Next-Generation Networking for the Age of Security

Brochure

Executive summary

In today's tech landscape, where cloud adoption and hybrid working have become the norm, networks are the backbone for securing connections, protecting data, and enabling reliable communications.

With business requirements changing rapidly, traditional network security methods are no longer enough to safeguard modern digital infrastructures. Our approach to security must evolve alongside networking solutions to prevent rising threats, ensure data protection, and maintain reliable connectivity.

What's in this article?

We explore the evolving landscape of network security and highlight how organisations can secure their infrastructure in the face of increasing cyber threats. We consider Secure Access Service Edge (SASE) and Zero Trust models as key security frameworks, alongside cutting-edge tools like Cisco Cyber Vision for operational technology (OT) security.

Through our partnership with Cisco, we aim to provide solutions that enhance security and ensure scalable, resilient network infrastructures.

Networks can’t be that important, right?

Secure networks are the backbone of innovation, communication, and protection against cyber threats.

As businesses move to the cloud and adopt hybrid working models, securing these networks has become paramount.

Networks play a vital role in safeguarding critical data and ensuring that communications between devices, users, and systems remain private and protected. Security and connectivity go hand in hand across various areas:

Secure communication

Networks enable encrypted data exchange, voice, and video communication, which are crucial for protecting sensitive information in transit.

Data transmission and storage

In the age of cloud computing, secure networks help protect large volumes of data from interception and ensure safe access from any location.

Internet of Things (IoT)

Networks connecting IoT devices are increasingly targeted by cybercriminals. Secure networks ensure these devices can communicate without compromising sensitive data.

Remote work

With more employees working remotely, networks ensure secure access to corporate resources, protecting against unauthorised access and ensuring compliance.

E-commerce and online transactions

Networks are critical for protecting online shopping and financial transactions, providing the encryption needed for secure and trusted digital experiences.

Cybersecurity and network defence

Facing growing cyber threats, organisations are deploying advanced security measures like firewalls, intrusion detection systems, and encryption to defend against unauthorised access, data breaches, and other risks.

Your legacy network is an open door

As businesses expand and cyber threats evolve, legacy network systems are becoming a liability. Traditional network infrastructures were not designed with modern security needs in mind, making them vulnerable to increasingly sophisticated cyberattacks.

Limited scalability and flexibility:

Legacy networks struggle to scale efficiently and securely as businesses grow. The increasing number of devices, applications, and remote users introduces more attack vectors, making it harder to protect the network.

Complexity and rigidity:

Older network architectures are complex and often rigid, making it difficult to quickly adapt to emerging security threats or enforce policies like Zero Trust.

Security concerns:

Traditional networks lack the advanced security features needed to combat evolving cyber threats. They are more vulnerable to data breaches, ransomware attacks, and unauthorised access - especially when trying to secure remote work environments and cloud-based applications.

Inadequate application security:

Legacy networks often don't prioritise security for critical applications. Without the ability to control and secure traffic effectively, they expose sensitive data and communications to higher risk.

Lack of visibility and control:

With older networks, IT teams often struggle to gain full visibility into network activity, making it harder to detect threats and respond to security incidents in real-time.

To protect against today's cyber threats, organisations need modern, secure, and scalable network infrastructures. By upgrading from legacy networks to solutions like SASE or implementing a Zero Trust framework, businesses can safeguard their data, users, and systems while staying agile in the face of growing security demands.

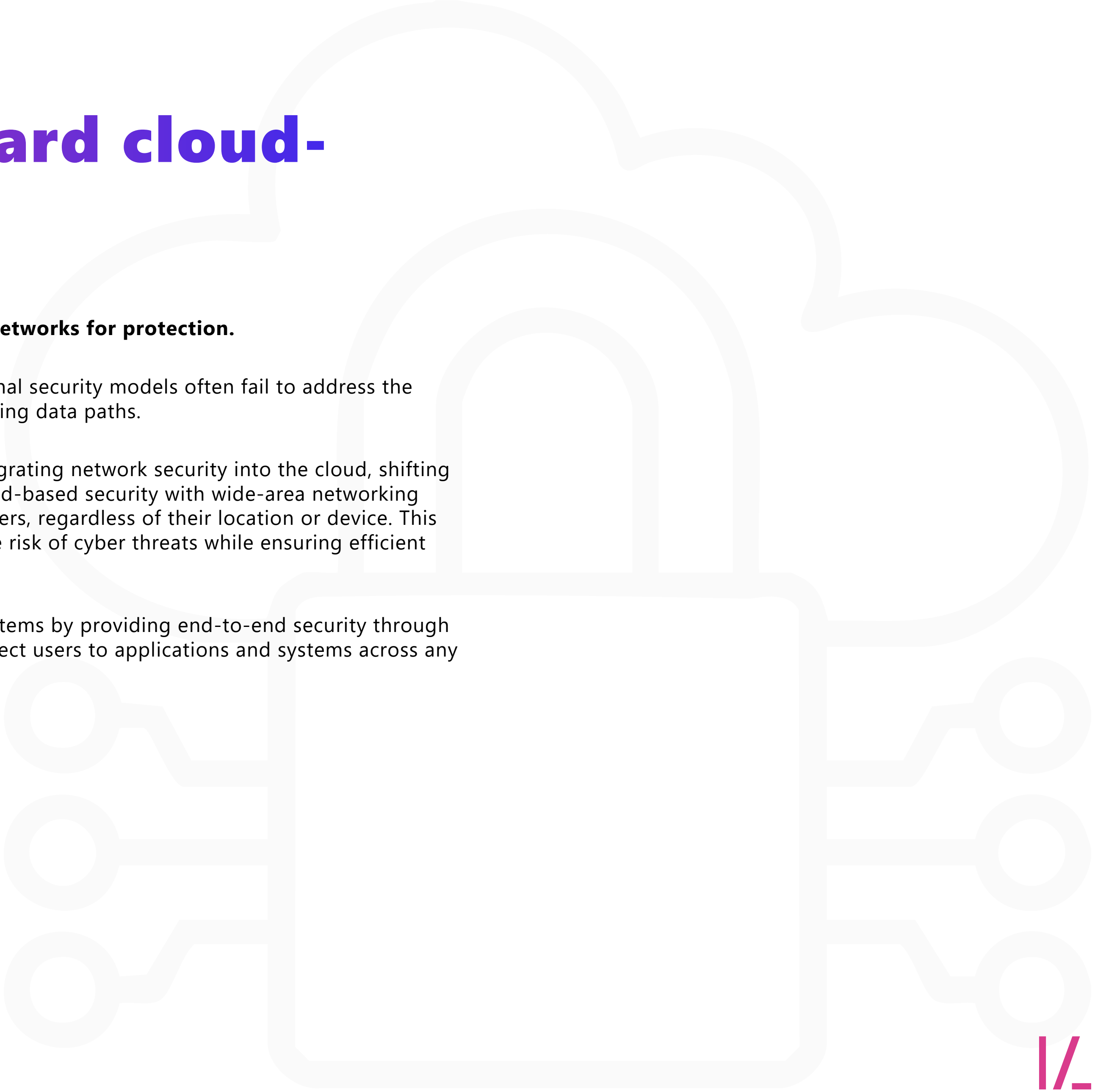
SASE: The shift toward cloud-native security

Organisations can no longer rely solely on on-premise private networks for protection.

As cloud adoption accelerates and hybrid workforces grow, traditional security models often fail to address the vulnerabilities posed by remote access, diverse devices, and expanding data paths.

Secure Access Service Edge (SASE) offers a modern solution by integrating network security into the cloud, shifting away from complex, centralised infrastructures. SASE combines cloud-based security with wide-area networking capabilities, enabling better control and visibility over traffic and users, regardless of their location or device. This scalable solution helps companies enhance protection, reducing the risk of cyber threats while ensuring efficient performance.

Our SASE solutions empower businesses to safeguard users and systems by providing end-to-end security through next-gen tooling. This ensures that organisations can securely connect users to applications and systems across any location while maintaining stringent security protocols.



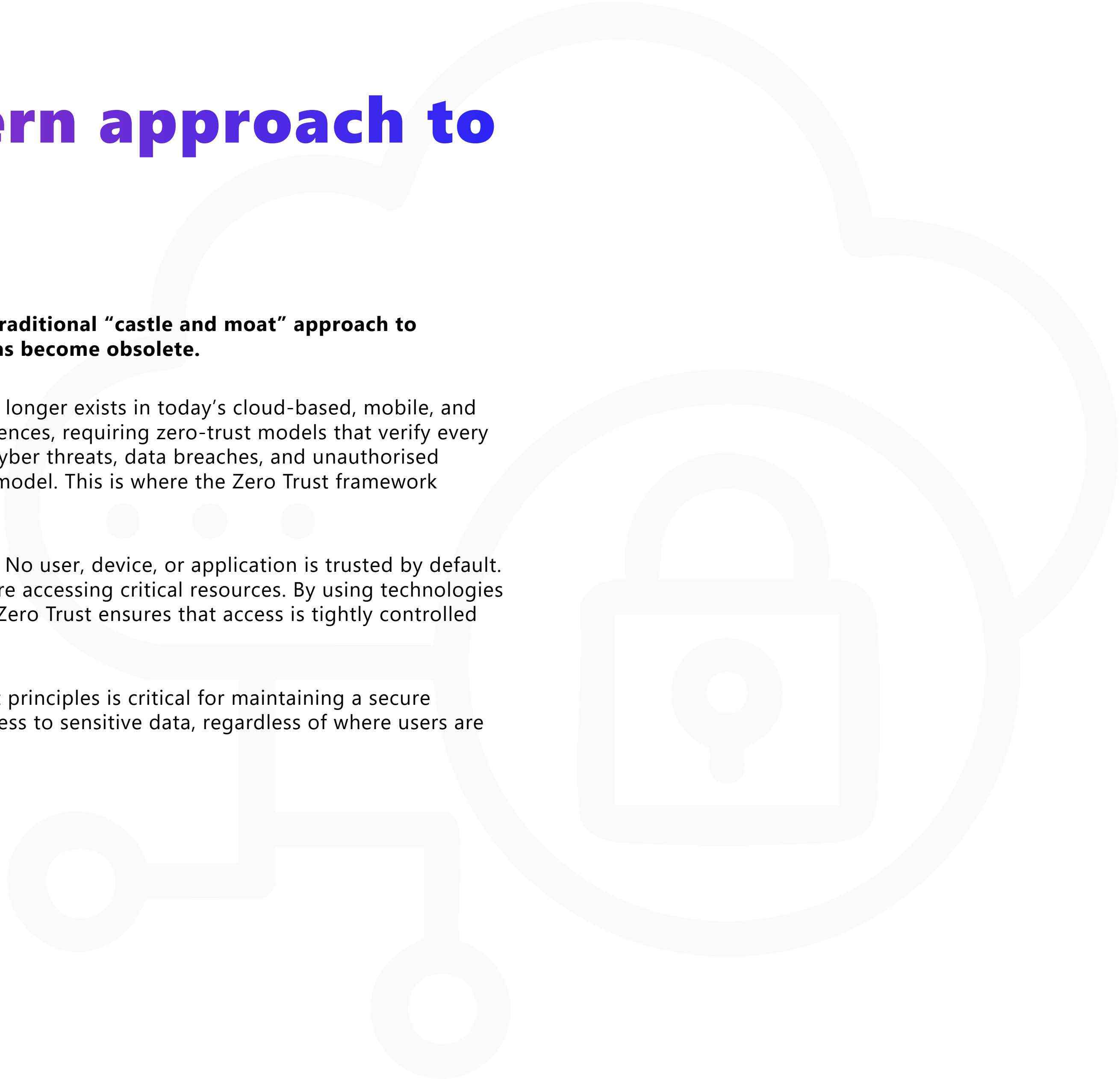
Zero Trust: A modern approach to security

In an era where public cloud and remote work dominate, the traditional “castle and moat” approach to security - where everything inside the perimeter is trusted - has become obsolete.

Castle-and-moat architecture assumes a clear perimeter, which no longer exists in today’s cloud-based, mobile, and remote work environments. Modern threats bypass traditional defences, requiring zero-trust models that verify every access request, regardless of location, to ensure robust security. Cyber threats, data breaches, and unauthorised access are now frequent risks that require a more robust security model. This is where the Zero Trust framework comes into play.

Zero Trust operates on the principle of “never trust, always verify.” No user, device, or application is trusted by default. Instead, each must be verified and authenticated in real time before accessing critical resources. By using technologies like Single Sign-On (SSO) and Multi-Factor Authentication (MFA), Zero Trust ensures that access is tightly controlled and continuously monitored.

As organisations expand into cloud platforms, adopting Zero Trust principles is critical for maintaining a secure posture. These measures are vital for preventing unauthorised access to sensitive data, regardless of where users are located.



Cisco Cyber Vision: Securing industrial networks

Security threats extend beyond IT networks, impacting industrial and operational technology (OT) environments as well. Cisco Cyber Vision provides a cyber security solution designed to protect industrial networks, ensuring the operational continuity and safety of critical infrastructures.

Cisco Cyber Vision delivers three key value propositions:

01

Comprehensive OT Visibility:

It uncovers every asset connected to the industrial network, providing detailed inventories and communication patterns. This visibility enables security teams to implement effective segmentation and manage OT security with precision.

02

Enhanced Security Posture:

With tools for protocol analysis, vulnerability detection, and threat intelligence from Cisco Talos, Cyber Vision helps industrial organisations proactively manage risks and reduce their attack surface.

03

Operational Insights for Enhanced Efficiency:

By monitoring industrial protocols, Cyber Vision delivers insights that help improve network performance, troubleshoot issues, and reduce downtime - ensuring both operational efficiency and security.

By bridging IT and OT, Cisco Cyber Vision offers a unified security architecture, ensuring robust protection across all layers of the industrial network.

Evolving network security: From fragmented tools to unified defence

With IT environments growing more distributed and diverse, the security landscape is becoming increasingly fragmented.

Organisations are faced with multiple security solutions ranging from cloud-native firewalls to networking tools with built-in firewall capabilities - each with its own set of advantages and limitations.

Organisations can no longer afford to compromise between ease of use and functionality. Instead, they need integrated solutions that offer both efficiency and robust security.

By adopting technologies like SASE and Zero Trust, and leveraging advanced tools such as Cisco Cyber Vision, businesses like yours can create a unified approach to network security that meets modern requirements.

Is your network future-ready?

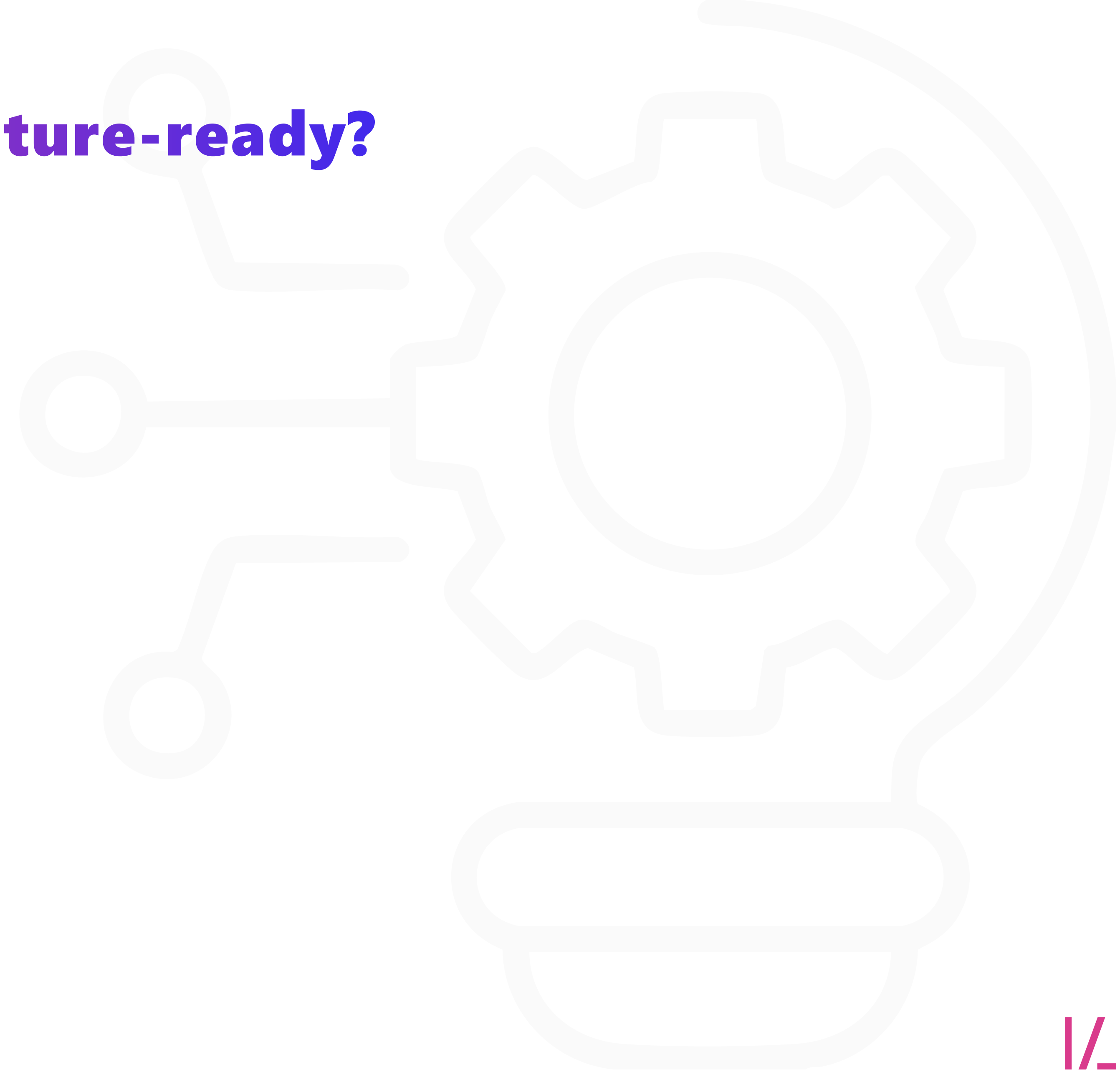
As cyber threats grow more sophisticated, securing your network has become a top priority for protecting business operations.

With the rise of remote work, cloud migration, and the increased reliance on connected devices, your network must be equipped to handle these changes securely.

Organisations face mounting pressure to defend against a variety of attacks, from data breaches to ransomware, while ensuring compliance with stringent security regulations.

Building a security-ready network involves adopting technologies that offer scalability, automation, and advanced security features. Solutions like SASE and Zero Trust provide the ability to secure access for all users, regardless of location or device, while protecting data as it moves across your network.

Businesses that prioritise security as part of their network infrastructure will be better positioned to handle both current and future security challenges.



Cloud and SD-WAN have changed the game

As organisations embrace the cloud and adopt more flexible working models, cloud computing and software-defined wide area networks (SD-WAN) are transforming how networks are secured and managed.

These technologies provide a new way to safeguard data and communications without the limitations of traditional, on-prem security models.

Cloud services offer the ability to scale security measures in real time, allowing businesses to respond quickly to new threats. With no need for large investments in physical security hardware, cloud-native security tools can be deployed to protect sensitive data and ensure continuous monitoring.

SD-WAN enhances network management by prioritising security across distributed locations. For example, Cisco SD-WAN integrates AI-driven security features like machine learning-based threat detection and response, which enables organisations to fend off emerging cyber threats proactively.

SD-WAN's adaptable architecture ensures that security is embedded throughout the network, adjusting dynamically to traffic patterns while protecting critical applications from attacks.

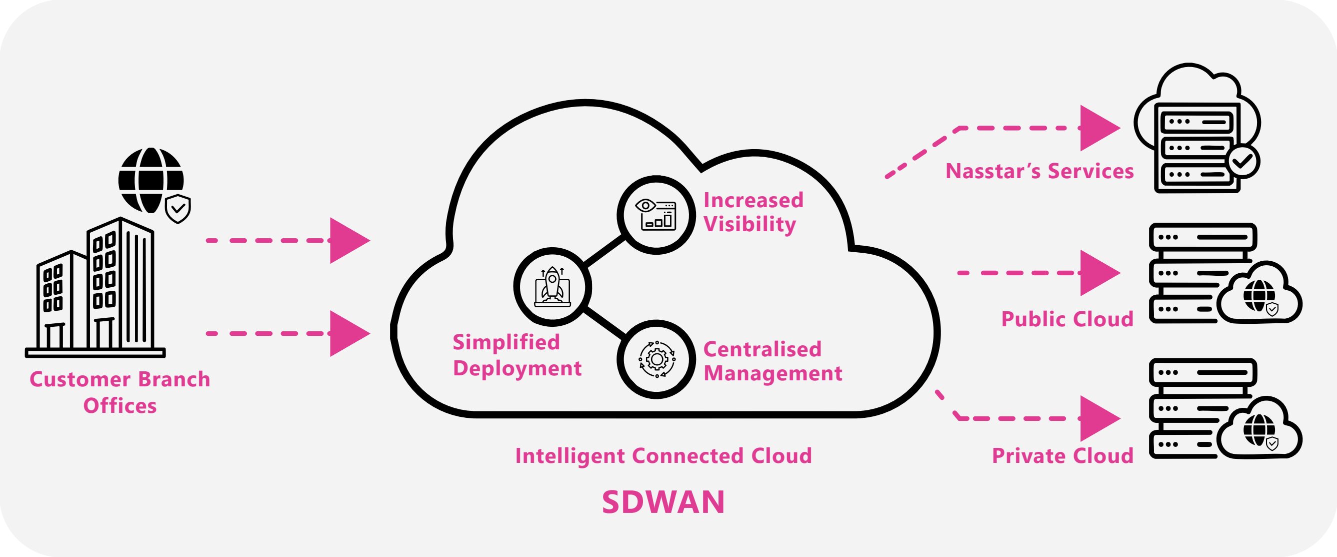
In essence, cloud and SD-WAN provide organisations with the tools needed to securely manage their network traffic while ensuring scalability, visibility, and protection against cyber threats.

Intelligent Connected Cloud (ICC)

Nasstar's ICC service offering has been designed to align with all the SD-WAN technologies we deploy, providing you with a cloud-first connectivity framework that future-proofs your IT environment.

Intelligent Connected Cloud (ICC) optimises the user experience with high-speed connectivity, guaranteed availability, and an integrated security fabric.

With ICC, you can embrace cloud adoption and migration more effectively, with a robust and dedicated connectivity fabric that allows optimal transformation in your organisation.



What we can do for you

At the core of our offerings is a focus on security - because protecting your network has never been more critical.

With the acceleration of cloud applications, remote working, and mobile devices, your network must be equipped with advanced security measures to protect users, data, and systems wherever they're located. Our security-focused solutions are designed to address the most pressing cybersecurity challenges, including:

Scalability

We provide solutions that grow with your business, ensuring that your network security remains robust as traffic volumes and user demands increase.

Visibility and control

With advanced monitoring tools, you gain full visibility into network activity, helping you quickly identify and resolve potential threats.

Optimised traffic

We prioritise critical business applications while ensuring that all network traffic is secured, improving overall performance and reducing latency.

Enhanced protection

Our technologies leverage AI-driven security to proactively detect and mitigate threats in real-time, reducing your exposure to cyberattacks.

Adaptive architecture

By integrating SASE and Zero Trust frameworks, our solutions adapt dynamically to secure all access points, applications, and data in transit.

Predictive analytics

AI-driven analytics enable predictive maintenance, keeping you ahead of issues and minimising the risk of downtime.

In partnership with Cisco, we offer end-to-end solutions that secure your network while optimising performance.

Whether you're looking to secure your cloud infrastructure, enhance visibility, or manage network traffic more effectively, our security-focused approach ensures that your business remains protected against evolving cyber threats.

A Cisco partner you can trust

Whether you need support with implementation or management, we'll find the right solution for you.

Equipped to navigate Cisco architectures, our specialists will help you streamline operations, enhance reporting capabilities, and optimise network performance.

Together, Nasstar and Cisco can fortify your network infrastructure and elevate service quality. We empower our customers with greater efficiency, security, and a transformative approach to AI adoption.

Partner with us and transform your network for the age of security.

Cisco Partner

Gold Integrator
Gold Provider
Collaboration SaaS Authorised Partner
Customer Experience Specialised
Environmental Sustainability Specialised
Small Medium Business Specialised
Advanced Enterprise Networks Architecture Specialised
Advanced Collaboration Architecture Specialised
Advanced Security Architecture Specialised
Webex Contact Center Specialised

NASSTAR

nasstar.com

0345 003 0000

salesenquiries@nasstar.com