paloalto NETWORKS | PRISMA

AI Access Security

Securing access to GenAI applications

GenAI Apps Need Rigorous Scrutiny for Data Uploads

Employees may **unknowingly share confidential data** when using GenAI apps.

Uploaded data can be used to train AI models, potentially compromising proprietary information or **leading to unintended data leak**.

Undetected GenAI Plugins May Lead to Unauthorized Data Access

Interconnected SaaS ecosystems with **AI-powered third-party integrations** create **security vulnerabilities**, **compli- cating detection and control**.

This leads to **increased risk of security breaches and non-compliance** with regulatory requirements.

paloalto NETWORKS | PRISMA

What's Needed to Secure GenAI App Adoption

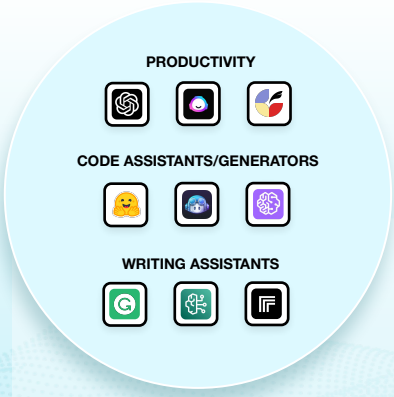
Challenges

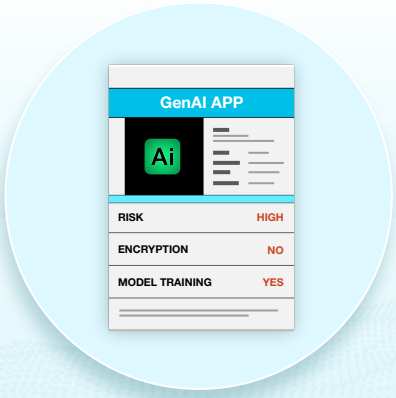
Democratization of AI app creation has led to sprawl of insecure apps.

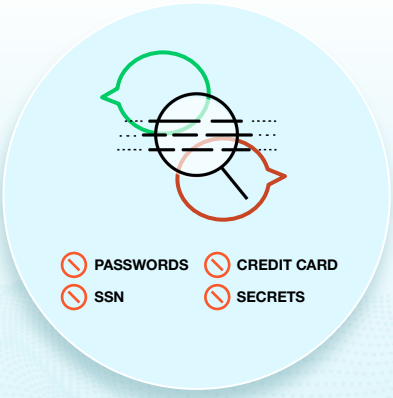
AI apps store, learn, and reiterate data.

AI apps ingest unstructured inputs and generate diverse outputs.

Rapidly evolving, powerful apps are readily accessible through marketplaces.







Comprehensive GenAI app catalog that keeps pace with the boom.

Visibility into AI apps that train on data.

Granular data controls with context-aware ML based detectors.

Ability to protect against threats in GenAI responses.

Visibility and control of 3rd-party AI plugins.

Detect plugins with excessive permissions.

Solutions

paloalto NETWORKS | PRISMA