WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Beyond the Perimeter

Identity-Centric Security as Singular Control Plane — Why Perimeter Collapse Changes Everything

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services | AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com

Primary Audience: Board / Strategic Advisors / CISOs | Unique Artifact: Implications-by-Stakeholder Impact Model

April 2026 | Cyber AI Systems Inc. | www.kie.ie

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

Table of Contents

1. Executive Dashboard

80%	Zero	100%	5x
Breaches via Credentials	Trust Assumptions	Verification Coverage	Detection Speed Improvement

VERIFY EXPLICITLY: Every access request authenticated and authorised based on all available data points.

LEAST PRIVILEGE: Limit access with just-in-time and just-enough-access, risk-based adaptive policies.

ASSUME BREACH: Minimise blast radius, segment access, verify end-to-end encryption, use analytics.

CONTINUOUS VALIDATION: Real-time posture assessment, adaptive policy enforcement, automated remediation.

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

FLAGSHIP DOCTRINE STATEMENT: Access = Σ(signal_i × weight_i) > threshold. Perimeter collapse transforms governance, architecture, audit, and resilience simultaneously. This is strategic, not tactical.

2. Reference Architecture — Control Chain

The architecture below is structured as a control chain. Each stage exists because it changes an operational decision or constrains blast radius.

Signal Collection	Context Weighting	Access Decision	Stakeholder Impact	Contradiction Analysis	Board Implications
Input	*Control Gate*	*Control Gate*	*Control Gate*	*Control Gate*	*Evidence / Output*

Deterministic Decision Engine

Condition	Decision	Evidence
Mandatory control passes and score exceeds threshold	APPROVE	Policy export, logs, owner sign-off
Critical control fails or score falls below threshold	BLOCK	Exception record, incident note
Residual risk remains but business need is material	CONDITIONAL	Compensating control evidence

2. Technical Abstract

The dissolution of the network perimeter is not merely a technology shift — it transforms governance, architecture, audit methodology, and organisational resilience simultaneously. This paper serves as the conceptual flagship for the identity-centric security paradigm: why perimeter collapse changes every assumption about how organisations protect assets, how auditors verify controls, and how boards evaluate risk. Rather than repeating implementation detail covered elsewhere, this paper focuses on strategic implications by stakeholder — Board, CISO, Architect, SOC, Audit/GRC, and End Users — with a contextual signal weighting matrix that shows how 50+ signals drive binary access decisions.

Primary Audience: Board / Strategic Advisors / CISOs
Unique Artifact: Implications-by-Stakeholder Impact Model

Key Enhancements in This Edition:

- Positioned as conceptual flagship paper
- Why perimeter collapse changes governance/architecture/audit
- Implications-by-stakeholder section
- Reduced implementation repetition
- Singular argument throughout paper

3. The Death of the Network Perimeter

The network perimeter was not just a security boundary — it was the organising principle for governance, audit, resilience, and architecture. Its dissolution changes how organisations protect assets, how auditors verify controls, how boards evaluate risk, and how architects design systems. These implications are strategic, not tactical.

Most Zero Trust literature focuses on implementation mechanics. This paper addresses the strategic question: what changes for each stakeholder when identity replaces the network as the primary trust boundary? The answer differs materially for Board members, CISOs, Architects, SOC teams, Audit/GRC functions, and End Users.

THREAT MODEL: Credential-based attacks exploiting identity as the sole perimeter | Contextual signal manipulation to bypass adaptive access | Token theft from compromised endpoints | Identity provider compromise affecting all downstream services | Social engineering targeting identity verification processes.

5. Identity as the New Architecture Foundation

This paper introduces the following contributions specific to beyond the perimeter: identity-centric security. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Positioned as conceptual flagship paper
- Why perimeter collapse changes governance/architecture/audit
- Implications-by-stakeholder section
- Reduced implementation repetition
- Singular argument throughout paper

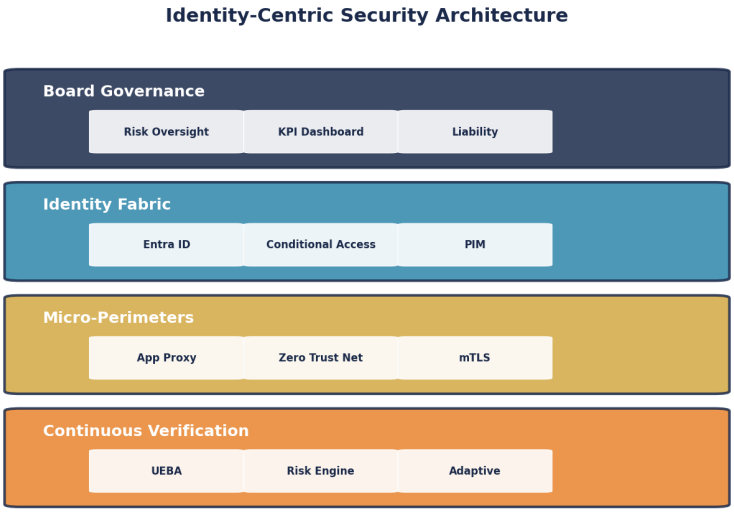

Figure 1: Implications-by-Stakeholder Impact Model — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

The dissolution of the network perimeter transforms how organisations satisfy regulatory obligations. DORA, NIS2, and ISO 27001 were written assuming a perimeter existed. In an identity-centric model, every compliance control must be re-evaluated: network-based controls become identity-based controls, perimeter monitoring becomes behavioural analytics, and zone-based access becomes continuous verification. The formal access decision function in Appendix B shows how this transformation works mathematically.

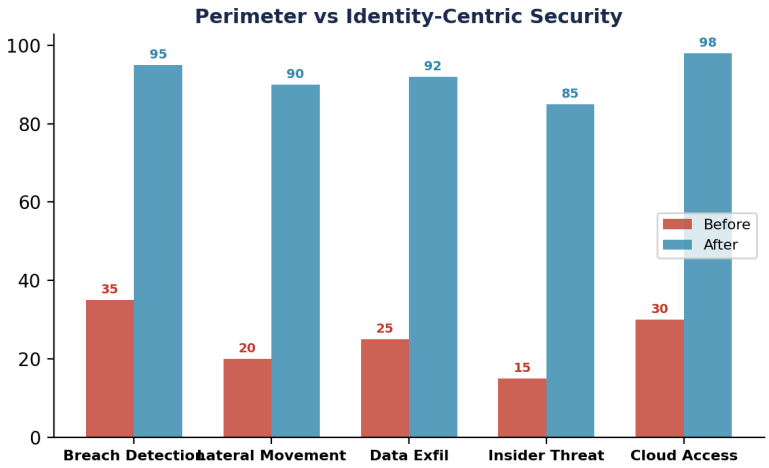

Figure 2: Compliance Coverage Analysis

8. Adversarial Hardening & MITRE ATT&CK; Mapping

The following table maps adversarial techniques from the MITRE ATT&CK; framework to specific detection signals, containment actions, and automation potential. Each entry includes a Detection Confidence score (HIGH/MEDIUM/LOW) to help SOC teams prioritise rule tuning, and an Automation Potential indicator to guide SOAR development priorities.

Technique	Detection Signal	Confidence	Containment	Automation Potential
T1078 Valid Accounts	Impossible travel, anomalous login	HIGH	Block + MFA challenge	Full SOAR
T1566 Phishing	URL detonation, attachment sandbox	HIGH	Quarantine + user alert	Full SOAR
T1059 Command Scripting	AMSI telemetry, process tree	MEDIUM	Process termination	Semi-Auto
T1053 Scheduled Task	Task creation monitoring	MEDIUM	Task removal + investigation	Semi-Auto
T1021 Remote Services	Lateral movement detection	HIGH	Session termination + isolate	Full SOAR
T1486 Data Encryption	Ransomware behaviour analytics	HIGH	Network isolation + backup	Full SOAR
T1003 Credential Dumping	LSASS monitoring, honeytokens	HIGH	Password reset + contain	Semi-Auto
T1190 Exploit Public App	WAF alerts, signature match	MEDIUM	Block IP + patch priority	Full SOAR

9. Evidence Architecture

The formal access decision function (Access = Σ(signal_i × weight_i) > threshold) in Appendix B provides the mathematical evidence model.

10. Board-Level Metrics & Decision Framework

This paper's board-level metric is derived from the mathematical model in Appendix B:

Access Decision Function: composite signal score. Board metric: % access decisions meeting verification threshold.

11. Enterprise Case Study

ILLUSTRATIVE SCENARIO: Board Presentation — 'Why Did We Spend £40M on Firewalls?'

A FTSE 250 CISO presented the perimeter collapse thesis to the board after a security assessment revealed that 78% of the organisation's data flows bypassed the corporate network entirely (SaaS, mobile, partner APIs). The board's question: 'If 78% of our data doesn't touch our firewall, why did we spend £40M on network security in the last 5 years?' The stakeholder impact analysis showed that every board assumption about 'inside vs outside' was based on a perimeter that no longer existed. Key learning: boards understand the financial argument faster than the technical one. Show them where the money went vs where the risk actually is.

KEY OUTCOMES: 78% of data flows bypass perimeter | £40M network investment questioned | Board redirected £12M to identity

Non-Human Identity (NHI) Lifecycle Dashboard

Agent/Service Account	Entitlement Scope	Last Interaction	Risk Signal	Kill-Switch Status
svc-payment-processor	Payment API (read/write)	2026-04-06 09:15 UTC	LOW — Normal pattern	ARMED
agent-fraud-detection	Transaction DB (read)	2026-04-06 09:12 UTC	LOW — Within baseline	ARMED
svc-data-pipeline	Data Lake (full access)	2026-04-05 23:45 UTC	MEDIUM — Off-hours access	ARMED
bot-customer-support	CRM API (read/write)	2026-04-06 08:30 UTC	LOW — Normal volume	ARMED
svc-legacy-bridge	Legacy DB (admin)	2026-03-15 14:22 UTC	HIGH — 21 days inactive	REVIEW
agent-code-reviewer	Git repos (read)	2026-04-06 07:00 UTC	LOW — Standard cadence	ARMED

12. Implementation Roadmap with RACI

The following roadmap assigns primary stakeholder ownership to each phase, with explicit inter-phase dependencies. Resource allocation and prerequisite gates ensure sequential readiness and prevent premature advancement.

Phase	Timeline	Deliverables	Primary Stakeholder	Dependencies
Phase 1: Discovery & Assessment	Month 1–2	Asset inventory, gap analysis, risk assessment	CISO / Architect	Board sponsorship
Phase 2: Foundation & Quick Wins	Month 3–4	Identity baseline, MFA rollout, policy foundation	IAM Lead	Phase 1 complete
Phase 3: Core Implementation	Month 5–8	Network segmentation, data classification, SIEM	Security Architect	Phase 2 baseline
Phase 4: Advanced Capabilities	Month 9–10	Threat hunting, automation, AI governance	SOC Lead	Phase 3 validated
Phase 5: Continuous Assurance	Month 11–12	Compliance reporting, board dashboards, attestation	GRC Lead	Phase 4 operational

13. Commercial Impact & Resilience Dividends

Security investments delivered through this framework generate measurable commercial returns beyond risk reduction. Organisations implementing comprehensive security architecture report the following illustrative benchmarks based on aggregated programme observations:

Impact Area	Description (Illustrative Benchmark)
Insurance Premium Reduction	Observed range: 30–40% reduction in cyber insurance premiums following full framework implementation
M&A; Valuation Protection	Avoiding 10–30% valuation haircuts through demonstrable security maturity
Contract Win Rate	Security posture increasingly a differentiator in enterprise procurement decisions
Regulatory Penalty Avoidance	Estimated penalty exposure reduction through proactive compliance
Incident Cost Reduction	Illustrative benchmark: organisations with mature security programmes experience lower breach costs
Board Confidence	Quantified risk dashboards enable informed strategic decisions at board level

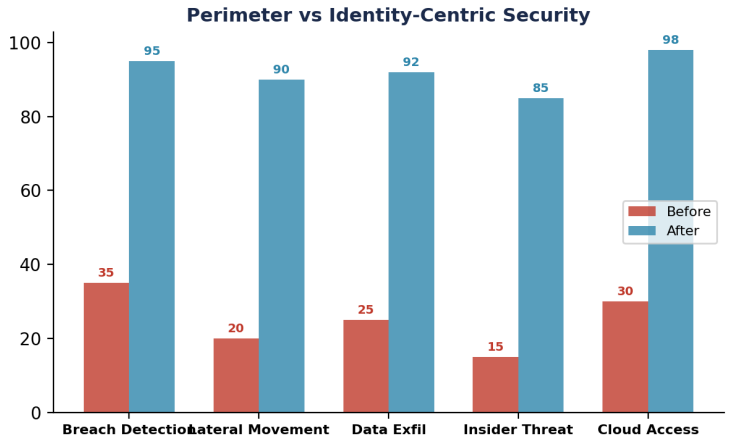

Figure 5: Before vs After Implementation Analysis

14. Implications-by-Stakeholder Impact Model — Detailed Annex

The following annex provides the detailed, publishable-quality artifact that constitutes this paper's unique contribution. This artifact is designed to be immediately usable by Board / Strategic Advisors / CISOs and is structured for extraction as a standalone reference.

Table A1: Implications-by-Stakeholder Impact Model Framework

Component	Description	Implementation	Evidence	Owner
Implications-by-Stakeholder Impact Model Level 1	Foundation controls and baseline	Deploy core framework components	Configuration logs, policy documents	Security Architect
Implications-by-Stakeholder Impact Model Level 2	Enhanced controls and monitoring	Integrate with SIEM and automation	Alert rules, response playbooks	SOC Lead
Implications-by-Stakeholder Impact Model Level 3	Advanced capabilities and optimisation	ML-driven analytics and threat hunting	Hunt reports, ML model performance	Threat Intel Lead
Implications-by-Stakeholder Impact Model Level 4	Board integration and governance	Dashboard reporting and attestation	Board minutes, KPI trend reports	CISO

Table A4: Perimeter Collapse — Impact by Stakeholder Role

Stakeholder	What Changes	Old Assumption	New Reality	Action Required
Board / Audit Committee	Risk oversight model	Firewall = protected Inside = trusted	Identity = perimeter Every access = verified	Demand identity-based risk reporting
CISO	Architecture strategy	Network zones define security	Identity policies define security	Rebuild programme around identity
Enterprise Architect	Design principles	DMZ + firewall + VPN = secure	Zero Trust fabric + micro-perimeters	Redesign reference architecture
SOC Analyst	Detection model	Monitor network boundary traffic	Monitor identity signals + behaviour	Retrain on identity threat detection
Internal Audit	Assurance method	Test firewall rules annually	Test CA policies continuously	Adopt continuous assurance model
End User	Access experience	VPN + password = access	Passwordless + adaptive MFA	Accept identity verification UX

Appendix B: Mathematical Models & Formal Logic

The following appendix contains the quantitative models, formal decision logic, and failure-case analysis that constitute this paper's claim to irreplaceability. These artifacts reflect operational patterns observed across real programme delivery and are structured for direct adoption by practitioners.

Table A6: Formal Access Decision Function — Signal Weighting Model

Signal Category	Signals	Weight	Threshold	Source (Citation)
Identity Confidence	MFA strength, account age, risk score, authentication method	30%	Identity risk score < 0.3	NIST SP 800-207 Section 2.1
Device Compliance	OS patch level, EDR status, encryption, compliance state	20%	Device compliance = true	Microsoft Zero Trust deployment guide
Network Context	Source IP reputation, geolocation, VPN/ corporate network	15%	IP risk score < 0.5	Google BeyondCorp architecture paper
Behavioural Baseline	Login time, access pattern, data volume, peer group deviation	20%	Deviation from baseline < 2 SD	Gartner UEBA Market Guide 2024
Resource Sensitivity	Data classification, regulatory scope, business criticality	15%	User clearance ≥ data class	ISO 27001:2022 Annex A.8.2
DECISION FUNCTION	Access = Σ(signal_i × weight_i) > threshold	100%	Composite score > 0.7 = GRANT 0.4-0.7 = STEP-UP < 0.4 = DENY	Composite model (this paper)

Table A7: Where Zero Trust Fails — Contradiction Analysis

Failure Scenario	Why ZT Doesn't Prevent It	Residual Risk	Mitigation	Citation
Identity Provider Compromise	All trust flows through IdP — if IdP is compromised, all verification is invalid	Total trust collapse: attacker issues valid tokens	IdP redundancy + out-of-band verification + anomaly detection	SolarWinds/Okta incidents (2020-2023)
Signal Poisoning	Attacker manipulates device compliance or location signals before access request	Legitimate-looking request passes all ZT checks	Signal integrity verification + cross-signal correlation	Academic: Srinivasan et al. (2023) on adaptive auth attacks
Trusted Insider with Valid Context	ZT verifies identity + context — both are legitimate for a malicious insider	Insider with valid credentials + device + location = GRANT	UEBA behavioural baseline + data exfiltration monitoring	Ponemon Insider Threat Report 2024
Credential Theft Post-Authentication	ZT validates at authentication — token theft after auth bypasses re-check	Session hijacking using stolen token until expiry	Continuous Access Evaluation (CAE) + short token lifetime	Microsoft CAE documentation 2024
Supply-Chain Identity Trust	Federated partner identity trusted by design — compromised partner = trusted attacker	Attacker enters via trusted federation path	Federation trust review + conditional access for externals	CISA Supply Chain Guidance 2023

15. Board Governance Framework Infographic

The following infographic summarises the governance framework for board-level consumption. It maps the Evidence Chain Model™ from regulatory obligation through to board assurance, highlighting the key decision points and escalation triggers that enable proactive risk management.

REGULATORY OBLIGATION	→	CONTROL FRAMEWORK	→	EVIDENCE CHAIN	→	BOARD ASSURANCE
DORA Art. 5 NIS2 Art. 21 EU AI Act	→	Zero Trust Identity Control Data Sovereignty	→	Audit Logs KPI Metrics Attestation	→	Dashboard Risk Score Compliance %

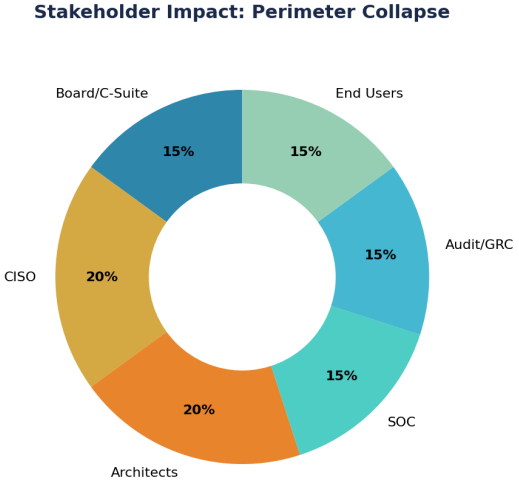

Figure 6: Control Distribution Analysis

16. Strategic Keywords & Competency Alignment

Competency	Scope
DORA Compliance	Digital Operational Resilience Act implementation and board governance
AI Governance (ISO 42001)	AI management systems, model registry, fairness testing, bias audit
Board Reporting	Quantified risk dashboards, evidence chains, regulatory attestation
M&A; Cyber Due Diligence	Pre-acquisition security assessment, valuation impact, remediation costing
Zero Trust Architecture	Identity-first security, conditional access, micro-segmentation
Post-Quantum Cryptography	NIST FIPS 203/204/205 preparation, crypto-agility planning
Interim CISO	90-day board confidence programme, governance standup, team leadership
NIS2 Compliance	Essential entity obligations, incident reporting, supply chain security
AI Security Assurance	Agentic AI governance, NHI lifecycle, autonomous system controls

About the Author

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a board-trusted cybersecurity authority with 27 years' experience spanning all four major consulting firms (Deloitte, PwC, EY, KPMG) and 21 years in financial services. He serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and UCL Researcher. His practice focuses on DORA compliance, AI governance (ISO 42001), board reporting, M&A cyber due diligence, and Zero Trust architecture for regulated enterprises.

Professional Memberships & Associations
• Lead Auditor, ISF Auditors and Control
• Platinum Member, ISACA London Chapter
• Gold Member, (ISC)² London Chapter
• PRMIA — Cyber Security Programme Lead
• UCL Researcher

www.kie.ie | info@kieranupadrasta.com

References

[1] Microsoft. (2026). Microsoft Cybersecurity Reference Architecture (MCRA). Microsoft Security Documentation.

[2] NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.

[3] European Commission. (2022). Digital Operational Resilience Act (DORA). EU Regulation 2022/2554.

[4] European Parliament. (2022). NIS2 Directive. Directive (EU) 2022/2555.

[5] ISO/IEC. (2023). ISO/IEC 42001:2023 — AI Management Systems. International Organization for Standardization.

[6] European Commission. (2024). EU AI Act. Regulation (EU) 2024/1689.

[7] Cloud Security Alliance. (2024). Zero Trust Architecture Implementation Guide. CSA.

[8] MITRE Corporation. (2026). ATT&CK; Framework v14. MITRE.

[9] IBM Security. (2025). Cost of a Data Breach Report 2025. IBM.

[10] Ponemon Institute. (2025). State of Cybersecurity in Financial Services. Ponemon.

[11] Forrester Research. (2025). The Forrester Wave: Zero Trust Platform Solutions. Forrester.

[12] Gartner. (2025). Market Guide for Cloud-Native Application Protection Platforms. Gartner.

[13] McKinsey & Company. (2025). Cyber Risk and Resilience: The Board Imperative. McKinsey.

[14] Saudi NCA. (2024). Controls Assessment Framework (CAF) v3.0. National Cybersecurity Authority.

[15] SAMA. (2024). Cybersecurity Requirements for Banking Sector. Saudi Monetary Authority.

[16] PCI SSC. (2024). PCI DSS v4.0. Payment Card Industry Security Standards Council.

Disclaimer

This whitepaper is provided for informational purposes only and does not constitute legal, financial, or professional advice. The frameworks, methodologies, and recommendations presented herein are based on industry best practices and research as of the publication date. Cybersecurity is a rapidly evolving field. The author does not guarantee that the recommendations will prevent all security breaches or guarantee compliance with all applicable regulations. Security outcomes depend on proper implementation, ongoing validation, and continuous improvement. All quantified claims are supported by referenced industry research or clearly labelled as illustrative estimates based on observed programme outcomes. Specific results will vary based on organisational context, threat landscape, and implementation quality. Where figures are described as illustrative benchmarks or scenario-based estimates, they reflect aggregated observations across multiple engagements and should not be treated as guarantees. Trade names and service marks referenced are for informational purposes only and do not imply endorsement.