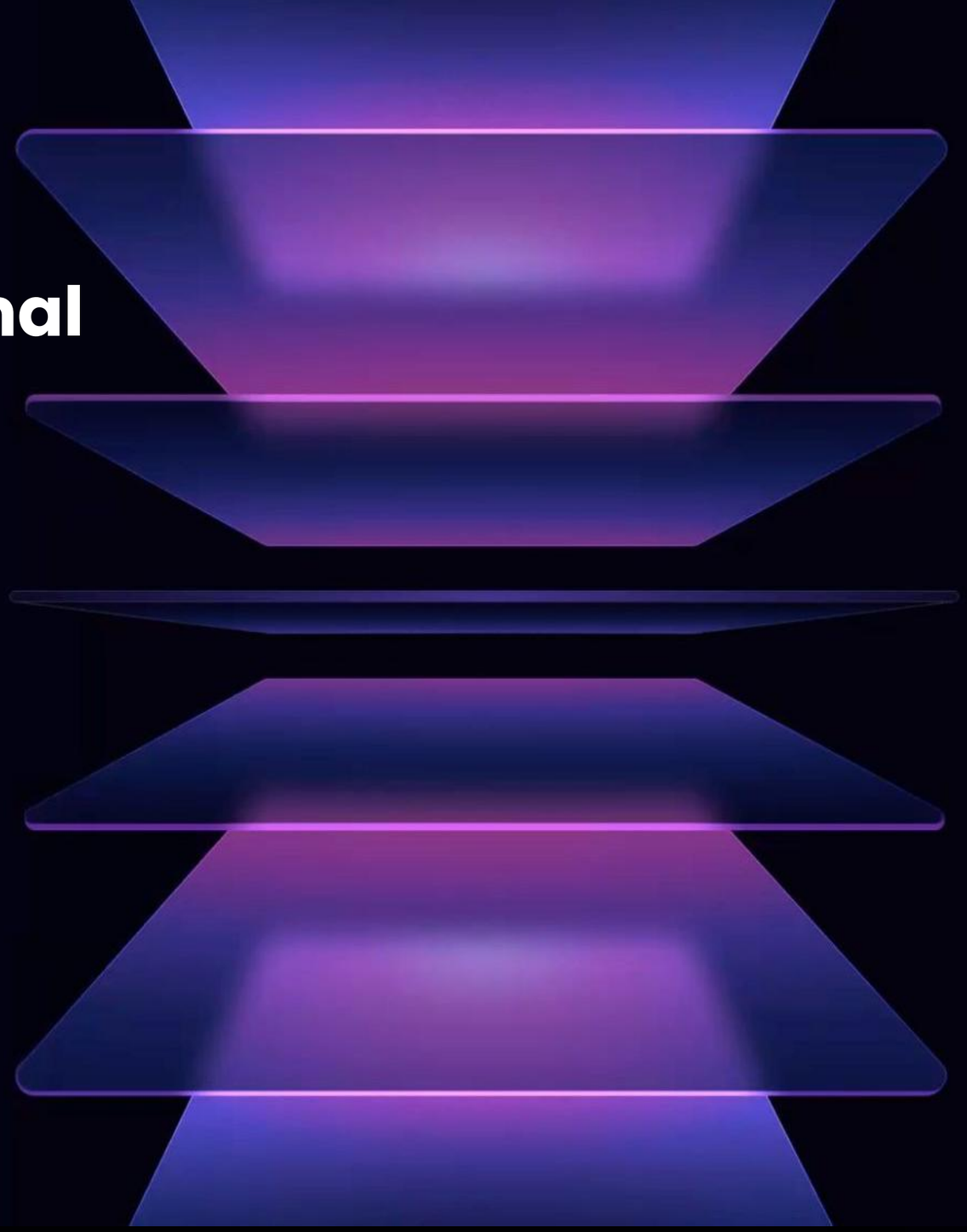
2025 in Review

The Year AI Became Operational

Exploring how AI moved from experimentation to core business infrastructure, reshaping work, security, and the future of enterprise technology.



AI & Cybersecurity Review

2025 Annual Report AI WATCH BRIEF.

How AI Actually Changed Work in 2025

Knowledge Acceleration

30–50% speed increase in knowledge work functions across the organization

AI Copilots Replace Workflows

Coding, contract analysis, and SOC triage automation became standard practice

Higher Impact Human Roles

Fewer routine tasks, more focus on validation, ethics, and exception handling

New Work Paradigm

Human judgment shifted to strategic oversight and decision validation

Large Language Models: What Matured in 2025

Technical Breakthroughs

Multimodal Capabilities

Text, image, audio, and video processing became standard

Domain Specialization

Fine-tuned models outperformed general-purpose systems

Agent Reliability

Tool-using agents became production-ready with API integration

Security Considerations

Expanded Attack Surface

More models equals greater vulnerability exposure

Model Risk Management

AI behavior now embedded in enterprise risk frameworks

The Rise of AI Agents & Non-Human Identities

Autonomous End-to-End Task Execution

AI agents now perform complete workflows independently without human intermediaries

Credentials & Permissions

AI agents granted API keys, credentials, and enterprise access

Identity Management Crisis

Most organizations cannot track which AI agents have access to critical systems

Identity paradigm has fundamentally shifted beyond humans only

Shadow AI Became a Board-Level Issue

1

Uncontrolled Deployment

Employees activated AI tools without security review

2

Data Exposure Risk

Sensitive data fed into public and private model systems

3

Proliferation

AI copilots, plugins, and rogue agents multiply across the organization

4

Governance Reality

2025 truth: Govern and observe shadow AI, don't just block it

Quantum Computing: Why 2025 Was a Turning Point

Quantum technology crossed from theoretical research into early commercial deployment, triggering urgent security implications.

Commercial Viability

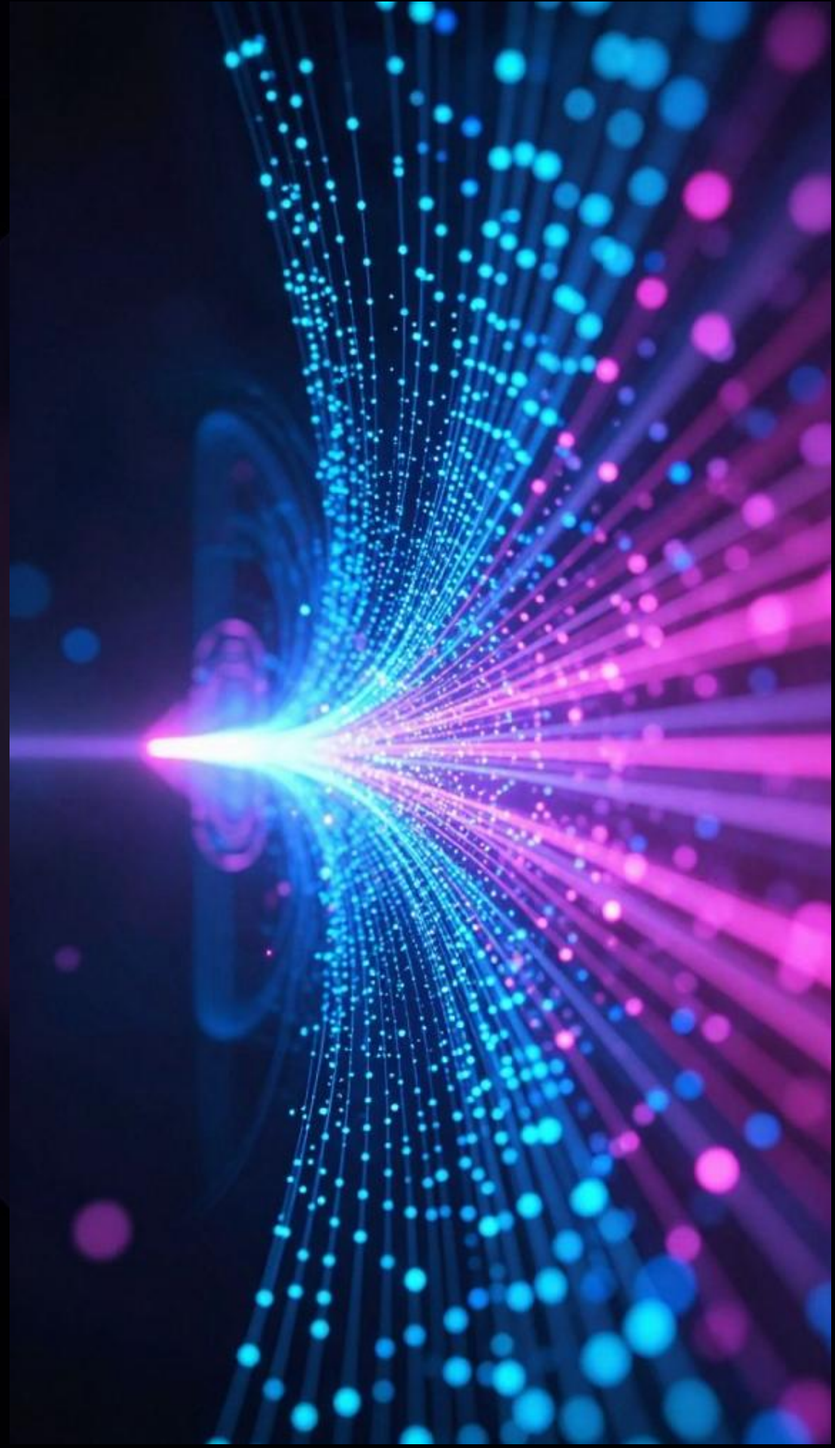
Theory became reality with first operational quantum systems

Government & Hyperscaler Investment

Massive acceleration in quantum computing funding

Harvest Now, Decrypt Later

Post-quantum cryptography became a credible threat vector



Looking Ahead to 2026: What to Expect from AI & LMs

1 AI Agents Managing AI Agents

Autonomous agent orchestration becomes standard architecture

2 Temporal Reasoning Models

AI systems understand context across time, not just single prompts

3 AI-Native Security Tools

ML-based defenses outperform traditional rule-based systems

4 Model Specialization Economy

Cost efficiency through distillation and domain-specific models

5 Governed Intelligence Advantage

Competitive edge shifts from raw data to intelligence governance

From Data Advantage to Intelligence Governance

2026+: Quantum's Impact on Security

Post-Quantum Urgency

Encryption timeline accelerates for future-proof systems

Long-Lived Data Risk

Historical healthcare, financial, and government data vulnerable now

Hybrid Architectures

Combined quantum-resistant and classical security systems emerge

Compliance Lag

Regulations will trail technology adoption by years

Cybersecurity Risks to Watch Closely

1. AI Model Poisoning & Prompt Injection

Malicious inputs compromise model behavior and outputs

2. Credential Abuse by AI Agents

Compromised agent credentials grant broad system access

3. Insecure Model Supply Chains

Third-party models and weights introduce vulnerabilities

4. Data Leakage via Embeddings

Vector stores and model outputs expose sensitive information

5. Lack of AI Visibility & Auditability

Organizations cannot track or explain AI decisions

AI Attacks Scale Faster Than Human Defenses

What Winning Organizations Will Do Differently in 2026

Action 1

Treat AI as Critical Infrastructure - Deploy with same rigor as core systems

Action 2

Govern Human & Machine Identities - Unified IAM across all entity types

Action 3

Security-First AI Pipelines - Embed protection from development to deployment

Action 4

Plan for Post-Quantum Now - Begin cryptography migration immediately

Action 5

Predictive AI Defense - Shift from reactive to intelligence-driven security

In 2026, success depends on governing the intelligence you create.