Aryaka Secure Web Gateway

Deploy Secure Web Gateway for Protection from Web Threats as part of Unified SASE

Solution Brief

Your Employees Are Surfing the Web – Make It Safe for IT and Them

In today's work environment accessing the internet is part of an employee's daily routine. The days of IT allowing employees access to applications and data that only sit in an on-premises data center are long gone. It's common to have employees access websites to seek information needed to improve their work, complete their job duties, support company-wide social media activities, or allow them to use their work laptop or mobile device to access the internet for personal business. However, with the internet being a notoriously unsafe place, IT must ensure that the spreading of malware or the leaking of any sensitive data is prevented.

Jan 2022

6H 58M

Average Daily Time Spent Using The Internet By Each Internet User

Source: DIGITAL 2022: GLOBAL OVERVIEW REPORT

Aryaka helps CIOs modernize their infrastructure and simplify operations by converging networking and security in an all-in-one service with an absurdly great customer experience.

Secure Internet Access for In-Office and Remote Employees

For a hybrid workforce, with users going on websites from anywhere and anytime, secure internet access plays a crucial role in the security posture of a modern enterprise. Aryaka's Secure Web Gateway, a cloud-based Internet gateway, acts as protection for Site-to-Internet and User-to-Internet traffic, providing full protection against web and internet-based attacks.

You need help with these challenges:

- You need to provide secure web access with URL filtering, malware detection and threat protection for users who are remote or in the office
- You are more concerned about ransomware and zero-day malware and need a solution
- You are managing too many network security solutions and would like to consolidate and simplify
- You need to reduce infrastructure costs (total cost of ownership) and/or reallocate costs to modernize

Who can help? Let's look at legacy WAN and modern, cloud-based architectures.

Legacy WAN Architectures Are Too Complex and Inflexible

By wanting to adopt 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, legacy WANs are becoming complex and inflexible.

Legacy WAN Architectures
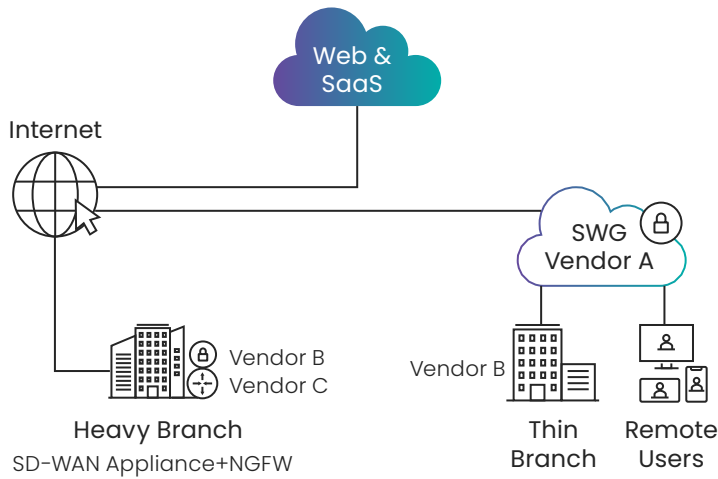
Fragmented Policies & Multiple Vendors for Cloud & On-Premise Security

SaaS only over best effort internet

🔒 Security   ⊕ Router
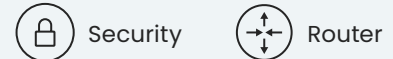
Complex: Legacy WAN architectures based on MPLS + Internet are not cloud-native and add additional complexity and cost.

Inflexible: Traditional edge security solutions require additional hardware and software and don't offer connectivity flexibility.

Fragmented Policies: Stitched together products from multiple vendors result in disjointed policies for SD-WAN and Security increasing vulnerabilities to attacks.

Aryaka's Modern WAN Architecture Provides Flexibility and Simplicity

Aryaka's 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.
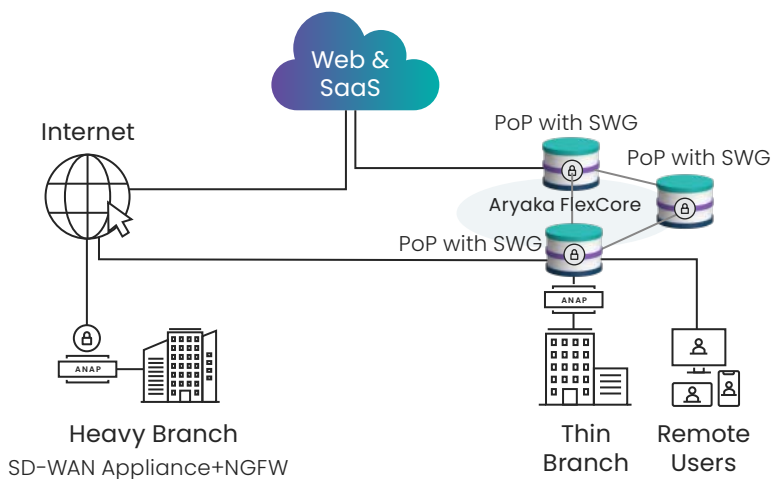
Coverged Policies & Single Vendor for Cloud & On-Premise Security

Easy option for acceleration of SaaS

NGFW: NextGen Firewall
SWG: Secure Web Gateway
ANAP: Aryaka Network Access Point

Simple: Modern, cloud-based WAN architecture based on Aryaka FlexCore and integrated edge and cloud security with software-defined workflows for simple management.

Flexible: Seamlessly integrated edge security and cloud security reduce appliance footprint and dual layer 2 and layer 3 core networks offers optimal cost/performance choice.

Converged Policies: Define and enforce policies across locations from a single console for reduced risk with consistent network and security policies across all users & sites.
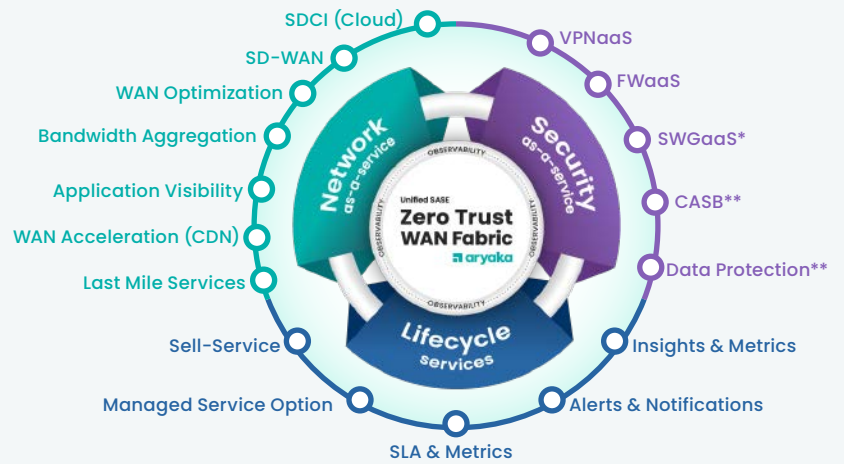
Check out the Aryaka Secure Web Gateway Datasheet for more information on features and capabilities.

See the Whole Picture With A Unified SASE

Secure Internet Access for employees surfing the web from the office, at home, at a hotel or a coffee shop is only one – albeit a crucial one - of several paths to access applications and data in the cloud and/or on-premises. A comprehensive, unified Secure Access Service Edge (SASE) solution that integrates observability ensures IT can protect an organization's assets without impacting network and application performance, ensuring employees get their work done efficiently.

Aryaka Unified SASE

Aryaka's Secure Web Gateway is a crucial part of our approach to providing a Unified SASE enabling a Zero Trust WAN Fabric. CASB and Data Protection are on our roadmap to be integrated to provide a single vendor solution. Full circle Observability and integrated Lifecycle services are equally important to our approach to the full convergence of all four key pillars.

SDCI (Cloud), SD-WAN, WAN Optimization, Bandwidth Aggregation, Application Visibility, WAN Acceleration (CDN), Last Mile Services, Sell-Service, Managed Service Option, SLA & Metrics, VPNaaS, FWaaS, SWGaaS*, CASB**, Data Protection**, Insights & Metrics, Alerts & Notifications — Unified SASE Zero Trust WAN Fabric — Network as-a-service, Security as-a-service, Lifecycle services, Observability

* H2 2022   ** Roadmap/Partnership

Enabling Aryaka Zero Trust WAN
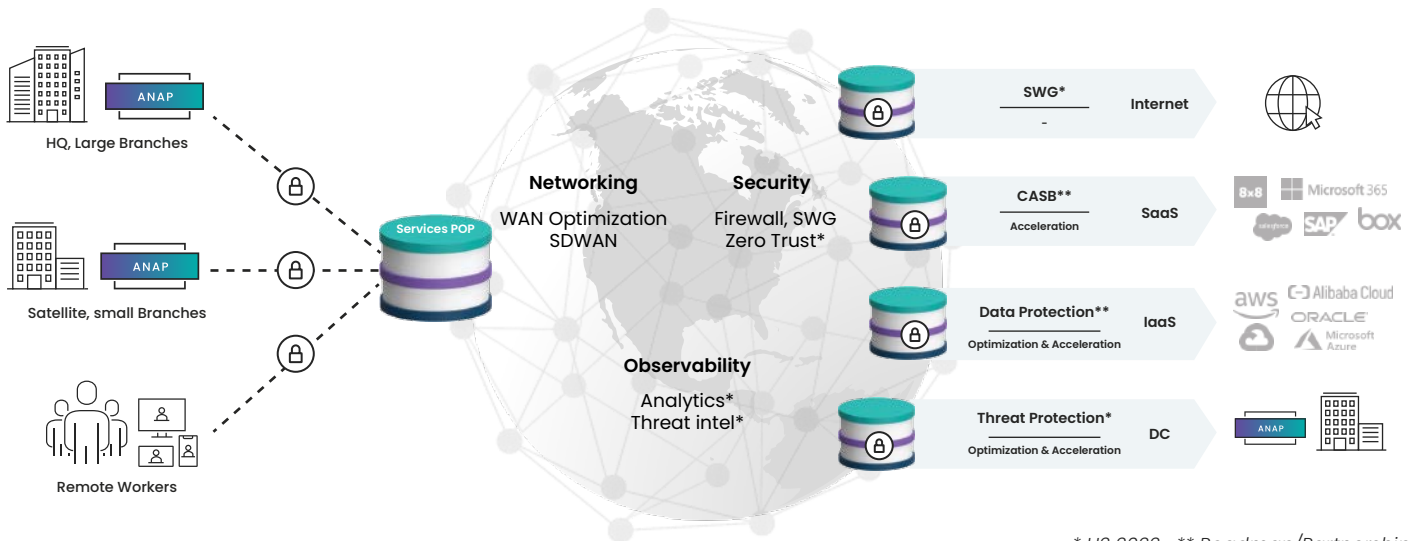
* H2 2022   ** Roadmap/Partnership

By converging Network and Security as-a-service, Lifecycle services, and integrated Observability enterprises will be able to consume services from a single vendor, greatly reducing the complexity and expense that are inherent with managing multiple solutions from multiple vendors. This approach ensures true convergence and delivers the best application experience, with security. Aryaka's Zero Trust WAN delivered as-a-service will provide ease of use and peace of mind for enterprises that want to move fast in transforming their infrastructure and business.

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. Getting started with Aryaka is easy as is adapting to evolving IT and business demands. Enterprises benefit from our converged approach in several ways.

Application Acceleration	**Advanced Security and Centralized Management**	**Observability**
Reduced Hardware Footprint	**Rapid Deployment**	**"White-Glove" Services Experience**

Check out the Aryaka Prime, our SASE as-a-Service, for detailed information about our managed SASE service offerings.

+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