



# CISCO *Live!*

## 2025 | Amsterdam

Key take-aways for driving your digital future

**BLOC**



# Thinking differently

The true pace of change in the tech industry is playing out in real time in front of us. Governments are placing technologies such as AI at the top of their agendas, signifying that we're on the precipice of even faster change. Of course, the reasoning for this backing is the potential impacts tech can have to how our societal systems work. But if we're to truly unlock the efficiencies on offer here, we must first understand the innovations.

One brand I truly believe to be at the forefront of these developments is Cisco – whose technology has long been integral to enabling some of Block's services, as has been evidenced through our Cisco Gold Provider status. It's Cisco's long-term and truly global relationship with technological advancements that makes its annual Cisco Live EMEA event such a credible source for those hoping to stay at the cutting edge.

Here, information is power – and it's valuable because it's easily accessible and shared among all within the tech community – an approach that chimes with Block's own ethos of journeying through this period of innovation together. So, continuing on this path, we've distilled some of the most important findings from Cisco Live EMEA 2025, in the hopes that you're able to keep building on the foundations you're currently laying down.

You'll find some of the crucial findings from Amsterdam, as well as how they can link to your network, collaboration, and smart building projects.

**Mark Walton, CTO at Block**



“Cisco Live goes beyond conversations about new technology, it challenges you to take on new perspectives which can help your organisations truly transform for the better.”



Block is Cisco's UK&I Innovation  
Partner of the Year 2024



# Contents

- 3 Cisco Live overview
- 4 Industry implications from AI
- 5 Defence dashboard
- 6 AI customer agents
- 7 Identity intelligence and security
- 8 Cloud management and firewalls
- 9 AI-ready data centres
- 10 Data centre security
- 11 Outshift's Incubation Engine
- 12 Operative AI in the stack
- 13 Cisco x Block





# 1335

sessions

# 21

Capture the  
Flag sessions

# 76

Technical  
seminars



## Overview

# 75

Showcase  
demos



# 100

Walk-in labs

# 70

instructor  
led labs

## More learning opportunities

► Cisco Live 2025: **San Diego**  
8th-12th June 2025

► Cisco Live 2025: **Melbourne**  
10th-13th November 2025

# 27

AI hub  
sessions

# 49

Product and  
strategy  
overviews

# 16

Technical  
solution clinics



**CISCO** *Live!*



# Industry implications from AI

ChatGPT was a watershed moment for the tech industry because it 'consumerised' data for the masses. Placing this insight at the fingertips of every employee around the world naturally brings previously analogue businesses into the tech fold – and digital resilience will grow in importance as a result. In 2025, the industry is at a stage where it's not fantasy to suggest artificial intelligence could exceed human intelligence or at least match it, which opens a realm of possibilities. However, many networks will not be able to support such a shift, which means implementing smart connectivity will be an essential focus for network transformations.

The introduction of AI has already ushered in two seismic shifts:

- ▶ **DeepSeek effect:** The emergence of Chinese AI platform DeepSeek is driving down the cost of training AI models, making AI more accessible and scalable. However, this holds concerns for security and safety.
- ▶ **The operator effect:** OpenAI is enabling tasks to be carried out on your behalf. This requires multiple agents in different data centres to communicate with one another, which will put network connectivity front and centre.

## Marc Chang, CEO at Block

"At Block, we are using AI to enhance human potential – delivering faster, more efficient, and people-centred solutions. The infrastructure and services we provide are critical and cannot fail, so we help our clients by combining AI with our expertise to improve service, enhance experiences, and ease day-to-day pressures."



**AI is fundamentally changing everything, and the speed and pace at which things are moving is so fast it's actually hard to keep up."**

Jeetu Patel, EVP and Chief Product Officer at Cisco



# Defence dashboard



Business need is going to drive AI adoption at unprecedented rates, with the majority of businesses believing they need an AI strategy within 18 months to avoid competitive disadvantage. In the wider political context governments are scrambling to obtain leaderships positions in AI technology, as it's widely seen as the next technical revolution.

These factors combined will lead to a proliferation of new vendors, new AI models, and new AI-enabled products. As with any emerging technology this opportunity will bring new risks to organisations, with new attack vectors such as AI prompt injection and sensitive data disclosure via generative AI models building upon the more traditional risks of data sovereignty and shadow IT.

Cisco has responded with 'Cisco AI Defense', which aims to provide protections to developers and consumers of AI products.

## Cisco AI Defense

- ▶ For consumers, AI Defense integrates into the Cisco Secure Access SASE solution, allowing organisations to safeguard staff using third-party generative AI apps. This includes Shadow AI App detection, risk identification, access control, AI learning guardrails, and blocking malicious or harmful responses.
- ▶ For AI developers the solution offers AI runtime protection, model, and application validation to manage and control risk in AI models.
- ▶ Cisco AI Defense is tightly integrated into the Cisco Security Cloud Control platform, which will gradually unify the Cisco Security product portfolio.

## Paul Yarwood, Architect – Enterprise Solutions at Block

"NHS Customers are already adopting AI applications, Shadow AI is likely to be a threat, gaining visibility and control early will help to control emerging risk."



**For every security organisation that we've had this conversation with, the very first thing they talk about is how visibility is top of mind."**

DJ Sampath, Vice President of Product,  
AI Software and Platform at Cisco



# AI customer agents

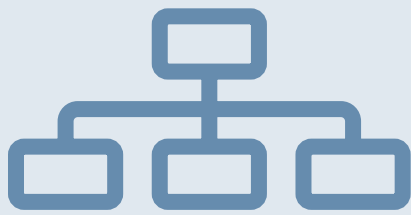
AI is also making waves in the customer services arena, with Cisco developing its virtual AI agent. This tool has the capacity to interpret the customer’s tone and emotion, and will be able to answer the questions asked of it 80-90% of the time. In the event it can’t answer the query, it will have the knowledge to ensure the customer is transferred to the right person. The agent also comes with the Webex AI agent studio which means organisations can design agents for very specific use cases. Alternatively, there are built-in templates which enable automatic agent creation.

The AI agent has been created with the aim of enabling professionals without a programmer background to use it. Key features include:

- ▶ A simple interface for easy navigation
- ▶ Templates for efficient agent creation
- ▶ The option for voice and chat channels

## Shaun Pell, Practice Lead: Collaboration at Block

“It’s an exciting time for collaboration technology and AI in healthcare. AI does more than route patient’s calls quickly; it learns from every interaction, seamlessly integrating with processes to personalise communication and empower self-service. AI can help tackle some of the real pain points in today’s communication, removing repetitive frontline interactions, significantly transforming patient experiences. With these advancements and the ease of access to AI technology, the market stands poised for a bold, disruptive transformation.”



“ **It’s not going to sound like a robot. It’s going to sound like a real human, and the latency is going to be low.”**

Caitlin Lacey, Director of Product Marketing, Collaborative Devices



# Identity intelligence and security

Cyberattacks are inevitable which means businesses must be prepared to detect and respond to threats. Many organisations focus on endpoint, network, and cloud native security. But identity threat detection is becoming a top priority, especially since the Talos report uncovered 80% of breaches exploit identity vulnerabilities. A huge problem here is that organisations are often operating multiple identity providers (such as Microsoft Entra, Okta, and Google Workplace). Each IDP has its own security policies, resulting in inconsistent enforcement, misconfigurations, and security gaps. Weak MFAs, such as push-only MFA, also increase the risk of MFA fatigue attacks. Although built-in security may be included within an IDP, it can only monitor what's within that environment. There needs to be centralised visibility.

Cisco's new identity intelligence (CII) has aimed to provide a unified view for identity intelligence. This has included:

- ▶ Building a cloud product and linking to the most common IDPs.
- ▶ Using all data sources to create an identity graph, showing linked identities, devices, and applications within your environment.
- ▶ Associating trust levels with users to enable security and firewall policy.
- ▶ Automating threat detection and escalation for unusual identity activity.

## Paul Yarwood, Architect – Enterprise Solutions at Block

"Cloud adoption is leading to a proliferation of ID providers and reducing visibility into the accounts, permissions, and usage of accounts. Organisations are exposed to risk from exploit of stolen credentials."



**Prevention is never enough...You have to detect what has happened and be able to respond to it."**

Aaron Woland, Distinguished Engineer at Cisco





# Cloud management and firewalls

The Firewall Group engineers at Cisco have been focusing heavily on cloud management as it believes it holds the potential to reduce the complexity, difficulty, and cost of managing a large fleet of firewalls. By using a cloud manager you’re bypassing some of the costs typically associated with running a firewall such as dealing with hardware, power allotment, and cooling. Cloud management can also simplify connectivity planning between the central manager, data centre, and distributed firewalls. If you’re running an environment where you can’t have loss of access to your management, on-prem solutions require two management pairings for high availability. However, cloud management removes this complexity by handling high availability automatically.

Cisco takes care of high availability by:

- ▶ Keeping software up-to-date
- ▶ Patching vulnerabilities quickly
- ▶ Running frequent updates
- ▶ Operating as a SaaS offering to remove complexity in management

## Rob Brady, Head of Solutions at Block

“Maintaining management appliances is a burden we could all do without. Cloud-based services, typically based on modern software architectures, will allow our customers to spend more time on security policy rather than appliance maintenance.”

“When we look at high availability and disaster recovery, we’re able to leverage these modern capabilities that the cloud brings us like multiple availability zones.”

Ted Bedwell, Distinguished Engineer at Cisco



# AI-ready data centres

Cisco has grown its focus on data centre modernisation over the past 12 months – partly driven by the new use cases beginning to emerge for AI. As a result, engineers are in the midst of getting data centre environments ‘AI ready’. This means that while organisations may not yet understand what their use cases will be, they’ve got the right networking environment, computer environment, storage, and data necessary to support AI workloads as they materialise in the pipeline. Scalability of storage combined with environmental considerations is a key development point within this because AI not only requires much larger amounts of data, but more energy.

AI has prompted organisations to assess their infrastructure, often concluding:

- ▶ Having a public and private cloud are imperative to supporting a hybrid environment.
- ▶ There’s a lot of technical debt which has built-up over the past few years.
- ▶ Existing investments need to be protected, and this needs to be taken into account.

## Katharine Corcoran, Head of Network Delivery at Block

“AI-driven innovation is reshaping data centres, requiring scalable, energy-efficient infrastructure. Organisations must modernise networking, compute, and storage to support future AI workloads while balancing cloud strategies and protecting existing investments. Future-proofing infrastructure today ensures long-term efficiency and adaptability.”



“Over the past 12 months, from a Cisco standpoint, we’ve really seen a big focus back on the data centre particularly with the new AI use cases that have come along.”

Matt Brown, Solutions Engineer, Cloud and AI infrastructure at Cisco



# Data centre security

Operating across private, public, and edge cloud environments has posed problems for those trying to implement network security at scale. Cisco believes the solution is to introduce greater automation and security, and it plans to do this through Hypershield (which allows for centralised policy management with distributed enforcement) combined with smart switches (which enable intelligent traffic redirection and Ultra Ethernet-ready DPUs). AMD is also playing a role in providing programmable DPUs, contributing to greater security and scalability. These technologies are part of Cisco’s proposition to provide security as built-in to the network, rather than bolt-on.

The use cases for smart switches include:

- ▶ Encrypting workloads at colocation points
- ▶ Providing layer three and four segmentation with micro-granular control
- ▶ Replacing traditional firewalls with integrated DPU-driven security

## Katharine Corcoran, Head of Network Delivery at Block

“As hybrid and edge environments grow, scalable security is critical. Automation, Hypershield, and smart switches help simplify protection by embedding security within the network itself. This proactive approach enhances resilience, reduces complexity, and ensures networks are ready for evolving threats.”



“ **Being able to manage security and network at scale for data centres and locations is actually a challenge [for customers], and its only increasing.”**

Murali Gandluru, Vice President of Product Management at Cisco



# Incubation Engine

Cisco’s Outshift incubator is currently nurturing what it sees as emerging technologies such as generative AI, cloud security, and quantum computing – it’s doing this in tandem with laying the foundations for the ‘internet of AI agents’, which it anticipates will ‘revolutionise’ the workplace. Meanwhile, it expects quantum computing to have a ‘ChatGPT moment’ in the next three to five years, which means engineers are focusing on creating strong security and seamless integration with classic computing. Incubating emerging tech, like Cisco has done, as opposed to acquiring mature technologies or partnering to expand can be a helpful strategy for businesses looking to grow their capabilities because it enables full control, credibility, and most importantly, integration with existing strengths.

The Outshift incubation engine defines its innovation model in five-phases.

- ▶ Phase one: Ideate
- ▶ Phase two: Build
- ▶ Phase three: Launch
- ▶ Phase four: Land
- ▶ Phase five: Scale

## Mark Walton, CTO at Block

“At Block, we’re thinking about how we’re going to evolve our managed service delivery model. So how we’re able to provide a managed service that meets the demand of modern IT but also acts as that foundational enabler for technology change, particularly in healthcare.”



**The secret to emerging tech and innovation in large organisations is building a systematic approach and we believe we have cracked the code for exactly that.”**

Vijoy Pandey, Senior Vice President, Outshift by Cisco



# Operative GenAI in the stack

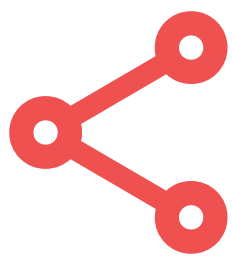
Cisco’s DevNet programme is integrating GenAI, alongside automation and security, into existing infrastructure management practices. The use cases in this space touch network troubleshooting and security, managing and securing IT environments, enforcing policy and compliance, as well as Infrastructure as Code. IT teams will have no choice but to embrace this programmability and automation if they’re to ensure their organisation remains efficient. While some concepts are far from ready to be deployed, IT teams can ready themselves by leveraging current tools such as APIs, IAC, and security frameworks. Now, could also be an apt time to invest in AI security and observability to prevent unauthorised access, data leaks, and infrastructure vulnerabilities in the future.

Operative GenAI use cases include:

- ▶ Reducing manual CLI-based configuration
- ▶ Creating playbooks and troubleshooting more efficiently
- ▶ Access real-time threat detection and enforcement at kernel level
- ▶ Automate code reviews, pull requests, and policy enforcement
- ▶ Detect unauthorised data transfers or block specific AI models being used

## Tom Barrett, Automation and Software Lead at Block

“Embracing GenAI empowers Block to transform IT operations, driving efficiency, security, and rapid detection of potential problems for fast root cause analysis and quick resolution. With programmability and automation, Block can create innovative tools and services for outstanding network performance and compliance. Exciting times ahead!”



**GenAI isn’t here to replace IT teams – it’s here to help us automate, secure, and optimise infrastructure at scale. The challenge for IT teams is not resisting change, but embracing programmability and automation to stay ahead.”**

Shannon McFarland, VP, Head of Cisco DevNet, at Cisco



# Cisco x Block

Block is a Cisco Gold Partner as well as the winner of Cisco's UK&I Innovation Partner 2024. The brands have worked together for two decades to ensure clients receive the best possible infrastructure to support their digital transformations.

## About Block

Block specialises in networks, collaboration, and smart building solutions. It aims to lay the critical foundations necessary to enable modern day organisations to succeed by:

- ▶ Allowing staff to connect anywhere on any device, quickly, simply and securely.
- ▶ Combining your systems into a single architecture to help your team work better together.
- ▶ Merging physical and digital to lower costs, cut emissions, and elevate user experience.

Block has more than 20 years' experience working with some of the UK's largest healthcare, education, and enterprise organisations. Some 90+ clients are supported by Block's expert UK-based teams, with projects including Barts Health NHS Trust, Birmingham and Solihull CCG, and Queen Mary University London.

**CISCO** *Live!*  
**2025 | Amsterdam**

Key take-aways for driving your digital future





# Build smarter with Block

- ▶ Block can work with you to develop a tailored solution for your digital transformation needs.  
Email: [marketing@block.co.uk](mailto:marketing@block.co.uk)

