Redefining Security Priorities in the Age of Generative and Agentic Intelligence

Yeşim Araç Öztürk

Senior Research Manager

March 26, 2026

The AI Shockwave: Why Security Is Being Redefined

AI-enhanced phishing & impersonation

Nearly 60% of organizations cite this as a top concern

AI-powered Ransomware

57.0% report real-time negotiation/extortion as a major risk

LLM prompt injection & model manipulation

57.6% are worried about adversarial attacks on AI models

Automated malware creation/distribution

56.8% see this as a growing threat

AI is not just another threat vector.
It compresses attack timelines and democratizes capability.

© 2026 IDC

Distribution is forbidden without written consent of IDC. All rights reserved.

A Security Inflection Point

Redefining Security Priorities in the Age of Generative and Agentic Intelligence

AI is no longer just software — it is becoming an autonomous decision-maker.

Generative AI changed productivity.

Agentic AI will change operations.

Security must evolve from protection → to orchestration → to resilience.

© 2026 IDC

Distribution is forbidden without written consent of IDC. All rights reserved.

“

We are not facing incremental change — we are facing architectural change.

© 2026 IDC

Distribution is forbidden without written consent of IDC. All rights reserved.

META is seeing substantial investment in AI security

“Dangerous Disconnect”

While 85% of MEA organizations have an AI strategy, less than 20% have a dedicated security framework for protecting those AI models

Emerging AI Security Areas

AI Quality & Evaluation	Application & Platform Security	Model Consumption Security
Runtime Control & Interface Security	AI Governance & Trust	AI Security-as-a-Service & Training
Counter-AI & Threat Protection	Data Security & Protection	Discovery & Observability
Identity Security for AI/Agents	Model Security	AI Security Automation & Operations

What matters for META now

1. **AI Governance & Trust**
   72% of META CISOs cite regulatory compliance as the main reason for AI project delays.
2. **AI/Agentic SOC**
   Region faces a 32–35% shortage of qualified cybersecurity professionals
3. **Identity security for AI/Agents**
   Banking saw a 140% rise in deepfake-driven fraud in 2025.
4. **Data Security & Protection**
   65% of META government entities mandate local data residency for AI training sets

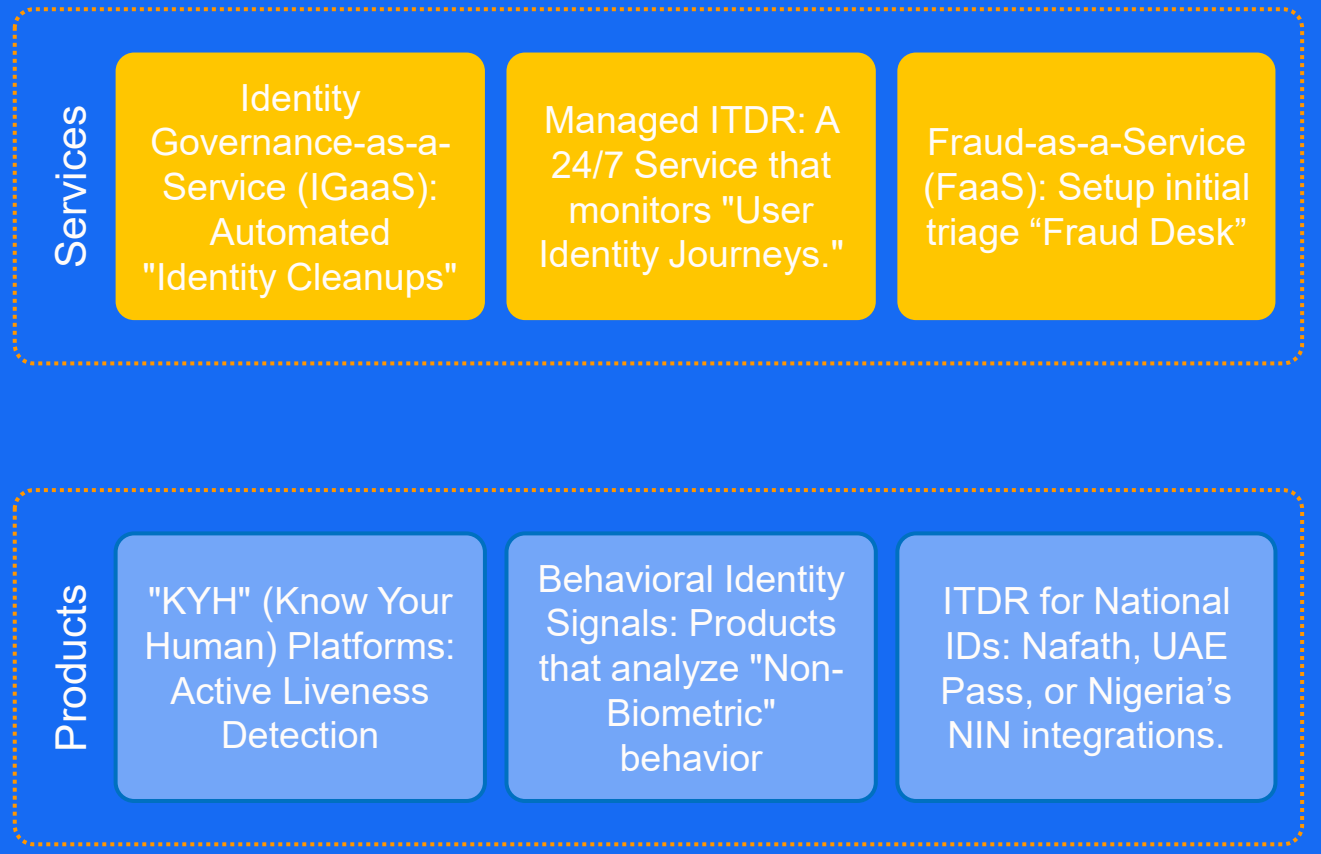
© 2026 IDC
Distribution is forbidden without written consent of IDC. All rights reserved.

Buzzwords – Identity, Deepfake, Fraud

IDC data highlights Identity as the "pivot point" for cybersecurity maturity in the region

Fraud has taken over Ransomware as the No.1 threat in META

- In 2025, regional banks reported a triple-digit increase in fraud attempts using GenAI
- IDC estimates that in 2026, 40% of large MEA enterprises will have a dedicated budget for **"GenAI Fraud Defense"**.



Source: IDC EMEA Security Tech Survey 2025

© 2026 IDC
Distribution is forbidden without written consent of IDC. All rights reserved.

Accelerate Cyber-Physical Systems (CPS) Protection

Cyber physical system security will see most deal activity and new investments in 2026

1. Over **45%** of organizations in the region reported an increase in "Cyber-Physical" threats compared to previous years

2. **70%** of regional enterprises have integrated their IT and OT networks, less than 25% have a dedicated security solutions for OT

Services

- OT-Managed Detection and Response : Integrate or Build
- OT-Specific Incident Response (IR)
- Cyber-Physical GRC: NCA-OT (Saudi) and DESC (Dubai) mandates

Products

- Protocol-Native AI Firewalls
- Hardware Root of Trust for Edge
- "Safe" Autonomous Response Agents
- Digital Twin Simulation for CPS

Source: IDC EMEA Security Tech Survey 2025, IDC Middle East and Africa Security Strategies

© 2026 IDC
Distribution is forbidden without written consent of IDC. All rights reserved.

MDR is commodity: META needs “Sovereign Trust Platform”

Business Priority	MUST ASK	MUST DO
Regulatory Alignment: Across the countries in the region, there were approximately 120+ significant regulatory updates, clarifications, or new mandates related to cybersecurity and data privacy.	• Can you prove licensed operations across META with local data processing? • Are you audit ready?	• Multi-license strategy • Sovereignty – Data, Platforms, LLMs
Adaptive Resilience : Predict, Self-Heal, Continuously Test	• Predict threats before they hit, not just respond after? • Isolate, patch, restore without human intervention? • Continuously test resilience?	• Predictive threat intelligence • Self-healing automation • Chaos engineering- Real-time resilience and auto-recovery. • Continuous compliance proof
Operational Simplicity: Platformization	• One platform for MDR, GRC, compliance, risk across IT/OT/IoT/AI/Cloud—or separate tools stitched together? • Can I see unified risk posture and automated response in one view?	• Single telemetry fabric • Unified control framework • Cross-domain correlation • Automated incident and evidence loop - MDR event to GRC audit artifacts.

Source: IDC Research POV

© 2026 IDC
Distribution is forbidden without written consent of IDC. All rights reserved.

Key Takeaways

Fraud

Identity

Cyber Physical Systems

AI Security

Sovereign Trust Platform

"In 5 years, META won't just consume cybersecurity, it will build and export it too."

Cyber innovation is booming here. The investment, talent, and regulatory momentum are real. What's built in the region for the region will solve problems no one else can and become the blueprint others follow.

© 2026 IDC ution is forbidden without written consent of IDC. All rights reserved.

IDC