AI Security Readiness

Secure your organization against the unknowns and vulnerabilities of emerging technologies.

Over the past year, AI adoption has seen explosive growth across a wide variety of businesses, regardless of industry. But that rapid adoption has brought with it new attack vectors, and a multitude of unknowns.

Despite the unknown vulnerabilities, security leaders are being tasked with the evaluation and vetting of new tools as business scrambles to stay ahead.

Tevora has combined emerging trends with learnings and experience across industries to help organizations implement GenAI securely.

Is your organization AI-ready?

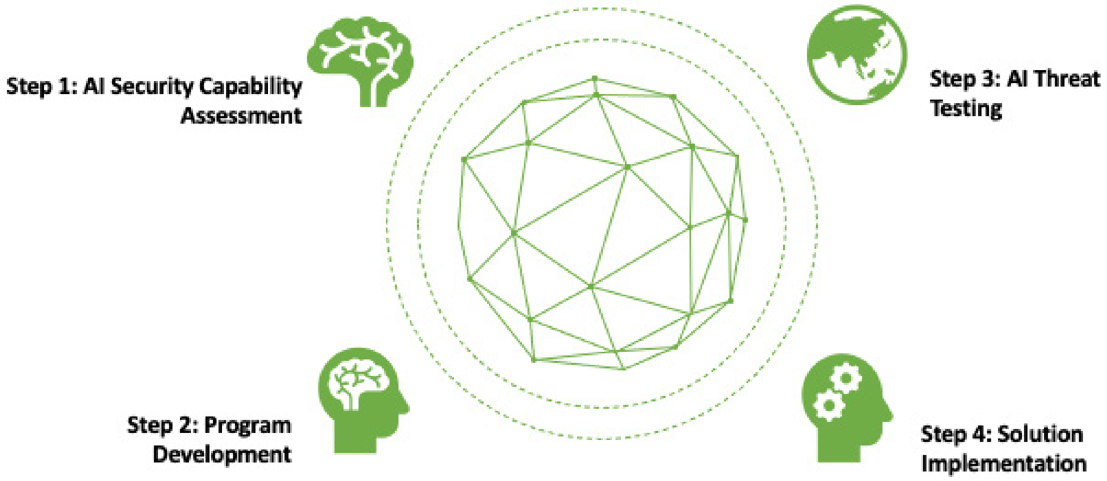
70%

organizations are currently using or exploring immenent implementation of generative AI

19%

of organizations are piloting or in production with generative AI

Source: Gartner, "Innovation Insight; Vector Databases", By Arun Chandrasekaran, Radu Miclaus, 4 Sept. 2023


Step 1: AI Security Capability Assessment
Step 3: AI Threat Testing
Step 2: Program Development
Step 4: Solution Implementation

AI Security Readiness

Tevora's 4-Step AI Security Program

Tevora's team of experts are skilled at assessing your business' unique needs to supplement your internal processes, or provide a comprehensive AI Security Program.

Step 1: AI Security Capability Assessment

Evaluate the current organizational usage and capability in AI and LLM including:

- Define AI Use Cases
- Define Population
- Define Data Input and Output from Generative AI tools
- Understand and Identify Risk
- Provide Recommendations for Controls

Step 2: Security Program Development

Tevora leverages industry frameworks (i.e. NIST, OWASP), security and risk best practices, and business acumen to develop best-in-industry AI Security Programs. Programs include the following.

- Policies & Procedures
- Third Party Risk Management
- Privacy, Legal & Compliance
- User Training

Step 3: AI Threat Testing

Ensure your organization is secure by testing your defenses before an attacker has the chance.

- Test API Integrations
- Test Retrieval Augmented Generation (RAG)
- Test Private vs. Public Hosting
- Testing for prompt injection
- Testing for data leakage, including prompt leaking

Step 4: Solutions Implementation

Identify, define requirements and implement tools to monitor or prevent LLM and Generative AI tools including:

- DLP
- UBE/UBA
- Security service edge (SSE) providers that can intercept web traffic to known applications
- Web Filtering
- Browser Isolation

TEVORA™ Compromise Elsewhere.

Tevora is a global leader in enterprise cybersecurity, risk, and compliance services. Founded in 2003, Tevora's team of expert consultants is devoted to supporting the CISO in protecting their organizations from digital threats, creating more secure and compliant business operations. With 20 years of consistent growth, Tevora has accumulated numerous awards and recognitions for growth and industry leadership. Most notably, Tevora has been recognized as one of Inc 5000's fastest growing companies for 9 years since 2014. Today, Tevora boasts over 1000 enterprise clients and robust practices around compliance, risk, threat management, and cyber solution integration.

Go forward. **We've got your back.**