aryaka

SmartSecure
Security-as-a-Service

Aryaka SmartSecure is designed to complement SmartConnect with managed SD-WAN Security-as-a-Service offerings.

- At the branch, an access firewall within the ANAP offers 'north-south' control, while an optional NFV-based Tier-1 managed firewall offers comprehensive L7 protection.
- **Aryaka Zones** extends this to the LAN with 'east-west' security, through site-segmentation with policy-based access. Together, the two capabilities segment WAN traffic, to Aryaka and to the internet, from LAN traffic, both internal and DMZ.
- The ANAP also supports **VRF-based micro-segmentation**, enabling multi-tenancy.
- Aryaka SmartSecure also extends security to the cloud through Aryaka's security partner ecosystem – including **Zscaler, Palo Alto Networks & Symantec.**

Core Capabilities

1.
Cloud Security

Secure, local Internet breakout is enabled through Palo Alto's Prisma Cloud Security Suite, Symantec's Web Security Service, and Zscaler's Cloud Security, protecting all ports and protocols without appliances.

2.
Micro-Segmentation

Micro-segmentation adds to the ANAP's zones functionality. On-site, VLANs provide the local segmentation for internal and DMZ zones. Micro-segmentation extends this across the Aryaka core network via a BGP-driven VRF 'lite' functionality.

3.
Virtual Firewall

Aryaka's ANAP supports NFV functionality for additional SDN-delivered services. We are partneriing with multiple Tier-1 security vendors, enabling choice.. Management of physical firewalls part of the SD-WAN deployment is also supported.

4.
Secure Remote Access

Aryaka's Secure Remote Access is the first clientless SD-WAN to software-defined remote access. It significantly enhances both on-premises and cloud/SaaS application performance for the remote and mobile workforce without requiring additional hardware or software clients.

5.
Aryaka Core Protection

In parallel, the Aryaka private core delivers partitioned connectivity to all enterprises, encrypting the data and protecting against DDoS attacks. Within the branch, enterprises have access to Syslog and Netflow logging, and at the network level, the MyAryaka cloud portal provides a single pane of glass for service configuration, monitoring and health.

6.
Edge Firewall

The ANAP includes a virtual stateful firewall that delivers north-south access protection as well as a 'zones' capability offering site-segmentation to secure east-west traffic within the branch. The ANAP aligns with the evolving Secure Access Service Edge (SASE), offering a choice of edge and cloud security.

Deployment Options

Remote Access

Secure Remote Access is an optional capability for both Global and Regional deployments

Aryaka + Zscaler

An enterprise may consume Zscaler's complementary cloud-based security-as-a-Service, with Aryaka directing traffic appropriately.
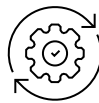
Aryaka + Palo Alto

Remote workers may access Aryaka via Palo Alto's Prisma Cloud Security Suite, providing authentication and acceleration

Benefits achieved by using Aryaka SmartSecure

Managed SD-WAN Security

With WAN security top-of-mind, Aryaka's SmartSecure offers enterprises an end-to-end secure infrastructure, first-mile, middle-mile, and into the cloud.

Operational Simplicity

Edge and cloud security leveraging Tier-1 partners is part of Aryaka's end-to-end managed SD-WAN, hiding complexity from the enterprise.
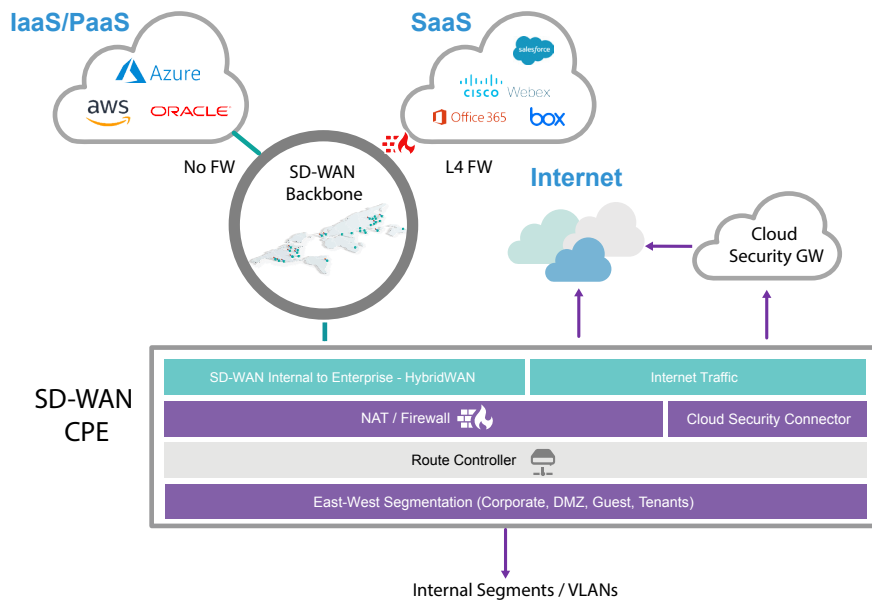
Lower TCO

SD-WAN security helps enterprises generate the maximum return on their SD-WAN investment, ensuring protection from external threats and the integrity of corporate data, anywhere in the world.

Aryaka's SmartSecure is aligned with the evolving Secure Access Service Edge (SASE) architecture. Our security offerings cover both the branch and the cloud, offering enterprises the choice of where to deploy their security based on individual requirements. Importantly, we plan a single operational model and feature set that spans both domains.

			Global	Regional
SmartSecure	Edge Essentials (Firewall, Micro-segmentation)	ANAP-based N-S and E-W access firewall; Branch micro-segmentation and multi-tenant support	Included	Included
	Virtual Firewall Hosting and Virtua;I/Physical FW Management	NFV FW on ANAP and management of enterprise physical and virtual firewalls	Optional	Optional
	Cloud Security Connector	Cloud-hosted security based on site capacity (Small/Medium/Large)	Included	Included
	Secure Remote Access	Global ExtraNET, Global VPN, or BYO VPN Concentrator	Optional	Optional

IaaS/PaaS

SaaS

No FW — SD-WAN Backbone — L4 FW

Internet

Cloud Security GW

SD-WAN CPE

SD-WAN Internal to Enterprise - HybridWAN	Internet Traffic
NAT / Firewall	Cloud Security Connector
Route Controller	
East-West Segmentation (Corporate, DMZ, Guest, Tenants)	

Internal Segments / VLANs

Secure Remote Access

Accelerate application performance for remote/mobile employees with the first clientless SD-WAN. Aryaka's Secure Remote Access significantly enhances both on-premises and cloud/SaaS application performance for the remote and mobile workforce without requiring additional hardware or software clients.

Up To 3X Faster Remote Access
Improve produtivity - Reduce complexity and cost

For Remote & Mobile Employees

- Accelerate both on-premises and cloud/SaaS application performance

- Access consistency fast data, voice and video from anywhere in the world

- Experiences fewer disconnects

- Use existing VPN client —no additional software required

For IT

- Simplify VPN infrastructure and reduce costs

- Gain end-to-end network and application visibility

- Enhance remote access security

- Deploy in hours globally without changes to security policy

Aryaka Security Architecture

The Aryaka Private Network delivers true multi-tenant data partitioning though virtualized compute, network, and storage resources. The resulting private backbone is more secure than competing MPLS services where customer traffic is not encrypted. This includes dedicated PoPs located in secured data centers, dedicated Layer 2 links, encryption with IPSec, key management, and DDoS protection. We manage this via a sophisticated orchestration platform, to ensure that your users have assured access to your vital applications and data, anywhere, and at any time.

Aryaka maintains a robust security program that meets internationally accepted security practices.
SOC 2: SSAE-16 Reports against Aryaka's policies and processes
Cloud Controls Matrix (CCM)
Consensus Assessments Initiative Questionnaire (CAIQ)
ISO27002 Framework
Third party network scan reports available within 48 hours upon request

About Aryaka Networks

Aryaka delivers the #1 fully-managed, end-to-end global SD-WAN service for the cloud-first era. Our unique technology integrates multi-cloud connectivity, application optimization, security, last-mile management and visibility into an SLA-driven OPEX-only solution that provides unmatched agility and improved TCO for the global enterprise.

LEARN MORE: info@aryaka.com