aryaka

Aryaka SmartSecure

Secure Web Gateway (SWG)

Datasheet

Unified SASE

Enterprises have adopted a cloud-first posture and have moved away from traditional hub-and-spoke architectures with an on-premises data center hosting applications and data. With an increase in cloud usage and a hybrid workforce model, where users access applications from anywhere, anytime, the role of data centers is diminishing. Organizations are converting the consumption of products into an "as-a-service" model, including networking, security, data protection, data in transit, and data at rest. With a hybrid workforce, organizations must be more cognizant about how they secure communication and connectivity to corporate applications and how and from where users access corporate and internet-based applications.

In such a distributed environment, secure Internet access is a must-have for organizations, ensuring hybrid users can access the Internet in a secure and controlled way, no matter where they are, at the office, from home, or on the go.

A traditional multi-vendor approach to this challenge is no longer scalable and often leads to failed security solutions. It requires expertise to maintain and operate multiple solutions for IT teams, which is in short supply, adding complexity and exposing an organization to security threats. Furthermore, traditional web-proxy solutions deploy multi-vendor solutions to protect different aspects of security for Web access for corporate users like Web gateways appliance, Malware/Content analysis, Firewall (NGFW), IDS/IPS, and DLP are among the required features to secure and protect an organization.

Customer Challenges	
Enterprises are adopting a cloud-first posture and moving away from traditional hub-and-spoke architectures that require a secure and high-performance connection to the public Internet.	
Complexity	**Inflexibility**
Legacy WAN architectures based on MPLS are not cloud-native and add additional complexity and cost.	Traditional edge security solutions require additional hardware and software and don't offer connectivity flexibility.

A distributed, cloud-based architecture with centralized orchestration and management enables security to converge with networking and offers a seamless, one-stop solution allowing for full Observability for both networking and security behaviors with simplified and fast change management. This is the approach Aryaka takes.

Aryaka Secure Internet Access

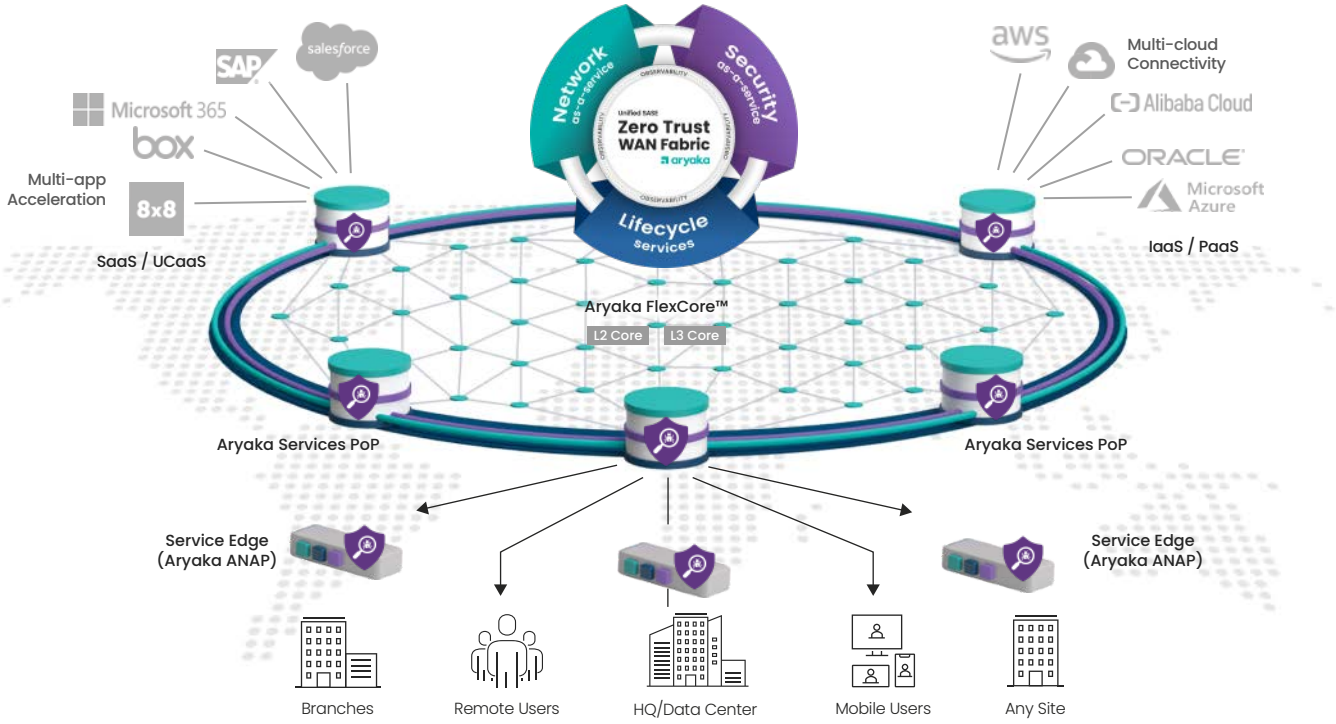
It is a comprehensive, integrated approach to delivering secure connectivity without compromising application performance based on a Unified SASE architecture.

Aryaka's secure internet access solution offers enterprises the best combination of internet connectivity and transport across the Aryaka middle mile - a private dual-core backbone consisting of layer 2 and 3 networks. It is a flexible architecture that includes a virtual NGFW at the edge and hand-offs to cloud security gateways, while Aryaka's SmartSecure SWG delivers the required flexibility for any enterprise WAN deployment.

Virtualized firewalls hosted on Aryaka's managed SD-WAN CPE, the ANAP, leverage partnerships with both Check Point and Palo Alto Networks, are ideal where an on-premises solution is mandated. Alternatively, advanced cloud security consisting of threat prevention, data protection, and access control is enabled through our partners Zscaler, Palo Alto Networks, Symantec, Cisco Umbrella, and Check Point. A third option leverages Aryaka's Secure Web Gateway capabilities deployed globally on our services POPs. Here, all traffic benefits from Aryaka's sophisticated last-mile optimization.

Aryaka SmartSecure services for Aryaka Secure Web Gateway includes Access Control, Threat Prevention, Configuration Management and Observability. The detailed features of each element is listed in table 1 of this datasheet. The initial capabilities focus on a Secure Web Gateway for both Site-to-Internet and User-to-Internet traffic. As shown in table 1, more features will be added over time to our SWG solution. These features are in addition to best-in-class security across the Aryaka core network and Aryaka's managed CPE edge appliance, the ANAP.

Aryaka Unified SASE



Benefits of Aryaka's Converged Approach

Digital and Cloud adoption has driven organizations to shift to an 'as-a-Service' consumption, frequently combined with a co-/fully managed service delivery, replacing complex and resource-intense CAPEX deployments with a simplified, on-demand OPEX model.

Benefits

Application Acceleration

Experience fast access to mission and business critical applications hosted locally or in the cloud, from both branches and remote offices.

Advanced Security and Centralized Management

Deliver comprehensive security and data protection for enterprise and web traffic, coupled with central definition and enforcement of security and access policies.

Visibility

Enjoy complete visibility on application usage and performance across both the Aryaka and cloud security services.

Reduced Hardware Footprint

Eliminate the need for additional security and optimization appliances with HybridWAN capabilities to connect to both the Aryaka core as well as to cloud security gateways.

Rapid Deployment

Configure, deploy, and activate new sites in days instead of weeks or months, positively impacting enterprise productivity.

White-Glove Services Experience

An unequalled customer support experience based on a virtuous cycle of people, processes, and technology is combined with end-to-end performance SLAs.

Aryaka Secure Web Gateway (SWG)

Aryaka's Secure Web Gateway, a cloud-based Internet gateway, acts as middle protection for Site-to-Internet and User-to-Internet traffic, providing full protection for web and internet-based attacks.

Access Control & Threat Prevention

Cloud Firewall	URL Filtering	Full/Bypass SSL Inspection
Security policy control/Inspection at Layer-3/ Layer-4 with ports/protocols including identity-aware enforcement for allow/deny.	Automatically categorizes webpages based on URL categorization with a built-in URL database. Granular policy control for users/user-groups for in-depth visibility.	Full inline inspection of the encrypted traffic for visibility, protection, and control with enhanced ability to bypass SSL inspection.

Hybrid Workers	Application Identification & Control	Analysis, Reporting, and Logs
Consistent Security policy and enforcement for hybrid workers regardless of location.	Control and visibility into sanctioned/unsanctioned applications. Includes more than 3500+ predefined native support for application identification and the option to add custom applications. *	Available via a centralized cloud-managed portal for visibility into real-time flow logs, event logs and log exports for offline to external SIEM.

Security and User Experience	User Identification & Control	Onboarding & Deployment
Identity/context-based traffic analysis for identifying threats/url/domain etc.	Security policy enforcement controlled by User/User-Group authentication using Active-Directory & SAML integration with 3rd party IDPs.	Flexible and white-glove service for onboarding and deployment for customers.

Cloud Portal Management
Aryaka SWG can be accessed, configured, controlled, and monitored via MyAryaka, our web-based and cloud-delivered portal. Cloud-delivered and management benefits increase operational efficiency and ensure simple workflows; managed, updated and maintained by Aryaka Team.

** Available today on ANAP, cloud-service is a roadmap item*

SWG - Secure Web Gateway Internet Access Solution with Complete Security and Visibility.

Features	SWG (GA)
Service Access	
Secure Web Gateway access from sites with an ANAP	✓
Secure Web Gateway access from sites without an ANAP	✗
Secure Web Gateway access for Private Access users - VPNaaS	✓
POP High Availability (HA) for sites	✓
Access Control	
User-based Access control	✓
Authentication & Authorization *Integration with Active-Directory & SAML-based authentication*	✓
Inline SSL Inspection	✓
SSL Bypass option	✓
URL Filtering *Based upon web-categories and URL definition*	✓
Firewall-as-a-service-L3/L4	✓
Firewall-as-a-service-application-aware	✗
User Behavior and Analytics	✗
Device Posture Assessment	✗
Deep Packet Inspection: Aryaka CPE (ANAP) *Application Identification & Control*	✓

Threat Prevention	
Antivirus & Malware Scanning	✓
IDS & IPS	✗
Sandboxing	✗
DNS Security	✗
Configuration Management	
Managed Identity Services	✓
Cloud Managed SD-WAN Portal: MyAryaka	✓
Secure Web Gateway Portal	✓
Observability - Secure Web Gateway Portal	
Flow Logs Visibility	✓
Top Talkers Visibility	✓
Top Risky users Visibility	✓
Top Visibility for Users/User-activity/web-Threats	✓
Log export to external SIEM*	✓
Log Retention*	✓
Scheduled Reports	✗
Alerts and Notifications	✗
Application Health Analytics	✗

Table 1: Aryaka SmartSecure | Secure Web Gateway

*Log export to external SIEM and Log retention are not available before GA release version.

aryaka

+1.877.727.9252

info@aryaka.com

Aryaka, the Cloud-First WAN and SASE company, and a Gartner "Voice of the Customer" leader, makes it easy for enterprises to consume network and network security solutions delivered as-a-service for a variety of modern deployments. Aryaka uniquely combines innovative SD-WAN and security technology with a global network and a managed service approach to offer the industry's best customer and application experience. The company's customers include hundreds of global enterprises including several in the Fortune 100.

About Aryaka