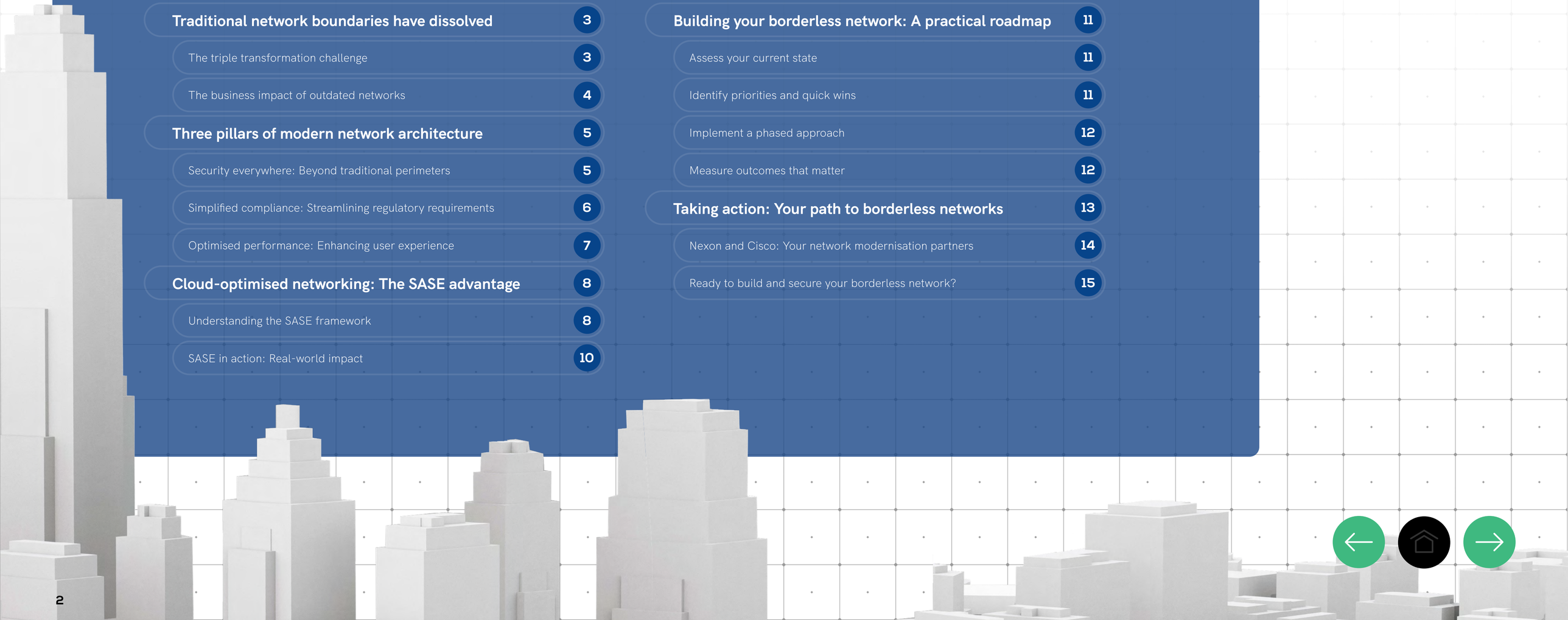
Borderless Networks

How to fortify your organisation wherever work happens

A practical guide to modernising your network architecture for security, compliance and performance in the cloud, AI and remote work era.

What's inside



Traditional network boundaries have dissolved

As organisations shift to cloud and AI while supporting distributed workforces, traditional networking models struggle to keep pace with evolving cyber threats, compliance rules and user demand.

With staff and customers engaging from anywhere, attackers can exploit gaps across fragmented, co-located, on-premise and cloud platforms. This shift requires a new security approach, transitioning from location-based to identity-based protection.

This guide outlines a practical roadmap for implementing cloud-optimised networking with secure access service edge (SASE) capabilities that protect you with identity-based security, unified compliance and intelligent connectivity – delivered wherever work happens.

Through proven frameworks and local success stories, you'll discover how a borderless network architecture enhances security, simplifies compliance and boosts productivity – no matter where your users, data or applications reside.

The triple transformation challenge

Australian organisations face an unprecedented convergence of three powerful forces that are reshaping network requirements:

The cloud-first enterprise has arrived

Organisations have moved critical workloads outside traditional perimeters. The rapid adoption of SaaS applications means that vital business processes no longer reside in controlled data centres but in distributed cloud environments.

Cloud-based platforms such as Microsoft 365 and many others have steadily become the backbone of core operations, from customer relationship management and enterprise resource planning to HR and marketing – creating data flows that bypass traditional security checkpoints entirely.

Work happens everywhere, not somewhere

A version of hybrid work is here to stay, with employees moving between office, home and mobile environments. According to the ABS, 36% of employed Australians regularly work from home[1], significantly higher than pre-pandemic levels. Each remote laptop, tablet and smartphone becomes a potential entry point to your network, expanding the attack surface security teams must protect.

Attackers target the gaps, not the walls

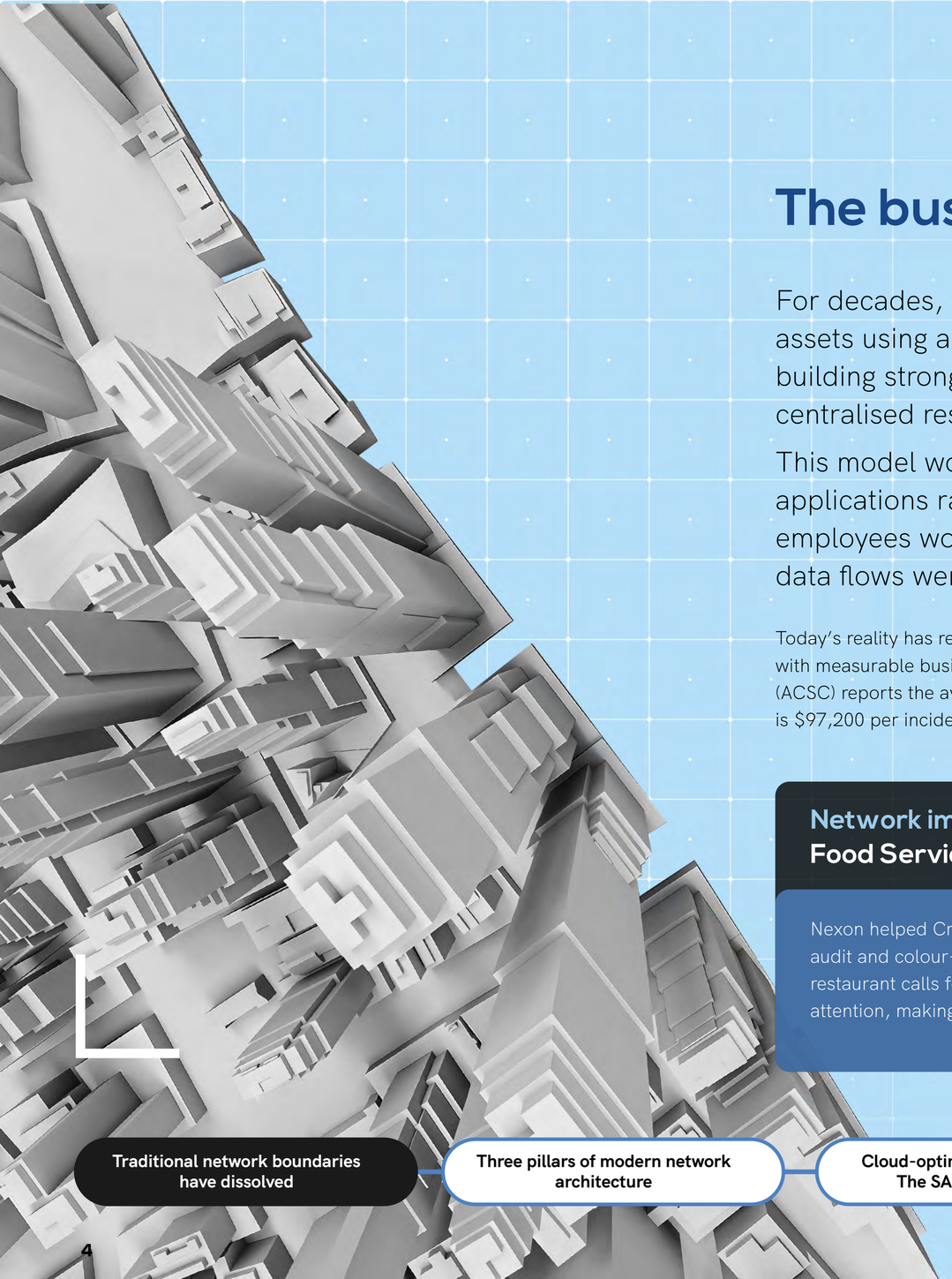
While security has long been an escalating risk, AI brings even more sophisticated attacks designed to exploit the gaps between fragmented security solutions. Cyber criminals are actively targeting remote workers and cloud application vulnerabilities, knowing these are often underprotected.

Expert contributor

Garth Sperring
General Manager – Network, Nexon Asia Pacific

Garth is a senior telecommunications engineer and solutions architect with deep expertise in network and cybersecurity, specialising in secure access service edge (SASE), Zero Trust architecture, and cloud-first security frameworks. He partners with enterprise leaders to design and deliver secure, high-performance network solutions that enable scalable digital transformation. With a focus on resilience, compliance, and business continuity, Garth brings a strategic lens to securing complex, distributed environments.

Garth shares insights from his experience helping organisations build borderless networks that support modern work patterns while maintaining strong security postures.



The business impact of outdated networks

For decades, organisations secured digital assets using a ‘castle and moat’ approach – building strong perimeter defences around centralised resources.

This model worked effectively when most applications ran in corporate data centres, employees worked primarily from offices and data flows were predictable.

Today’s reality has rendered this approach increasingly inadequate, with measurable business costs. The Australian Cyber Security Centre (ACSC) reports the average cost of cybercrime for medium businesses is $97,200 per incident and rising.[3]

Outdated network security contributes to several specific vulnerabilities:

- **Security gaps:** Fragmented solutions create visibility blind spots where threats can hide and propagate
- **Compliance challenges:** Regulatory frameworks become increasingly difficult to satisfy when data flows across multiple environments
- **Performance issues:** Poor user experience due to complex connectivity requirements impacts productivity and satisfaction
- **Rising costs:** Managing multiple point solutions across different environments increases operational complexity and capital expenses
- **Innovation constraints:** The inability to fully leverage AI and cloud technologies limits competitive advantage

Many organisations in sectors like retail and manufacturing compound these issues by operating with decade-old network components long past their intended lifespan. This ‘sweating of assets’ can reduce short-term capital expenditure but increases vulnerability and support costs over time.

Network impact:
Food Service – Eliminating blind spots across 600+ restaurants

Nexon helped Craveable Brands develop a standardised infrastructure, comprehensive cable audit and colour-coded labels to ensure network integrity across all locations. Now, when a restaurant calls for remote support, it’s simple to identify which cables or equipment need attention, making support much faster.

Three pillars of modern network architecture

As organisations adapt to the borderless nature of modern work, Nexon has identified three fundamental pillars that are essential components of a robust, future-ready network architecture.

Security everywhere: Beyond traditional perimeters

Simplified compliance: Streamlining regulatory requirements

Optimised performance: Enhancing user experience

The first pillar shifts security from a location-based model to an identity-based approach that follows users wherever they go.

Zero trust: Never trust, always verify

The core principle of modern security is 'zero trust' – the idea that trust is never assumed, and verification is required from everyone trying to access resources on your network, regardless of location:

Traditional approach:

- Trust based on network location
- Once inside the perimeter, relatively open access
- VPN provides a trusted path to internal resources
- Focus primarily on external threats
- A breach can give attackers access to the entire network

Zero trust approach:

- Trust based on identity and context
- Continuous verification for all access
- Least-privilege access to specific applications
- Focus on threats from any source, internal or external
- Each user has the minimum access required for their specific role to limit exposure

Unified threat protection

Borderless networks require unified threat protection that works consistently across all environments:

- Trust based on network location
- Advanced threat prevention that stops malware, ransomware and other attacks before they breach your network
- Data loss prevention (DLP) that protects sensitive information regardless of where it travels
- Integrated security services that provide consistent protection for users, devices and applications

Manufacturing and Operational Technology (OT)

In manufacturing, security challenges extend beyond IT to the OT that controls physical processes. Modern network architecture must securely segment these critical industrial systems while enabling data flow for analytics and optimisation. This requires specialised approaches to protect legacy equipment never designed for connectivity, while supporting industrial IoT capabilities that drive manufacturing innovation.

Network impact:

Food Service – Unified security and support across 600 restaurants

For Craveable Brands, the solution introduced direct three-way technical support conversations between stores, the service desk and Nexon, with agreed troubleshooting steps. "When we need help, everyone stays on the line to resolve it quickly without frustrating waits, double-ups or callbacks," explains Simon Revelman, CIO of Craveable Brands.

Three pillars of modern network architecture

As organisations adapt to the borderless nature of modern work, Nexon has identified three fundamental pillars that are essential components of a robust, future-ready network architecture.

Security everywhere: Beyond traditional perimeters

Simplified compliance: Streamlining regulatory requirements

Optimised performance: Enhancing user experience

The second pillar addresses the growing complexity of compliance requirements through automation and centralised control.

Unified policy management

Modern compliance demands consistent implementation of security controls across all environments. Borderless networks enable:

- Centralised policy creation that ensures consistent rules across cloud, on-premise and remote environments
- Automated implementation that eliminates the manual configuration errors that often create compliance gaps
- Contextual policy application that adapts to different user scenarios while maintaining security

This approach is particularly critical for organisations subject to specific regulatory frameworks such as the Notifiable Data Breaches scheme, the Security of Critical Infrastructure Act (SOCI), industry-specific regulations like APRA CPS 234 for financial services, healthcare data protection requirements, and the statutory obligations faced by manufacturing and critical infrastructure providers.

Comprehensive visibility

Compliance depends on complete visibility into network activity, user behaviour and data movement. Modern network architecture provides:

- End-to-end visibility across all environments
- Centralised logging and audit trails that document all access and activities
- Automated compliance reporting that reduces the burden of regulatory documentation

For local councils and state and federal government agencies, this visibility is essential for meeting their statutory obligations while functioning efficiently in a cloud-enabled, hybrid work environment.

The compliance challenge is growing more complex each year. Organisations must navigate an expanding web of regulations, from the SOCI that now covers more sectors than ever, to the Privacy Act's evolving requirements, industry-specific frameworks and the unique statutory obligations faced by government agencies. Modern networks must be designed to adapt to this changing regulatory landscape.

Network impact:
Healthcare – Secure vaults protect personal health data

For a leading national healthcare provider supporting thousands of clients, Nexon implemented a unified security approach critical for protecting sensitive client data while enabling consistent service delivery. By separating sensitive healthcare data into secure vaults while maintaining accessibility for legitimate staff needs, they could meet strict regulatory requirements without compromising client care.

Three pillars of modern network architecture

As organisations adapt to the borderless nature of modern work, Nexon has identified three fundamental pillars that are essential components of a robust, future-ready network architecture.

Security everywhere: Beyond traditional perimeters

Simplified compliance: Streamlining regulatory requirements

Optimised performance: Enhancing user experience

The third pillar focuses on delivering exceptional performance that supports modern work patterns and technologies.

Direct-to-cloud access

Traditional networks that backhaul all traffic through centralised security checkpoints create significant performance issues, especially for cloud applications. Modern architectures enable:

- Direct and secure access to cloud applications from any location
- Optimised routing that minimises latency and maximises throughput
- Application-aware policies that prioritise critical services

Intelligent connectivity

Modern networks leverage AI and automation to optimise connectivity in real-time:

- Adaptive bandwidth allocation that prioritises critical applications
- Automated path selection that routes traffic through the optimal network path
- Proactive issue resolution to identify and fix performance problems before users notice

Scalable infrastructure

As organisations' needs evolve, modern network architecture scales efficiently:

- Cloud-native design that grows seamlessly with changing requirements
- Standardised deployment that simplifies adding new locations or users
- Consumption-based models that align costs with actual usage

While each pillar delivers significant value independently, their true power emerges when they work together as an integrated system, enabling security that enhances rather than impedes performance, compliance that's built in rather than bolted on and performance that's secure by design.

Network impact:
Retail – Secure foundation for 500+ ANZ stores

Nexon helped Retail Apparel Group (RAG) implement greater efficiencies and management by consolidating networking and telephony across ANZ, fully redundant store communications, local and responsive 24x7 management and support. They also standardised network and security architecture and fixed price service provisioning to create a stable, secure and modern network platform for future digital transformation.

Cloud-optimised networking:

The SASE advantage

As organisations seek to implement the three pillars of modern network architecture, Secure Access Service Edge (SASE) has emerged as the leading framework for delivering borderless networks.

SASE provides modern businesses with comprehensive protection and performance by unifying networking and security functions in a cloud-delivered model.

Understanding the SASE framework

SASE represents a convergence of networking and security capabilities delivered as a cloud service that follows users rather than being tied to physical locations.

First defined by Gartner in 2019, SASE has rapidly evolved from concept to essential architecture as organisations adapt to cloud and remote work realities.

Key characteristics of SASE

What makes SASE fundamentally different from traditional approaches?

Cloud-native architecture

SASE services are delivered from the cloud rather than through hardware appliances, enabling:

- Global reach with local presence
- Automatic scaling to meet demand
- Continuous updates without disruptive upgrades
- Reduced infrastructure footprint and management

Identity-driven access

SASE makes access decisions based on identity - who you are, not where you are:

- User identity becomes the foundation of security policy
- Device health and compliance influence access decisions
- Application sensitivity determines security requirements
- Contextual factors modify access in real-time

Consolidated services

SASE brings together previously separate functions:

- Network connectivity optimisation
- Comprehensive threat protection
- Data security and compliance controls
- Application-specific security policies

Cloud-optimised networking:

Traditional approach vs SASE

Network function	Traditional Approach	Network function
Web Security	On-premise web proxy appliances	Cloud-based secure web gateway (SWG)
Remote Access	VPN concentrators with broad network access	Zero trust network access (ZTNA) with application-specific access
Cloud Security	Limited visibility into cloud apps	Cloud access security broker (CASB) for comprehensive cloud protection
Threat Protection	Separate firewalls and security tools	Unified firewall as a service (FWaaS) with integrated threat defence
WAN Connectivity	Fixed MPLS circuits with limited flexibility	Software-defined WAN (SD-WAN) with dynamic path selection
Management	Multiple separate consoles	Single cloud-based management platform

The Building Blocks of SASE

While vendors may use different terminology, most SASE solutions incorporate multiple core components:

Security Service Edge (SSE)

Including the SWG, CASB, ZTNA and FWaaS security components that protect users, applications and data regardless of location.

Network Service Edge (NSE)

Including the SD-WAN and NaaS networking components that optimise connectivity and routing across environments.

Network impact:
Healthcare – Higher performance, stronger national network

For an Australia-wide healthcare organisation, Nexon helped transform its fragmented IT infrastructure into a cloud-optimised network. This unified approach eliminated technology silos between states, enhanced data visibility and significantly improved service reliability for both staff and clients - reducing service disruptions by eliminating processes that previously varied by location.

Cloud-optimised networking:

SASE in action

To understand how SASE transforms network operations, consider a typical day for an employee at a financial services firm:

Morning

Logs in at the office

- Employee connects to the corporate network
- SASE automatically applies appropriate security policies
- Direct cloud access is provided with inline security
- All traffic inspected and secured – no performance impact

Afternoon

Works from home

- Employee connects via home broadband
- SASE provides the same security regardless of location
- Access to sensitive systems requires added verification
- Policies adjust based on connection type and risk

Evening

Checks in while travelling

- Employee connects via public Wi-Fi at a hotel
- SASE enforces stricter security due to higher risk
- Sensitive data access may be limited
- Suspicious activities trigger an immediate risk response

Throughout the day, the employee experiences consistent security, performance and user experience regardless of location – the essence of a borderless network.

Benefits beyond security

Implementing SASE delivers quantifiable business benefits beyond pure security:

- **Enhanced security posture:** More consistent security across all locations with standardised policies
- **Operational efficiency:** Simplified management and billing with predictable costs
- **Improved user experience:** Better performance for cloud applications with direct secure access
- **Business agility:** Faster deployment and support for new locations with standardised technology

Network impact:

Pest Control – Enhanced security and business continuity

Flick Anticimex chose to partner with Nexon due to the fully integrated nature of the proposed solutions and Nexon's values-led approach. By transitioning to Nexon cloud services across multiple data centres, Flick benefits from a distributed model, which helps it avoid potential single points of failure. It ensures Flick possesses a greater ability to securely back up critical data, recover rapidly from any downtime and maintain business continuity in all circumstances.

Building your borderless network

A practical roadmap

Transforming traditional network architecture into a borderless network requires a structured approach that balances long-term vision with practical, incremental steps.

Assess your current state

Before developing a transformation roadmap, it's essential to understand your current network maturity across key dimensions:

Performance and user experience assessment

- How directly can users access cloud applications?
- What level of visibility exists across different environments?
- How quickly can new locations or users be added to the network?

Security maturity assessment

- Are access decisions primarily based on network location or user identity?
- How consistently are security policies applied across different environments?
- Do cloud applications receive the same level of protection as on-premise systems?

Compliance readiness assessment

- Can you demonstrate consistent policy enforcement across environments?
- How effectively can you track and report on security controls?
- What capabilities exist for protecting data in cloud applications?

Identify priorities and quick wins

After completing your assessment, the next step is identifying the most critical gaps and prioritising improvements based on risk, business impact and implementation complexity.

Evaluate identified gaps based on:

Security risk exposure

- Which gaps create the greatest vulnerability to threats?
- What is the potential impact of a security breach in affected areas?

Compliance impact

- Which gaps create the most significant compliance risks?
- What penalties or consequences could result from these gaps?

Operational impact

- Which gaps most significantly affect business operations?
- How do these gaps impact user productivity or experience?

Categorise potential improvements based on implementation complexity, time to value and strategic alignment to identify quick wins that deliver immediate value and strategic initiatives that build toward your borderless network vision.

Network impact:
Healthcare – Assessment reveals cross-state inconsistencies

When a national healthcare provider engaged Nexon to conduct a network assessment, the process uncovered operational inefficiencies. Staff used different IT processes depending on their location, critical client data was siloed across states and security policies varied by region. This assessment provided the roadmap for prioritising unified data access and standardised security controls, enabling Nexon to develop a phased transformation plan that addressed critical vulnerabilities while minimising disruption.

Building your borderless network

Consider a phased approach to implementation

With priorities established, develop a phased implementation plan that balances immediate needs with long-term objectives:

1 Phase 1 Foundation and quick wins

- Implement enhanced endpoint protection for remote workers
- Deploy monitoring tools for comprehensive network visibility
- Establish baseline security policies across environments

2 Phase 2 Core transformation

- Deploy core SASE components based on prioritised use cases
- Implement zero-trust access for critical applications
- Establish cloud-delivered security services

3 Phase 3 Expansion and optimisation

- Expand implementation to the remaining locations and user groups
- Deploy AI-driven security analytics and response
- Optimise operational processes and procedures

Measure outcomes that matter

Throughout implementation, track progress using metrics that align with your business objectives:

Security metrics

- Reduction in security incidents and vulnerabilities
- Improved mean time to detect and respond to threats

Operational metrics

- Decreased management complexity and operational overheads
- Reduced time to implement changes and updates

Business impact metrics

- Improved user satisfaction and productivity
- Faster deployment of new business capabilities

Network impact:
Food Service – Delivering more value without increasing costs

"We're delivering new switches, access points, cables, service improvements and better speed, security and reliability – all for the same price as five years ago," says Simon Revelman, CIO of Craveable Brands. "Now, we have predictable costs and simplified billing across all locations."

Taking action:

Your path to borderless networks

The shift to borderless networks represents both a necessary response to today's challenges and a strategic opportunity to enhance your organisation's security, compliance and performance.

Traditional network boundaries have dissolved

The convergence of cloud adoption, remote work and evolving threats has fundamentally changed the network landscape. Security and performance can no longer depend on well-defined perimeters, requiring a new approach that secures and optimises connections wherever users work.

Security must follow users, not locations

Identity-based security that travels with users provides consistent protection across all environments. Organisations can secure access to applications and data regardless of user location or device by implementing zero trust principles through a SASE framework.

Integration delivers cumulative benefits

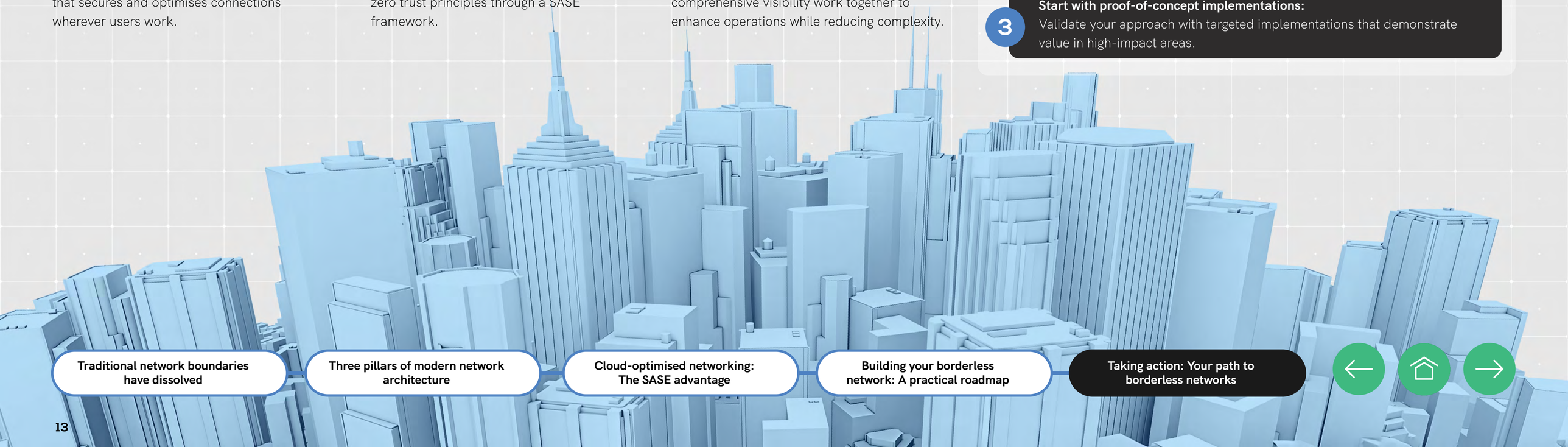
While individual improvements to security, compliance or performance deliver value, their integration through borderless architecture creates multiplicative benefits. Unified management, consistent policies and comprehensive visibility work together to enhance operations while reducing complexity.

Transformation is a journey, not an event

Implementing borderless networks is an evolutionary process that balances immediate needs with long-term objectives. A phased approach that delivers incremental value while building toward a comprehensive vision enables sustainable transformation with minimal disruption.

To begin your borderless network journey, consider these practical next steps:

1. **Conduct a focused assessment:** Evaluate your current environment, focusing on security, connectivity and user experience.
2. **Define your vision and roadmap:** Establish measurable objectives and prioritise key use cases for maximum business value.
3. **Start with proof-of-concept implementations:** Validate your approach with targeted implementations that demonstrate value in high-impact areas.



Nexon and Cisco: Your network modernisation partners

Implementing borderless networks requires technical expertise and a deep understanding of business requirements.

Nexon and Cisco combine industry-leading technology with proven implementation experience to guide your transformation journey.

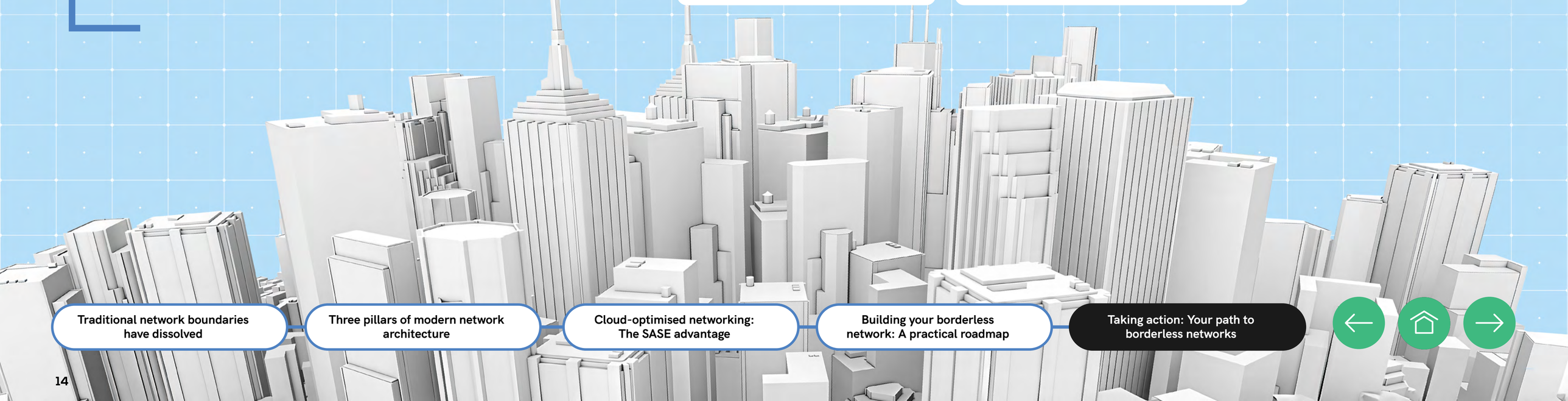
The Nexon advantage

- Proven methodology for successful network transformation
- Cross-domain expertise in networking, security, cloud and compliance
- Local implementation experience with Australian organisations

Cisco's technology platform

- Complete SASE portfolio including Cisco Umbrella, Cisco Duo and Cisco SD-WAN
- Integrated security and networking functions
- Future-ready architecture that adapts to emerging threats experience with Australian organisations

Cisco Partner



Ready to build and secure your borderless network?

Book your no-obligation SASE assessment today

To help you begin your borderless network journey, Nexon offers a complimentary assessment that provides a current state analysis, gap identification, transformation roadmap and business case development to secure and optimise your organisation wherever work happens.

About Nexon Asia Pacific

Nexon is an award-winning digital consulting and managed services partner for mid-market, enterprise and government organisations across Australia. We offer clients a uniquely broad suite of solutions requiring end-to-end capabilities coupled with specialist expertise in security, cloud and digital solutions. As a certified and accredited local and state government provider, CREST and ISO-certified, Nexon partners with world-class technology vendors to deliver innovative and integrated solutions.

To find out about Nexon, call us at 1300 800 000, email us at enquiries@corp.nexon.com.au or visit nexon.com.au

References:

1 Australian Bureau of Statistics (ABS): Working arrangements 2024

2 Gartner: 3 Bold and Actionable Predictions for the Future of GenAI, 2024

3 Australian Cyber Security Centre (ACSC): ASD Cyber Threat Report 2022-2023