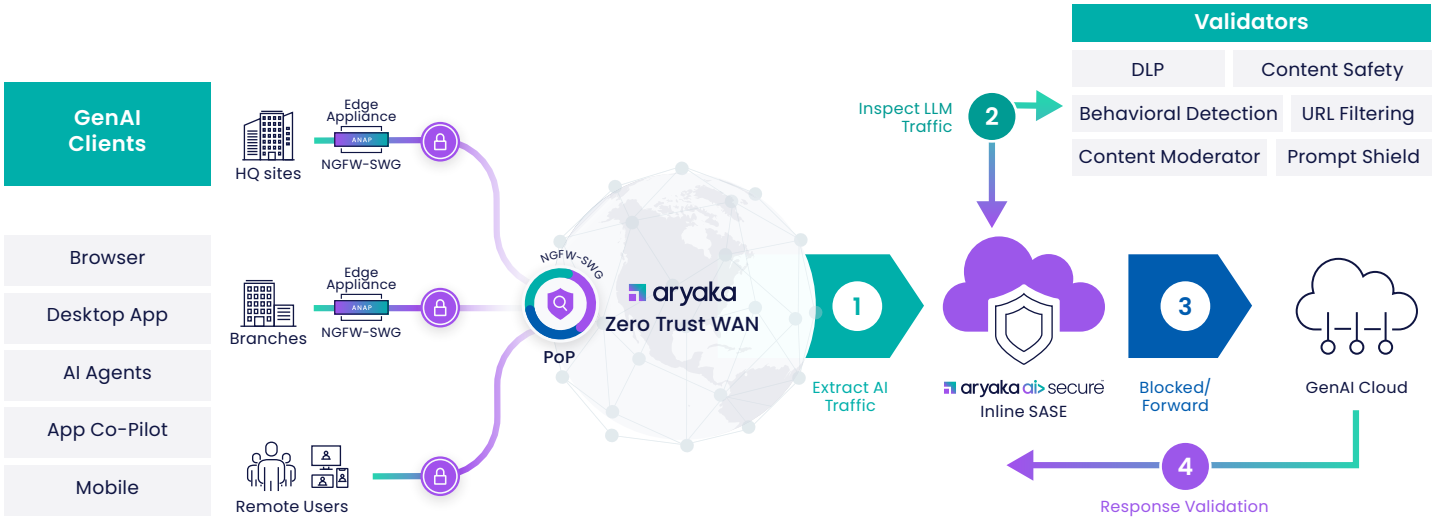
# aryaka ai> secure™

The rapid adoption of generative AI applications is transforming how enterprises operate-but it's also introducing a new wave of security challenges. Unapproved "shadow AI" tools are proliferating across departments, often without visibility or oversight, while sensitive data is at risk of leaking into external AI models through careless prompts or integrations.

At the same time, the emergence of a new AI-driven attack surface is giving adversaries fresh opportunities to exploit these technologies. Traditional security tools were never designed to secure GenAI workloads, leaving organizations blind to how these applications are used, what data they access, and where that data goes. Closing these gaps is essential to safely harness the power of AI without compromising security, compliance, or trust.

## Accelerating Enterprise with a Secure AI Future

Aryaka AI>Secure brings end-to-end protection to generative AI workloads by inspecting, validating, and securing every interaction as it traverses the Aryaka Zero Trust WAN. It eliminates the blind spots that traditional security tools leave behind, providing deep visibility into how AI applications are accessed, what data they touch, and where that data flows. With built-in policy enforcement and real-time traffic analysis, AI>Secure helps organizations prevent data leakage, detect malicious prompt injections, and maintain full control over sensitive information moving into and out of AI models.




| | | | |
|---|---|---|---|
| **Full visibility into AI activity** | **Shadow AI** | **Knowledge Loss Prevention/DLP** | |
| **Policy Enforcement** | **Privacy and Governance** | **Prompt Injection** | **Content Safety** |

Delivered through Aryaka Unified SASE as a Service, AI>Secure enables enterprises to embrace AI innovation without introducing new risks. It strengthens compliance by enforcing governance policies across all AI traffic, reduces the likelihood of costly breaches, and simplifies incident response with unified observability across networks, users, and applications. By combining security, visibility, and control into a single platform, Aryaka ensures that enterprises can confidently deploy AI technologies at scale—without compromising on trust, safety, or regulatory requirements.

## Use Cases

### Eliminating Shadow AI Across the Enterprise

- **What:** Identify and control unsanctioned AI tools and services being used by employees without IT or security oversight.
- **Why:** Shadow AI creates major visibility gaps, increasing the risk of sensitive data exposure, compliance violations, and unmonitored data flows.
- **Outcome:** Organizations gain full visibility into all AI usage, can enforce policies to block or allow tools safely, and dramatically reduce the risk of unapproved AI services introducing vulnerabilities.

### Preventing Knowledge Leakage into Public AI Models

- **What:** Detect and block sensitive or regulated data before it's shared with external generative AI platforms through prompts, integrations, or outputs.
- **Why:** Once leaked, proprietary information or customer data cannot be retracted, potentially causing regulatory penalties, IP loss, or reputational harm.
- **Outcome:** Enterprises proactively protect confidential data, maintain compliance with global regulations, and ensure sensitive information never leaves their controlled environment.

### Defending AI Applications from Prompt-Based Attacks

- **What:** Monitor and secure interactions with AI applications to prevent prompt injection, jailbreak attempts, and other emerging GenAI-specific threats.
- **Why:** These attacks can manipulate AI behavior, bypass safety guardrails, or extract sensitive data, putting both users and systems at risk.
- **Outcome:** Enterprises secure their AI workloads against manipulation, maintain trust in AI-driven processes, and safely scale GenAI initiatives without compromising security.

## Key Capabilities

| Area | Feature | Description |
|---|---|---|
| | | **Aryaka Next-Gen Data Loss Prevention (DLP)** |
| Security | **OnePASS™ Architecture** | Aryaka inspects traffic once, applying URL filtering, DNS security, IPS signatures, anti malware scanning, application control and DLP evaluation in a unified process that adds negligible latency. |
| | **Deployment and Traffic Interception** | AI/LLM client traffic is intercepted by the AI Secure Gateway, an instance/per customer that is deployed and managed by Aryaka in public cloud environments such as AWS, GCP. |

| | | |
|---|---|---|
| Security | **Gen AI App Discovery and Classification** | Automatically discover and map all sanctioned, unsanctioned & tolerated AI applications/tools/plug-ins being accessed. Provide clear insights into AI application usage across the organization. |
| | **Advanced Contextual Analysis** | Using AI-powered named entry recognition (NER), Next-Gen DLP identifies and categorizes sensitive entities like names, locations, or credit card numbers, and other PII. |
| | **AI Threat Detection and Response** | Block malicious input/output such as URLs and files in GenAI prompts/responses. Coach end users when unapproved apps are accessed or if sensitive data is detected. Protects enterprise AI chatbot/agent interactions from malicious prompts. |
| | **AI Usage Access Controls** | Safeguard sensitive data through real-time monitoring, ensuring compliance with organizational policies. Prohibit the upload of private or sensitive information to public AI applications to prevent data leaks. |
| Management | **Unified Observability** | Security events (policy hits, IPS alerts) and asset data are presented in a common UI over MyAryaka. |

## Technical Specifications

| Category | Details |
|---|---|
| PoP Security Stack | NGFW, Secure Web Gateway, DNS Security, IPS, Anti Malware, CASB, Next-Gen DLP, and Universal ZTNA - all orchestrated in a single pass architecture. |
| Compliance Coverage | Aryaka Unified SASE as a Service aligns with ISO 27001, PCI DSS, HIPAA, and GDPR requirements. |

## Licensing

Aryaka AI>Secure is available as add-on service to Aryaka Unified SASE as a Service and three deployment service plans. The add-on service has two types of licenses to meet different deployment needs: site licenses and remote user licenses. Site licenses are used to enable AI>Observe service at a specific location.

| Security Service | Prerequisite | Entitlement Upon Subscription |
|---|---|---|
| AI>Secure | Aryaka SD-WAN | All Aryaka SD-WAN features |

## Aryaka SD-WAN Features

- Secure SD-WAN
- Global Connectivity
- Multi-Cloud
- WAN Optimization
- AI> Perform
- Secure Remote Access

## Aryaka Unified SASE Features

- NGFW-SWG
- IPS
- Anti-Malware

## Aryaka Advanced Security Features

- CASB
- Next-Gen DLP

## About Aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com.

Schedule a Free Network Consultation with an Aryaka Expert

See How It Works Live

+1.888.692.7925 | info@aryaka.com