northbound
NETWORKS

The definitive guide to modern Access Control

How Zero Trust, NAC, ZTNA and secure SD-WAN create a unified security fabric for South African enterprises.

Credential misuse accounted for

22%

of global breaches (Verizon DBIR 2025)

The new reality of access control

The way businesses connect has changed. Employees now work from multiple locations, on multiple devices, accessing systems hosted both in the cloud and on-premise.

Traditional network boundaries no longer exist, and passwords alone are not enough to protect sensitive data. In this new reality, access control must go beyond the perimeter. It must verify every user, every device, and every connection, every time.

Modern access control is not only a technical challenge; it is a business requirement tied directly to trust, compliance, and resilience.

For South African organisations operating under the Protection of Personal Information Act (POPIA) and Joint Standard 2 of 2024, the ability to prove who accessed what, and when, is now an essential governance obligation.

This guide explores how Network Access Control (NAC), Zero Trust Network Access (ZTNA), and Secure SD-WAN can work together to deliver a unified, intelligent access-control framework.

Why legacy models fail

Legacy access control is built on a perimeter-based model. It assumes that anyone inside the corporate network is trusted, while anyone outside is not.

This approach no longer reflects how people work or how data flows.
Attackers exploit this gap. Once a single device is compromised, they move laterally across the network without resistance. VPNs, once used to connect remote users securely, often extend that same trust to unmanaged devices, making lateral movement even easier.

THE PERIMETER-BASED MODEL FAILS BECAUSE:

- Users and devices are no longer in fixed locations.
- Applications and data are hosted in multiple clouds.
- Threat actors now use legitimate credentials rather than brute force.
- Traditional VPNs grant broad, network-wide access instead of application-specific access.

The result is that security becomes reactive rather than proactive.

To protect today's distributed networks, organisations must transition to a Zero Trust approach — one that assumes no connection is safe until verified.

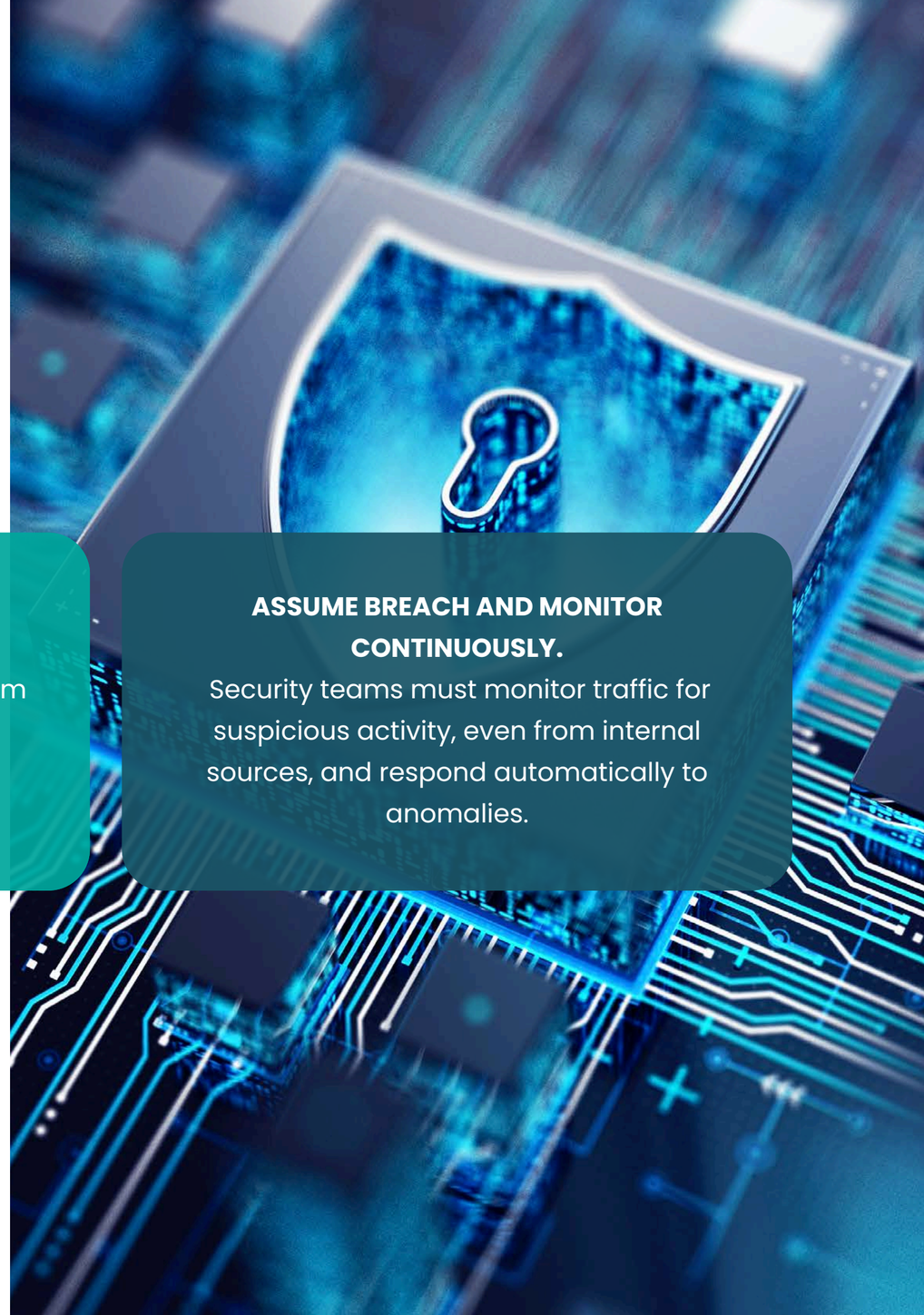
Principles of Zero Trust

Zero Trust is not a product or feature. It is a security philosophy built on three key principles:

NEVER TRUST, ALWAYS VERIFY.
Every user, device, and connection must be authenticated and authorised before access is granted.

ENFORCE LEAST PRIVILEGE.
Access should be limited to the minimum resources required for a task.

ASSUME BREACH AND MONITOR CONTINUOUSLY.
Security teams must monitor traffic for suspicious activity, even from internal sources, and respond automatically to anomalies.



By applying these principles consistently across all environments — from the office to the cloud — organisations can reduce the impact of breaches, improve compliance, and gain full visibility into user behaviour.

Compliance and governance in South Africa

Access control is not only a security measure — it is a legal and governance requirement. Both POPIA and Joint Standard 2 of 2024 emphasise the need for organisations to maintain complete oversight of data access and protection.

Regulation	Key Requirement	Supported By
POPIA	Prevent unauthorised access to personal information	NAC and ZTNA
Cybercrimes Act 19 of 2020	Prevent negligent exposure and unauthorised access	Unified access control
Joint Standard 2 of 2024	Continuous monitoring and incident reporting	NAC, ZTNA, and Secure SD-WAN
ISO 27001 / NIST CSF	Identity and access management	Unified model

Unified access control simplifies compliance reporting by generating audit-ready logs and maintaining continuous visibility across all systems.

Implementation roadmap

01

Assess current access landscape

We begin with an in-depth consultation to understand your business requirements, current systems, and workforce challenges.

02

Deploy NAC for visibility and control

Establish a device inventory and begin enforcing posture checks.

03

Integrate identity providers & define policies

Centralise user authentication and align policies with business roles.

04

Replace broad VPN access with ZTNA

Connect users directly to applications using least-privilege principles.

05

Secure the network fabric with SD-WAN

Unify remote connectivity under consistent policy enforcement.

06

Monitor and improve continuously

Feed telemetry into your SOC or MDR platform for ongoing optimisation and threat detection.

Business and technical benefits

Business Outcome	Description
Reduced risk	Devices and users verified before access is granted
Simplified compliance	Unified reporting and audit logs for POPIA and financial regulations
Improved user experience	Seamless, secure access across hybrid environments
Operational efficiency	Automated enforcement reduces manual workload
Scalability	Supports hybrid and remote work models
Lower total cost of ownership	Fewer overlapping tools and reduced complexity

By applying these principles consistently across all environments — from the office to the cloud — organisations can reduce the impact of breaches, improve compliance, and gain full visibility into user behaviour.

CASE STUDY
South African financial services firm

CHALLENGE:
A mid-sized financial services provider struggled with limited visibility over remote connections. VPN credentials were being shared between employees and contractors, and compliance audits revealed gaps in access logging.

SOLUTION:
Northbound Networks deployed a combined NAC and ZTNA solution. All devices were registered and profiled through NAC, while ZTNA replaced VPN access with application-specific authentication. Secure SD-WAN provided consistent policy enforcement between branches.

RESULTS:
- 90 percent reduction in unauthorised access attempts
- Improved compliance reporting for POPIA and Joint Standard 2
- Enhanced user experience with faster, more stable remote access

“The shift to NAC and ZTNA transformed our visibility. We now know exactly who is connecting, from where, and to which system — all in real time.”

Access control without borders

Passwords alone can no longer protect the modern enterprise.

As networks expand and threats evolve, organisations need a unified model that continuously verifies identity, enforces policy, and adapts to context.

By integrating NAC, ZTNA, and Secure SD-WAN into a single access-control fabric, businesses can protect users, applications, and data wherever they reside.

northbound
NETWORKS

Request your free Endpoint Security Health Check today!

Phone Number
087 743 2626

Email Address
sales@northbound.co.za

Website
www.northbound.co.za