

Frontier AI Models and Security Coverage Statement

Hitachi Vantara recognizes that frontier AI models may accelerate defensive security research as well as adversarial vulnerability discovery. Customer assurance is addressed through established governance, mature vulnerability management, security-by-design practices, documented escalation paths, and ongoing control improvements as the threat landscape evolves. Hitachi Vantara has established AI governance, product security, vulnerability management, cyber risk management, third-party security, infrastructure security, and business continuity practices that collectively support a risk-based response to frontier AI-related threats. Where approved and appropriate, Hitachi Vantara uses advanced security-focused AI capabilities defensively to support cybersecurity activities, including vulnerability analysis, security testing, and risk review. These capabilities are governed through established approval, oversight, and risk-management processes, complement existing security controls, and do not replace human review or established remediation, escalation, and risk-acceptance procedures.

This statement is intended to provide a customer-facing overview of relevant security coverage areas. It does not replace product-specific security documentation, contractual commitments, formal assurance reports, or customer-specific risk reviews. Hitachi Vantara’s current coverage of frontier AI-related security risks is grounded in its established security operating model, rather than in a standalone response to a single industry development. The key coverage areas include:

Key Areas	
Frontier AI Access and Defensive Use	Hitachi Vantara uses approved and restricted access to advanced, security-focused AI capabilities defensively to support cybersecurity activities such as vulnerability analysis, security testing, and risk review. These capabilities complement existing security controls and remain subject to established governance, oversight, and risk-management processes.
Vulnerability Management and Risk-Based Remediation	Hitachi Vantara maintains established procedures for identifying, assessing, and addressing vulnerabilities. Vulnerability intake and disclosure channels facilitate communication with engineering and cybersecurity teams, enabling reported risks to be investigated and managed through the appropriate remediation, exception, or risk-acceptance process.
Product, Managed Services, and Supply-Chain Security	Hitachi Vantara’s customer coverage spans product security, managed services security, and enterprise and supply-chain security, supported by secure development practices, vulnerability management, security architecture review, automated scanning, penetration testing, risk-based remediation governance, service-specific operating practices, third-party security, infrastructure security, cyber risk management, monitoring, and business continuity practices.
AI Governance and Responsible Use	Hitachi Vantara continues to mature its enterprise AI governance model to enable responsible adoption while coordinating security, legal, privacy, data, compliance, procurement, and business-value considerations. The governance model addresses AI tools, agents, internally developed capabilities, third-party solutions, and AI-enabled business use cases.

Together, these practices provide a structured basis for monitoring frontier AI-related security developments, assessing potential impact, and coordinating appropriate defensive, remediation, and governance responses across the relevant parts of the organization.