

CHAPTER 8

Identity and Zero Trust

Identity as the New Perimeter

“Trust is a vulnerability. In a modern enterprise, we do not grant access based on where you are, but based on who you are and the context of your request.”

The previous chapter built the foundation. This chapter decides who is allowed to stand on it.

EXECUTIVE SUMMARY

The traditional security perimeter no longer exists.

Employees work from multiple locations, applications run across cloud environments, and organisations collaborate with partners and suppliers around the world.

For Nordic Ventures Group, operating across fourteen countries with 6,000 users, 180 applications, and five manufacturing facilities, security can no longer depend on network boundaries.

Identity becomes the new perimeter.

This chapter shows how Zero Trust and Microsoft Entra ID replace that vanished perimeter with something more durable: a security foundation built on identity, not geography.

- international expansion,
- mergers and acquisitions,
- AI innovation,
- business resilience,
- and regulatory compliance.

The principle is simple:

Never trust. Always verify.

Why Identity Matters

Many successful cyberattacks begin with compromised identities rather than direct network intrusion.

Traditional security models assume that once users are inside the corporate network, they can be trusted.

Zero Trust rejects this assumption.

Every request must be continuously verified based on:

- identity,
- device health,
- location,
- risk signals,
- application sensitivity,
- and user behaviour.

The Nordic Ventures Group Challenge

Current State	Future State
Multiple identity silos	Unified identity platform
Network-based trust	Identity-based trust
Manual access reviews	Automated governance
Fragmented security policies	Centralised Conditional Access
High administrative overhead	Automated lifecycle management
Increased cyber risk	Zero Trust architecture

The Three Principles of Zero Trust

Based on NIST SP 800-207

1. Verify Explicitly

Every access request is evaluated continuously.

Verification considers:

- User identity

- Device health
- Location
- Application sensitivity
- User risk
- Session risk

In practice, this means that an employee accessing SAP from a factory in Germany is evaluated differently than a privileged administrator accessing production data remotely.

Business Value

- Reduced identity attacks
- Improved visibility
- Better regulatory compliance
- Lower operational risk

TRUSTED ADVISOR INSIGHT *Inexperienced architects treat Conditional Access as a checkbox exercise. Experienced ones treat every policy as a business decision about acceptable risk.*

2. Use Least Privilege Access

Users receive only the permissions required to perform their jobs.

This is implemented through:

- Role-Based Access Control (RBAC)
- Just-in-Time Access (JIT)
- Privileged Identity Management (PIM)
- Just-Enough Administration (JEA)
- Separation of Duties

Business Value

- Reduced attack surface
- Lower insider risk
- Improved auditability
- Better compliance posture

TRUSTED ADVISOR INSIGHT *The organisations that recover fastest are rarely the ones with the most controls. They are the ones that rehearsed the failure before it happened.*

3. Assume Breach

Modern organisations must assume that compromise will occur.

The objective becomes:

Contain the blast radius.

In practice, this means:

- Network segmentation
- Hub-and-Spoke architecture
- Encryption everywhere
- Continuous monitoring
- Rapid isolation capabilities

Business Value

- Faster incident response
- Reduced business disruption
- Improved cyber resilience
- Better factory uptime

Microsoft Entra ID

The Identity Platform Behind the Transformation

Microsoft Entra ID becomes the central trust platform for:

- 6,000 employees
- External partners
- Suppliers
- Acquired companies
- Developers
- Service accounts

Core Capabilities

Capability	Business Outcome
Single Sign-On	Better user experience
Multi-Factor Authentication	Reduced credential attacks
Conditional Access	Risk-based protection
Identity Governance	Automated lifecycle management
Privileged Identity Management	Controlled administrative access
B2B Collaboration	Faster acquisitions and partnerships
Access Reviews	Improved compliance

Conditional Access

The Intelligent Gatekeeper

Conditional Access evaluates:

User Signals

- Identity risk
- Group membership
- Role

Device Signals

- Compliance state
- Device health

Location Signals

- Country
- IP reputation
- Named locations

Application Signals

- Application sensitivity
- Session controls

Example Policy

Scenario	Action
Access from trusted corporate device	Allow
Access from unmanaged device	Require MFA
High-risk sign-in	Block
Access from risky country	Block
Privileged access request	Require MFA and approval

Identity Governance

Automating Compliance

For organisations operating across fourteen countries, manual access management is unsustainable.

Identity Governance automates:

- Joiners
- Movers
- Leavers
- Access reviews
- Entitlement management
- Separation of duties

Business Value

- Reduced administrative effort
- Faster onboarding
- Better GDPR compliance
- Reduced security risk

TRUSTED ADVISOR INSIGHT *Boards do not fund Zero Trust because it is best practice. They fund it because the Trusted Advisor translates it into acquisition speed and audit outcomes.*

Zero Trust and Business Value

Security is not merely protection.

Security becomes an enabler of growth.

Faster Mergers and Acquisitions

Identity-first integration allows newly acquired companies to gain secure access within days instead of months.

Reduced Complexity

A centralised identity platform replaces fragmented security solutions and lowers operational costs.

Innovation Without Risk

Development teams can experiment with AI services while access remains governed through identity policies.

The Nordic Ventures Group Security Model

Business Objective	Identity Capability
International expansion	B2B collaboration
Regulatory compliance	Identity Governance
Factory resilience	Conditional Access
Cyber resilience	Zero Trust
M&A acceleration	External identities
Cost reduction	Centralised identity services

NVG Zero Trust Maturity Model

Level	Characteristics
Level 1	MFA enabled
Level 2	Conditional Access
Level 3	Device compliance

Level	Characteristics
Level 4	Identity Governance
Level 5	Continuous risk evaluation
Level 6	Fully integrated Zero Trust platform

The Nordic Ventures Group Lesson

The organisations that win in the digital era will not be those with the strongest networks.

They will be those with the strongest identity foundations.

Identity becomes:

- the control plane,
- the trust plane,
- and the business enablement plane.

Key Takeaways

Principle	What It Means
Identity is the new perimeter.	Trust identities, not networks.
Zero Trust is a business strategy.	Security enables growth.
Automate governance.	Manual security does not scale.
Least privilege reduces risk.	Access should always be temporary and justified.
Assume breach.	Design systems to contain compromise.
Identity accelerates business.	Security should make the organisation faster, not slower.

Reflection Questions

Could your organisation operate securely without a traditional network perimeter?

Which privileged accounts represent your greatest risk today?

How long does it take to onboard a new employee or acquisition?

Are your compliance processes automated or manual?

If an identity were compromised today, how large would your blast radius be?

References

NIST Special Publication 800-207. Zero Trust Architecture.

Microsoft Security. Zero Trust Adoption Framework.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). NIST SP 800-207: Zero Trust Architecture.

Microsoft. Microsoft Entra Architecture Guidance.

Microsoft. Identity and Access Management Design Area.

European Union. NIS2 Directive.

European Union. General Data Protection Regulation (GDPR).

Microsoft. Cybersecurity Reference Architecture.

TRUSTED ADVISOR PRINCIPLE

Trust is not a location.

It is a decision, verified continuously.

Every identity is a perimeter.

Every access request is an audition.

Zero Trust does not mean zero access — it means
zero assumptions.

The Trusted Advisor secures identity before
securing infrastructure, because infrastructure
without identity has nothing left to protect.

Now that identity is governed, one question
inevitably follows: how does data move safely
between everything we have just secured?