



AI Security & Data Sovereignty.

Zero-trust AI security with
complete data sovereignty.

Service Brief | Security & Privacy

AI security is not optional. It's a requirement.

Gartner predicts that **45% of organizations** will face an AI-related security incident by 2027. Average damage: 4.8 million euros. Meanwhile, the EU demands increasingly strict data sovereignty. Organizations not investing in AI security now are building on quicksand.

45%

Security Incident

Of organizations will face AI security incident by 2027 (Gartner)

€4.8M

Avg. Damage

Per AI-related security incident (IBM 2024)

92%

Want Sovereignty

Of EU organizations demand data sovereignty (IDC)

2.1x

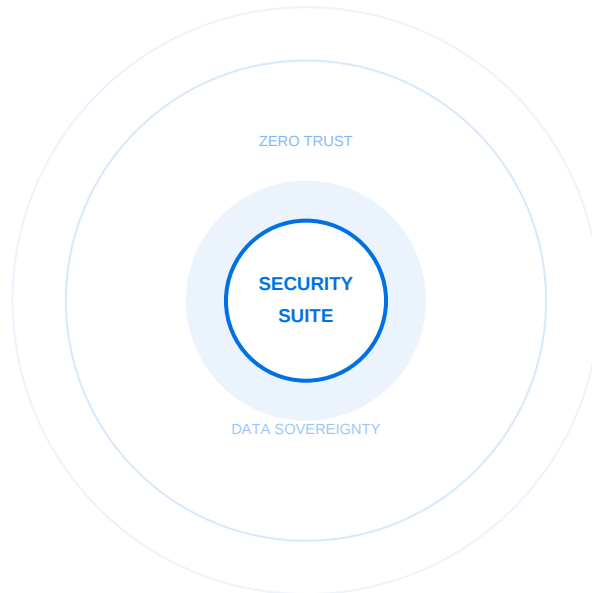
Faster Recovery

Organizations with AI security framework vs. without

"Data sovereignty isn't a technical choice — it's a strategic necessity."

The AI Security Suite

Five security layers for end-to-end AI protection and data sovereignty.



- **Zero-Trust AI Architecture**

Defense-in-depth security for every layer of your AI stack: network, data, model and inference.

- **Data Sovereignty Design**

Architectures guaranteeing your data stays within desired jurisdictions: EU-only, on-premise or hybrid.

- **Model Security**

Protection against model theft, adversarial attacks, prompt injection and data poisoning.

- **Privacy Engineering**

Privacy-by-design: differential privacy, federated learning and synthetic data for GDPR compliance.

- **Incident Response**

AI-specific incident response plan with automated detection, containment and recovery procedures.

Cross-cutting: Zero Trust and Data Sovereignty principles are integrated into all security layers.

Trust nothing. Verify everything.

How zero-trust principles protect your AI systems against internal and external threats.

1 AI Threat Modeling

W69 conducts systematic threat modeling for all your AI systems. From prompt injection to model extraction — every attack vector is identified and mitigated.

2 Secure AI Pipeline

End-to-end security from data ingest to model serving. Encrypted data at rest and in transit, secure enclaves for sensitive workloads and automated vulnerability scanning.

3 Access Control & Audit

Granular access control for AI resources: who can use which model, with what data, and for what purpose. Complete audit trail for compliance.

Your data, your rules. Always and everywhere.

How W69 guarantees your data never leaves your jurisdiction.

1 EU Data Residency

Architectures guaranteeing all your AI data stays within the EU. No US Cloud Act risks. EU-only compute, storage and processing with verifiable compliance.

2 On-Premise AI

For maximum control: fully on-premise AI deployment. W69 designs architectures delivering enterprise-grade AI without any cloud dependency.

3 Hybrid Sovereignty

Best of both worlds: public cloud for non-sensitive workloads, private infrastructure for sensitive data. Intelligent routing based on data classification.

From reactive security to autonomous protection

Traditional security reacts to incidents. **Agentic Security** prevents them. W69 implements AI agents that continuously detect threats, scan vulnerabilities and adapt security measures — faster than attackers can operate.

1 Threat Detection

Real-time anomaly detection across all your AI systems. Recognizing patterns human analysts miss.

2 Automated Response

Automated containment and mitigation. Blocking suspicious requests, isolating models and activating incident response.

3 Human-in-the-Loop

Strategic security decisions escalate to your CISO. Operational security runs autonomously.

4 Adaptive Defense

The security framework learns from every attempt and grows stronger. Continuously evolving defense.

Your Security Readiness Score

How secure is your AI landscape? The AI Scan™ shows your security maturity in 5 minutes.

Exploration

10 – 20

No AI-specific security policy. Standard IT security applied to AI. No data sovereignty strategy.

Integration

20 – 35

AI threat model established. First security controls implemented. Data residency requirements documented.

Strategic AI

35 – 50

Zero-trust AI architecture operational. Full data sovereignty. Automated threat detection and response.
Audit-ready.

Start your AI Scan™

Discover the security maturity of your AI landscape in 5 minutes.

w69.ai/en.html#scan

W69 PROOF™



✓ Enterprise-Grade

✓ GDPR Compliant

✓ NDA-Protected

Every system W69 delivers carries the W69 Proof™ seal — your guarantee for security, sovereignty and measurable results.

What you receive:

Strategic Assessment · Architecture Roadmap · Implementation Plan

■ We respond within 24 hours

“We don't build for today's threats, but for tomorrow's sovereignty.”

NEXT STEPS

Ready to get started?



Scan for AI Scan™

1

Scan the QR code

Or go to w69.ai/en.html#scan

2

Complete the AI Scan™

5 minutes, no registration required

3

Receive your AI Readiness Report

Including personalized recommendations

4

Strategic conversation

We discuss your results and opportunities

5

Implementation roadmap

Concrete steps toward enterprise AI



W69 AI Consultancy

Enterprise AI Architecture & Strategy

AI Security & Data Sovereignty

w69.ai · hello@w69.ai · Amstelveen

+31 6 2797 3800