

CISCO *Live!*



#CiscoLive



The bridge to possible

Protecting Users, Networks and Endpoints

The SASE WAY

Marla Mingee-Earle, Chief of Staff Cisco Talos Incident Response

Frank Lynn, Leader CX Marketing – Support and Security

PSOCX-1101



#CiscoLive

Cisco Webex App

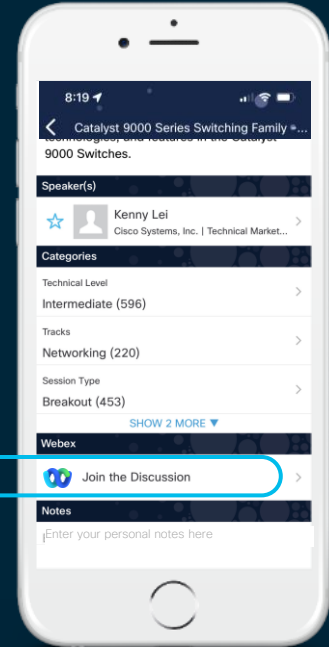
Questions?

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://ciscolive.ciscoevents.com/ciscolivebot/#PSOCX-1101>



Agenda

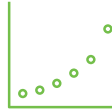
- Today's security landscape
- Customer challenges
- Secure Access Services Edge
- Secure Endpoint Pro
- Cisco Talos Incident Response
- Conclusion

Today's Security Landscape

Cyberattacks are on the rise and the threat landscape is expanding




Hybrid work decentralizing and expanding the threat landscape from networks to endpoints



Cyberattacks and ransomware continue to increase



Security talent and expertise continues to be scarce



In 2021, average data breach cost went up from \$3.86 million to \$4.24 million.

Breaches caused by remote work cost \$1.06 million more.

Cost of a Data Breach Report 2021, IBM

Customers top security challenges

Keeping users, applications,
and devices secure in the
hybrid work environment



Fortifying the
infrastructure

Proactively hunting
for and responding to
threats



Daily prevention
and maintenance

Uncovering attacks faster
and stopping them



Rapid response
to cyberattacks

Cisco CX security solutions

Reactive

Cisco Talos Incident
Response (CTIR)

Managed Detection
and Response (MDR)

Proactive

Secure Endpoint Pro

MITRE Attack Framework

Zero Trust Security

Predictive

Threat assessments

Penetration Testing

Healthcare customer case study

- Cisco Talos IR responded to ransomware
- Customer implemented a SASE security strategy for their network and cloud applications
- Cisco helped implement a security strategy for remote workers – including deploying Secure Endpoint Pro
- SASE for network and cloud, Secure Endpoint Pro for endpoints and CTIR for security emergencies is a winning combo

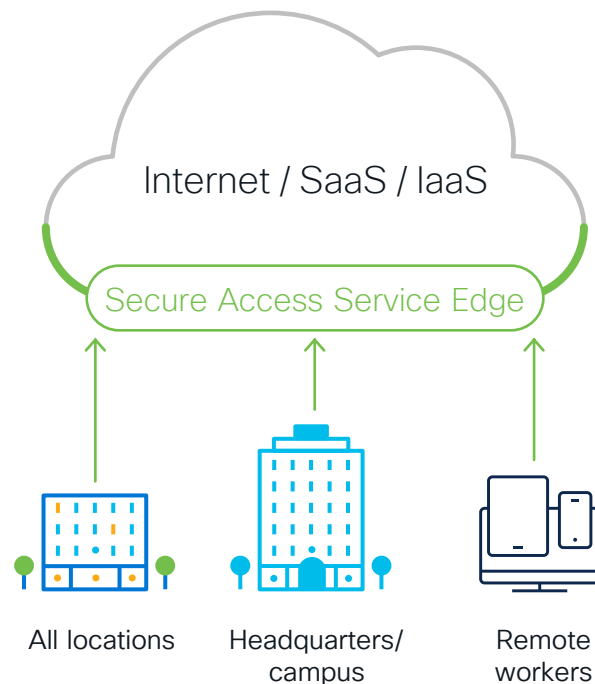
Secure Access Services Edge (SASE)



Fortifying the infrastructure

Drives the need for a secure access service edge (SASE) architecture

- Combine networking and security functions in the cloud
- Connect users to the apps and data needed – in any environment, from anywhere
- Control access and enforce the right security protection consistently



The three Cs for SASE

Deliver secure access to applications anywhere users work with an integrated security architecture

Connect



Deliver secure, seamless connections to applications anywhere

Control



Establish zero trust access and secure with leading threat protection

Converge



Integrate cloud-delivered networking and security

Secure Endpoint Pro



Daily prevention and maintenance challenges

Let Cisco experts help you hunt threats, patch devices and prioritize your response

Challenge: Expertise

“My team can’t be experts on every new threat or all be experts in threat hunting.”

Challenge: Time

“I don’t have enough time to go after every new threat, alert, patch and compromised devices.”

Challenge: Evidence

“We can’t always identify which threats to prioritize or get to the root cause of every attack.”



How Cisco Helps:

10

Person-hours saved per security incident

97%

Reduction in response and remediation time

86%

Improvement in security operations effectiveness

Secure Endpoint Pro

Combines human and machine power prevention and remediation of attacks from user devices



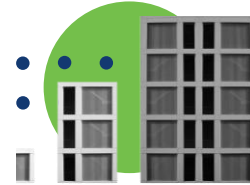
We do the heavy lifting of securing your endpoints

Cisco security **experts** perform 24x7x365 endpoint monitoring, detection, and response



We detect and respond to threats in minutes, not hours

Cisco specialists use automation and Cisco SecureX playbooks to reduce detection and response **time**



We investigate every threat and prioritize the most critical ones

Cisco conducts in-depth investigations of every incident based on **evidence** from our experts

Cisco Talos Incident Response (CTIR)



Rapid Response to Cyber Attacks

Cisco Talos Incident Response provides proactive and emergency services on retainer



Full suite of **proactive** services to help you prepare or test before a cyber security breach



Service Level Objective:
4 Hours by phone and
24 hours in transit



Why Talos?

Unmatched security capabilities and **threat intelligence** facilitated by **400+** global responders and intelligence researchers

Proactive

- Intel on Demand
- Plans/Playbooks
- Tabletop Exercises
- Threat Hunting
- Red/Purple Team
- Assessments

Emergency

- Coordination
- Triage
- Investigation
- Containment
- Remediation Recommendations

Talos Incident Response Retainer Services

Comprehensive, configurable portfolio gives you what you need

Core



Emergency
Incident Response



Intel on
Demand

Prepare



IR Plans/
Playbook



IR Readiness
Assessments

Training



Tabletop
Exercises



Cyber Range
Training

Hunting



Compromise
Assessments



Threat
Hunting

Simulating



Pen
Testing



Purple/Red
Team

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

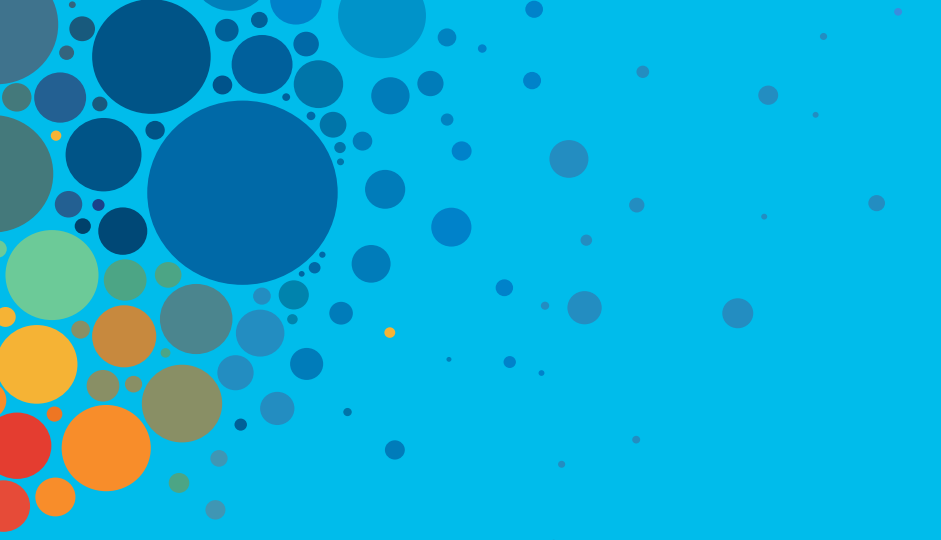
Cisco Guided Study Groups

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!*



#CiscoLive