

ITPro Expert Guide

The ITPro Expert Guides offer a targeted collection of key articles designed to keep IT and Cybersecurity leaders and professionals ahead in a fast-moving field. Hand-selected to tackle the Tech industry's most critical, high-impact topics, each guide cuts through the noise to deliver clear, actionable insights.

For sponsors looking to align their brand with editorially relevant trends, these low-lift campaigns deliver maximum impact for your brand and your lead-generation efforts.

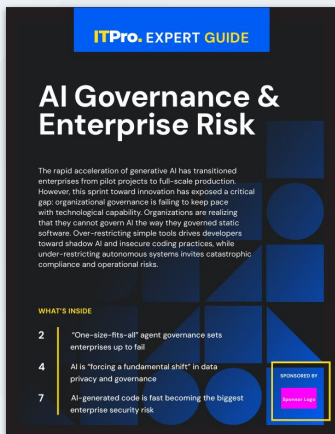
Sponsorship Details: 200 Guaranteed Leads* @ \$12,000

- Designed asset in a PDF format, on a customer-selected topic category from a predefined list of articles picked by ITPro editors. Each guide features three articles from the ITPro website. [View Sample](#)

Available Topic Categories:

- AI Governance & Enterprise Risk
 - Cyber Resilience
 - AI Security
- **Prominent Co-Branding** throughout the entire Expert Guide, positioning your brand as a source of meaningful insight
 - **Dedicated vendor profile** and inclusion of up to three branded resources
 - **Highly qualified intent-driven leads**, from IT & Cybersecurity decision makers who are actively engaged in pre-purchase research

* Starting price includes IT cybersecurity manager+ title filtering. Additional lead requirements subject to price increase



"One-size-fits-all" agent governance sets enterprises up to fail

Gartner recommends a graded approach for agents, depending on their level of autonomy

Governance failures are set to lead to four in ten organizations demoting or decommissioning autonomous AI agents over the next year.

In a new report, Gartner warns that a "one-size-fits-all" approach to governance means that organizations are failing to distinguish between an agent's ability to act and the scope of access it is granted - and that governance gaps are often identified only after production incidents occur.



"Organizations are treating AI agent governance as binary, either locked down or fully trusted, and that is the root cause of failure," said Shiva Varma, senior director analyst at Gartner.

"Agents operate at different autonomy levels and across different trust boundaries. When the same controls are applied indiscriminately, organizations encounter two common failure modes: over-restriction of simple agents, which slows delivery and drives shadow development, or under-restriction of more autonomous agents, which increases operational, security and compliance risk."

Gartner believes it has the solution, in the form of a proportional governance approach that classifies AI agents across distinct autonomy levels, with each level representing a different trust boundary and corresponding governance requirements.

The first covers "observant" agents, limited to read-only access to defined data sources, with outputs visible only to the user making a request - functions such as document summarization, data or knowledge retrieval and code explanation.

AI GOVERNANCE & ENTERPRISE RISK

ITPro

For more information, contact

Brenna Smith
Publisher, Technology
brenna.smith@futurenet.com

Karen Hattan
Director of Business Development
karen.hattan@futurenet.com

Sara Schiano
Account Director
sara.schiano@futurenet.com

FUTURE
B2B
TECH