opentext™

Enterprises Rush into GenAI Without Security Foundations, New Ponemon Study Finds

2026-03-23

Global research from OpenText and Ponemon shows strong security foundations are critical to scaling Enterprise AI

WATERLOO, ON, March 23, 2026 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX) (TSX: OTEX) today released a new global report, "Managing Risks and Optimizing the Value of AI, GenAI & Agentic AI," developed in partnership with the Ponemon Institute. The research revealed that, while more than half of enterprises (52%) have fully or partially deployed GenAI, security and governance is falling behind.

This gap highlights a growing challenge for the industry as organizations are adopting generative AI quickly, but many are doing so without the governance and security foundations needed to manage its risks.

"AI maturity isn't just about adopting AI tools—it's about doing it responsibly," said Muhi Majzoub, EVP, Product & Engineering. "Security and governance are foundational to getting real value from AI. When they're built into AI systems from the start, organizations can operate with greater transparency, monitor systems continuously, and trust the outcomes AI delivers."

Only 1 in 5 enterprises report reaching AI maturity – where AI in cybersecurity activities is fully deployed and security risks are assessed – and fewer than half (43%) have adopted a risk-based strategy to govern AI systems. As AI systems become more autonomous and embedded in critical operations, closing this maturity gap will be essential for ensuring trust, compliance, and long-term business value.

AI Security and Governance are Lagging

According to the survey, significant gaps between the pace of AI deployment and the practices needed to govern and secure it effectively.

- Nearly 8 in 10 organizations (79%) have not yet reached full AI maturity in cybersecurity, where systems are fully deployed and security risks are assessed.
- Only 41% of organizations have AI-specific data privacy policies in place.

- A majority (62%) of respondents say it is difficult to minimize model and bias risks (like the breach of ethical and responsible AI principles) in the language model development.
- Fewer than half (43%) of respondents have adopted a risk-based AI governance approach that addresses AI-related risks like bias, security threats, or ethical issues.
    - Fifty-eight percent (58%) say prompt or input risks (e.g., misleading, inaccurate, or harmful responses) are very or extremely difficult to minimize.
    - Over half of respondents (56%) also report challenges in managing user risks, including the unintended spread of misinformation.
- Nearly six in ten respondents (59%) say AI makes it more difficult to comply with privacy and security regulations, yet only 41% report having AI-specific data privacy policies in place.

Without Trust and Explainability, AI is Failing to Deliver Results and Requiring Human Oversight

Many organizations are deploying AI to improve efficiency, including within security operations. Yet reported challenges around trust, reliability, and explainability suggest the very tools designed to enhance security may be limiting effectiveness and AI autonomy due to governance and maturity gaps.

- AI falls short in threat detection as bias and reliability risks persist:
    - Just 51% of respondents say AI is effective in reducing the time to detect anomalies or emerging threats. Fewer than half (48%) rate AI as effective in threat detection and hunting for deeper insights and reducing manual workload.
    - AI model and bias risks are limiting effectiveness. Nearly two-thirds (62%) of respondents say it is very difficult or extremely difficult to minimize model and bias risks, including unfair or discriminatory outputs.
    - Operational reliability also presents a challenge, with 45% of respondents citing errors in AI decision rules as a top barrier to effectiveness, while 40% report errors in data inputs ingested by AI.
- Fully autonomous AI still far from reach:
    - Fewer than half of organizations (47%) say their AI models can learn robust norms and make safe decisions autonomously, reflecting tempered confidence as AI models take on more independence.
    - As a result, more than half of respondents (51%) say human oversight is needed in AI governance due to the speed at which attackers can adapt.

"The leaders in this next phase of AI adoption will be those who build transparency and control into AI from the start," said Majzoub. "As AI becomes embedded in day-to-day operations, organizations need secure information management as the foundation; clear governance frameworks, policy-based controls, and continuous monitoring

that ensure AI systems remain trustworthy and compliant. Just as important is aligning AI with the right data, security practices, and oversight from the outset so innovation can scale responsibly and deliver measurable business value."

Survey Methodology

The Ponemon Institute independently surveyed 1,878 IT and IT security practitioners across North America, Asia-Pacific, Europe, the Middle East, Africa, and Latin America. The study captured input from organizations of varying sizes and industries, including financial services, healthcare, technology, energy, and manufacturing. The research was conducted in November 2025. Respondents included executives, decision-makers, and practitioners across IT security, engineering, infrastructure, risk and compliance, and other roles involved in AI and security strategy.

Additional Resources

- Read the full report for deeper insights into AI governance and security risks: **Ponemon Institute AI Study | OpenText**
- Learn more about OpenText Cybersecurity solutions for enterprise protection:**Enterprise Cybersecurity Solutions & Services | OpenText**

About OpenText

OpenText™ is a global leader in secure information management for AI, helping organizations protect, govern, and activate their data with confidence. Our technologies turn data into information with context to form the knowledge base for AI. Learn more at **www.opentext.com**.

Cautionary Statement Regarding Forward-Looking Statements

Certain statements in this press release may contain words considered forward-looking statements or information under applicable securities laws. These statements are based on OpenText's current expectations, estimates, forecasts and projections about the operating environment, economies and markets in which the company operates. These statements are subject to important assumptions, risks and uncertainties that are difficult to predict, and the actual outcome may be materially different. OpenText's assumptions, although considered reasonable by the company at the date of this press release, may prove to be inaccurate and consequently its

actual results could differ materially from the expectations set out herein. For additional information with respect to risks and other factors which could occur, see OpenText's Annual Report on Form 10-K, Quarterly Reports on Form 10-Q and other securities filings with the SEC and other securities regulators. Readers are cautioned not to place undue reliance upon any such forward-looking statements, which speak only as of the date made. Unless otherwise required by applicable securities laws, OpenText disclaims any intention or obligations to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise. Further, readers should note that we may announce information using our website, press releases, securities law filings, public conference calls, webcasts and the social media channels identified on the Investors section of our website (**https://investors.opentext.com**). Such social media channels may include the Company's or our executive's blog, X, formerly known as Twitter, account or LinkedIn account. The information posted through such channels may be material. Accordingly, readers should monitor such channels in addition to our other forms of communication.

OTEX-G

View original content to download multimedia:**https://www.prnewswire.com/news-releases/enterprises-rush-into-genai-without-security-foundations-new-ponemon-study-finds-302721434.html**

SOURCE Open Text Corporation