Cisco Helps Federal Agencies Bridge the AI Infrastructure Gap

Federal agencies are racing to deploy artificial intelligence, but existing infrastructure solutions fail to meet emerging needs.

Government agencies must embrace artificial intelligence or risk falling behind. The Trump Administration's recent Executive Order on Removing Barriers to American Leadership in Artificial Intelligence calls for ambitious AI strategies that champion trust, transparency and innovation.

While the Trump Administration's call to action is clear, federal agencies face overwhelming tech debt from legacy infrastructure. **Agencies cannot meet tomorrow's needs with yesterday's technology.** Now is the time for leaders to invest in new ways of thinking, from network architecture to data governance.

"You need to be looking ahead to see what the next generation looks like. What are its characteristics and how do you build for it?" asked Kapil Bakshi, chief technology officer and distinguished engineer at Cisco's Office of the CTO.

As leadership and IT collaborate on strategy, mission owners are partnering with cloud providers like AWS and Google to try a few models out, build applications and prove a point: Cloud does an excellent job of supporting these proof-of-concept outcomes, but when it comes to mission-critical workloads, on-premises solutions are emerging as a forerunner due to security and cost considerations.

"Cloud is good for a lot of things, but cloud may not be the best for your enterprise data strategy. Costs can compound quickly when you start talking about the infrastructure and computational power required for AI, and customers are struggling with that," explained Dan Morehead, AI strategy lead for Cisco's U.S. Public Sector.

Optimizing for on-prem AI workloads

Recent memoranda from the Office of Management and Budget (OMB) underscore the need for agencies to invest in modernization efforts with OMB M-25-21 and M-25-22 mandating agencies establish an AI strategy, appoint Chief AI Officers (CAIOs) and modernize existing infrastructure all while maintaining public trust.

Agencies looking to support AI on-prem face a daunting task. Leaders must consider the following factors:

- AI workloads consume massive amounts of computational power, leading to fewer resources for other projects
- AI workloads generate east-west traffic patterns that strain traditional network configurations
- AI workloads require energy-efficient data centers with sophisticated cooling solutions designed to keep systems running (or otherwise risk losing access)

Then there are the security concerns. AI introduces novel attack vectors, which threat actors are exploiting for their benefit. Securing AI models is paramount to earning confidence from the general public. Citizens must be able to trust and see how a model came to a specific outcome.

"Cisco AI Defense gives you a sense of how good or not so good the AI safety is in these models. We measure for hallucinations, toxicity, harmfulness and things of that nature, so you can make a choice as to whether you want to have this model in your enterprise or not," said Bakshi.

Bridging the gap between on-prem and cloud

One practical step organizations can take today is to contact their network provider and initiate a Transformation Roadmap (TRM) discussion.

"We can tell you what changes to make so that your network is optimized for AI workloads," explained Kevin Manwiller, senior operations director of national security at Cisco.

The process starts with an honest assessment. How much compute power does each use case require? Where should data be stored? What security protocols must be implemented?

Answering these questions can be complicated, but it doesn't have to be. Partnerships with industry, academia and other public sector institutions could help leaders effectively bridge the gap between on-prem and cloud-based workloads.

For example, while Cisco is known for its infrastructure-level investments in networking, compute, security and observability, the company also invests in agentic or enterprise-wide applications.

"We're investing $1 billion in the technologies, capabilities and partnerships needed to do it because we know just how difficult modernization can be," said Manwiller

Success in AI requires partnerships across the spectrum. Together, federal agencies and industry can move from pilot projects to production-ready systems designed to support citizen needs, but that window is quickly closing. Agencies must act now to capitalize on AI's potential or risk falling behind.

The question isn't whether AI will transform public service, it's whether agencies will be ready to make an investment in their organization's mission, vision and values.