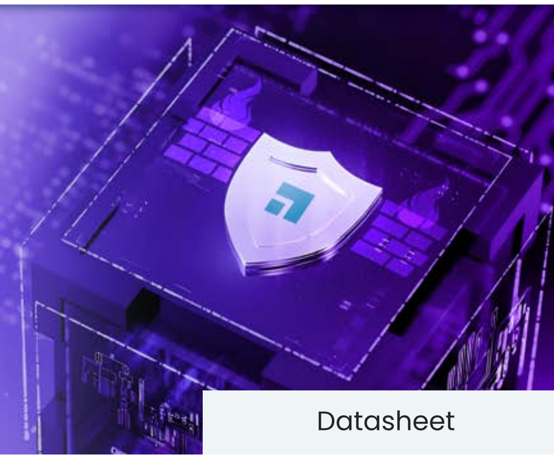
Aryaka SmartSecure NGFW-SWG, Anti-Malware, and IPS Datasheet



Datasheet

Enterprises have moved away from traditional hub-and-spoke architectures where network security was focused on safeguarding the network perimeter—the boundary between the trusted internal network and the untrusted external network. In today's landscape, enterprise users and workloads are highly distributed due to a surge in cloud adoption, SaaS usage, and a hybrid workforce model. Enterprises must also cope with an increasing number of sophisticated cyberattacks. Threat actors are constantly finding innovative ways to exploit enterprise IT infrastructure and compromise its data and digital assets.

In this dynamic and distributed environment, it is important to ensure that both remote and branch users experience peak application performance and have secure access to applications, data, and the internet. To address these networking and security needs, enterprises must rely on multiple-point solutions that increase operational complexity, present management challenges, and raise costs. Enterprises are looking to transition from conventional product-centric solutions to a cohesive as-a-service model.

Aryaka Unified SASE with Single-Pass Architecture

Aryaka Unified SASE combines networking and security into an as-a-service ('all-in-one') solution that helps enterprises modernize their infrastructure. This solution allows an enterprise to configure, manage, and observe its network, security, applications, and users, all through a single management console without having to rely on disaggregated single-point solutions for each function independently. A defining feature of the Aryaka Unified SASE solution is its single-pass architecture that allows enterprises to perform comprehensive inspections and processing, while examining a given data packet only once. This approach reduces the attack surface and minimizes latency that would otherwise result from processing individual functions separately.

Aryaka has built an integrated architecture that offers a hybrid deployment solution to meet the needs of the enterprise for both on-premises and remote users. Security enforcement for workloads and users takes place directly at the edge appliance: either at the Aryaka Network Access Point (ANAP) for site users or at the Aryaka POP for remote users. Additionally, enterprises can benefit from our integrated lifecycle management support and managed services that offer a personalized experience for deployments and issue resolution 24/7. Aryaka plans to incorporate additional capabilities and features in the future, all seamlessly integrated into our single-pass architecture.

Use Cases

The Aryaka SmartSecure NGFW-SWG (Next Generation Firewall- Secure Web Gateway) strategy is to allow enterprises to replace traditional multi-vendor networking and security services with a unified platform from a single vendor. The primary focus is described in the following two distinct use cases:

1. Replace Third-Party-On-Prem-Premises Firewall with Aryaka NextGen Firewall

The first use case is replacing an enterprise's existing on-premises firewall from a third-party security vendor with our natively built Aryaka solution. To accomplish this, Aryaka has built a dedicated security stack on top of our Software Defined Wide Area Network (SD-WAN) architecture that applies a common framework to a series of security policy engines.

Many vendors must tunnel traffic to POPs for security inspections. Aryaka can inspect traffic on the ANAP itself for on-premises users. Policy engines perform Next Generation Firewall and Secure Web Gateway (NGFW-SWG) security inspections, ensuring traffic is only sent to its intended destination when required. Both inbound and outbound traffic undergoes thorough examination for both pre-SSL and post-SSL data flows for the connections initiated from the LAN interface. In this use case, internet breakout occurs at the ANAP.

2. Replace Cloud-Native Secure Web Gateway Vendors

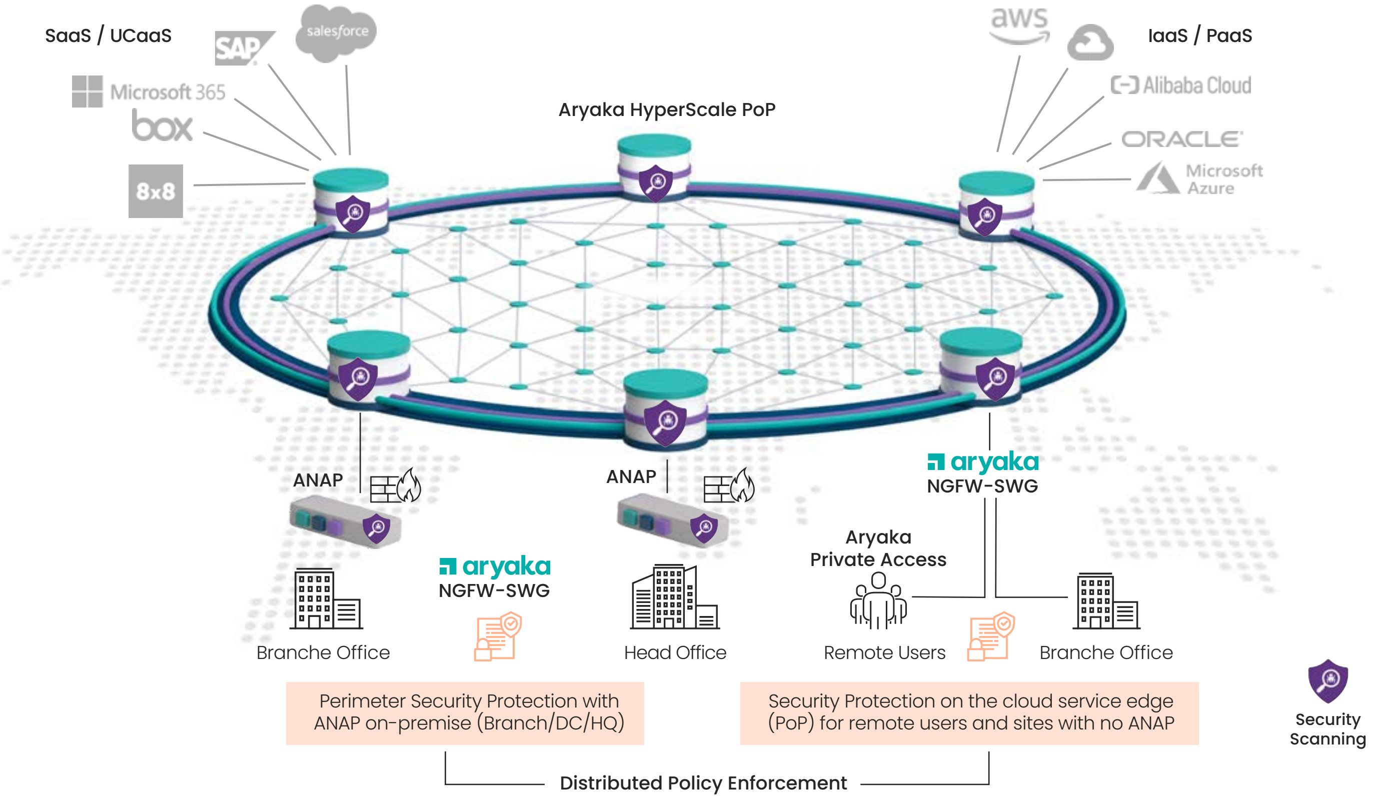
The second use case is replacing an enterprise's cloud-based Secure Internet Access (SIA) or Secure Web Gateway (SWG) vendors with Aryaka's natively built security stack on both POPs and ANAPs. The Aryaka NGFW-SWG protects web-based and SaaS application users from internet-borne threats.

Using our POP-centric cloud service delivery, Aryaka offers comprehensive security directly from the POP to remote users who access enterprise resources and cloud applications using the Aryaka VPNaaS client. This ensures secure connectivity for direct connections from headquarters and branch offices that do not have an ANAP within a cloud-as-a-service model. In these scenarios, internet breakout occurs at the POP. The ANAP and the POP both host identical security stacks to secure enterprise users and workloads from modern internet-borne threats. This ensures a consistent user experience whether the user is on-premises or remote. User licenses are used to provide NGFW-SWG security services to private access users.

Key Highlights

- Cloud-Native Unified Platform
- Single-Pass Architecture
- Secure Branch & Remote Access
- Secure Internet Access
- Secure Cloud Access
- Distributed Policy Enforcement
- Operational Simplicity
- Unified Management & Observability
- Lifecycle Management Support Services 24/7

The following graphic depicts distributed policy enforcement on Aryaka POPs and ANAPs. Security scanning occurs at the service edges to protect both on-premises and remote users.



Key Differentiators

Single-Pass Architecture

The Aryaka single-pass architecture processes network and security policies in a single pass, without the need for a packet to go through multiple security processing stages that can introduce latency and increase processing requirements. We process a packet once and only perform one TLS inspection across the entire packet flow.

Our management interface—MyAryaka— provides dashboards, analytics, observability, management, and monitoring for all networking and security services. Telemetry is collected in near-real time from all security engines and provides insights into security incidents, threat management, and performance. Using our intuitive interface, enterprises have the flexibility to self-manage security policies and create access controls without having to switch between multiple management consoles.

Our unified control plane combines networking and security capabilities to provide consistent policy enforcement on the ANAP, the POP, or both. This protects the enterprise's users wherever they are.

The distributed data plane allows for policy enforcement at the nearest POP and at the ANAP edge, allowing security enforcement to happen closer to the source. For enterprises with site users behind an ANAP, network, security and application processing are performed at the ANAP itself. For private access users and enterprise sites without an ANAP, traffic is processed at one of our 40+ globally distributed hyperscale POPs that reach 95% of the world's business population across six continents (including China).

Multi-Table Policy Management

The conventional approach to policy management places all security policies into one complex table. This approach leads to confusing and error-prone configurations, a degraded user experience, cumbersome policy management, and complicated troubleshooting that increases the risk of security breaches. Our modular, multi-table approach to policy management includes multiple security engines, each with distinct security functions such as threat protection, reputation services, and application- and user-based access controls. Each security function has its own set of policy configurations, match criteria, and policy actions. With our approach, enterprises can benefit from ease of maintenance, operational simplicity, and the flexibility to create granular policies for pre-TLS, pre-SSL, and post-SSL traffic.

Aryaka SmartSecure Services

1. Aryaka SmartSecure Next Generation Firewall – Secure Web Gateway (NGFW-SWG)

2. Aryaka SmartSecure Anti-Malware Add-on

3. Aryaka SmartSecure Intrusion Prevention System (IPS) Add-on

1. Aryaka SmartSecure NGFW-SWG

The NGFW-SWG is an integral component of the Aryaka SASE solution. It is a natively built, easy to use, managed solution that combines NextGen Firewall and Secure Web Gateway security services into a single unified service. The primary objective of the Aryaka SmartSecure NGFW-SWG is to protect users from internet-born threats and evolving cyber threats. It achieves this by intercepting user traffic and applying various security controls to network traffic. The Aryaka SmartSecure NGFW-SWG performs deep packet inspection (DPI) that thoroughly examines the actual content of the data payload for inbound and outbound traffic associated with connections originating from LAN interface.

2. Aryaka SmartSecure Anti-Malware Add-on

The optional Aryaka SmartSecure Anti-Malware service provides an additional layer of defense that enhances enterprise security by detecting known malware, viruses, and file-based threats for inbound and outbound traffic. The Anti-Malware security engine performs DPI to evaluate network traffic against a database of known malware signatures and patterns. If a match is found, the event is logged for further forensic analysis.

3. Aryaka SmartSecure Intrusion Prevention System (IPS) Add-on

The optional Aryaka SmartSecure IPS service includes security engines that inspect inbound traffic on the WAN interface and outbound traffic on the LAN interface. This encrypted and unencrypted traffic is continuously monitored for malicious intrusion activities using a signature-based detection mechanism that intercepts user traffic and applies various IPS policies to the data packets. Both branch and remote users are protected and monitored for potential intrusions across 53 categories including those related to Trojans, worms, shellcode exploits, adware, and more.

Feature List

All Aryaka SmartSecure features are made available to branch and private access users through site and user licenses. Aryaka SmartSecure Anti-Malware and Aryaka SmartSecure IPS are offered as add-on services in two regions: Mainland China and Rest of the World (ROW). Enterprises can choose either or both options as required. Aryaka plans to offer additional features as our security service evolves.

1. Aryaka SmartSecure NGFW-SWG

2. Aryaka SmartSecure Anti-Malware Add-on

3. Aryaka SmartSecure Intrusion Prevention System Add-on

4. Aryaka SmartSecure NGFW-SWG, Anti-Malware Add-on, and IPS Add-on

Features	Description
1. Aryaka SmartSecure NGFW-SWG	
Domain Reputation	Protects users from malicious domains using reputation scores for more than 750 million domains. For HTTP traffic, domain names are extracted from HTTP headers. For HTTPS traffic, domain names are extracted from “Server Hello” message during the SSL/TLS handshake.
URL Reputation	Protects users from accessing malicious URLs using reputation scores for more than 32 billion URLs.
IP Reputation	Restricts users from accessing malicious IPs using IP reputation verdicts (Good or Bad) for more than 4.3 billion IPs (includes all IPv4 and in-use IPv6).
Category-based Filtering	Simplifies policy management by grouping overarching web categories and enforcing policies to permit or deny traffic based on these predefined categories.
Application-based Access Control (Basic CASB)	Aryaka’s inline CASB identifies and classifies network traffic and applications using Deep Packet Inspection (DPI), then applies access controls to the sanctioned and unsanctioned applications that are discovered.
DNS Filtering	Inspects DNS queries and responses to permit or deny access to specific websites based on the domain and IP reputation scores. If non-DNS protocol messages arrive on port 53, the packets are automatically discarded.
Web Access Control	Provides access control for post-SSL traffic, including matches against HTTP headers for both HTTP and HTTPS traffic. HTTP headers can be saved as reusable assets that security policies can reference.
Network Access Control	Provides access control for pre-SSL traffic. Traffic can be permitted, denied, or allowed to skip to all subsequent processing engines.
Identity and Access Management (User-based Access Control)	Allows enterprises to connect to third-party identity providers (IdPs) or use Aryaka as the IdP. Supported IdPs are Enterprise LDAP, on-premises AD, Okta, Azure AD, and Aryaka DB. Azure AD and Okta are based on SAML and OIDC authentication standards. The IdP redirects the user to the captive portal for authentication and authorization. Unauthorized users are redirected to customized block pages.

Features	Description
2. Aryaka SmartSecure Anti-Malware Add-on	
Malware Protection	Provides an additional layer of defense and frees up bandwidth by detecting known malware of all types and dropping the malware at the on-premises and cloud edges. Aryaka consistently updates its edges with the latest threat intelligence to effectively stop the distribution of emerging threats.
File-based Threat Protection	Scans file contents and makes dynamic, byte-by-byte determinations based on the file reputation while the content is being downloaded or is in transit on a network. Industry-standard MD5 file hashes are used as fingerprints to uniquely identify files regardless of filename, platform, and encryption. High-speed file processing ensures no impact to the end-user experience.
Anti-Virus (AV) Protection	Prevents virus infections by consulting automatically updated indicators of compromise (IOC) and signatures from a threat intel database.
3. Aryaka SmartSecure Intrusion Prevention System Add-on	
Signature-based Detection	Continuously inspects WAN and LAN interfaces encrypted and unencrypted traffic for malicious intrusion activities using signature-based detection. Potential threats are blocked before they can harm digital assets.
Packet Anomaly Detection	Identifies protocol deviations from expected standards based on signatures, then alerts system administrators to perform remediation.
Common Vulnerability Exposure (CVE) Protection	Reduces an enterprise's attack surface by mitigating known vulnerabilities and exploits.
Command & Control (Botnet) Protection	Detects and blocks communication with C2 servers and botnet activities to protect internal assets.
DoS and DDoS Protection	Uses signature-based detection and rate-limiting mechanisms to prevent downtime by protecting enterprise network assets from DoS and DDoS attacks.

Features	Description
4. Aryaka SmartSecure NGFW-SWG, Anti-Malware Add-on, and IPS Add-on	
SSL/TLS Inspection and Decryption	Detects attacks in encrypted and unencrypted traffic using dynamic certificate generation with the option of selectively decrypting packets based on the sensitivity of personally identifiable information (PII). To better detect anomalies in encrypted traffic, TLS inspection is used to decrypt packets. Packets are then re-encrypted after the inspection is complete.
Centralized Management	Allows you to define SD-WAN and security policies consistently across distributed network and cloud resources.
Real-time Threat Insights	Delivers visibility and observability of security events and threat insights using the Aryaka unified console.
Security Reports and Analytics	Provides comprehensive summary reports and graphs of an enterprise's threat landscape over a configurable time period.
Alerting	Notifies administrators about security events for rapid incident response.
Logging	Creates and updates security logs with useful information about the event for debugging purposes.
Self Service	Provides enterprises with the flexibility to configure and self-manage security policies in the MyAryaka user interface.

**Aryaka security services will continue to evolve, including more services.*

Licensing

NGFW-SWG, Anti-Malware, and IPS services have two types of licenses to meet different deployment needs: site licenses and user licenses. Site licenses are used to enable NGFW-SWG, Anti-Malware, and IPS services at a specific location. User licenses are used to enable NGFW-SWG, Anti-Malware, and IPS services for remote users.

Security Service	Prerequisite	Entitlements Upon Subscription
NGFW-SWG*	Aryaka SD-WAN or Aryaka SmartSecure-Private Access	FWaaS and NGFW-SWG security features
Anti-Malware Add-on	Aryaka SD-WAN or Aryaka SmartSecure-Private Access and NGFW-SWG	FWaaS, NGFW-SWG, and Anti-Malware Add-on security features
IPS Add-on	Aryaka SD-WAN or Aryaka SmartSecure-Private Access and NGFW-SWG	FWaaS, NGFW-SWG, Anti-Malware, and IPS Add-on security features

**NGFW-SWG site licenses are offered in the same tiers as site licenses (XS, S, M, M+, L, XL, and BYO).*

Key Business Outcomes and Benefits

Global, Scalable, and Flexible

Receive comprehensive security for any user, anywhere, anytime. With 40+ POPs, Aryaka can accommodate enterprise growth, changes in demand, and can adapt to unique operational needs.

End-to-End Connectivity with One Vendor

Maintain a single point of contact for networking and security services with Aryaka's as-a-service solution.

Consistent Protection Everywhere

Offer uniform security for both on-premises and remote workers with networking and security tied together under a common security policy framework.

Operational Simplicity

See a reduction in the complexity, overhead, and training required to deploy and maintain a multi-vendor network and security solution with Aryaka's unified management console—MyAryaka.

Superior User Experience

Deliver speed and seamless access to applications while securing data in transit and at rest.

Lower Total Cost of Ownership (TCO)

Reduce costs by eliminating the burden of sizing, purchasing, installing, upgrading, patching, and managing multiple-point hardware and software solutions in a complex, ever-changing threat environment.

aryaka

☎ +1.888.692.7925

✉ info@aryaka.com

About Aryaka

Aryaka is the leader and first to deliver Unified SASE as a Service, the only SASE solution designed and built to deliver performance, agility, simplicity and security without tradeoffs. Aryaka meets customers where they are on their unique SASE journeys, enabling them to seamlessly modernize, optimize and transform their networking and security environments. Aryaka's flexible delivery options empower enterprises to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for cloud-based software-defined networking and security services. For more on Aryaka, please visit www.aryaka.com.