Zscaler and AWS Join Forces to Secure GenAI Across Government, Healthcare, and Education

June 23, 2026

Zscaler and Amazon Web Services have entered into a Strategic Collaboration Agreement designed to help government agencies, health systems, and education institutions adopt generative AI without compromising security or compliance. The partnership brings together Zscaler's Zero Trust Exchange with AWS services including Amazon Bedrock and Amazon SageMaker, combining inline security controls with cloud-native AI infrastructure to address the specific risks these sectors face as they scale GenAI into production.

Under the agreement, Zscaler and AWS will collaborate on integrations, reference architectures, and joint go-to-market activities. The work will include coordinated customer workshops, pilots, and field engagements to help organizations move from proof-of-concept to production safely. It is a direct response to growing demand from public sector and public-serving institutions that want to use generative AI for everything from cyber defense to citizen services but lack validated security blueprints for doing so.

Why This Matters Now

The timing is not accidental. Generative AI adoption is accelerating across mission-critical environments, and the security gaps are widening in parallel:

- **Prompt-based data exposure.** Sensitive information entered into GenAI prompts, responses, or retrieval-augmented generation pipelines can leak beyond approved boundaries. For organizations handling patient records, student data, or classified intelligence, a single exposure event carries regulatory and operational consequences.
- **Identity compromise and lateral movement.** GenAI applications connect to multiple data sources, APIs, and external services. Each integration point expands the identity surface and creates potential paths for adversaries who gain a foothold through a single compromised credential.
- **Shadow AI outpacing governance.** Research from Wolters Kluwer flagged shadow AI as one of the top healthcare concerns for 2026, with staff adopting generative AI tools faster than IT teams can inventory or secure them. The same dynamic plays out across government and education.
- **Regulatory pressure without clear frameworks.** Government organizations must satisfy FedRAMP, FISMA, and CMMC. Education institutions operate under FERPA. Healthcare has HIPAA. All demand demonstrable data governance, yet few GenAI deployments today meet those standards.

Gartner recently predicted that by 2028, half of all organizations will implement a zero-trust posture specifically for data governance as unverified AI-generated data proliferates. The trajectory is clear, and the organizations that act now will be better positioned than those that wait.

Why Traditional Security Falls Short

Perimeter-based architectures were built to protect a defined set of users accessing applications inside a network boundary. Generative AI breaks this model. AI workloads span multiple cloud environments. Users interact with models from any location. Data flows between development, training, inference, and retrieval layers in patterns that firewalls and VPNs cannot meaningfully inspect or control. Bolting legacy tools onto GenAI workflows creates blind spots rather than closing them.

Three Pillars of the Zscaler-AWS Collaboration

1. Secure Access to GenAI Applications and Data

Rather than granting broad network access, the collaboration enforces least-privilege connections with continuous identity verification. Policy controls govern what data can enter and exit prompts, responses, and connected data sources. This prevents accidental exposure of regulated information while preserving the ability to use AI tools across hybrid and multi-cloud environments, whether users are in an office, a clinic, a campus, or a remote location.

2. Protection for AI Development and Deployment Workflows

Organizations building custom applications on Amazon Bedrock or Amazon SageMaker need security across the full development lifecycle. The partnership addresses workload segmentation, unauthorized access prevention for training data and model endpoints, and governance throughout the build-test-deploy pipeline. Engineering and data science teams can iterate quickly without introducing lateral movement paths that adversaries could exploit.

3. Centralized Visibility, Governance, and Audit Readiness

Public sector organizations must demonstrate compliance to auditors, oversight bodies, and regulators on an ongoing basis. The collaboration includes centralized policy enforcement and security analytics designed to support continuous monitoring, documentation of data flows, access decisions, and security events.

Priority Use Cases

The SCA focuses on three high-impact GenAI scenarios already in demand across these sectors:

1. **SOC copilots** that improve analyst productivity and accelerate investigation and response while protecting sensitive security telemetry and case data from unauthorized access.
2. **OT visibility applications** that enhance situational awareness for operational technology environments, helping organizations identify risk and segment access without expanding the attack surface.
3. **Citizen and patient service bots** that enable AI-assisted self-service while safeguarding regulated data and reducing the risk of unintended disclosure.

What Security Leaders Should Do Now

1. **Inventory your GenAI exposure.** Catalogue every sanctioned and unsanctioned AI tool in your environment. You cannot govern what you have not identified.
2. **Apply Zero Trust to every AI interaction.** Treat each GenAI access event as a policy decision. Enforce least-privilege, verify identity continuously, and inspect data flows inline.
3. **Classify data before it enters AI workflows.** Sensitivity labels and DLP policies must apply to data feeding RAG pipelines, model training, and prompt interactions.
4. **Adopt validated reference architectures.** Leverage joint guidance from your cloud and security providers rather than building one-off solutions that will not scale.
5. **Build for audit from day one.** Integrate logging, policy documentation, and monitoring into GenAI deployments at the start, not as a retrofit.

Looking Ahead

Zscaler and AWS plan to begin joint customer engagements immediately, including solution workshops and reference architecture development. Additional technical guidance and deployment resources will follow. For organizations in government, healthcare, and education that are already piloting GenAI, this collaboration provides a path to move from experimentation to production with security built in from the ground up rather than layered on after the fact.

What steps is your organization taking to secure GenAI in mission-critical environments?

Learn more at our Cloud Security page