NORTHBRIDGE
CYBER RESILIENCE BY DESIGN

CASE STUDY · RETAIL

VPN → ZERO TRUST

A scalable security model.

Delivered by Northbridge | Powered by Netskope

SECTOR	SIZE	PLATFORM	SERVICE
Retail	100–250 staff	Netskope SSE	Fully managed

01 OVERVIEW

Executive Summary

A national technology services provider engaged Northbridge to modernise secure access across a portfolio of mid-market customers in the retail sector.

These organisations typically employed between 100 and 250 staff and relied heavily on cloud platforms, remote access, and SaaS applications to run their businesses.

Most of those customers still depended on traditional VPNs, on-premise web gateways, or early cloud security tools. These had served their purpose historically, but introduced growing security and operational challenges as workforces became more remote and cloud adoption increased. Once users connected via VPN, they were typically granted broad network access, and the controls applied to them varied depending on where they were working.

At the same time, employees across these organisations had rapidly adopted generative AI tools as part of everyday work. Because that activity sat outside any inspected path, IT teams had no visibility into which AI applications were being used, by whom, or what business information was being entered into them.

Northbridge was engaged to design and deploy a modern Zero Trust security architecture, powered by Netskope, practical and scalable enough to be rolled out consistently across multiple customers, yet simple enough to operate day to day. Northbridge then took the solution on as a fully managed service.

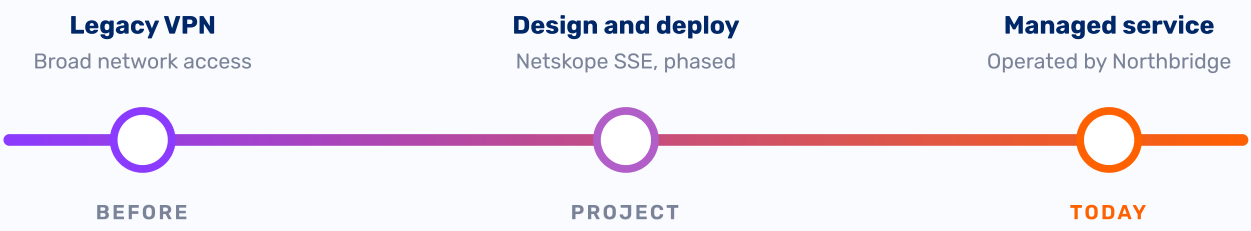
Over several months, Northbridge deployed a cloud-delivered Secure Service Edge (SSE) platform that replaced VPN-based access with application-level Zero Trust Network Access and unified web and cloud security. For the first time, IT teams could also see generative AI usage across the organisation — which tools were in use, who was using them, and what data was moving into them. The result was a significantly stronger security posture, visibility and control over AI usage, reduced operational complexity, and a repeatable Zero Trust model well suited to service providers and growing organisations alike.

IN SHORT

- ✓ VPN access replaced with application-level Zero Trust
- ✓ Most deployments completed within weeks
- ✓ Generative AI usage made visible and governable
- ✓ Consistent controls in the office and remote
- ✓ Operated end-to-end as a fully managed service

THE ENGAGEMENT

From legacy platforms to a managed Zero Trust service



Deployed over several months, then taken on end-to-end as a managed service.

02

CONTEXT

Customer Environment

The customers involved were mid-sized organisations with lean IT teams and limited in-house security expertise. Most had already adopted cloud services such as Microsoft 365, SaaS business applications, and hosted internal systems, but their security architecture remained network centric.

Remote employees reached those systems through VPN appliances, while internet security was enforced by a mix of endpoint agents, firewalls, and legacy web gateways. Because these tools operated independently, enforcement was fragmented and visibility was limited, placing ongoing pressure on small IT teams already constrained by capacity.

Common characteristics included

- Retail
- 100–250 employees
- Hybrid workforce
- Cloud identity platforms already in place
- Limited internal security resources
- Strong reliance on external IT and security support

These customers needed strong security without enterprise-level complexity: a cloud-first approach that was quick to deploy, centrally managed, cost-effective, and able to scale as the business grew.

03

THE PROBLEM

The Security Challenge

01 ACCESS

Overexposed network access

The primary issue was overexposed network access. Once authenticated through VPN, users were effectively placed onto the internal network, often with far more access than their role required. This magnified the impact of any credential compromise and made least-privilege access difficult to enforce.

02 POLICY

Inconsistent enforcement

Security enforcement was also inconsistent. Remote users were frequently subject to different controls than those in the office, and in some cases traffic bypassed inspection entirely limiting the organisation's ability to monitor activity, enforce acceptable use policies, and detect threats.

03 INSIGHT

No single source of truth

Visibility was a further concern. With multiple point solutions in place, IT teams had no single source of truth for user activity, cloud application usage, or access to internal systems. Shadow IT was difficult to identify, and audit and compliance requirements were harder to meet.

04 AI

Ungoverned generative AI

Generative AI widened that gap considerably. Staff were already using AI assistants and AI-enabled SaaS tools independently of IT, frequently through personal accounts and unmanaged browsers. IT teams could not answer basic questions: which AI applications were in use, how widely, or whether company data was being pasted into them. Without visibility there was no way to govern the activity, and blocking AI outright was neither practical nor in the interests of the business.

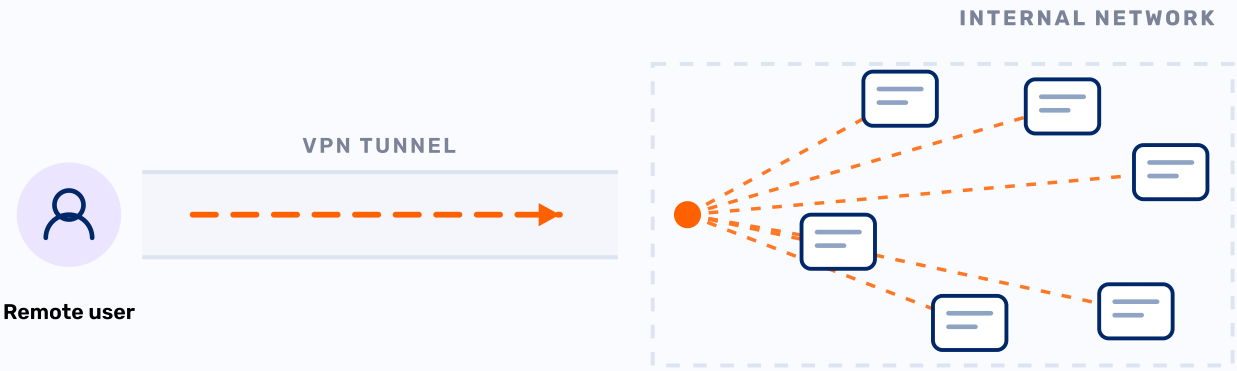
05 EFFORT

Operational complexity

Operational complexity compounded all of it. Maintaining VPN appliances, endpoint agents, and on-premise gateways consumed time and resources, making it difficult for small teams to scale securely. What they needed was a single unified platform that could centralise these challenges rather than multiply them.

WHAT THAT LOOKS LIKE

One VPN login, the whole network in reach



Authentication puts the user **on the network** — every internal system becomes reachable, whether the role needs it or not.

03

THE SHIFT

Before and After

BEFORE

Network-centric access

- VPN places users on the internal network
- Controls differ by user location
- Separate VPNs, agents and gateways
- Fragmented visibility across tools

AFTER

Zero Trust access

- Access granted per application, not per network
- The same controls wherever users work
- One cloud-delivered SSE platform
- Central visibility of users, apps and access

Unrestricted Access

Broad internal network access once VPN-authenticated

Inconsistent Security

Different controls depending on user location

Operational Complexity

VPNs, agents and gateways maintained separately

Limited Visibility

No single source of truth for user, SaaS and AI activity

04

THE WORK

Solution Design and Deployment

Northbridge led the architecture design and technical deployment of Netskope's Zero Trust framework. The design focused on three principles:

1

Access at the application level, not the network level

2

Continuous identity verification

3

Consistent security regardless of user location

Rather than exposing internal networks, private applications were published securely through lightweight connectors deployed in cloud environments. Users authenticated through their existing identity platforms, and access was granted only to the applications they were authorised to use.

NORTHBRIDGE MANAGED

- ✓ Solution architecture and design
- ✓ Identity integration and configuration
- ✓ Structured migration from VPN environments
- ✓ Policy translation from legacy platforms
- ✓ Deployment of secure application connectors
- ✓ Discovery and policy control for generative AI applications

A pilot deployment validated the approach before wider rollout, with legacy systems permitted to run in parallel during transition to minimise user disruption.

The platform also delivered consistent web and cloud security controls, ensuring all traffic was inspected and logged regardless of user location.

Because all traffic was inspected inline, the same controls surfaced generative AI activity, allowing AI applications to be identified, categorised and governed rather than left unmonitored. This unified approach simplified management while significantly reducing risk.

05

HOW WE DELIVER

Implementation Approach

A structured, four-stage transition — validated in a pilot before it touched a wider audience.

01 PLAN

Northbridge worked closely with the service provider and customer IT teams to plan and execute the transition to Zero Trust. During planning, application dependencies, user roles, and access requirements were documented, and a least-privilege access model was defined.

02 INTEGRATE

Integrations with existing identity platforms were established to enable Single Sign-On and multi-factor authentication. Lightweight connector services were deployed in cloud environments to securely broker access to private applications without exposing internal networks.

03 PILOT

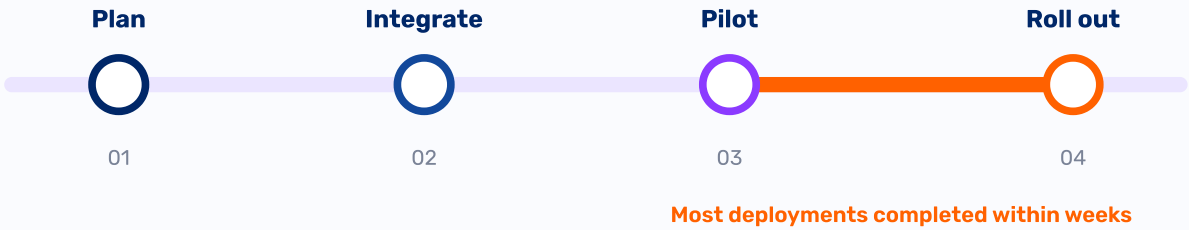
A pilot deployment was completed first to validate the approach in a live environment, with legacy solutions running in parallel during migration to minimise disruption. Following the successful pilot, the solution was rolled out to additional customers in a phased manner.

04 ROLL OUT

Most deployments were completed within weeks, even where legacy VPN and web security platforms were being replaced. Careful planning and structured cutover processes ensured minimal impact to end users.

ROLLOUT

Pilot first, then phased across the portfolio



Legacy runs in parallel

Old platforms stay live through cutover

Minimal user impact

Structured cutover, phased by customer

06

ONGOING

Operational Handover and Support

Documented and handed over

Following deployment, Northbridge produced detailed as-built documentation for each customer, capturing access policies, security configurations, and operational procedures. Knowledge transfer sessions ensured the service provider and customer IT teams were comfortable operating in the new environment.

Run as a managed service

Ongoing support is delivered as a fully managed service. Northbridge operates the platform end-to-end monitoring, policy administration, change management, and escalation acting as the single point of accountability for the service provider and its customers. This removed the operational burden from lean IT teams and ensured consistent service delivery across the entire portfolio.

What Northbridge operates day to day

- **Monitoring**
- **Policy administration**
- **Change management**
- **Escalation**

A single point of accountability for the service provider and every customer in the portfolio.

07

THE RESULT

Security and Business Outcomes

VPNs fully removed

The transition to Zero Trust significantly strengthened security across all customers. VPNs were fully removed, internal networks were no longer exposed, and applications became accessible only through identity-verified access.

Consistent policy everywhere

Security policies became consistent across all locations. Whether users were in the office or remote, traffic was inspected, logged, and governed by the same controls eliminating enforcement gaps and improving overall visibility.

Reduced attack surface

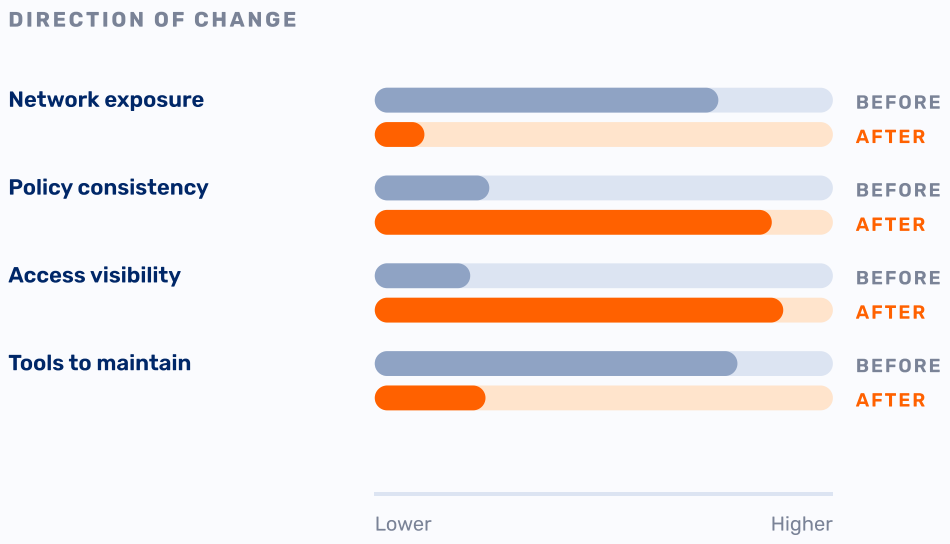
Customers reduced their attack surface by decommissioning VPN infrastructure and removing public-facing firewall rules. End users benefited from a smoother experience, with seamless access to applications and improved performance.

Centralised visibility

IT teams gained centralised visibility into user activity, cloud application usage, and access events. This improved monitoring, simplified audits, and surfaced previously unknown SaaS usage.

THE POSTURE SHIFT

Where the portfolio moved



Indicative direction of change across the portfolio, not measured figures.

08

THE AI GAP

Visibility and Control over AI

AI usage became visible for the first time.

The platform identified which generative AI applications were in use across each organisation, how widely they were being used, and what data was being submitted to them. Rather than blocking AI outright, customers were able to steer staff toward sanctioned tools, apply data protection controls to unsanctioned ones, and give leadership an evidence-based view of AI use across the business.

Discover

Which AI applications are in use, and how widely across the organisation.

Attribute

Who is using them, through managed accounts or personal ones.

Protect

What data is being submitted, with controls applied to unsanctioned tools.

Steer

Staff guided toward sanctioned tools rather than blocked outright.

FROM BLIND SPOT TO GOVERNED

AI activity moved inside the inspected path

BEFORE

Outside the inspected path

Personal accounts, unmanaged browsers

No record of what was submitted

AFTER

Identified, categorised, governed

Inline inspection of every AI request

Data protection on unsanctioned tools

09

IN CLOSING

Conclusion

1. Working alongside a national technology services provider, Northbridge transitioned multiple mid-market customers from legacy, network-based security models to a modern Zero Trust architecture.

2. Northbridge provided the technical leadership to design and deploy a secure, scalable solution, and continues to operate it as a fully managed service built for service providers and growing businesses.

The result was stronger security, reduced risk, improved visibility across cloud and AI usage, and a simplified operating model aligned to the realities of small and mid-sized organisations — Zero Trust adopted in a way that is sustainable, effective, and grounded in real-world business needs

Stronger security

Identity-verified access to every application

Lower risk

No exposed networks, no public firewall rules

Simpler to run

One platform, operated by Northbridge

NORTHBRIDGE
CYBER RESILIENCE BY DESIGN

CYBER RESILIENCE BY DESIGN

Zero Trust, built for your business.

Talk to Northbridge about a secure access model that scales with you — designed, deployed and fully managed.

TALK TO US

YOUR CONTACT

Andrew Thomas

Sales Executive — Cyber Security

athomas@north-bridge.com.au