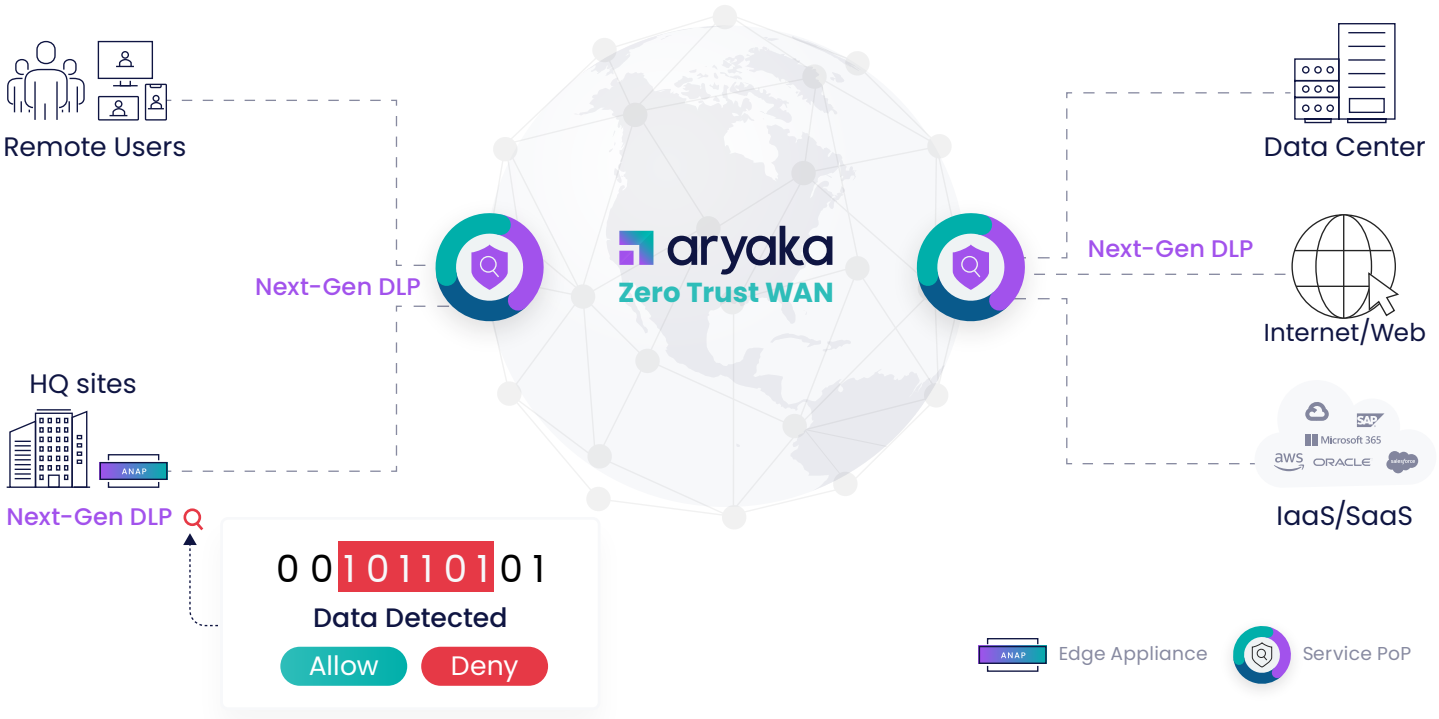
Aryaka Next-Gen DLP

The Overview

Data leakage, whether intentional or not, has become a critical risk in today's hybrid, cloud-first world. Employees routinely share sensitive information across SaaS applications, cloud platforms, Gen AI workloads, large language models (LLMs), and remote networks, making it increasingly difficult to maintain visibility and control. Left unchecked, data leakage can trigger regulatory fines, intellectual property loss, reputational damage, and diminished customer trust. At the same time, inconsistent security controls slow down response, increase compliance exposure, and strain already limited security resources.

Safeguarding Data with Advanced Data Loss Prevention

Aryaka Next-Gen DLP is an advanced data loss prevention capability built directly into the Aryaka Unified SASE as a Service platform. It goes beyond traditional pattern matching by applying AI-powered natural language processing, contextual analysis, and granular policy tuning to safeguard sensitive data wherever it moves—across applications, networks, users, and locations. By embedding this intelligence into a single, cloud-delivered framework, enterprises can eliminate gaps created by siloed tools and ensure consistent protection for both remote and on-site users.



With Aryaka Next-Gen DLP, organizations gain real-time visibility into sensitive data flows and the ability to block leakage before it happens, rather than after an incident is detected. This proactive approach not only strengthens compliance with evolving regulations but also reduces operational overhead by streamlining policy enforcement and reporting. The result is a stronger security posture, fewer manual processes for security teams, improved workforce productivity, and minimized risk of financial penalties or reputational harm.

Use Cases

Protecting Customer PII in SaaS Applications

- **What:** Monitor and control the transfer of personally identifiable information (PII) across SaaS platforms like Salesforce, Office 365, and ServiceNow.
- **Why:** Accidental or unauthorized exposure of PII can result in regulatory fines, reputational damage, and loss of customer trust.
- **Outcome:** PII is automatically identified and safeguarded in real time, ensuring compliance with GDPR, HIPAA, and other global regulations while maintaining customer confidence.

Safeguarding Intellectual Property in Hybrid Work

- **What:** Detect and block attempts to share sensitive design files, source code, or proprietary documents via email, collaboration tools, or unmanaged devices.
- **Why:** With distributed teams and hybrid work, intellectual property is more likely to leave controlled environments—intentionally or accidentally.
- **Outcome:** Critical business IP stays protected, reducing the risk of competitive loss while enabling secure collaboration across geographies.

Preventing Data Exfiltration by Malicious Insiders

- **What:** Identify and stop unauthorized attempts to upload large volumes of confidential files to personal cloud accounts or removable storage.
- **Why:** Insider threats remain one of the hardest risks to mitigate, as trusted employees already have access to sensitive data.
- **Outcome:** Suspicious activity is flagged and blocked before data leaves the organization, protecting against financial loss, brand damage, and legal exposure for compliance and operations.

Compliance and Audit-Ready Operations

- **What:** Enforce consistent DLP controls and produce audit evidence across regions/tenants. Centralize policies; apply masked-at-ingestion evidence, data residency, retention windows, and export controls (metadata-only). Govern access with RBAC.
- **Why:** Regulators and DPAs require demonstrable controls and minimal sensitive data in operational logs. Fragmented tools slow audits and raise exposure.
- **Outcome:** Faster audits and fewer findings: standardized reports mapped to GDPR/HIPAA/PCI, immutable audit logs, and one-click audit packs. Reduced compliance risk without sacrificing analyst effectiveness.

Key Capabilities

Area	Feature	Description
		Aryaka Next-Gen Data Loss Prevention (DLP)
Security	**OnePASS™ Architecture**	All Aryaka SD-WAN and Unified SASE features plus CASB (see below)
	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.
	EDM Data Classification	Detects sensitive information by comparing against secure, hashed databases of known sensitive data records. Results in highly accurate identification and fewer false positives
	Image Based Detection	Enables the extraction of text from images or document formats for identification and categorization, including PNG, JPEG, TIFF, BMP, PNM, WEBP, PDF and JPEG2000.
	API Request Detection	Able to scan and detect both API request and response bodies for sensitive information, including APIs accessing LLMs.
	General Detection	Able to detect, read, categorize, and enforce against data in motion, archived files, compressed files, and many others.
	Redaction and Masking	Protects data through sensitive data removal and masking, including full text redaction, partial field masking, and inline traffic redaction.
	Policy Enforcement	Support actions per detection match result: Permit, Drop, Log Only, Redact, Masking & Skip. Additional granular enforcement capabilities for SaaS are available when enabled with CASB.
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

Next-Gen DLP has two types of licenses to meet different deployment needs: site licenses and user licenses. Site licenses are used to enable Next-Gen DLP at a specific location. User-licenses are used to enable Next-Gen DLP services for remote users.

Security Service	Prerequisite	Entitlement Upon Subscription
Next-Gen DLP	Aryaka Advanced Security	All Aryaka SD-WAN and Unified SASE features plus CASB (see below)

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