

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

Resiliency & Efficiency with Secure Firewall

Bill Mabon, Cloud & Network Security Products
PSOSEC-1022

CISCO *Live!*

#CiscoLive

Cisco Webex app

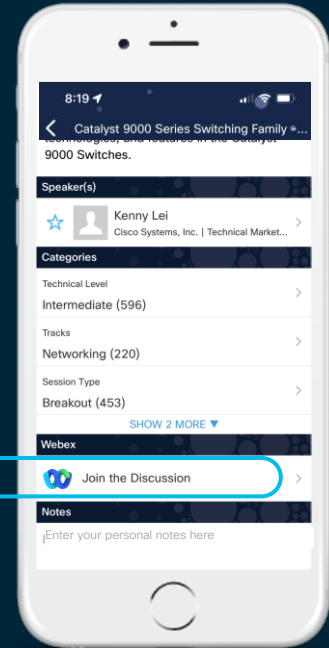
Questions?

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 17, 2022.



<https://cicolive.ciscoevents.com/cicolivebot/#PROSEC-1022>



Agenda

- Total Economic Impact Report Results
- Cloud-delivered Firewall Management Center
- Visibility innovations
- Firewalling your “hybrid” world
- New Secure Firewall 3100 Series

Secure Firewall Total Economic Impact



Total Economic Impact™ Report – March 2022

- Independent Forrester Consulting measurement of Secure Firewall business value
- More information
 - <https://blogs.cisco.com/security/the-total-economic-impact-of-cisco-secure-firewall>

OR



Prior-state challenges

- Limited visibility and threat defense
- High costs deploying and managing firewalls
- Sub-optimal network performance

Select interview feedback

“... I no longer have to sit around and babysit the upgrade process.”

“Ease of administration and integration has been one of the advantages of Cisco. We also benefit from data enrichment as different systems more easily feed each other.”

“We’re no longer dealing with one-off configurations.”

“... enabled us to quickly ramp up and deploy new firewalls. We didn’t have to grow employees as we grew firewalls.”

“We previously lacked capabilities like modern application control. We couldn’t tell how our users were using the network...”



55 labor
hours saved
for policy
deployment
& updates



95%
reduction
in routine firewall
task time



NPV: \$12.29m
ROI: 195%
over three years



10 Month
Payback Period


Key Results



Up to 80%
reduction in data
breach risk



49%
time savings in
threat detection



83%
faster incident
response (IR)



Cisco SecureX
additional benefit
*a further 77%
acceleration in IR*

cloud-delivered
Firewall Management Center



Cloud-delivered Firewall Management Center

Recent enhancements reduce routine task time over 90%*.
Now, we boost your productivity even further.



Eliminate manager
update overhead



Support 1000+
firewalls per tenant



No rack space, lowering
operational cost



Cisco ensures
uptime



Same look and feel,
no learning curve

Same FMC User Experience ... now cloud-delivered

The screenshot shows the Cisco Defense Orchestrator (DO) interface. At the top, the navigation bar includes 'Monitoring', 'Policies', 'Devices', 'Objects', and 'Integration'. The current view is 'Policies / Access Control / Intrusion / Intrusion Policies'. The selected policy is 'Intrusion_S3'. The mode is set to 'Prevention' with a 'Base Policy' of 'Balanced Security and Connectivity'. Statistics show 37,680 Disabled, 469 Alert, 8,838 Block, 0 Overridden, 0 Rewrite, 0 Pass, 0 Drop, and 0 Reject rules.

The 'Recommendations' tab is active, showing a 'Summary' section with 50 items. A sidebar on the left lists categories: All Rules, Browser (6 groups), Server (8 groups), Policy (1 group), Indicator (4 groups), Potentially Unwanted Applications (3 groups), File (9 groups), Malware (5 groups), Operating Systems (5 groups), and Protocol (9 groups).

The 'All Rules' section displays a table of 46,987 rules. The table has columns for Rule Action, Info, Rule Action, and Assigned Groups. The rules listed are:

Rule Action	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	GID:SID	Alert (Default)	Browser/Internet Explorer
<input type="checkbox"/>	1:28496	Alert (Default)	Browser/Internet Explorer
<input type="checkbox"/>	1:32478	Alert (Default)	Browser/Internet Explorer
<input type="checkbox"/>	1:32479	Alert (Default)	Browser/Internet Explorer
<input type="checkbox"/>	1:26633	Alert (Default)	Browser/Internet Explorer
<input type="checkbox"/>	1:31622	Alert (Default)	Browser/Internet Explorer
<input type="checkbox"/>	1:31621	Alert (Default)	Browser/Internet Explorer

Ease of Migration

Defense Orchestrator | Inventory / Change FTD Manager

Change FTD Management

Change FTD Manager from Firewall Management Center to CDO

1 Select FMC **FMC: FMC_Beta2**

2 Select Devices

Select FTD devices to change management from FMC to CDO and specify an action in bulk or per device.

0 device(s) selected Multi-Device Action Retain on FMC for Analytics

<input type="checkbox"/>	Name	IP Address	Domain	Action
<input type="checkbox"/>	FMC_Beta2_OnPremFT...	10.10.14.146:443	Global	Retain on FMC for Analytics
<input type="checkbox"/>	FMC_Beta2_eventsFtd-...	10.10.16.83:443	Global	Retain on FMC for Analytics
<input type="checkbox"/>	FMC_Beta2_OnPremFT...	10.10.14.136:443	Global	Retain on FMC for Analytics
<input type="checkbox"/>	FMC_Beta2_OnPremFT...	10.10.14.141:443	Global	Retain on FMC for Analytics

Change FTD Management


3 Finish

After completing the change FTD manager process, you have up to 14 days to try CDO as your FTD manager and commit or revert to FMC as your FTD manager. After 14 days have passed, the actions you selected during this process will be automatically applied to your devices on the on-premise FMC without requiring further action from you. [Learn more.](#)

Simple Onboarding

- Registration Key based Onboarding
- Low Touch Provisioning using S/N


Follow the steps below




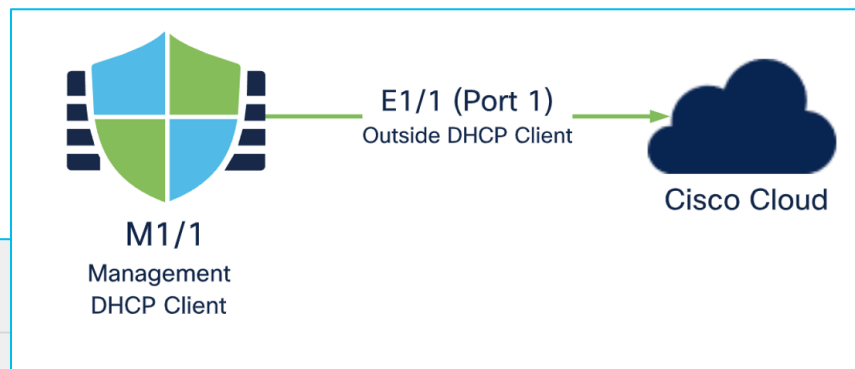
Firepower Threat Defense
Management Mode:

FTD ⓘ **FDM** ⓘ
(Recommended)

90-day Evaluation License:
87 days left
[Manage Smart License](#) ↗

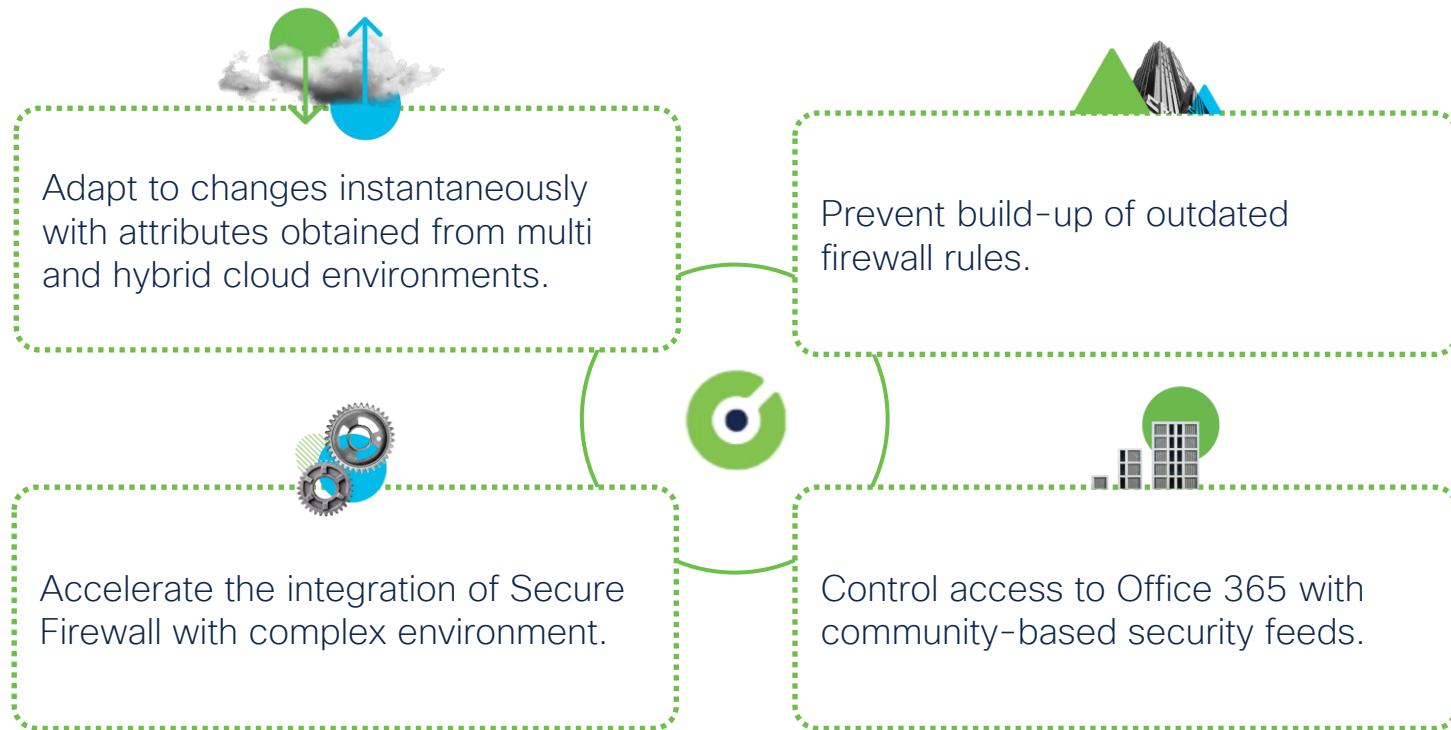

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface.


Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 7.2+)

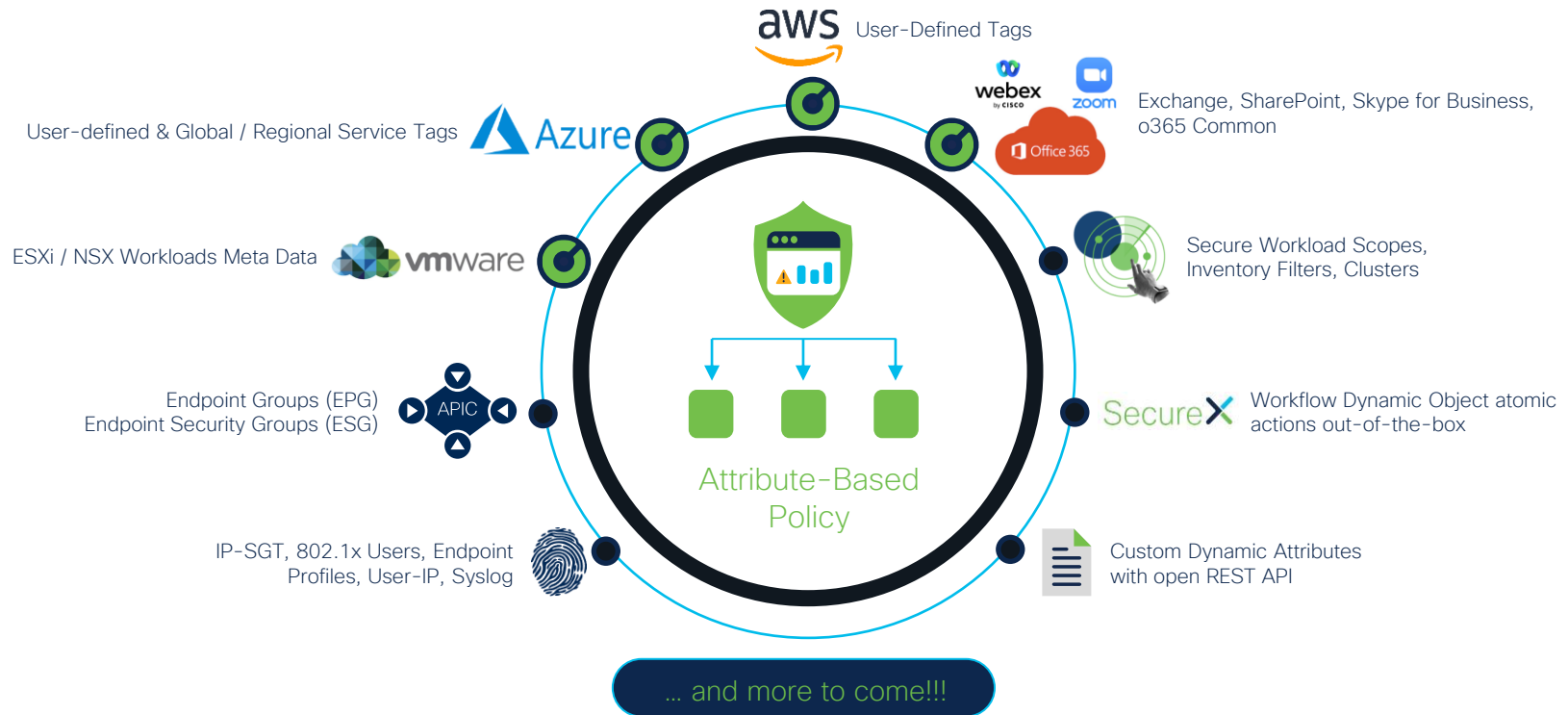


Cisco Secure Dynamic Attribute Connector

Real time policy updates using attributes from cloud environments



Attribute Based Policy



Visibility innovation



Superior visibility – deep packet inspection & beyond



Server Identity
Discovery

FTD 6.7



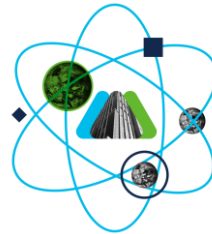
Snort 3

FTD 7.0



Encrypted
Visibility Engine

FTD 7.2



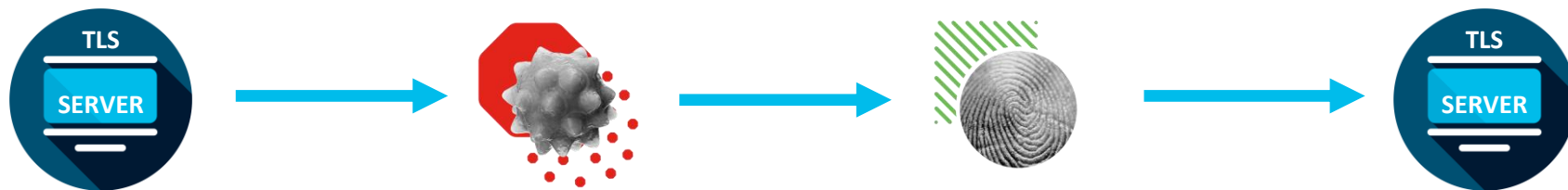
Real-time
flow context
from client

Future

Encrypted Visibility Engine IDs threats w/o decryption

Only Secure Firewall sees encrypted traffic of interest, like malicious VPNs, Tor, shadow IT apps, and more

- The competition says *decrypt everything*, but in the real world that's not realistic
- Based upon Cisco's open-source Project Mercury; supports TLS & QUIC
- Advanced machine learning identifies client apps/processes/browsers
- Identifies malware based upon fingerprints



Resilience for hybrid work

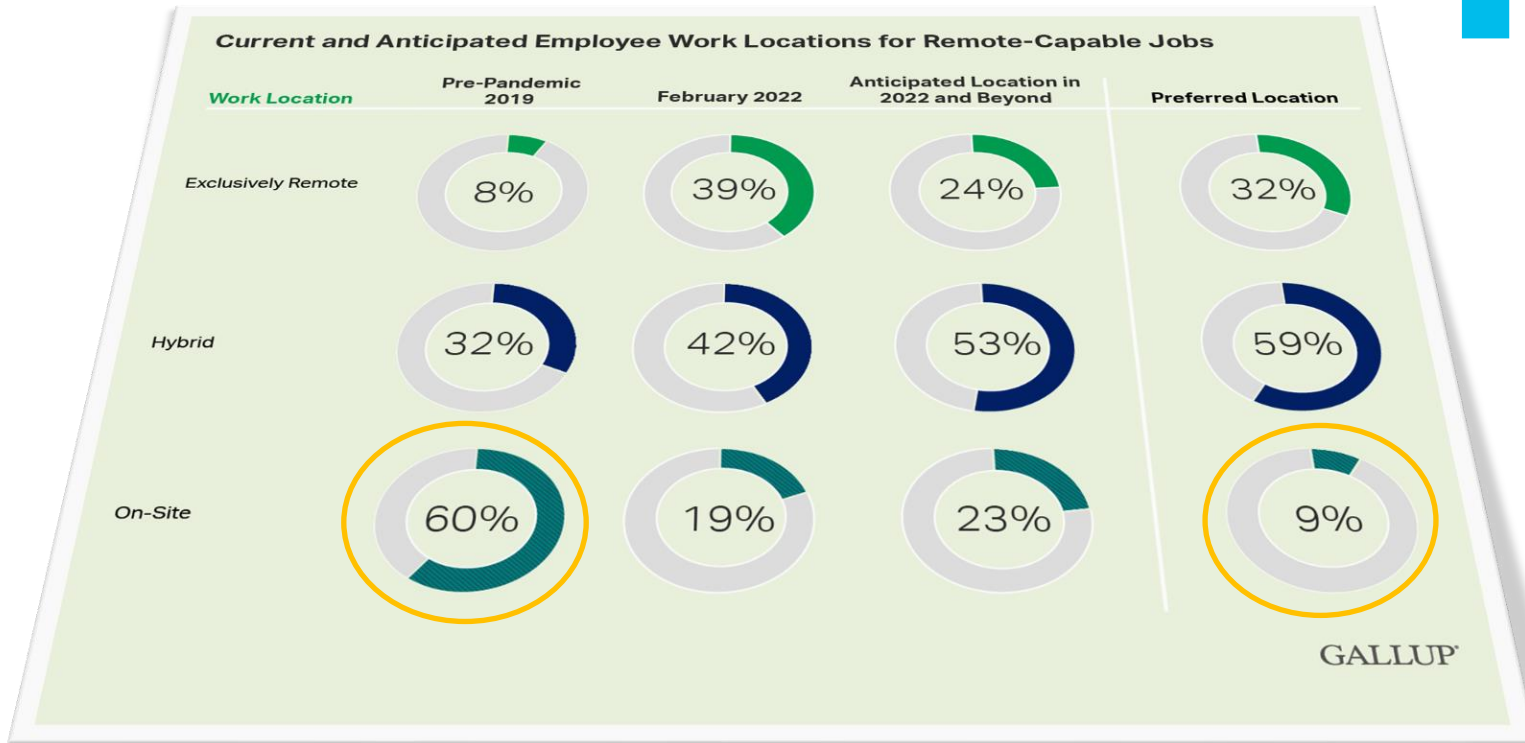


I'm working from home



and you...?

What employees want



Source: <https://www.gallup.com/workplace/390632/future-hybrid-work-key-questions-answered-data.aspx>

What are organizations planning?



Stanford University

Stanford | Institute for Economic Policy Research (SIEPR)

Menu

Publication

Hybrid is the future of work

Key Takeaways

- Hybrid working arrangements balance the benefits of being in the office with the benefits of working from home.
- Before implementing hybrid policies, executives and managers need to think through the implications of how and when employees work remotely.
- Issues of equity and equal treatment need to be carefully considered in a hybrid work arrangement.

Source: <https://siepr.stanford.edu/publications/policy-brief/hybrid-future-work>

As businesses and everyday life slowly return to pre-pandemic activity, one point is becoming clear: The home office isn't about to shut down. In my [research](#) and discussions with hundreds of managers across different industries, I'm finding that **about 70 percent of firms — from tiny companies to massive multinationals like Apple, Google, Citi and HSBC** — plan to implement some form of hybrid working arrangements so their employees can divide their time between collaborating with colleagues on site and working from home.

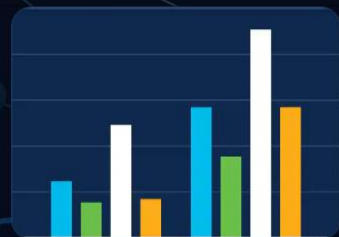


Hybrid Work Index

February 2022

Data-driven insights to guide your decisions for the hybrid work era.

What is New



Small branch traffic growth continues to outpace the large – indicating large corporate offices may have begun moving locations to smaller branch offices closer to where people want to live and work

98% of all meetings will include participants joining from home

Source:

<https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/global-workforce-survey.pdf>

58% employees will work 8 or more days a month from home

Resilience for hybrid & multcloud



Sector: 
Oil & Gas

“AWS and Azure both have unique differences which caused us to have totally separate security designs. It’s like building two completely different datacenter architectures.”

Sector: 
Public Utility

“To stitch together end-to-end policy, we have to write documentation and then distribute it to four different teams to implement... Inevitably the original intent is lost.”

Sector: 
Financial Services

“We have no way to control policies from specific containers to other resources on premises. **Managing 3 different isolated policy domains is difficult.**”

Sector: 
Large Retail

“We need a solution that takes policy entry, brings in contextual metadata about the environment and then applies policy to all the relevant enforcement points. Nothing does this today.”

Sector: 
Health Care

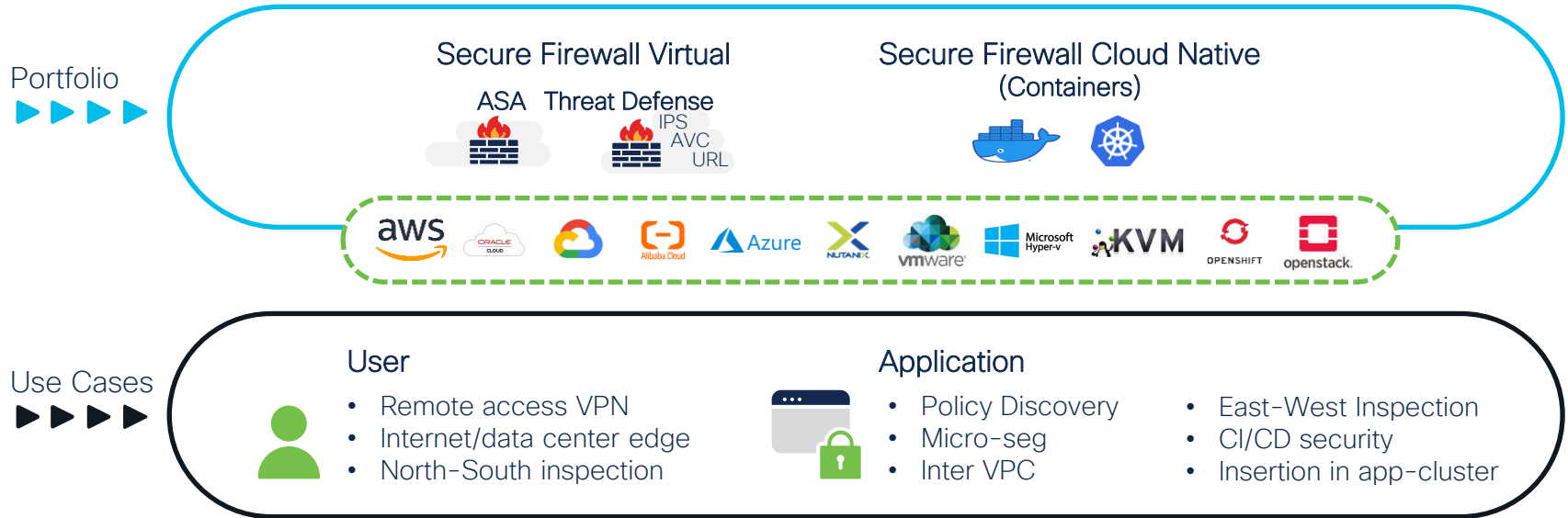
“Policy management across departments is a nightmare. Our departments are disconnected, but there needs to be a single source of truth for policy that spans them.”

Sector: 
Financial Services

“We want to move toward having all policy changes requested through a central portal that then distributes policy to all of our products: firewalls, workload security, endpoint security.”

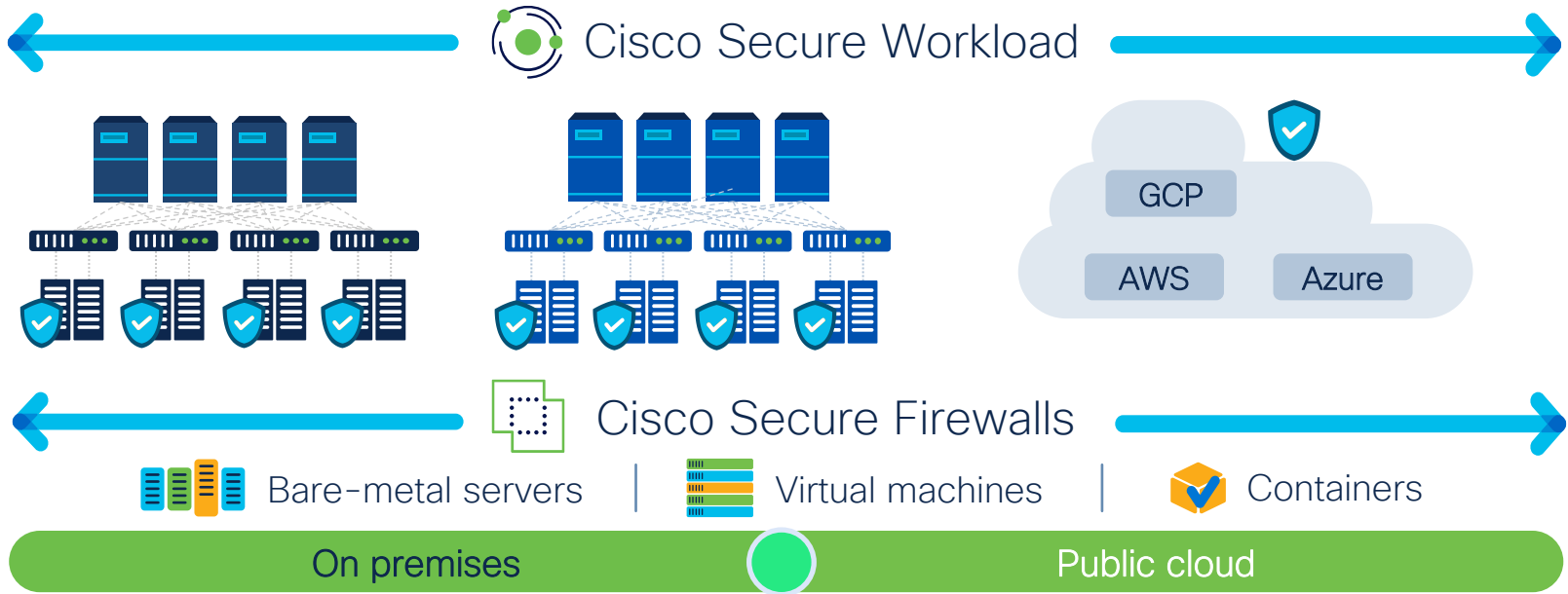
Protecting users and applications at scale

Insert cloud security controls in public and private clouds and HCI



Provide consistent microsegmentation everywhere

And anywhere: Across any cloud, application, and workload



Secure Firewall 3100 Series



3100 Series makes hybrid work practical, with flexibility for strong return on investment



Performance & Flexibility

Provide an exceptional hybrid
work experience



Visibility & Enforcement

Keep the network from going dark and
strengthen your zero-trust posture



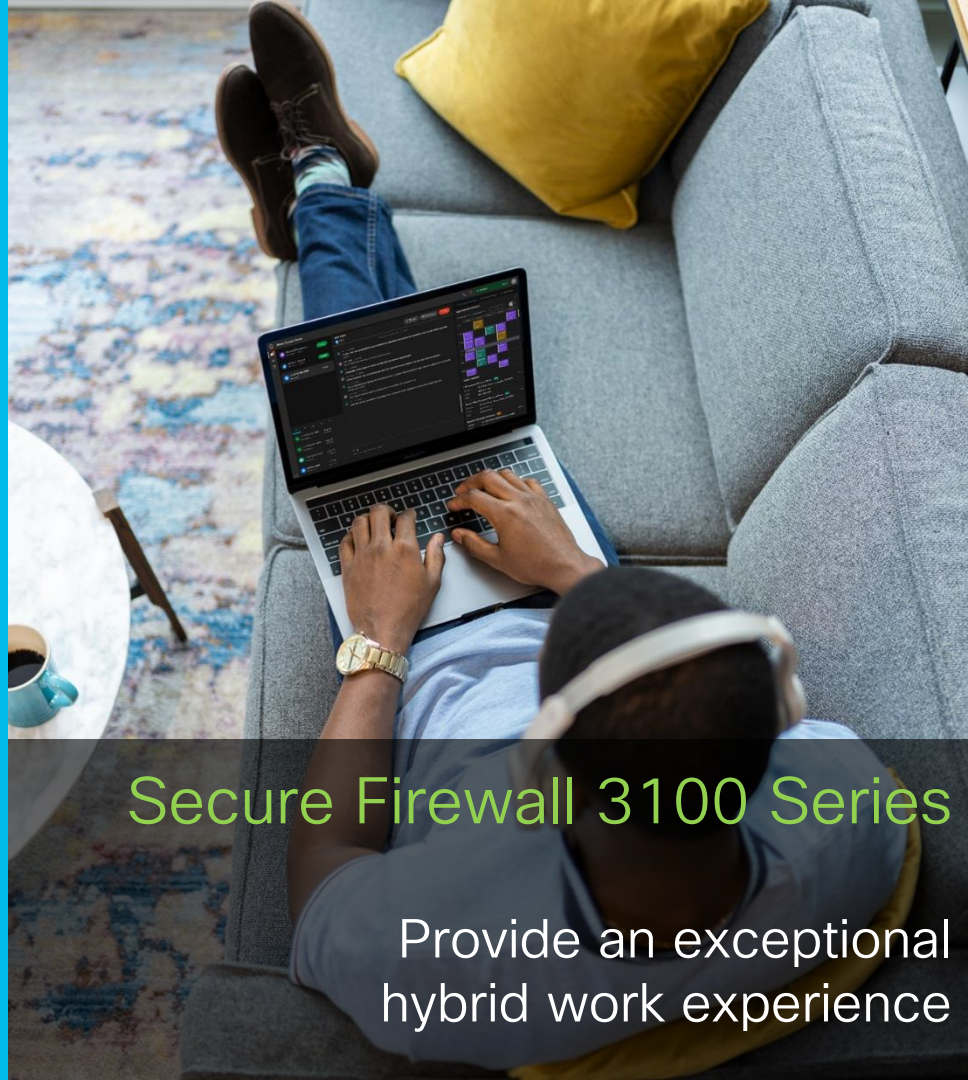
Efficiency & Simplicity

Automation and integrations drive cost-
savings for modern environments

Why 3100 Series?

- Empower hybrid workers
 - Support up to 20,000 remote VPN users – up to 17X VPN performance enhancements
- Delight your employees
 - Up to 7X inspected throughput with multithreaded traffic handling techniques, delivering strong video conferencing
- Get investment protection
 - Clustering and high port density flexibility allow your firewall to grow with you

CISCO *Live!*



Secure Firewall 3100 Series

Provide an exceptional hybrid work experience

Physical Appliances

Supporting your choice of FTD or ASA software

650 Mbps AVC
650 Mbps AVC+IPS

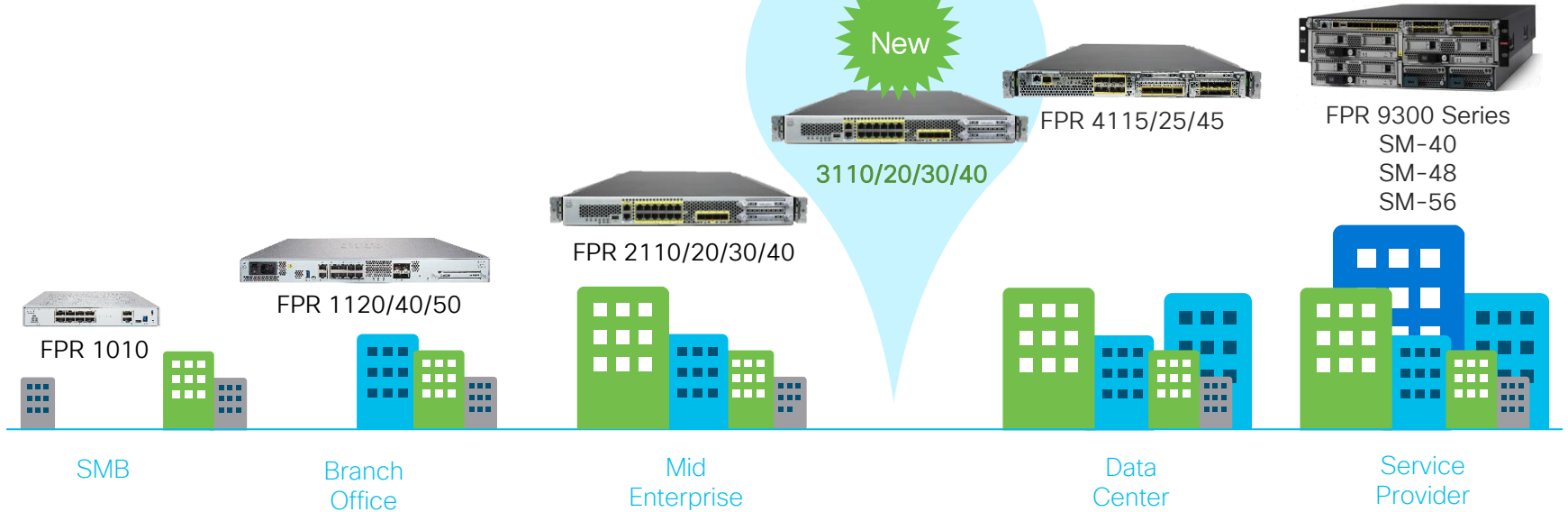
1.5-2.2 Gbps AVC
1.5-2.2 Gbps AVC+IPS

2.3-20 Gbps AVC+IPS

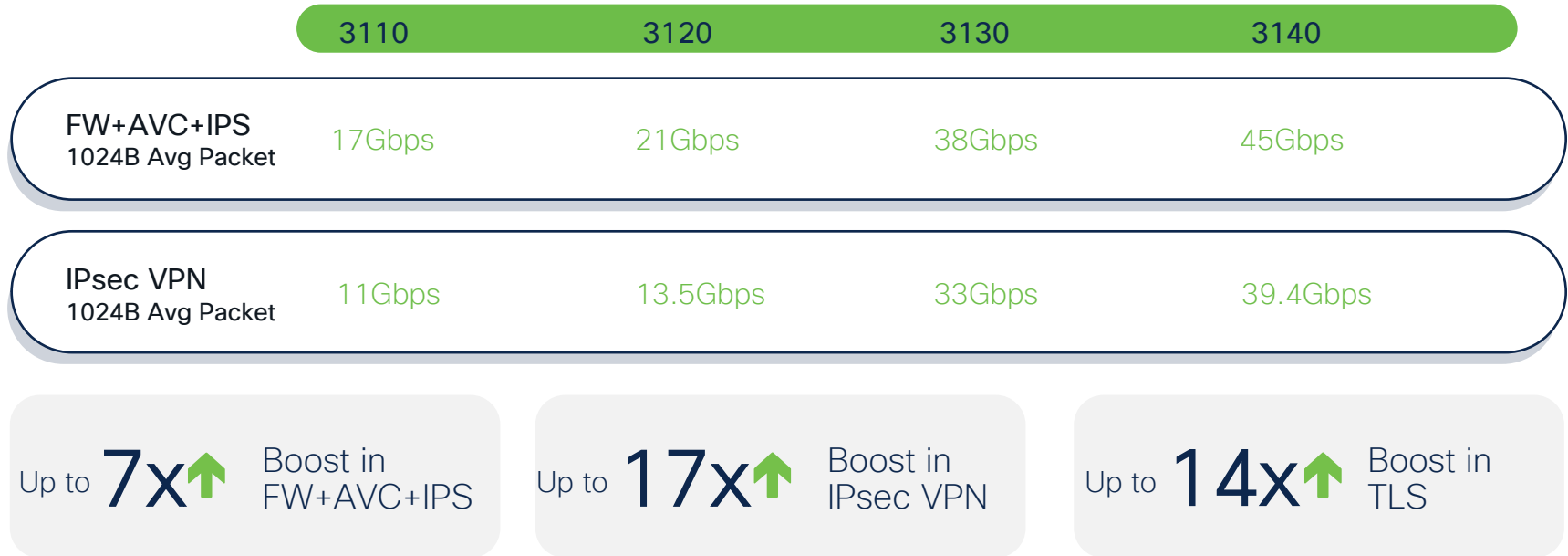
17-45 Gbps AVC+IPS
8 - 39.4 Gbps IPSec VPN

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS 6
Six node cluster:
Up to 254 Gbps AVC
Up to 226 Gbps AVC+IPS

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Six node (2 chassis) cluster:
Up to 336 Gbps AVC
Up to 307 Gbps AVC+IPS



3100 Series: class-leading performance, hybrid work optimized



**Performance Estimates are subject to protocol type, traffic profile, and other configured features. IPsec VPN performance assumes FTD 7.2 software.*

Technical session surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- 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.



Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn



Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

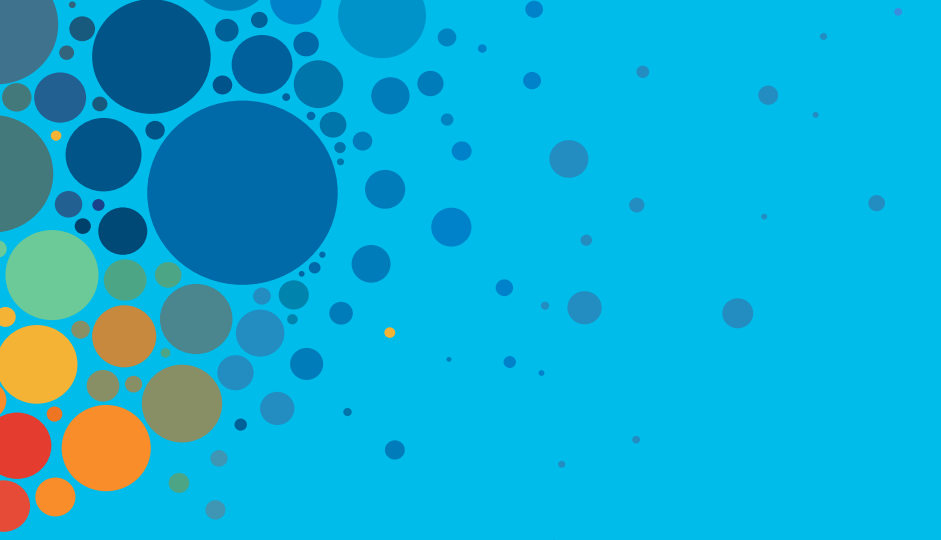
Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



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!*

ALL IN

#CiscoLive

Security Operations

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

SECURE X (XDR)

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility) Device Mgmt Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) ZERO TRUST PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Threat Protection | Secure Access Control | Managed Remote Access Reliable | Scalable | Flexible

Umbrella/Duo

ZTNA DNS-layer security Secure web gateway L7 firewall + IPS Cloud access security broker/shadow IT

RAaaS SSL decryption Remote browser isolation Data loss prevention Cloud malware detection

SDWAN

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes Cloud DDoS, WAF

On-Premises

SASE/SDWAN ZERO TRUST

Scalable | Flexible | Visibility | Comprehensive Security Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Network Edge Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router Industrial Firewall Industrial Switch/AP Cyber Vision ISE TrustSec

Secure DDoS Meraki Full Stack Secure Network Analytics Secure Firewall ISE TrustSec DuoCloud SSO+IDP Network Gateway Cisco DNA Center

Security Analytics and Logging Secure Web Appliance

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security API Security

Secure Workload Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private Public Cloud

Secure Cloud Analytics Secure Firewall

ThousandEyes Secure DDoS, WAF/Bot