FIFTEEN

NORTHBRIDGE
CYBER RESILIENCE BY DESIGN

Every customer.
One security service.

How a national technology services provider moved its retail base off VPN with Northbridge Managed SSE

01 Executive Summary

A national technology services provider supports a portfolio of mid-market retail customers — typically 100 to 250 staff, heavily reliant on cloud platforms, remote access and SaaS applications.

Its customers were running on traditional VPNs, on-premise web gateways or early cloud security tools. Once a user connected, they were often granted broad network access, and policy varied depending on where they were working. At the same time, staff had adopted generative AI tools as part of everyday work, outside any inspected path — so nobody could see which tools were in use, by whom, or what business information was going into them.

The partner's problem was scale as much as security. Every customer needed the same shift to Zero Trust, but treating each one as a bespoke project was not something a lean bench could sustain.

Working with Fifteen, the partner brought Northbridge Managed SSE to its retail customers. Northbridge designed the Zero Trust architecture, deployed it, and now operates it 24/7 as a managed service from its Security Management Centre (SMC). Fifteen packaged the service for the partner, supported the commercial model and enabled the partner's team to sell and onboard it. Throughout, the partner remained the customer's single point of contact.

The result for the partner: one standardised Zero Trust offer, sold and deployed repeatably across multiple customers, with delivery and operations carried by Northbridge. For the partner's customers: application-level Zero Trust Network Access, unified web and cloud security, consistent policy in every location, and — for the first time — visibility and control over generative AI use. Reliance on the VPN-and-firewall setup fell away, and where customers chose to, VPN infrastructure was decommissioned entirely.

A Zero Trust offer the partner can take to every customer — sold once, deployed in weeks, operated by Northbridge.

BEFORE

Network-centric access

- VPN appliances for remote access
- On-premise web gateways
- Endpoint agents and firewalls
- Policy varies by user location

AFTER

Northbridge Managed SSE (Security Service Edge)

- Zero Trust Network Access per application
- Unified web and cloud security
- Identity-verified, least-privilege access
- Consistent policy in every location

02 Customer Environment

The partner's customers were mid-sized retailers with lean IT teams and limited in-house security expertise. Most had already embraced Microsoft 365, SaaS business applications and hosted internal systems, but their security architecture remained network-centric.

Remote staff reached systems through VPN appliances, while internet security was enforced through a mix of endpoint agents, firewalls and legacy web gateways. These tools operated independently, producing fragmented enforcement and limited visibility — and the effort of maintaining them fell on small IT teams, and on the partner supporting them.

Common characteristics included:

- **Retail**
- **100–250 employees**
- **Hybrid workforces**
- **Cloud identity platforms already in place**
- **Limited internal security resources**
- **Strong reliance on the partner for security**

Customers wanted strong security without enterprise-level complexity: cloud-first, easy to deploy, centrally managed, cost-effective and able to scale as the business grew. The partner wanted the same thing one level up — a service it could deploy the same way at every customer.

- **Easy to deploy**
- **Centrally managed**
- **Cost-effective**
- **Scales as the business grows**

03 The Security Challenge

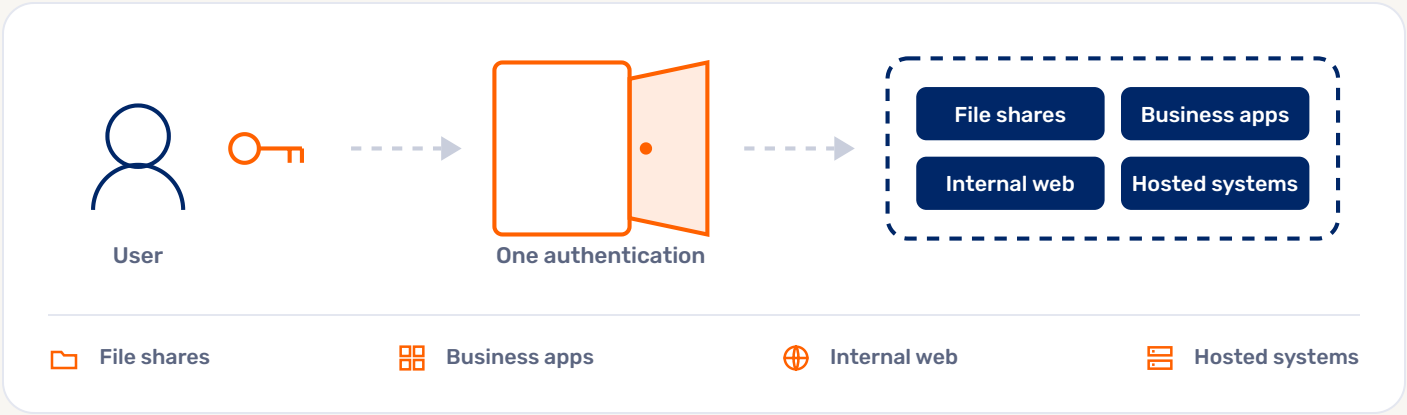
Overexposed network access. Once authenticated through VPN, users were effectively placed on the internal network, often with access well beyond their role. This magnified the impact of any credential compromise and made least-privilege access hard to enforce.

Inconsistent enforcement. Remote users were subject to different controls from office users, and in some cases traffic bypassed inspection entirely — limiting the ability to monitor activity, enforce acceptable-use policy and detect threats.

Fragmented visibility. Multiple point solutions meant no single source of truth for user activity, cloud application usage or access to internal systems. Shadow IT was hard to identify; audit and compliance were harder to meet.

Generative AI widened the gap. Staff were using AI assistants and AI-enabled SaaS independently of IT, often through personal accounts and unmanaged browsers. IT could not answer basic questions — which AI applications were in use, how widely, or whether company data was being pasted into them. Blocking AI outright was neither practical nor in the interests of the business.

The partner's challenge. Maintaining VPN appliances, endpoint agents and on-premise gateways across a whole portfolio of customers consumed time the partner's team did not have. The partner needed a single, unified service — one it could stand behind, deploy consistently, and hand to Northbridge to operate.



One authentication grants access far beyond the user's role.

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, at every customer

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

04 Solution Design and Deployment

Northbridge led the architecture design and technical deployment of the Zero Trust framework that underpins Northbridge Managed SSE. The design rested on three principles:

01

Access at the application level, not the network level

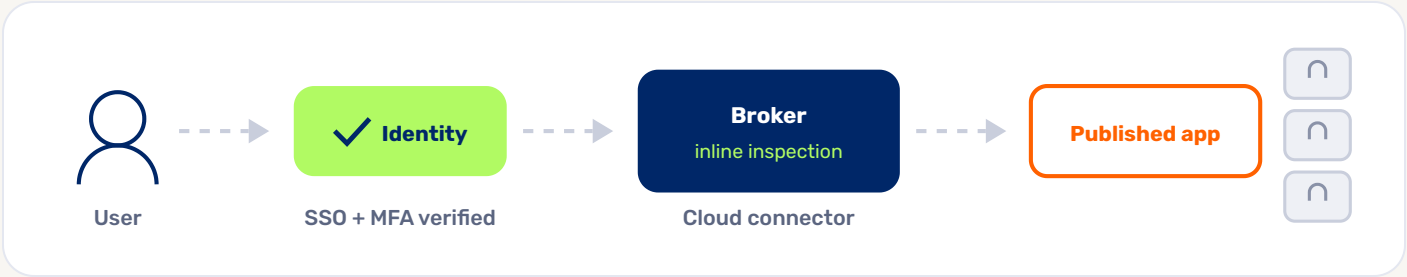
02

Continuous identity verification

03

Consistent security regardless of user location

Rather than exposing internal networks, private applications were published through lightweight connectors deployed in cloud environments. Users authenticated through their existing identity platforms and were granted access only to authorised applications. Because all traffic was inspected inline regardless of location, the same controls surfaced generative AI activity — allowing AI applications to be identified, categorised and governed rather than left unmonitored.



Private applications are published through connectors — the internal network is never exposed.

Northbridge managed:

Solution architecture and design	A least-privilege Zero Trust architecture designed around the customer's applications
Policy translation from legacy platforms	Existing VPN and web gateway rules mapped to application-level policy
Identity integration and configuration	Existing identity platforms wired in for Single Sign-On and multi-factor authentication
Deployment of secure application connectors	Lightweight cloud connectors publishing private applications without network exposure
Structured migration from VPN environments	Phased cutover with legacy platforms running in parallel
Discovery and policy control for generative AI applications	AI tools identified, categorised and governed inline rather than left unmonitored

05 Service Delivery Model

Implementation approach

Northbridge worked with the partner's engineers and each customer's IT team to plan and execute the transition. Application dependencies, user roles and access requirements were documented and a least-privilege model defined; identity platforms were connected for Single Sign-On and multi-factor authentication; connectors were deployed. Most deployments were completed within weeks, even where legacy VPN and web security platforms were being retired, with minimal impact on end users.

01
Plan
Applications, roles and access requirements documented

02
Integrate
Identity platforms connected for SSO and MFA

03
Pilot
Approach validated at one customer before wider rollout

04
Roll out
Phased cutover, legacy platforms in parallel during migration

05
Hand over
As-built documentation and knowledge transfer

Most deployments were completed within weeks.

How the service runs

Ongoing service is delivered through the Fifteen partner model. The partner owns the customer relationship, contract and billing, and is the customer's primary point of contact. Northbridge operates the service 24/7 from the SMC, owns the SLA, and provides escalation and deep technical expertise. Fifteen owns the programme — packaging, deal support, enablement and co-sell — so the partner can take the service to the next customer without rebuilding it.

ROLE

Customer
Day-to-day users and IT

ROLE

Partner (MSP)
Owns the relationship; primary point of contact

ROLE

Northbridge
Operates the service 24/7, owns the SLA, escalation and technical expertise

ROLE

Fifteen
Programme, enablement and commercial model

06 Security and Business Outcomes

For the partner

The partner now has a standard Zero Trust offer for its retail base rather than a series of one-off projects. Each new customer follows the same five-step path, and once live, Northbridge carries operations and escalation — freeing the partner's engineers from maintaining VPNs, agents and gateways customer by customer. The partner remains the trusted face to its customers, with a stronger security story and a recurring service line to show for it.

One repeatable offer
Same service, same path, every customer

Deployed in weeks
Even where legacy VPN and web security were retired

Operations carried by Northbridge
24/7 from the SMC, escalation included

Stronger customer relationship
The partner stays the primary contact

For the customers

Security strengthened across every customer. Applications became accessible only through identity-verified access, and internal networks were no longer exposed. Policy became consistent across locations — traffic inspected, logged and governed by the same controls whether users were in the office or remote. The attack surface shrank as reliance on VPN and public-facing firewall rules fell away; where customers chose to, VPN infrastructure was decommissioned entirely. End users gained seamless access and improved performance.

IT teams gained centralised visibility into user activity, cloud application usage and access events, simplifying audits and surfacing previously unknown SaaS. AI usage became visible for the first time: which generative AI applications were in use, how widely, and what data was being submitted to them. Rather than blocking AI outright, customers steered staff toward sanctioned tools, applied data protection controls to unsanctioned ones, and gave leadership an evidence-based view of AI use across the business.

Reduced reliance on VPN
Internal networks no longer exposed

Consistent policy
Same controls in the office and remotely

Reduced attack surface
Public-facing firewall rules removed

Centralised visibility
Simpler audits, shadow IT and AI use surfaced

07 Conclusion

A national technology services provider set out to move its mid-market retail customers off legacy, network-based security and onto Zero Trust — without turning each customer into a bespoke project. With Northbridge Managed SSE, enabled through Fifteen, it did exactly that.

Northbridge provided the technical leadership to design and deploy the architecture, and operates it as a managed service. Fifteen made it a repeatable, sellable offer for the partner. The partner kept the customer relationship — and delivered stronger security, reduced risk, visibility across cloud and AI usage, and a simpler operating model to every customer it touched.

PARTNER

Owns the customer, leads the conversation, delivers the outcome

NORTHBRIDGE

Technical leadership: design, deployment, 24/7 operation

FIFTEEN

Programme and enablement that make it repeatable

Stronger security	**Reduced risk**	**Improved visibility across cloud and AI usage**	**Simplified operating model**

FIFTEEN

Start the conversation.

If your customers are still relying on VPN and firewall for secure access, this is a conversation worth having.

OFFICE

52 Chandos St, St Leonards, Sydney 2065

Get in touch →