INSIGHTS | SOLUTIONS BRIEF

Defending at Machine Speed

Frontier AI Has Changed the Rules of Cybersecurity

Frontier AI is not reinventing attack techniques; it is compressing timelines. The window between vulnerability discovery, weaponization, and exploitation is collapsing from weeks to hours.

For security leaders, this reframes the central challenge. The question is no longer simply whether your organization can identify exposures, it is whether you can discover, validate, prioritize, and remediate them faster than an AI-enabled adversary can exploit them.

Organizations who continue to build around dated quarterly scans, annual penetration tests, and manual remediation workflows are operating at human speed in a threat landscape that now moves at machine speed.

This brief outlines the strategic capabilities, program gaps, and organizational capacities that define AI-era security maturity. Synthesizing leading frameworks with real-world insights from the WEI CISO community to answer the question every security leader is asking: *What are other organizations in my space doing today?*

THE BUSINESS CHALLENGE

Expectations placed on security leaders continue to expand. Boards, regulators, and executive teams demand greater visibility into organizational exposure, faster risk reduction, and clearer articulation of cyber risk in business terms.

Today's security leaders must answer questions such as:

- Which attack paths present the greatest business risk?
- How quickly can we reduce exposure?
- Are we resilient enough to recover when controls fail?

The WEI Approach: Proactive & Proven

WEI takes a holistic, risk-based approach to cybersecurity, integrating people, processes, and technology to build a defense strategy that addresses every layer of risk. Our methodology ensures proactive, adaptable security measures.

STRATEGIC SECURITY SERVICES

- Strategy Development & Analysis
- Maturity Assessments

SECURITY COMPETENCIES

- Cyber Security Strategy
- Cloud Security
- SIEM & SOAR Orchestration
- CTEM
- Incident Response
- Vulnerability Management

Yesterday's Questions	Today's Questions
How many critical vulnerabilities do we have?	Which attack paths pose the greatest business risk right now?
Did we pass the annual pen test?	Do our controls work under adversarial conditions?
Are our controls deployed?	How fast can we reduce exploitable exposure?
What does our vulnerability count look like?	What is our Expected Annual Loss from current exposures?
Did we meet compliance requirements?	Are we resilient enough to recover when controls fail?

WEI CYBERSECURITY

SEVEN CAPABILITIES OF AN AI-READY SECURITY PROGRAM IN THE AGE OF FRONTIER AI

Leading security programs confront the AI-accelerated threat landscape by advancing deliberately across seven capability areas — from visibility and validation to automation and identity, to resilience, supply chain, and AI governance. These are not done sequentially, and each organization must figure out for themselves what order makes sense. WEI can assist in this effort with our AI Readiness Assessments to meet clients where they are today.

1. Continuous Threat Exposure Management (CTEM)

Move beyond vulnerability counts to identify and prioritize the attack paths that present the greatest business risk.

2. Continuous Validation

Continuously verify that security controls perform as expected through breach simulation, adversary emulation, and ongoing testing.

3. Security Automation & AI-Augmented Operations

Reduce analyst workload, accelerate investigations, and automate repetitive response activities using AI-driven security operations.

4. Identity Security

Strengthen privileged access, govern human and non-human identities, and continuously monitor identity-based threats.

5. Cyber Resilience & Incident Preparedness

Assume breaches will occur by strengthening incident response, recovery planning, tabletop exercises, and business continuity.

6. Supply Chain & Third-Party Risk

Monitor third-party risk, validate vendor security practices, and improve software supply chain resilience.

7. AI Governance & Secure AI Adoption

Establish governance, policies, and controls that enable responsible AI adoption while managing emerging AI-related risks.

WEI Helps Security Leaders Stay Ahead of AI-Accelerated Threats

Strategic Services:

- Vulnerability Management Program Review
- Security Maturity Assessments
- Operationalizing CTEM
- Threat & Attack Simulation
- Red Team Testing
- Purple Team Testing
- Incident Response Planning
- Penetration Testing Services
- Tabletop Exercises

Talk to WEI Today

WEI's cybersecurity experts help organizations assess current capabilities, identify exposure gaps, and build practical roadmaps for AI-era resilience.

Get started today.

43 Northwestern Drive, Salem, NH 03079
(800) 296-7837