AI Access Security

Modern businesses are rapidly evolving with today's digital landscape. Artificial intelligence (AI) has emerged as a transformative force in this evolution, reshaping the way we work across operations, engineering, sales, marketing, and other critical functions. As we stand on the cusp of a new technological revolution, it's clear that AI will continue to serve as a catalyst for innovation, efficiency, and productivity. The more deeply ingrained AI becomes in our everyday work, our work will inevitably become embedded into AI apps and models. With the potential for sensitive data—ranging from proprietary source code to company trade secrets—leaking into generative AI (GenAI) tools, an AI-related data breach has the potential for significant financial, legal, and reputational consequences.

As workers gravitate toward GenAI apps to drive greater productivity, shadow IT has morphed into shadow AI. The lack of full visibility, control, and protection from third-party-provisioned GenAI tools—both sanctioned and shadow AI—will make a robust security posture challenging for InfoSec professionals and meanwhile more enticing for threat actors.

Limitations of Traditional CASB and DLP

Traditional cloud access security broker (CASB) and data loss prevention (DLP) tools aren't designed to mitigate the unique data and security risks that stem from GenAI apps. Traditional methods struggle to keep pace with the rapid proliferation of GenAI apps, along with their unique characteristics and evolving AI ecosystems. What's more, complex AI-based interactions require a large language model (LLM)-powered context—something many traditional solutions lack—to accurately identify and classify sensitive data within unstructured conversational chats.

To complicate matters, threat actors are poisoning third-party LLMs and manipulating vulnerable AI apps to deliver malware and phishing URLs. A purpose-built solution with comprehensive visibility, control, data security, and continuous risk monitoring is required to mitigate many of these emerging AI-related risks.

How to Approach the Problem

For organizations today, a paradigm shift to a purpose-built solution for GenAI is required to empower users and enable modern businesses. Some of the most important requirements to consider for effective GenAI security include:

- **Understand GenAI usage and control what is allowed:** Implement conditional access management to limit access to GenAI platforms, applications, and plugins based on users and/or groups, location, application risk, compliant devices and/or browsers, and legitimate business rationale.
- **Guard sensitive data from unauthorized access and leakage:** Enable real-time content inspection with centralized policy enforcement across the infrastructure and within data security workflows to prevent unauthorized access and sensitive data leakage.
- **Defend against modern AI-based cyberthreats:** Implement a zero trust security framework to identify and block highly sophisticated, evasive, and stealthy malware and threats within GenAI responses.

AI Access Security Enables Safe GenAI Adoption

AI Access Security™ empowers organizations to monitor the adoption and usage of sanctioned and unsanctioned GenAI apps, proactively preventing sensitive data leakage and providing continuous risk monitoring so organizations can safely adopt and use third-party GenAI tools.

Table 1. Key Use Cases

Use Cases	Benefits
Discover and monitor GenAI apps, usage, and risk.	Regardless of whether organizations choose to block, restrict, or freely allow all GenAI apps, they seek to gain comprehensive visibility into their entire GenAI estate. This includes insight into marketplace plugins, AI agents, app usage, and data risk posture to systematically codify AI security strategies.
Prevent sensitive data loss.	Sensitive data leakage (e.g., company data, proprietary source code, user credentials, and customer data) to third-party GenAI tools can increase the risk of regulatory noncompliance. Organizations seek to accurately classify and block sensitive data from leaking into GenAI apps and models outside their control.
Monitor and mitigate AI-based risk.	Organizations seek robust data protection, effective AI posture management, and zero trust security. They want comprehensive data and threat protection for all users—whether they're accessing GenAI apps from the office, at home, or on the go.

Features and Capabilities

AI Access Security is natively integrated with Prisma® Access, Prisma Access Browser, and Palo Alto Networks Next-Generation Firewalls (NGFWs) to secure GenAI usage from the cloud, browser, or on-premises. It provides user access controls, data loss prevention, AI posture management, and threat protection by inspecting prompts and responses from GenAI platforms, apps, and plugins in real time.

Table 2. AI Access Security Features and Capabilities

Feature	Capability
GenAI Discovery	Provides an up-to-date application dictionary of over 3,100 GenAI apps and more than 80 attributes to help accurately discover GenAI apps, monitor their usage, and assess risk for sanctioned and shadow AI apps. GenAI-specific attributes include terms and conditions for security and privacy, input and output modes, whether data is used in training models, compliance checks, presence of security guardrails, and more.
Access Controls	Classify apps as sanctioned, unsanctioned, or tolerated, and implement access controls based on classification and use case. Administrators have the ability to revoke access based on scope of privileges and risk factors, as well as fine-grained control over actions such as upload and download.
AI SaaS Security Posture Management	Enables visibility into GenAI plugins detected via GPT marketplaces with the ability to detect, monitor, and remediate unauthorized AI bots that might be present in virtual meetings. Controls access, monitors permissions, and implements protection for GenAI app configurations.
Data Loss Prevention	Uses LLM-powered and context-aware machine learning (ML) models to accurately classify data across more than 300 classifiers. Has the ability to detect sensitive data inline with over 100 pretrained and customer-trainable ML models, with the ability to block sensitive text- and file-based data transfer to GenAI apps. Inline DLP controls are available for over a hundred GenAI apps.
Threat Protection*	Blocks malicious URLs and files in GenAI responses with zero trust. Takes advantage of high-fidelity alerts and GenAI-specific reporting for security inspections available via a unified command center and data map with integrated threat detection.
End-User Notifications	Coach end users when unapproved apps are accessed or if sensitive data is detected. End-user notifications are natively integrated with Slack, Microsoft Teams, and email. Admins can implement trigger exemptions and business justification workflows to improve the end-user experience.
Executive Reports	Enables end users to view and download executive reports that provide observability and explainability into GenAI usage and its associated risks.
Best Practice Recommendations	Provides contextual real-time recommendations for policy configurations based on industry best practices and traffic insights. Recommendations, delivered via Strata Copilot™, help configure more effective access, data, and security policies.
Flexible Deployment	Integrates natively with the Palo Alto Networks Strata® network security platform to work alongside all major data loss vectors—including email, browsers, SaaS, cloud, and endpoints (managed and unmanaged). AI Access Security can be deployed via hardware NGFWs, a secure browser, or secure access service edge (SASE)-native cloud architecture with Prisma Access.
User Experience	Strata Cloud Manager with a centralized Data Risk Command Center and asset manager provides holistic visibility and management. It streamlines data and security operations, accelerates incident response, and reduces ongoing costs for faster time to value.
Integrations	The OpenAI Compliance API integration enables scanning of data at rest in ChatGPT Enterprise. It scans conversations (prompt input and responses) for sensitive data at-rest, inspects responses to protect against malware and threats, and monitors interactions with marketplace GPT apps for sensitive data exposure. Admins can also monitor overly permissive sharing of custom-trained GPTs to secure sensitive training data.
Unified Console	Strata Cloud Manager or Panorama®

* AI Access Security leverages Precision AI® security services delivered via NGFW, Prisma Access Browser, and/or Prisma Access to provide threat protection.

Low Friction. High Confidence. Strong Security.

In today's interconnected digital world, uncovering hidden dangers and securing users and data across all GenAI apps and platforms is paramount. AI Access Security—an extension of Palo Alto Networks SaaS Security solution—reduces data and security risks across all GenAI apps. It also simplifies management, reduces complexity, and ensures sensitive data remains protected regardless of where it resides or how it's accessed.

Global Customer Services

Global Customer Services delivers the guidance, expertise, and resources necessary for maximizing the value of your investment. Professional Services, Customer Success, Support Services, ongoing education, and adoption tools ensure protection from intruders at every stage of your cybersecurity journey. Your Palo Alto Networks account manager can work with you to obtain the services that fit your needs.

Deploying a consistent and integrated GenAI solution—as part of a secure service edge (SSE) or SASE architecture—stops sophisticated cyberattacks, streamlines operations, and improves user experience. Securely connect your employees to the internet and all business-critical SaaS apps, including GenAI apps, with the highest level of security without compromise.

Connect with an expert to get a personalized demo of AI Access Security or try our interactive product tour.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com