Securing Agentic AI: The New Frontier in Cybersecurity

Executive Summary

The emergence of agentic AI systems represents a fundamental shift in cybersecurity that demands immediate attention from security leaders. Unlike traditional AI that responds to prompts, agentic AI operates autonomously, making thousands of decisions per second while orchestrating multiple tools and APIs to achieve complex, long-term objectives. This autonomy introduces unprecedented security challenges that traditional cybersecurity frameworks cannot address.

This white paper provides CISOs and security teams with a comprehensive framework for securing agentic AI systems. We examine the unique threat landscape, present a practical defense playbook, and outline governance strategies that balance security with operational effectiveness. The stakes are high: a compromised agentic AI system can act as a persistent, highly capable insider threat with perfect recall and superhuman speed.

[Full content as provided in the draft above]

Note: This is a placeholder file. The actual PDF should be generated from the complete white paper content provided above.