B2B SAAS PLATFORM

LudiSec

WHITEPAPER

Zero Trust Architecture: A Practical Guide

Document Information

Published	June 10, 2026
Uploaded	2026-06-10
Author	LudiSec Research Team
Download	http://localhost:8000/es/staff/whitepapers/96/export/
Classification	Public

Executive Summary

THE ZERO TRUST PRINCIPLE

"Never trust, always verify." Zero Trust assumes breach and verifies every request as though it originated from an open network.

THE FIVE PILLARS

1. Identity — Strong authentication (MFA, passwordless) for every user and service account
2. Devices — Device health verified before granting access
3. Networks — Micro-segmentation eliminates lateral movement
4. Applications — Per-session access grants, not standing permissions
5. Data — Classify, encrypt, and monitor data at rest and in transit

IMPLEMENTATION ROADMAP

Phase 1: Foundations (Months 1-3)
- Deploy MFA across all identities
- Asset inventory and device compliance policy

Phase 2: Segmentation (Months 4-6)
- Micro-segment crown-jewel systems
- Implement just-in-time (JIT) access for privileged accounts

Phase 3: Automation (Months 7-12)
- Continuous risk scoring for users and devices
- Automated policy enforcement and anomaly alerting

HUMAN FACTOR

Technology alone is insufficient. Staff must understand why access controls exist and how to recognise social engineering attempts that try to bypass them.

1. Introduction

> *This guide provides a pragmatic, step-by-step approach to transitioning legacy enterprise networks to a Zero Trust Architecture (ZTA).*

2. Background & Context

> *The traditional 'castle-and-moat' security model is obsolete in the era of cloud computing, remote work, and sophisticated persistent threats, necessitating a perimeter-less approach.*

3. Methodology

> *We synthesized implementation frameworks from NIST, CISA, and leading cybersecurity practitioners into an actionable, phased roadmap.*

4. Findings

> *Organizations that implement identity-based micro-segmentation reduce the blast radius of a ransomware infection by up to 85%.*

5. Recommendations

> *Begin with robust identity and access management (IAM), followed by device health validation, before attempting complex network micro-segmentation.*

6. Conclusion

> *Zero trust is a strategic journey that requires alignment between IT, security, and business units. It is a philosophy, not a single product you can buy.*

7. References

> *1. NIST Special Publication 800-207, Zero Trust Architecture. 2. CISA Zero Trust Maturity Model.*

About LudiSec

LudiSec is a cybersecurity risk management platform headquartered in Barcelona, Spain. Serving enterprise clients across financial services, healthcare, manufacturing, and the public sector. Available in English, Spanish, and Catalan.