Next-gen Cisco security & observability: Engineering digital resilience at scale

Scott Manson
Director, Cyber Security
Cisco UK & Ireland

cisco *Connect*

#CiscoConnect

How we're transforming

1 Fusing security into the network

2 Making security simpler

3 Innovating with AI

FY25 Security Platform GTM

1 Future-Proofed Workplaces

2 AI-Ready Data Centers

3 Digital Resilience

Where to focus with us

Universal ZTNA

Hybrid Mesh Firewall/Hypershield

AI Defense

XDR + Meraki

Splunk

cisco Connect

FY25 Security Platform GTM

Future-Proofed Workplaces

AI-Ready Data Centers

Digital Resilience

1 User Protection

2 Cloud Protection

3 Security Analytics and Response

People

Managed

Unmanaged

Things

Universal ZTNA
from **CISCO**

Modern
private apps

SaaS
apps

Internet
apps

Traditional
apps

Remote | Campus | Branch | Airplane Remote | Oil rig | Stadium | Field | ...

#CiscoConnect

cisco Connect

Universal ZTNA
from **CISCO**

Cisco SASE

Remote | Campus | Branch | Airplane | Oil rig | Stadium | Field | ...

#CiscoConnect

One client, multiple functions

One client, multiple functions

FY25 Security Platform GTM

Future-Proofed Workplaces

AI-Ready Data Centers

Digital Resilience

1 User Protection

2 Cloud Protection

3 Security Analytics and Response

SOFTWARE DEFINED
INFRASTRUCTURE

SOFTWARE DEFINED
INFRASTRUCTURE

No rip and replace

Writes
own rules

Tests
own rules

Deploys
own rules

Lifecycle manages
own rules

Updates itself while you sleep.

Knows how to earn your trust

Security Cloud Control

Define policy once and you can change
what enforces

Secure Firewall
(FTD, ASA)

Hypershield

Multicloud
Defense

Secure
Workload

Secure Access
(FW as a service)

AI Defense

3rd party
firewalls

FY25 Security Platform GTM

Future-Proofed Workplaces

AI-Ready Data Centers

Digital Resilience

1. User Protection

2. Cloud Protection

3. Security Analytics and Response

Future of AI with Cisco

AI Supply Chain & Risk Management

- Enforcement across Cisco Security Cloud
- Coverage across AI app development lifecycle

Agentic Security and Orchestration

- Security for AI agents
- AI agents for security workflows

Foundation Models for Security

- Trained on threat data across Cisco platform
- Supported by Cisco Foundation AI team

Agentic for XDR: Multiple AI Agents Driven

Generative AI

- Instant Attack Verification: AI validated threat to trigger instant response
- Attack Storyboard: Comprehend attack in 30 seconds via visual narration

MITRE ATT&CK

- Attack graph mapped to MITRE tactics & techniques
- Agentic AI builds and executes tailored investigation plans

Equitable Forensics

- Trigger forensic artifacts & backup snapshot before you know you need it
- Gather evidence, even from a compromised device

Cyber Resilience

- Automated playbooks to respond to common attacks
- AI-guided containment & recovery next steps

Secure Access: protecting the usage of AI

Protect intelectual property as it flows in and out of AI systems

Threat Visibility

Discover and
Assess Activities

Leakage Prevention

DLP Inspection of
Prompts/Uploads

Threat Prevention

Block Apps and
Control Downloads

Discovers and controls more than 70 Gen AI apps (including APIs)

Unified AI Assistant for Security
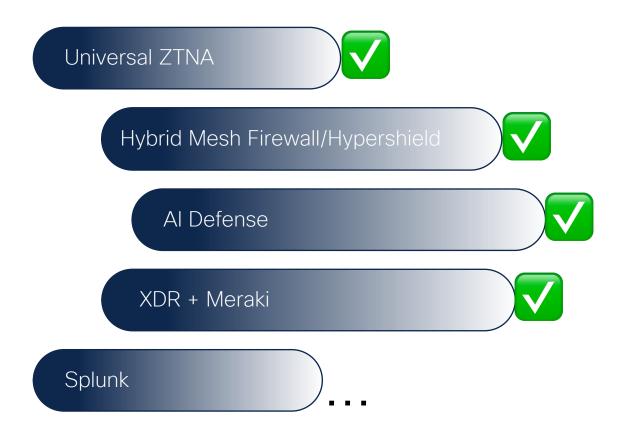
Simplify policy administration by up to 70%

How do I secure my network with Cisco **Security**?

Unified AI Assistant

AI assistance for policy

Proactive AI ops

Real world policy testing

Some capabilities are future.

Where to focus with us

Universal ZTNA ✅

Hybrid Mesh Firewall/Hypershield ✅

AI Defense ✅

XDR + Meraki ✅

Splunk …

Thank you

cisco Connect