cisco The bridge to possible

Making Sense of the Alphabet Soup of Cybersecurity Solutions

Adam G. Tomeo, Sr. Product Marketing Manager, Cisco Secure Endpoint

cisco Live!

PSOSEC-1212

Cisco Webex App

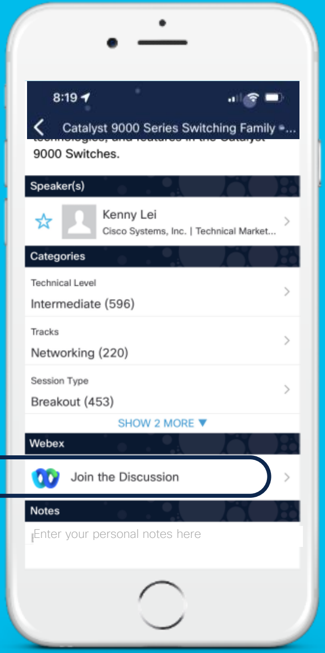
Questions?

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
until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family ▪...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Agenda

- Endpoint Security Landscape
- Choosing a Solution
  - EDR
  - mEDR
  - MDR
  - XDR
- Key Questions to Ask
- The Cisco Solution
- Next Steps

Endpoint Security Landscape

Endpoint Security Landscape

More threats, more challenges

Endpoints are the most common attack targets

There are more endpoints off-premises than ever before

Endpoint visibility is critical to a secure environment

What to do?

Organizations can respond by increasing their security maturity and resilience

Choosing a Solution

Which Solution Do You Choose?

Choosing the right solution for your organization can be confusing

Security solutions offerings:

- Endpoint Detection and Response (EDR)
- Managed Endpoint Detection and Response (MEDR)
- Extended Detection and Response (XDR)
- Managed Detection and Response (MDR)

EDR

Overview of EDR Solutions

Rapidly identify and recover from endpoint attacks with EDR Solutions

Major Capabilities

- Endpoint monitoring
- Threat detection and analysis
- Threat containment
- Recommended remediation steps
- Threat hunting

Key Benefits

- Gain deep endpoint visibility
- Effectively detect unknown threats
- Contain threats before its too late
- Quickly respond to attacks
- Take a proactive approach to security

mEDR

Overview of mEDR Solutions

Offload endpoint protection to security experts with mEDR solutions

Major Capabilities

- Managed EDR service
- 24x7 endpoint monitoring by experts
- Threat analysis and prioritization
- Comprehensive investigation
- Guided remediation

Key Benefits

- Focus on your core business
- Get always-on endpoint security ops
- Address every threat to your endpoints
- Stay ahead of the latest attacks
- Accelerate incident response times

MDR

Overview of MDR Solutions

Outsource or augment your cybersecurity to security experts with MDR solutions

Major Capabilities

- Managed security service powered by a technology stack
- 24x7 monitoring by experts
- Threat analysis and prioritization
- Comprehensive investigation
- Guided remediation

Key Benefits

- Focus on your core business
- Get always-on security ops
- Address every threat to your organization
- Stay ahead of the latest attacks
- Accelerate incident response times

XDR

Overview of XDR Solutions

Maximize your security ops with unified detection and response via XDR solutions

Major Capabilities

- Security telemetry across multiple sources
- Consolidated view with a single pane of glass
- Correlated, high-fidelity detections
- Automated, orchestrated response

Key Benefits

- Decrease alert fatigue and false positives
- Streamline security ops with improved efficiency
- Gain actionable, contextual insights
- Speed detection and response times

Key Questions to Ask

Key Questions to Ask

Find the right security solution for your organization

- Where are we in our cybersecurity journey?
- Do we have a security operations center (SOC) or want to build a SOC?
- Do we have the right cybersecurity talent, skills, and knowledge?
- Do we have enough visibility and context into security incidents?
- Do we suffer from too many alerts and/or too many security tools?
- How long does it take us to detect and respond to threats? Is that adequate?

The Cisco Solution

The Cisco Secure Endpoint Solution

Have no fear in the face of relentless cyberattacks

Protect Hybrid Workers

Protect your hybrid workforce at home, in the office, or anywhere with simple, comprehensive endpoint security powered by unique insights from 300,000 security customers and 80% of the world's Internet traffic via the leader in networking

Stay Resilient

Stay resilient against threats and reduce incident response times by as much as 97% with enriched context from built-in XDR that natively includes rapid EDR and deep insights from a team of industry-recognized Cisco security experts

Protect What's Next

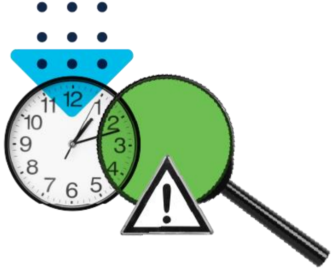
Secure "what's next" and stay ahead of the latest threats with endpoint security fueled by an integrated cybersecurity solution and actionable threat intelligence from the Cisco Talos security research team

Protect Hybrid Workers

Shield your hybrid workers with simple, powerful defense fueled by rich endpoint insights

Powerful Prevention

Stop breaches before they compromise your workers with enriched threat intelligence via the world-class Talos threat research team



Prioritized Response

Investigate and respond to prioritized incidents from telemetry across networks, apps, operating systems, vulnerabilities, clouds and more

Simplified Management

Manage your endpoints at scale with simplified controls from a single agent managed natively in the cloud

Stay Resilient

Recover faster from attacks with end-to-end expertise from the global cybersecurity authority

Unique Threat Detection and Response

Emerge stronger from attacks with scalable defense that natively includes built-in XDR and advanced EDR capabilities

Always-On Security Expertise

Focus on what you do best while experts from Cisco Talos secure your endpoints for you with 24/7 monitoring, detecting, and responding

Proactive Threat Hunting

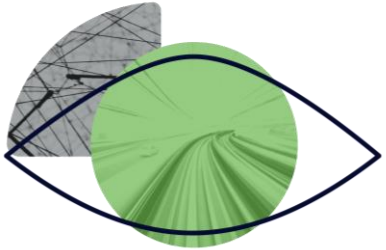
Prevent attacks before they happen through automated threat hunting driven by Cisco Talos analysts

Secure What’s Next

Protect against the threats of today and prepare for the threats of tomorrow

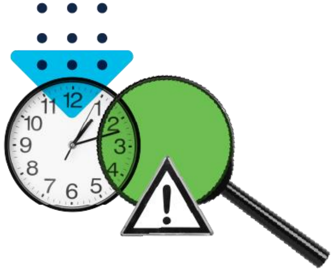
End-to-End Defense

Stop new and emerging threats with a robust solution which spans your environment and that can be managed by Cisco Talos experts



Deep Visibility

Anticipate the next attacks with rich telemetry from an integrated solution powered by the latest insights from the Cisco Talos team



Rapid Detection and Response

Quickly investigate and remediate threats via an open and extensible XDR solution that natively includes advanced EDR capabilities

Secure Endpoint Customer Stories

Norwegian University of Science and Technology

Renowned center for technological education, research, and innovation

- Gained unified visibility regardless of user and device location
- Improved advanced threat detection and response capabilities
- Reduced investigation and remediation time by 83%

Pima Community College

Higher education institution in Tucson, Arizona with thousands of student and faculty

- Reduced alerts from hundreds to a few while saving time on investigation and remediation
- Gained unified visibility regardless of user and device location
- Achieved advanced threat detection and response capabilities

Per Mar Security Services

Provider of physical security services to 75,000 homes and businesses across 16 U.S. states

- Gained unified visibility and control through a single pane of glass
- Dramatically improved threat hunting and investigation capabilities
- Enabled hybrid work while maintaining cyber resilience

Secure Endpoint Customer Offerings

Essentials	Advantage	Premier	Complete
Powered by Cisco Talos - see a threat once and block it everywhere. Automated threat response with one-click isolation of an infected host.	Simplify security investigations with advanced EDR with easy access to powerful malware analysis and unique threat intelligence.	Elite Cisco security experts proactively search for threats in your environment and provide high-fidelity alerts with remediation recommendations.	Get your endpoints completely managed - combines human and machine intelligence to reduce endpoint detection and response tasks and times.
Includes • Endpoint Isolation • Retrospective Security • Vulnerability Identification • Dynamic File Analysis • Next-Gen Antivirus Protection • Private Cloud [on-premise]	Includes • Essentials Tier + • Orbital Advanced Search • Secure Malware Analytics	Includes • Advantage Tier + • SecureX Threat Hunting	Includes • Premier Tier • MDR for Endpoint • Talos Incident Response Retainer
	Optional Services*	Optional Services*	

*Optional Services: MDR for Endpoint
Talos Incident Response Retainer
[DFIR Investigations, Red Team Capabilities, Proactive IR Services]

Next Actions

Next Actions

- Visit us at the Cafe Cisco Secure and Security Showcase Booth
- Learn more about Secure Endpoint: cisco.com/go/endpoint

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

The bridge to possible

Thank you

Are you playing the Cisco Live Game?

Scan the QR code and earn your Cisco Theater points here cisco Live!