



Application Security in the Age of AI™

Securing Software That Can Interpret, Decide, and Act

Stephen R. Jordan

Volume VIII of The Operating Discipline for AI Library™

Pillar II: AI Risk Governance & Security™

How to secure software that can interpret, decide, and act. Once an application calls a language model or hands control to an agent, the AppSec stack sees only part of its behavior, and scans pass while real risk drifts. The book names that condition the Runtime Determinism Gap and rebuilds application security around behavioral validation rather than pattern matching. Written for AppSec leaders, security architects, and engineering managers, Volume VIII offers libraries a current reference on AI application security. Recommended for computer security, information technology, and business collections.

BIBLIOGRAPHIC

Title	Application Security in the Age of AI™
Author	Stephen R. Jordan
Publisher	SRJ Consulting & Services Publishing
Pub. Date	September 14, 2026
Pages	350

FORMATS & PRICING

Hardcover	ISBN 979-8-9981369-4-8 · \$109.99 USD
Paperback	ISBN 979-8-9981369-1-7 · \$46.99 USD
eBook	ISBN 979-8-9981369-3-1 · \$24.99 USD

Order in hardcover, paperback, and Kindle editions through Amazon. For acquisition inquiries, contact the publisher directly.

WHAT IS INSIDE

- The Behavioral Attack Surface™:** the application surface areas that change once AI is introduced.
- The Semantic Vulnerability Class™,** a bug taxonomy at the meaning layer extending the OWASP Top 10 and OWASP LLM Top 10.
- The AppSec Capacity Equation™:** vulnerability management math when AI changes both code output and inspection rate.
- The AI Application Security Lifecycle™,** merging DevSecOps with AI specific controls.
- The Continuous Validation Loop™,** replacing point in time scanning with ongoing behavioral validation.

ABOUT THE AUTHOR

Stephen R. Jordan is the founder of SRJ Consulting & Services LLC, an operator led AI advisory practice serving mid market to multinational organizations. His career spans senior roles at Citi, Intel, McAfee, and Optiv across technology operations, security, and enterprise risk. He is the author of *The Operating Discipline for AI Library™*, a nine volume executive reference series organized into two pillars, AI Business Services™ (Volumes I through IV) and AI Risk Governance & Security™ (Volumes V through IX), all nine now published. Based in Frisco, Texas. Works nationwide.

LIBRARY APPEAL

Public libraries: A strong fit for technology and career sections serving IT and security professionals, and for business readers who need to understand AI risk without a technical background. **Academic libraries:** Recommended for cybersecurity, computer science, and information systems programs, and for business schools teaching technology risk. Aligned with the OWASP LLM Top 10 and the Google Secure AI Framework, and suitable for course adoption in application security, software engineering, and DevSecOps. **Corporate and special libraries:** Useful for security, risk, and compliance teams preparing for AI audits, customer security reviews, and regulatory inquiries.

PUBLISHER CONTACT

SRJ Consulting & Services Publishing
Frisco, Texas, USA

EMAIL

info@srjconsultingservices.com

PHONE

(415) 413-7772

WEB

srjconsultingservices.com