CARAHSOFT

Protecting government data in the AI era



With the right visibility and controls, data protection becomes a framework for enabling agencies to use AI with confidence

Brian Snell | Carahsoft

Artificial intelligence dramatically expands the ways employees can interact with, transform and share information. As a result, it is fundamentally changing the data security conversation. Historically, agencies could focus much of their data protection strategy on relatively well-defined channels such as email, web, endpoints, applications and cloud services. Now an employee can take information from multiple sources, combine it into a prompt, summarize it, analyze it or potentially expose sensitive information to an AI service in a matter of seconds.

That means agencies increasingly need to think about protecting the data itself, not just the system where it resides. They need visibility into what information is sensitive, how it's being used, where it's going and whether that use is consistent with agency policy. In other words, AI is shifting the conversation from protecting where information lives to protecting information wherever it goes, including into AI workflows

Importantly, that shouldn't translate into simply blocking AI at a high level. These technologies can deliver tremendous productivity and mission benefits. The challenge is creating the guardrails that allow agencies to embrace AI tools responsibly so they don't damage the mission or tarnish public trust.

Applying data-centric policies to AI interactions

Enabling employees to take advantage of AI while safeguarding sensitive information involves understanding which AI tools employees are using, what information is moving into them and where sensitive data may be at risk. From there, agencies can apply data-centric policies that distinguish between acceptable and risky behavior. Instead of treating every AI interaction the same way, they can identify sensitive information and establish controls appropriate to the data, the user, the application and the mission.

The goal shouldn't be choosing between AI productivity and data security. Instead, the objective should be safe AI-enablement with system guardrails rather than blanket or policy-based restrictions. If employees see value in AI but the approved AI tools are too difficult to use, the agency might inadvertently encourage workarounds and shadow AI. Providing sanctioned capabilities with appropriate data protection controls gives employees a productive path while providing security teams with visibility and governance.

Agencies don't need to solve every element separately. Technology providers, integrators, resellers and distribution partners can help build repeatable architectures and deployment models that allow protections to scale in complex, federated agency environments.

From policy to architecture to successful implementation

Broadcom is helping agencies put guardrails directly into the security infrastructure through which their users and data already move. Symantec's data protection and web security capabilities provide an important foundation for that strategy.

> "As AI adoption accelerates, the ability to scale proven security and governance approaches is vital for delivering mission outcomes."

Symantec Data Loss Prevention can identify and protect sensitive information based on the data itself and apply policy as users interact with applications and AI services. Secure Web Gateway capabilities provide visibility and control over web-based interactions, including access to generative AI services. Together, those technologies can help agencies move beyond a simple allow-or-block approach toward more granular control of how AI is used.

Our role is also to make those capabilities easier to consume and deploy at scale. To that end, Carahsoft connects Broadcom with the integrators, resellers and solution providers that understand individual agency environments. That ecosystem can help agencies translate policy into architecture, architecture into implementation, and successful implementations into repeatable models across programs and organizations.

As AI adoption accelerates, the ability to scale proven security and governance approaches is vital for delivering mission outcomes. Broadcom can help agencies put the guardrails around AI that allow them to say yes more often so they can protect sensitive information without standing in the way of mission innovation.

Brian Snell *is director of the Broadcom software business at Carahsoft.*



