No perimeter?
No problem

Elevating cyber defence in a hybrid world

Just compliant… or ready for anything?

The shifting threat landscape demands a robust cybersecurity posture

Digital technology fuels incredible growth and innovation across multiple domains. And cybercrime is no exception. Danger lurks in all directions – from nation-states and organised crime to lone hackers and even your workforce. Meanwhile, cloud and hybrid models create significant opportunities for organisations and attackers alike.

How can you confidently pursue digital transformation in a world of swiftly evolving, rapidly multiplying threats? Better still, how can you ensure security adds value, supports good user experiences and drives productivity? In this guide, we explore the crucial considerations, tools and frameworks for implementing a robust cyber defence posture aligned with your core objectives – and why the Insight Cisco partnership is best placed to guide you on your journey.

Proactive cyber security is vital to protect your assets, achieve compliance, and ensure business continuity – while supporting long-term growth

The cyber threat landscape

Threats

Phishing
Malware
Ransomware
Data breaches
Social engineering
Supply chain attacks
Zero-day exploits
Insider threats
Social engineering
DDoS attacks
Advanced Persistent Threats (APTs)
IoT vulnerabilities
Credential stuffing
Impact of AI

Attackers

Nation states
Organised crime
Lone hackers
Disaffected/manipulated employees

Empower your organisation to pursue growth

Cyber defence is an enabler – not an end in itself

Cyber defence goes beyond safeguarding your data and infrastructure; it's about creating an environment that fosters innovation, productivity, and customer trust.

The emergence of the hybrid, cloud-first model exemplifies the need to balance security with user experience. Despite the challenges presented by the dispersed attack surface, the scalability, flexibility, and efficiency benefits of hybrid working are too big to ignore. Organisations must empower employees to be connected, collaborative and secure, regardless of location – increasing network agility, ensuring proactive, preventative action, and responding rapidly to disruptions.

Can you optimise security while minimising costs, complexity and compromise?

Meanwhile, cyber security should add value beyond defence. For example, automation and AI can help organisations manage, monitor, triage, and respond to security data – freeing up IT departments to focus their expertise where it's needed most. Because time is precious, few in-house teams have the resources to mitigate every threat. That's why savvy organisations recognise their limitations. Leveraging the right tools – and the right partner – provides the peace of mind to focus on your core objectives.

Rapidly evolving attacks demand rapidly evolving defence

Cyber defence should deliver…

Protection

- Mitigate internal and external threats
- Shift from reactive to proactive stance
- Become "ready for anything", not "just compliant"

Productivity

- Align security with business goals and drive ROI
- Enable secure multi-cloud, hybrid working
- Ensure a good user experience

Peace of mind

- Streamline management with automation and AI
- Free up your IT team for high-level tasks
- Rely on trusted specialists

Of course, every case is unique. Security controls vary dramatically across businesses, let alone between them. But there's one seismic change that virtually all organisations have embraced in the last few years – and it has dramatic implications for how they secure their operations…

Hello productivity, goodbye perimeter

Hybrid working creates more opportunities – and more threats

Once upon a time, most of our critical assets were on-premise: our people, our data and our systems.

We drew a line around them. We assumed everything inside was good and safe – and everything outside was risky. Naturally, we placed most of our defences at the perimeter between the two, typically our data centre. Hopefully, these controls would block most malicious activities from getting in. But not always; security can never be perfect.

(And when attackers did breach our defences, they had free run at everything – stealing data, disrupting production, installing ransomware.)

Then the corporate network turned 'inside out'.

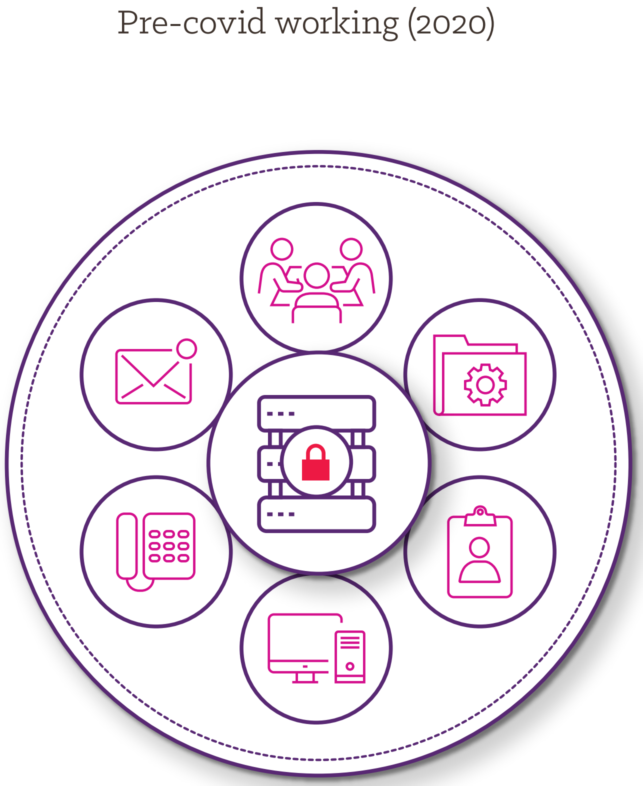
With the emergence of the cloud and hybrid working, suddenly there were more important assets outside networks than within them. Now most networks are a complex mesh of internet-based traffic. Crucially, there is no more perimeter to defend. Your users can be anywhere – and so can your data.

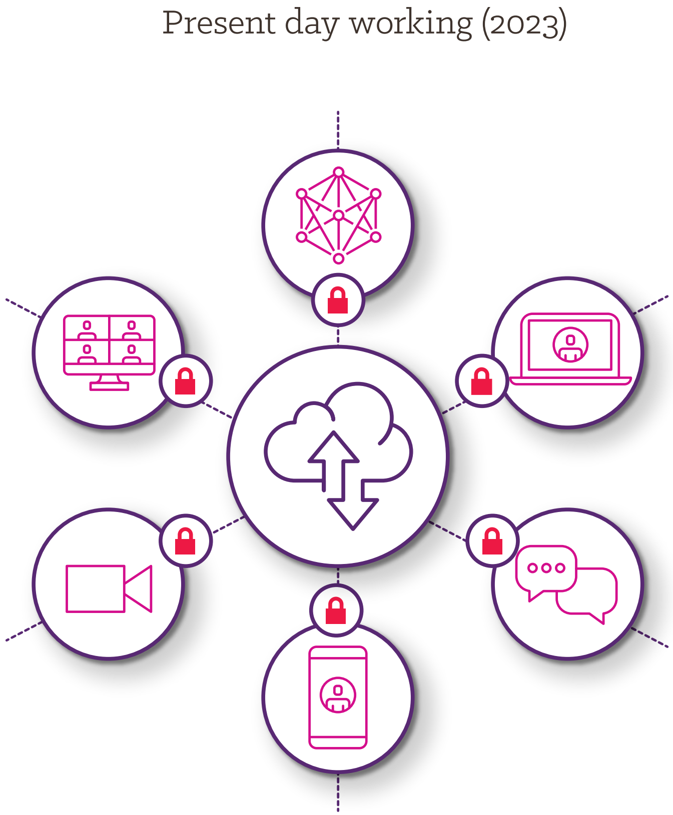
Incredibly powerful. And impossible to defend with the traditional perimeter model.

Now organisations can't rely on location to identify real users from malicious ones. This calls for a paradigm shift.

Enter: perimeterless security.

The office is still key, but is now one of several, entry points to work

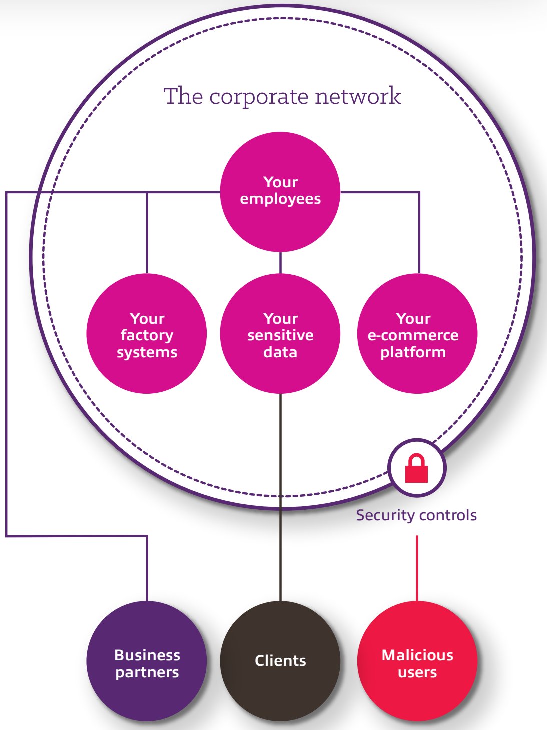




More users, apps, networks, data centres, platforms, devices, geographies

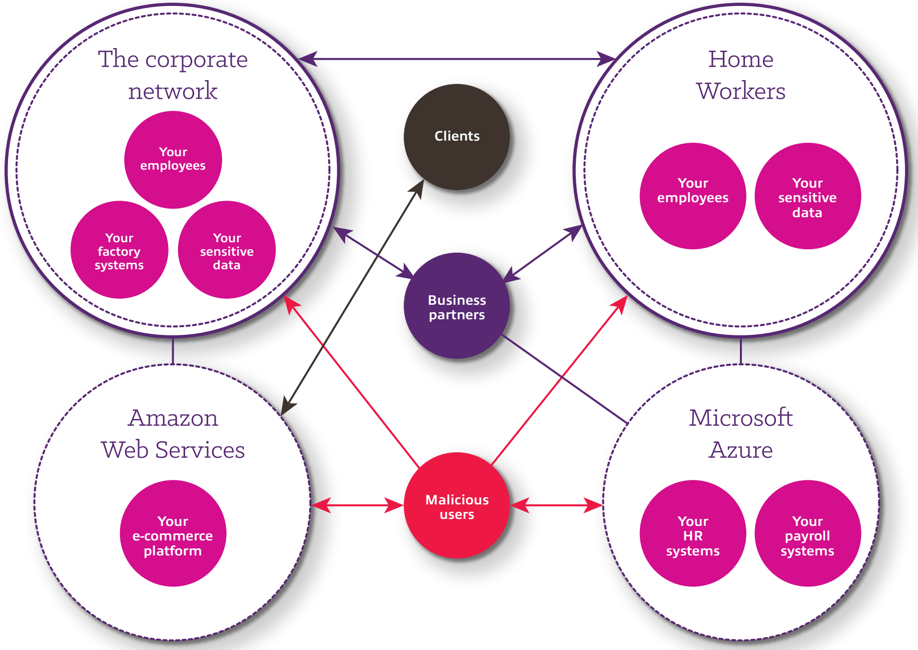
= more risk

The perimeter-based model



Old-school defence won't cut it in a hyper-connected world

Blurred boundaries demand a different model



Perimeterless security

The pillars of perimeterless security

Why organisations need Zero Trust and SASE

How can you protect all users, devices, data, infrastructure, networks and assets, regardless of who is accessing them or where they're being accessed? There is no 'one-size-fits-all' answer to the challenge of perimeterless security. But there are two critical components: Zero Trust and Secure Access Service Edge (SASE).

Let's unpack them.

Zero Trust

Don't trust anyone, or anything, by default

- Reduce risk of breaches
- Achieve granular access control
- Mitigate impact of successful attacks

A Zero Trust security model verifies all users and systems before they can access anything, regardless of their location. It doesn't matter if you're within the corporate firewall: every request must be authenticated, authorised, and encrypted. Zero Trust continually monitors the network for security threats and even assumes the network has already been compromised – only granting minimum access and segmenting the network to limit the impact of a breach.

CORE PRINCIPLES OF ZERO TRUST

1. **Verify explicitly:** Always verify and never trust any user, device, or application that requests access to the network or resources.
2. **Least privilege access:** Grant only the minimum access required to perform a specific task or job and continuously monitor access to prevent unauthorised activity.
3. **Assume breach:** Assume that the network has already been compromised and operate on the basis that attackers may have already gained access.
4. **Micro-segmentation:** Divide the network into smaller segments to minimise the impact of a breach and limit access to sensitive resources.
5. **Continuous monitoring:** Monitor all network activity in real-time, detect and respond to suspicious behaviour, and thoroughly investigate security incidents.

Zero Trust isn't: ✗

- A single product or technology
- A cast iron guarantee, but it's the best we have
- A drop-in replacement for what you do today
- One size fits all

Zero Trust is: ✓

- A risk management approach
- A way of looking at security holistically
- Already here
- A 'must have'

SASE

Streamline security and enhance user experience

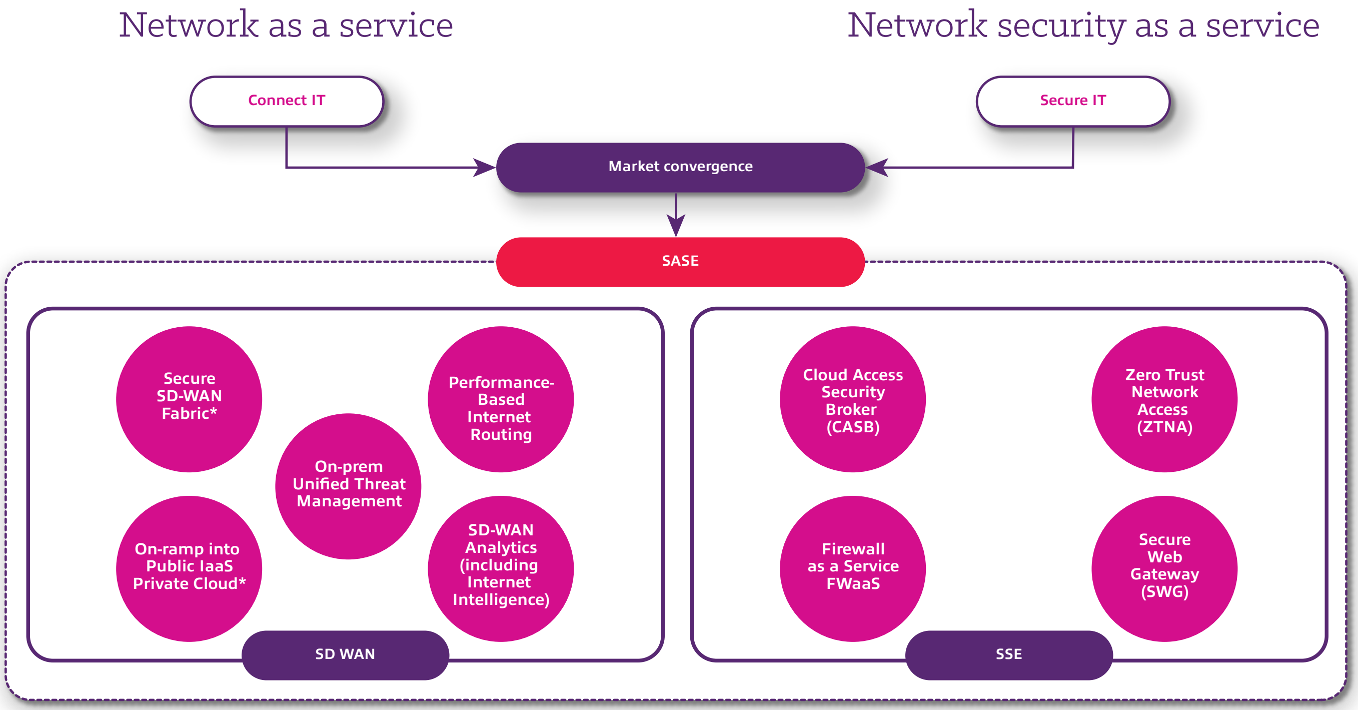
- Reduce attack surface and improve threat detection
- Optimise network performance and enhance user experience
- Scale security and networking on demand
- Minimise cost and complexity

Secure Access Service Edge (SASE) combines wide area networking (WAN) capabilities with network security services in a unified cloud-based model to provide comprehensive security and networking services to users, regardless of location.

CORE PRINCIPLES OF SASE

1. **User-centric security:**
   Secure users rather than the network perimeter to enable users to work from anywhere.
2. **Network security and connectivity:**
   Integrate networking and security to optimise network performance and connectivity across multiple locations.
3. **Cloud-native architecture:**
   Leverage the cloud to deliver flexible, scalable services.
4. **Identity and access management:**
   embrace Zero Trust principles and verify all users based on identity and security posture.
5. **Integrated security:**
   Combine services such as firewalling, secure web gateways, intrusion detection and prevention, data loss prevention, and more into a unified cloud-first platform to deliver consistent security for all users.
6. **Micro-segmentation:**
   Divide the network into smaller segments to contain and control lateral movement in case of a security breach.
7. **Threat intelligence and analytics:**
   Monitor network traffic, detect anomalies, and respond to security incidents in real time.

SASE is the convergence of network as a service and network security as a service



Network as a service

Network security as a service

Connect IT

Secure IT

Market convergence

SASE

Secure SD-WAN Fabric*

On-prem Unified Threat Management

Performance-Based Internet Routing

On-ramp into Public IaaS Private Cloud*

SD-WAN Analytics (including Internet Intelligence)

SD WAN

Cloud Access Security Broker (CASB)

Zero Trust Network Access (ZTNA)

Firewall as a Service FWaaS

Secure Web Gateway (SWG)

SSE

KEY SASE USE CASES

Secure network access wherever users are located

Secure Remote Worker

- Seamless connection to apps and data anywhere users work
- Secure access to internet and cloud apps
- Authenticate users and ensure device health before establishing connection

Secure Office Worker

- Streamline connectivity to public and private apps across all office locations
- Provision SD-WAN fabric across thousands of users and locations
- Secure access to apps and direct internet access

SASE achieves Zero Trust (and more)

Zero Trust and SASE isn't an either/or choice: they work together to deliver enhanced security, scalability and efficiency. Your organisation can move towards Zero Trust by implementing a SASE solution that improves overall security and resilience while minimising cost and complexity.

Naturally, the world of cybersecurity extends beyond Zero Trust and SASE. Are you ready to explore your unique challenges with our experts?

From survive to thrive

It’s time to think long-term

Hybrid work. Perimeterless security. Escalating threats.

Recent times have forced security to play catch-up. However, the era of reactive measures alone is behind us. The reality is that organisations and potential attackers alike are in perpetual flux. Tomorrow will bring yet more opportunities and challenges: the only way to ensure lasting resilience and prosperity is to adopt a proactive, continuously evolving cyber defence.

SURVIVE MODE

What we’ve seen

- Rush to expand existing infrastructure
- Short-term thinking; accepting technical debt
- Patchy multi-factor authentication (MFA)
- Tickbox security training
- Best-of-breed security controls, poorly implemented
- Simple security models that constrain productivity

THRIVE MODE

What we’re seeing now

- Acceptance of new models
- Recognition of need to repay technical debt
- MFA everywhere
- People as the last line of defence
- Suites of highly integrated security controls
- Complex security models that enable productivity

Where we’ve been

Reacting

Remote working, workplace changes, new technology implementations

Adapting

Hybrid workforce, strategic business realignment

Surviving

Temporary/transitional strategies and solutions

Where we’re going

Integrating

Digesting change, remediating gaps, defining new directions

Innovating

Building for the future, energising around a new economy

Optimising

Realise big goals and drive bold changes

The Insight approach

Holistic, proactive, customer-centric security

Protecting increasingly complex networks from proliferating threats can often feel overwhelming. Fortunately, help is at hand.

At Insight, we collaborate closely with customers to develop and implement a bespoke 'Goldilocks' security framework: user-focused, outcomes-driven, and precisely tuned to your aims. Our specialists help you navigate your software lifecycle to unlock the full potential of your investment. We pride ourselves on delivering a comprehensive, proactive, predictive service with rapid remediation.

Our services include:

Consulting:
Whether refining existing systems or constructing new ones from the ground up, we provide the expertise to fortify your security posture.

Lifecycle services:
From seamless integration to ongoing maintenance and responsible asset disposition, we ensure a holistic approach across the entire lifecycle.

Managed services:
We provide invaluable technical assistance and outsourced management, relieving your team of operational burdens while maximising security.

INSIGHT SECURITY AND COMPLIANCE SERVICES

- Governance, Risk & Compliance
- Identity & Access
- Threat Detection & Response
- Human Factors
- Endpoint Security
- Application Security
- Cloud Security
- Datacentre, Network & IoT Security
- Data-Centric Security
- Managed Security Operations Services

Our solutions integrator approach

We pride ourselves on delivering a comprehensive, proactive, predictive service with rapid remediation.

Consulting Services

EVALUATE AND PLAN

- Strategy and roadmap development
- Assessments and workshops
- Architectural design
- User testing and research
- Proof of Concepts (PoC's) and solution vetting
- Cloud & software optimisation

Lifecycle Services

REALISE YOUR STRATEGY

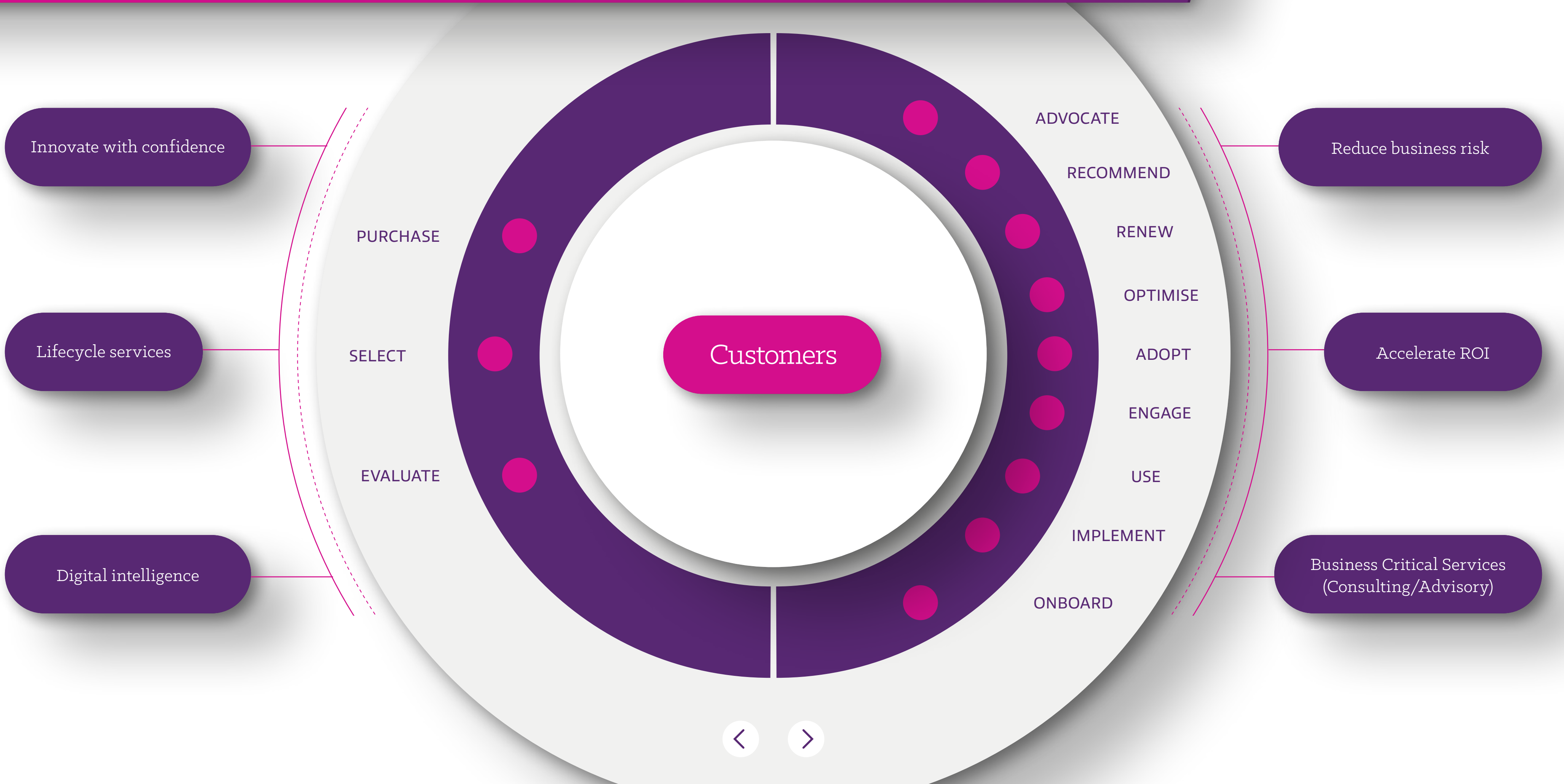
- Provisioning and deployment
- Cloud migration
- Procurement services
- Software asset management
- Adoption and change management

Managed Services

OPTIMISE AND MANAGE

- Monitoring and reporting
- Strategic guidance
- Optimisation measures
- Troubleshooting and support
- Securing and Protecting
- Device break-fix and end-of-life care
- Managed Detection & Response

Prioritising customer experience to reduce risk and maximise ROI

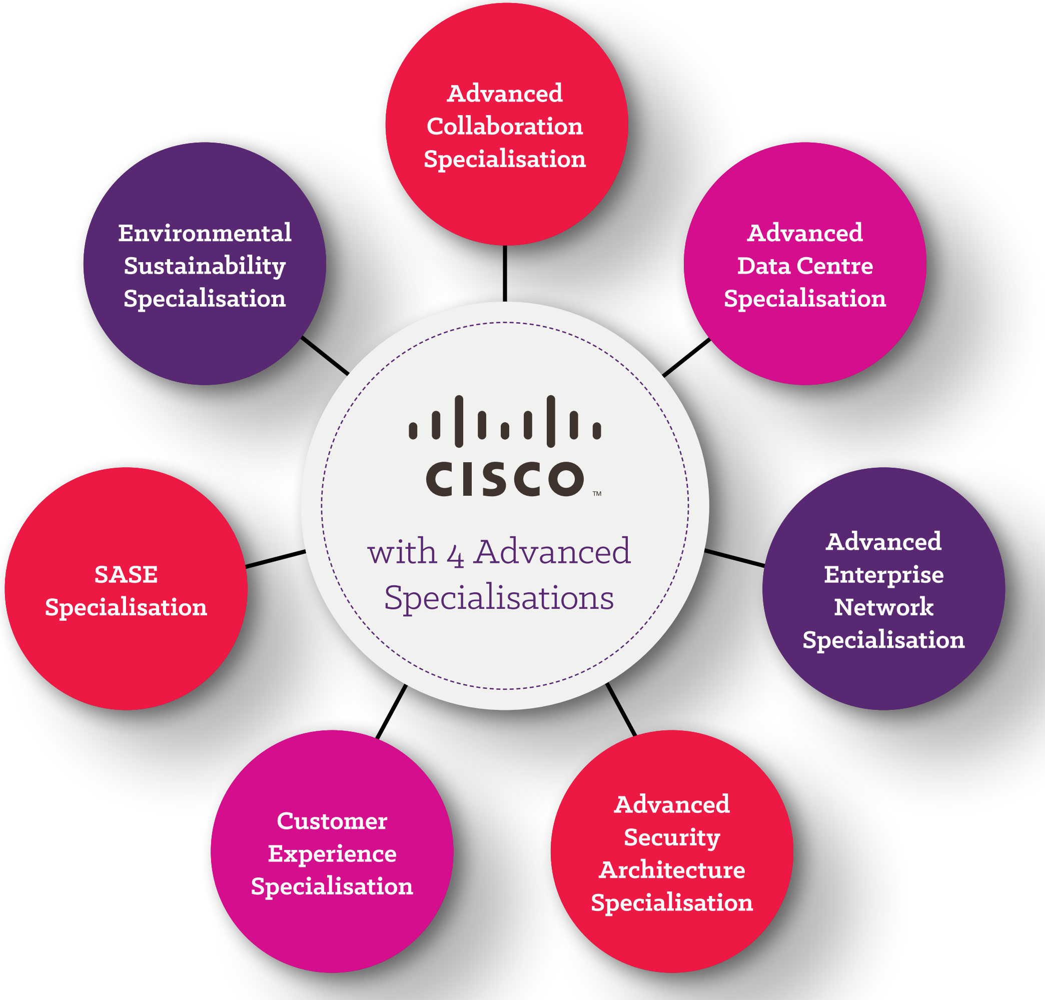


The Insight Cisco partnership: Elevating your defence

Choose a partner with unparalleled expertise in the Cisco security ecosystem

With a strong heritage as a trusted Cisco Gold partner, Insight can help raise your cyber defence posture while supporting broader business goals.

- Established and mature partner delivering a variety of Cisco Solutions
- Comprehensive in-house capability with experienced, highly accredited teammates across Cisco, Azure, AWS, Security, and Modern Workplace
- Wide-ranging services and solutions spanning all Cisco technology pillars
- Investment in CX Services to enhance customer experience and maximise ROI
- ‘Plan,’ ‘Build,’ and ‘Manage’ capabilities within the Insight Cisco Services team



CISCO with 4 Advanced Specialisations

Advanced Collaboration Specialisation

Advanced Data Centre Specialisation

Advanced Enterprise Network Specialisation

Advanced Security Architecture Specialisation

Customer Experience Specialisation

SASE Specialisation

Environmental Sustainability Specialisation

Plan and build

A virtuous cycle for an ever-evolving security posture

Technical Consultancy and Design

Planning and Scoping

Project Management

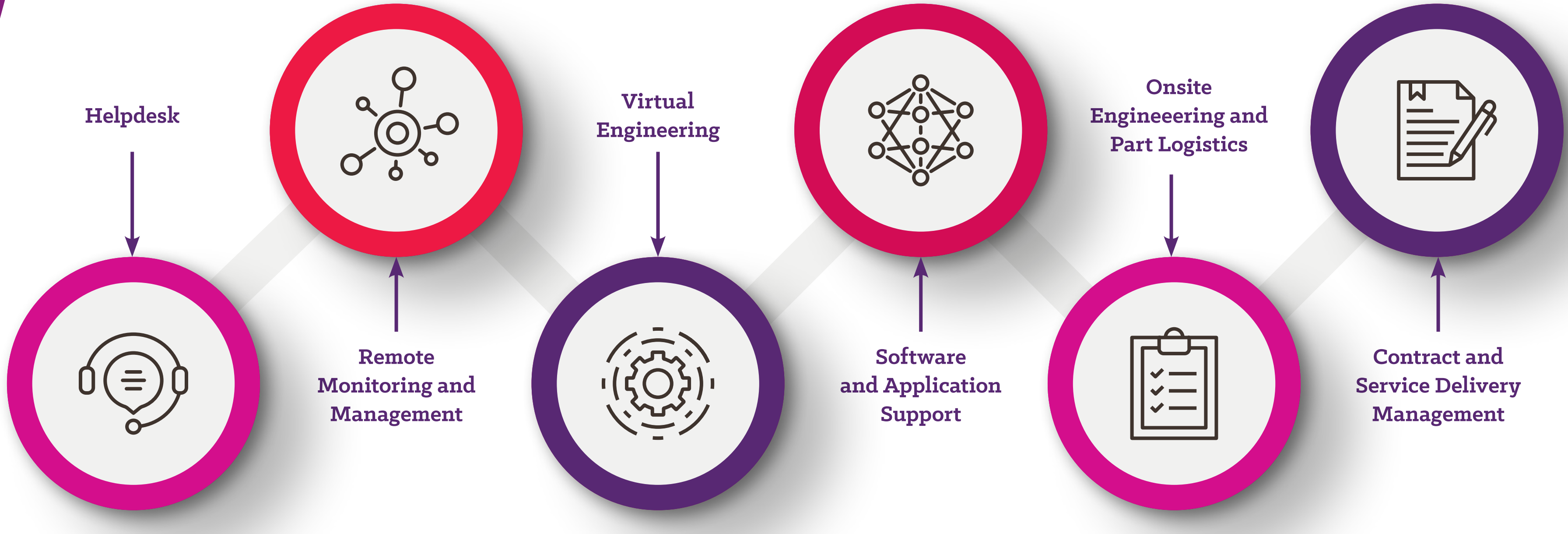
Training and Support

Installation and Commissioning

Pre-build and Testing Facilities

Manage and support

Comprehensive support and expertise, when and where you need it



Helpdesk

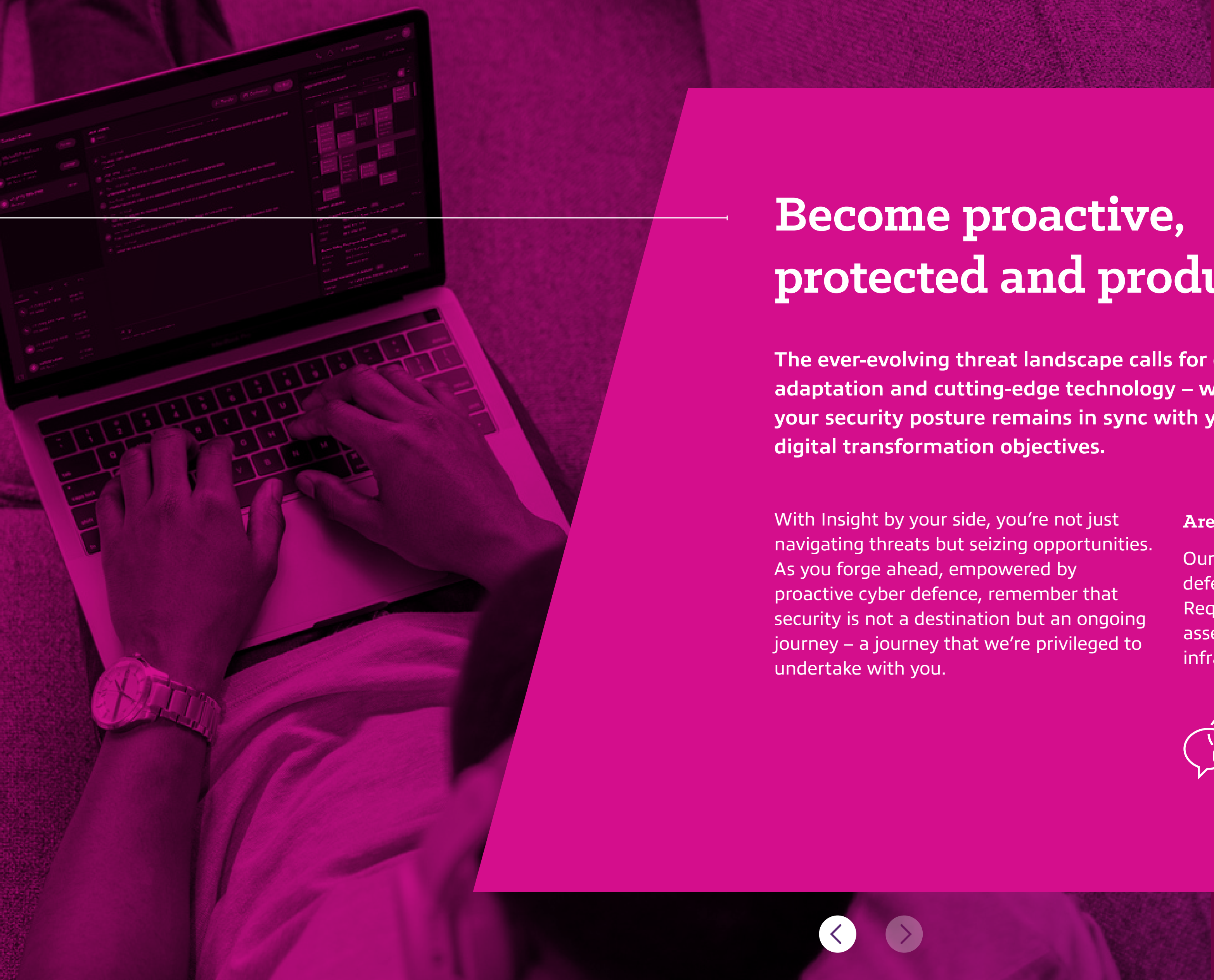
Remote Monitoring and Management

Virtual Engineering

Software and Application Support

Onsite Engineeering and Part Logistics

Contract and Service Delivery Management



Become proactive, protected and productive

The ever-evolving threat landscape calls for constant adaptation and cutting-edge technology – while ensuring your security posture remains in sync with your broader digital transformation objectives.

With Insight by your side, you're not just navigating threats but seizing opportunities. As you forge ahead, empowered by proactive cyber defence, remember that security is not a destination but an ongoing journey – a journey that we're privileged to undertake with you.

Are you protected? Get an expert opinion

Our specialists can find the holes in your defence – before attackers get there first. Request a vulnerability and life cycle assessment to ensure your data and infrastructure are secure and fit for purpose.

Contact
UKCiscoPresales@insight.com