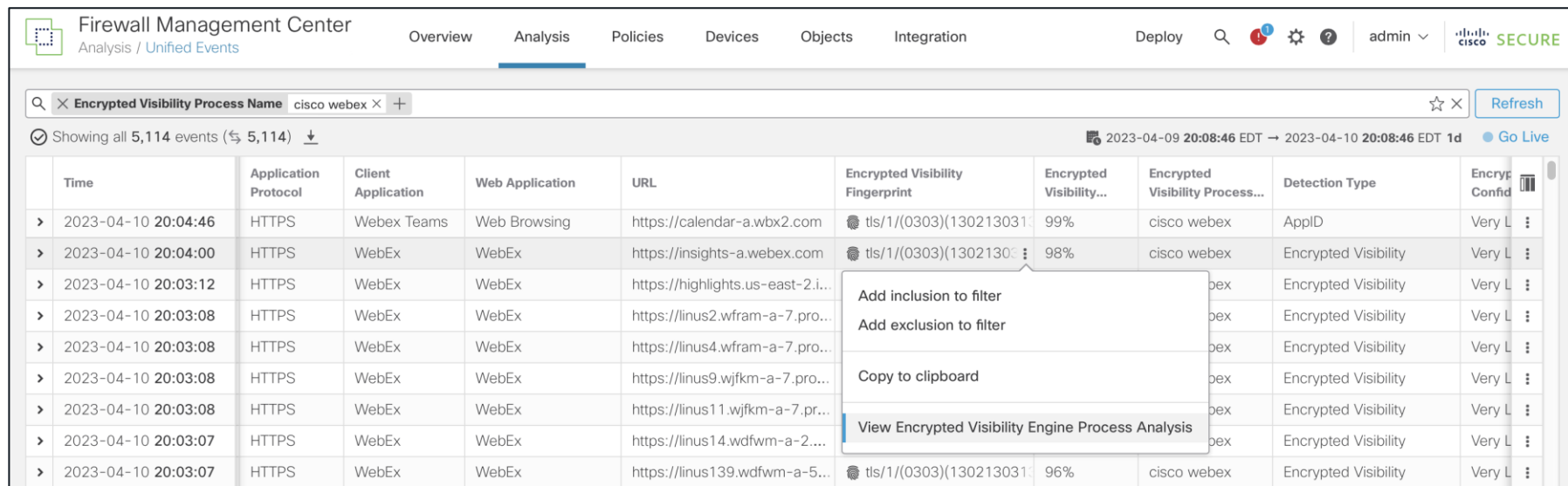
- New Connection Field: Encrypted Visibility Fingerprint
- Exposes the uniqueness of a fingerprint to users for additional traffic analysis

Firewall Management Center										
Analysis / Unified Events		Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	admin	CISCO SECURE
Encrypted Visibility Process Name cisco webex										
Showing all 5,114 events (5,114)										
2023-04-09 20:08:46 EDT → 2023-04-10 20:08:46 EDT 1d										
Time	Application Protocol	Client Application	Web Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility...	Encrypted Visibility Process...	Detection Type	Encryp Confid	
2023-04-10 20:04:46	HTTPS	Webex Teams	Web Browsing	https://calendar-a.wbx2.com	tls/1/(0303)(130213031	99%	cisco webex	AppID	Very L	
2023-04-10 20:04:00	HTTPS	WebEx	WebEx	https://insights-a.webex.com	tls/1/(0303)(130213031	98%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:12	HTTPS	WebEx	WebEx	https://highlights.us-east-2.i...	tls/1/(0303)(130213031	99%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus2.wfram-a-7.pro...	tls/1/(0303)(130213031	96%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus4.wfram-a-7.pro...	tls/1/(0303)(130213031	96%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus9.wjfk-m-a-7.pro...	tls/1/(0303)(130213031	96%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus11.wjfk-m-a-7.pr...	tls/1/(0303)(130213031	96%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:07	HTTPS	WebEx	WebEx	https://linus14.wdfwm-a-2....	tls/1/(0303)(130213031	96%	cisco webex	Encrypted Visibility	Very L	
2023-04-10 20:03:07	HTTPS	WebEx	WebEx	https://linus139.wdfwm-a-5...	tls/1/(0303)(130213031	96%	cisco webex	Encrypted Visibility	Very L	

Encrypted Visibility Engine Process Analysis

New drop-down menu for Encrypted Visibility Fingerprint.

- “View Encrypted Visibility Engine Process Analysis” redirects to appid.cisco.com for additional details for this fingerprint.



Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin ▾ cisco SECURE

🔍 X Encrypted Visibility Process Name cisco webex X + ☆ X Refresh

🕒 Showing all 5,114 events (↔ 5,114) ⬇ 📅 2023-04-09 20:08:46 EDT → 2023-04-10 20:08:46 EDT 1d 🟢 Go Live

Time	Application Protocol	Client Application	Web Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility...	Encrypted Visibility Process...	Detection Type	Encrypted Confidentiality
2023-04-10 20:04:46	HTTPS	Webex Teams	Web Browsing	https://calendar-a.wbx2.com	tls/1/(0303){130213031	99%	cisco webex	AppID	Very Low
2023-04-10 20:04:00	HTTPS	WebEx	WebEx	https://insights-a.webex.com	tls/1/(0303){130213031	98%	cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:12	HTTPS	WebEx	WebEx	https://highlights.us-east-2.i...			cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus2.wfram-a-7.pro...			cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus4.wfram-a-7.pro...			cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus9.wjfk-m-a-7.pro...			cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:08	HTTPS	WebEx	WebEx	https://linus11.wjfk-m-a-7.pr...			cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:07	HTTPS	WebEx	WebEx	https://linus14.wdfwm-a-2....			cisco webex	Encrypted Visibility	Very Low
2023-04-10 20:03:07	HTTPS	WebEx	WebEx	https://linus139.wdfwm-a-5...	tls/1/(0303){130213031	96%	cisco webex	Encrypted Visibility	Very Low

View from appid.cisco.com: Process Analysis

 Secure Firewall Application Detectors

HomeRelease NotesSupport ▼Documentation ▼Resources ▼

Feedback

Encrypted Visibility Engine Process Analysis

Customer Contact

Customer Email

Customer Name

Costas Kleopa

Customer Name

Encrypted Visibility Details ⓘ

Fingerprint

VDB Version

tls/1/(0303)(130213031301c02cc030c02bc02fc0adc024c028c0acc023c027009d009c003c00ff)[(0000)(000500050100000000)(000a000c000a001d0017001e00190018)(000bc

latest

Application Debug Log(Optional)

Server Name

IP Address

Port

highlights.us-east-2.intelli

3.14.63.31

443

View Request

 ⓘ To provide feedback about any of the processes from the list below, select the applicable entries and submit your request. If there are no results you can still submit your request.

☰	Process Name ↑↓	Prevalence ↑↓	Server Name ↑↓	IP Address ↑↓	Port ↑↓
☐	cisco webex	0.9994	0.9997	0.0000	0.9994
☐	ciscocolabhost	0.0007	0.0004	0.0000	0.0007
☐	spark-client-framework-integrati	0.0001	0.0000	0.0000	0.0001
☐	lockdown mac tunnel	0.0000	0.0000	0.0000	0.0000
☐	zscaler tunnel	0.0000	0.0000	0.0000	0.0000
☐	clashx pro	0.0000	0.0000	0.0000	0.0000
☐	chromium	0.0000	0.0000	0.0000	0.0000

Submit Request

 Secure Firewall Application Detectors

HomeRelease NotesSupport ▾Documentation ▾Resources ▾Feedback

Encrypted Visibility Engine Process Analysis

Customer Contact

Customer Email

Customer Name

Costas Kleopa

Customer Name

Encrypted Visibility Details ⓘ

Fingerprint

VDB Version

tls/1/(0303)(130213031301c02cc030c02bc02fc0adc024c028c0acc023c027009d009c003c00ff)[(0000)(000500050100000000)(000a000c000a001d0017001e00190018)(000bc

latest

Application Debug Log(Optional)

Server Name

IP Address

Port

highlights.us-east-2.intelli

3.14.63.31

443

View Request

 ⓘ To provide feedback about any of the processes from the list below, select the applicable entries and submit your request. If there are no results you can still submit your request.

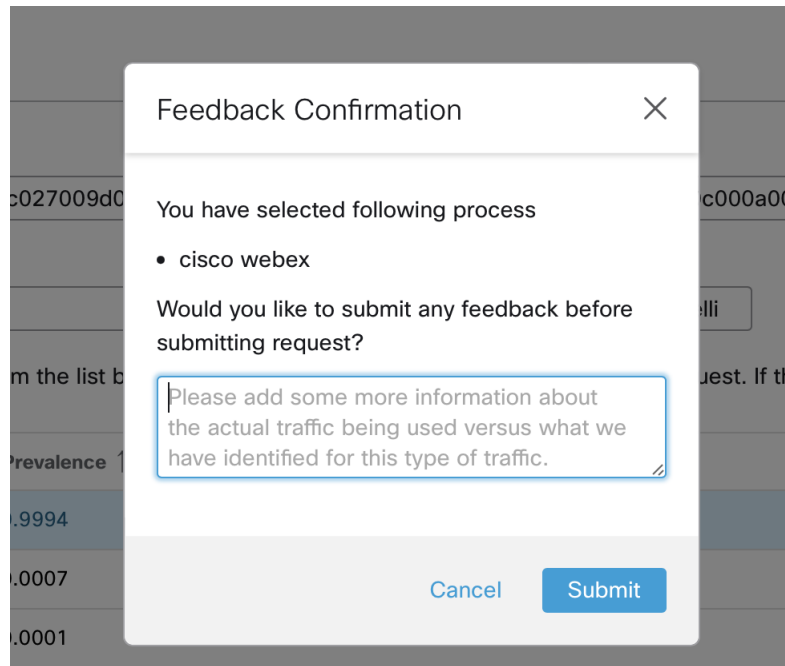
☰	Process Name ↑↓	Prevalence ↑↓	Server Name ↑↓	IP Address ↑↓	Port ↑↓
☒	cisco webex	0.9994	0.9997	0.0000	0.9994
☐	ciscocollabhost	0.0007	0.0004	0.0000	0.0007
☐	spark-client-framework-integrati	0.0001	0.0000	0.0000	0.0001
☐	lockdown mac tunnel	0.0000	0.0000	0.0000	0.0000
☐	zscaler tunnel	0.0000	0.0000	0.0000	0.0000
☐	clashx pro	0.0000	0.0000	0.0000	0.0000
☐	chromium	0.0000	0.0000	0.0000	0.0000

Submit Request

Submit a Request for Feedback

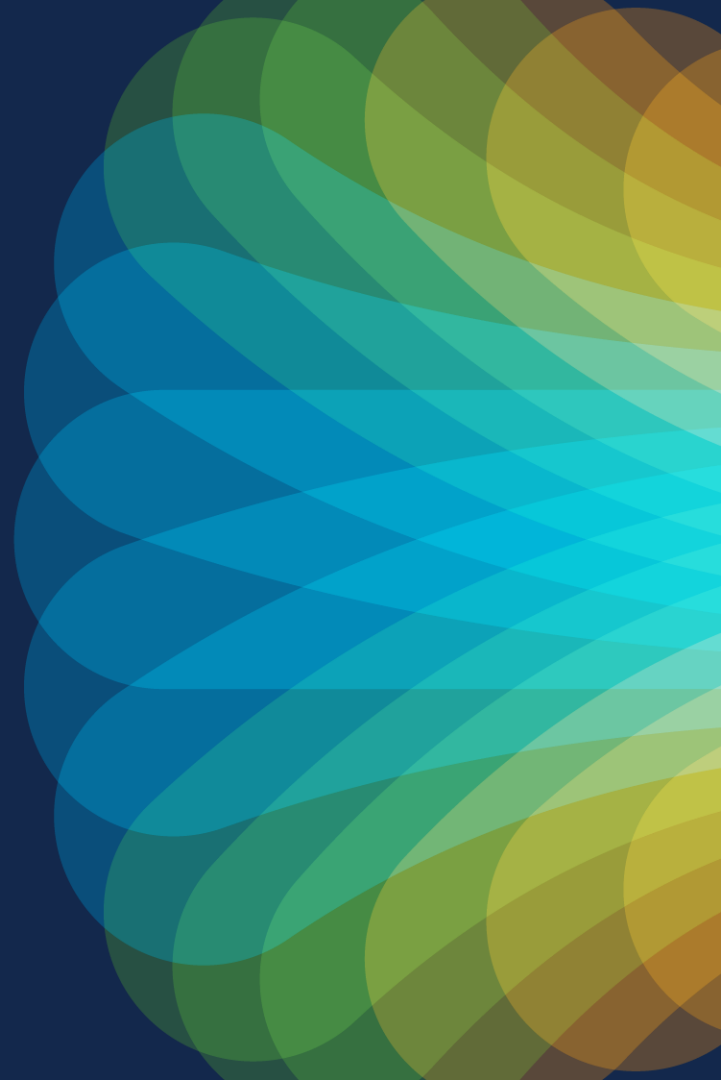
<https://appid.cisco.com/eve>

- AppID Portal provides direct feedback for any discrepancy for process identification
- Helps Improve efficacy and additional coverage for unknown processes
- Direct feedback with the respective teams for any request made for this request.



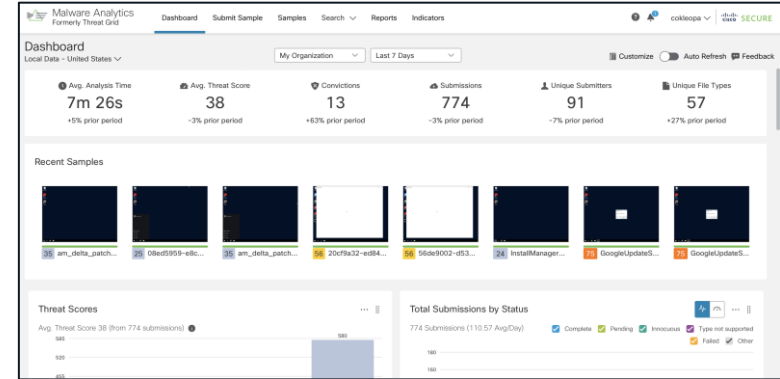
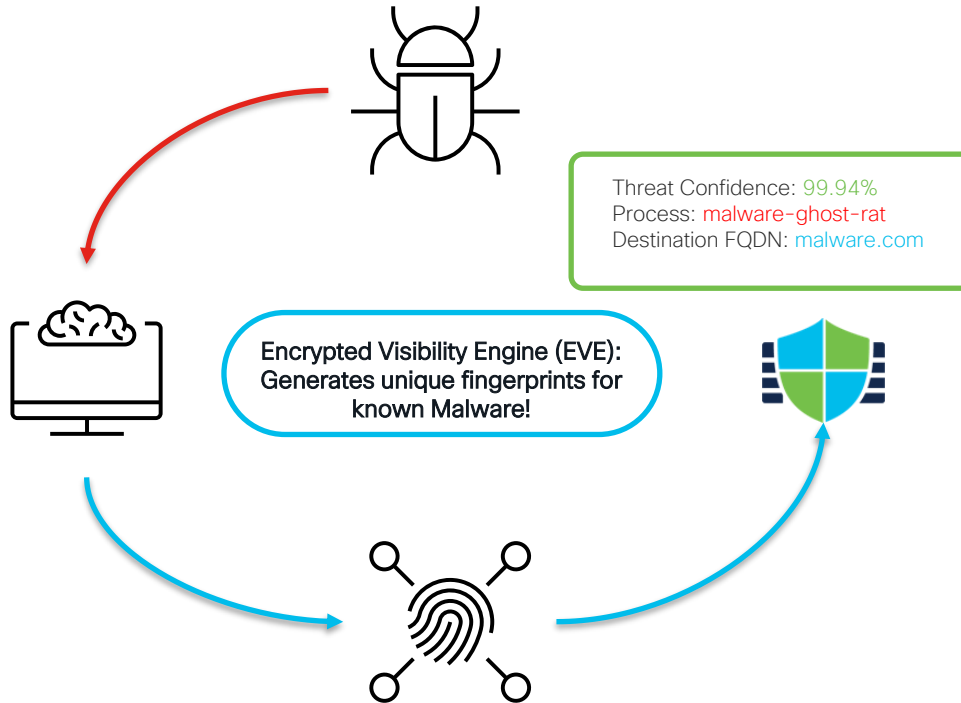
The screenshot shows a 'Feedback Confirmation' dialog box with a close button (X) in the top right corner. The text inside the dialog reads: 'You have selected following process' followed by a bulleted list containing 'cisco webex'. Below this, it asks 'Would you like to submit any feedback before submitting request?'. There is a text input field with the placeholder text 'Please add some more information about the actual traffic being used versus what we have identified for this type of traffic.' and a small icon of a notepad and pencil to its right. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Submit'.

Threat Detection

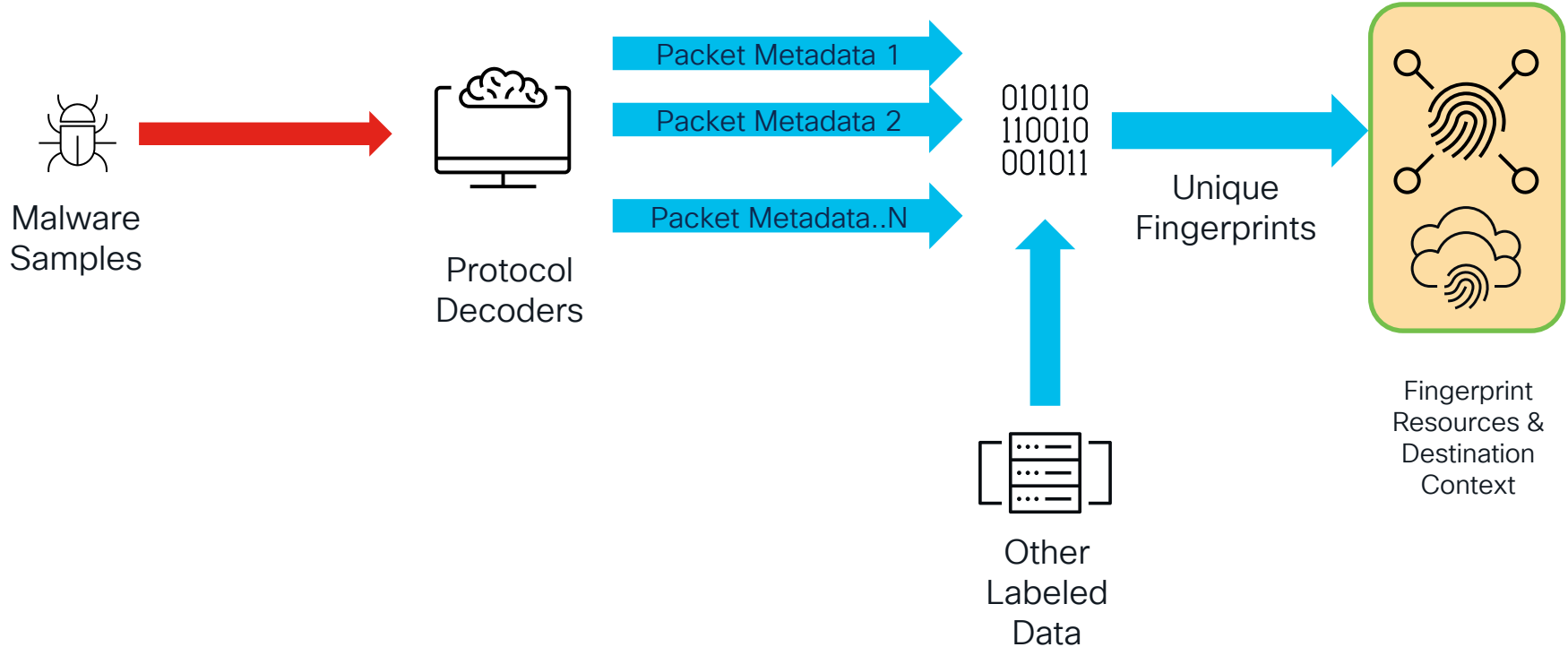


EVE and Threat Detection

Improving Threat Detection using Malware Analytics Labeled Data Sets

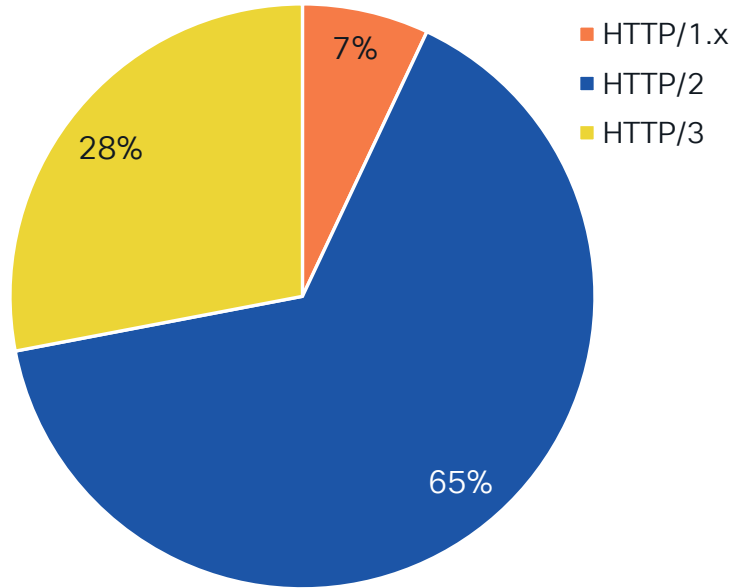


Machine Learning Process



EVE and Threat Detection

From Initial Slide: Your Network Encrypted



- EVE has created a Unique Fingerprint Analysis with a Machine Learning Process for all types of protocols
- Applies the Labeled malware resources through ML analytics

EVE and Threat Detection

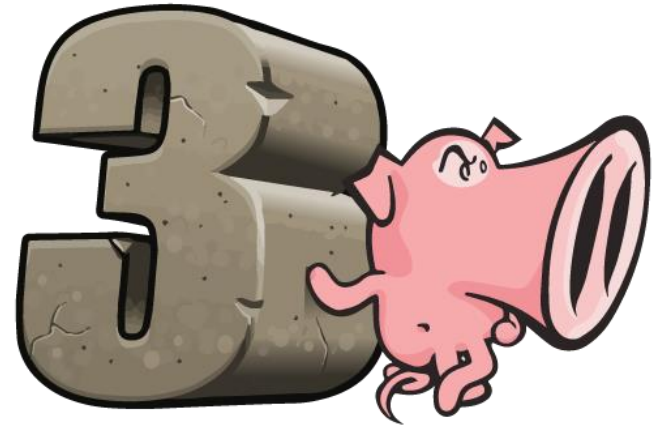
Current Protocol Support with Fingerprinted Traffic

Protocol	Unique Metadata Analysis
TLS	Client Hello
HTTP/3	QUIC -> Client Hello
HTTP	HTTP Headers

EVE and Threat Detection

Benefits

- New Coverage from all our Threat Centric Capabilities
 - EVE provides additional protection with
 - Security Intelligence (IP & URL Reputation)
 - Intrusion Protection Snort (IPS) Rules
 - Malware Analysis to Cloud
 - and now the **Encrypted Visibility Engine**
- Direct Correlations to Malware Analytics Portal (Formerly Threat Grid)



EVE and Threat Detection

Direct Correlations to Malware Analytics Portal (Formerly Threat Grid)

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

1

⚙️

?

ckleopa ▾

CISCO

SECURE

Q

✕ Encrypted Visibility Process Name

malware

✕

+

☆ ✕

Refresh

🕒 Showing all 182 events (🔍 182) ⌵

📅 2023-03-31 13:52:40 EDT → 2023-04-14 13:52:40 EDT 2w

Go Live

	Time	Destination IP	Destination Port / ICMP Code	Encrypted Visibility Process Name	Encrypted Visibility Fingerprint	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score	Encrypted Visibility Process Confidence Score	
➤	2023-04-14 10:48:36	184.29.170.137	80 (http) / tcp	malware-known-trojan	🔒 http/(48454144)(485...	Very High	97%	60%	⋮
➤	2023-04-14 10:48:35	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:32	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:31	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:31	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:31	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:31	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:31	23.45.112.9	80 (http) / tcp	malware-adware			97%	60%	⋮
➤	2023-04-14 10:48:31	23.45.112.9	80 (http) / tcp	malware-adware	🔒 ht...		97%	60%	⋮

Add inclusion to filter

Add exclusion to filter

Copy to clipboard

View Encrypted Visibility Engine Process Analysis🔗

View Encrypted Visibility Engine Process Analysis

EVE and Threat Detection

 Secure Firewall Application Detectors

HomeRelease NotesSupport ▾Documentation ▾Resources ▾Feedback

Encrypted Visibility Engine Process Analysis

Customer Contact

Costas Kleopa

Customer Email

ckleopa@cisco.com

Customer Name

Customer Name

Encrypted Visibility Details ⓘ

Fingerprint

http/(48454144)(485454502f312e31)((486f7374)(557365722d4167656e74)(4163636570743a202a2f2a))

VDB Version

latest

Application Debug Log(Optional)

Server Name

184.29.170.137

IP Address

184.29.170.137

Port

80

View Request

To provide feedback about any of the processes from the list below, select the applicable entries and submit your request. If there are no results you can still submit your request.

	Process Name ↑↓	Prevalence ↑↓	Server Name ↑↓	IP Address ↑↓	Port ↑↓
☐	sogoucloud	0.0000	0.0000	0.0000	0.0000
☐	xmlspy	0.0000	0.0000	0.0000	0.0000
☒	malware-known-trojan	0.0000	0.0000	0.0000	0.0000
☐	malware-adware	0.0000	0.0000	0.0000	0.0000
☐	malware-unknown	0.0000	0.0000	0.0000	0.0000
☐	malware-trojan-begseabug	0.0000	0.0000	0.0000	0.0000
☐	malware-synares	0.0000	0.0000	0.0000	0.0000

Submit Request

Redirecting to Malware Analytics

EVE and Threat Detection: Malware Analytics

 Malware Analytics
Formerly Threat Grid

Dashboard Submit Sample Samples Search Reports Indicators

?

1

cokleopa

 **SECURE**

Indicators

Local Data - United States

IndicatorsATT&CK

DownloadCategory InformationFeedback

FilterAPI

malware-known-trojan

Recent Indicators

☐ Added Last 30 Days

☐ Updated Last 30 Days

Show Indicators

☒ All

☐ Active Only

☐ Inactive Only

Scope

☒ All

☐ My Organization

☐ My Samples

Date Range

☐ Last 24 Hours

☐ Last 7 Days

☐ Last 30 Days

Reset

Show Indicators: AllScope: AllLast 90 DaysActive Xmalware-known-trojan X

Indicator	Indicator Score	Sample Hits	Trend	Prior Period Change	Categories
Artifact Flagged as Known Trojan by Antivirus	95	1.429M		▲ 29%	Anti-Virus
Artifact Flagged as Known Trojan by Antivirus					
Indicator Score: 95 Description An antivirus engine flagged an artifact as a Trojan. A Trojan is a program that gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload, often a backdoor allowing unauthorized access to the system. Trojans may steal information or infect the host systems. They are commonly installed by drive-by downloads or embedded into games or Internet driven applications. Trigger This indicator is triggered when antivirus flags an artifact and the signature contains 'Trojan'.					
Signed Artifact Flagged as Known Trojan by Antivirus	85	24.65k		▲ 10%	Anti-Virus

125 per page

CISCO *Live!*

#CiscoLive BRKSEC-2099

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

78

Conclusion

Encrypted Visibility Engine

- A new differentiator for Cisco Secure Firewall
- Visibility for Encrypted Networks
- Adopts detection through a continuously changing world
- Provides Protection and Control without Decryption

Fill out your session surveys!



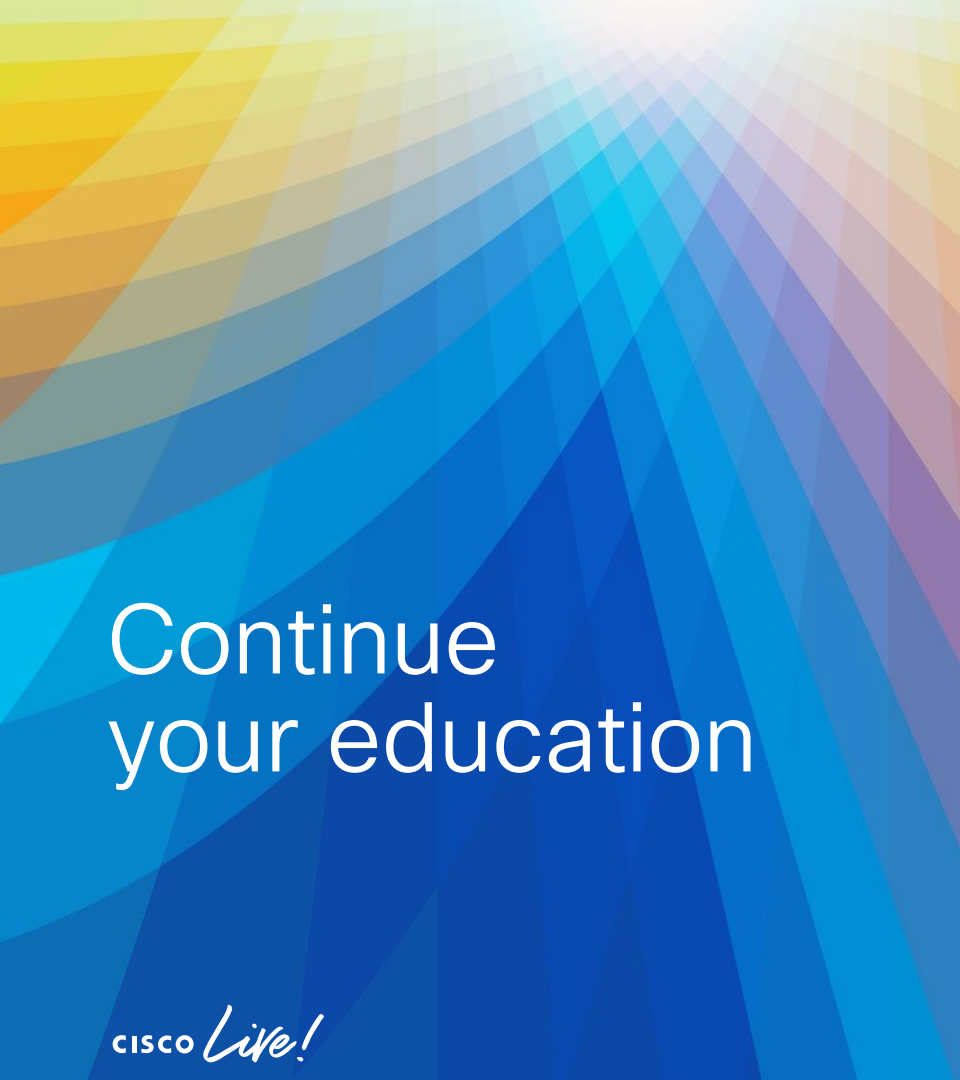
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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



The bridge to possible

Thank you

CISCO *Live!*

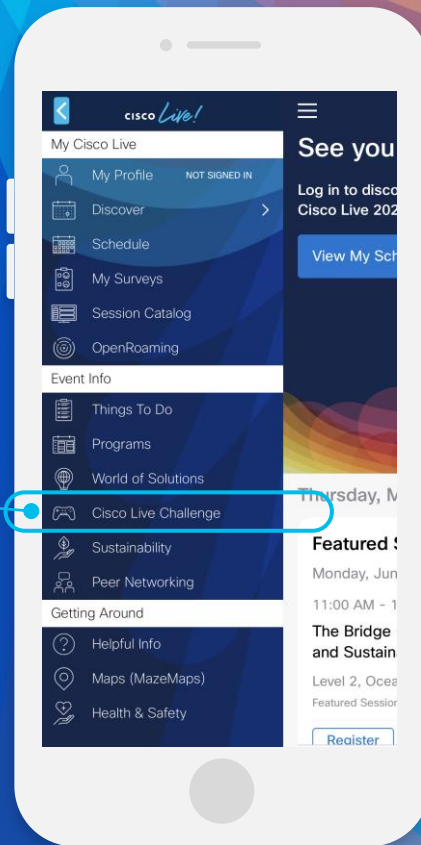
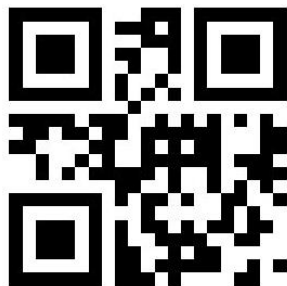
#CiscoLive

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background of the slide is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow and green on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, with colors ranging from blue and purple to yellow and orange. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive