e92cloud

SASE Simplified

The network is dead, long live the network.

The incredible acceleration of digital transformation in the past 18 months has transformed how we think about the traditional network perimeter, and our perceptions of the importance of connectivity. It's now about the Anywhere Worker, regardless of their device or location, and ensuring they can be productive and efficient.

However, cybersecurity threats have matched this pace of change, and as the network perimeter walls that protected our on-premise infrastructure has become a legacy solution, so the attacks have evolved to target those users no longer secure behind the gateway firewall.

The challenge is no longer connecting fixed networks and devices, but creating a flexible architecture that allows any user and any device the ability to securely access key resources wherever they are, maximising productivity without reducing security.

Rather than a single technology, the concept of SASE was identified as a way to integrate key technologies.

First developed by Gartner in 2019, Secure Access Service Edge (SASE) is expected to be adopted as a strategy by 40% of enterprises by 2024.

It converges networking and security, looking to creating a simplified architecture that's more agile, and often delivered as a service rather than simple point products. It places the integration requirements on the vendor technologies, so necessitating a seamless approach and unified management.

The emergence of SASE leverages how over 50% of enterprise WAN traffic is now to and from the cloud, and the majority of the workforce now accessing corporate resources from outside the traditional network (either on VPN or directly – and possible from unsecured BYOD hardware).

SASE requires a cloud-native platform, ubiquitous security and application acceleration without adding network complexity.

> Digital business transformation inverts network and security service design patterns, shifting the focal point to the identity of the user and/or device.... Security and risk management leaders need a converged cloud-delivered secure access service edge to address this shift
>
> **Andrew Lerner, Gartner**

Key trends

- **Cloud-first networking, and an agile consumption model rather than multi-year hardware agreements**
- **Flexibility to support workers wherever they are, with offices no longer the only gateway.**
- **Defined SLAs for performance and connectivity, as organisations relinquish network ownership**
- **Reliance on managed services, and automation to reduce costs and minmise potential gaps in security**

SASE Simplified with Check Point and Aryaka

To help organisations embrace the potential of SASE, we've integrated best of breed solutions to provide a simplified, cloud-native offering.

SASE, Simplified encompasses the most advanced threat protection solutions for cloud environments, on-premise networks and remote workers from Check Point with accelerated networking connectivity from Aryaka.

Replacing legacy MPLS networks and expensive point-to-point solutions, while providing an elastic architecture that scales with the company and it's users, SASE Simplified is the affordable solution for organisations of all sizes.

- **Straightforward, centralized branch network management**
- **Advanced threat prevention**
- **Cost-effective and simplified deployment**
- **Extended branch office connectivity**

Key Benefits

Secure

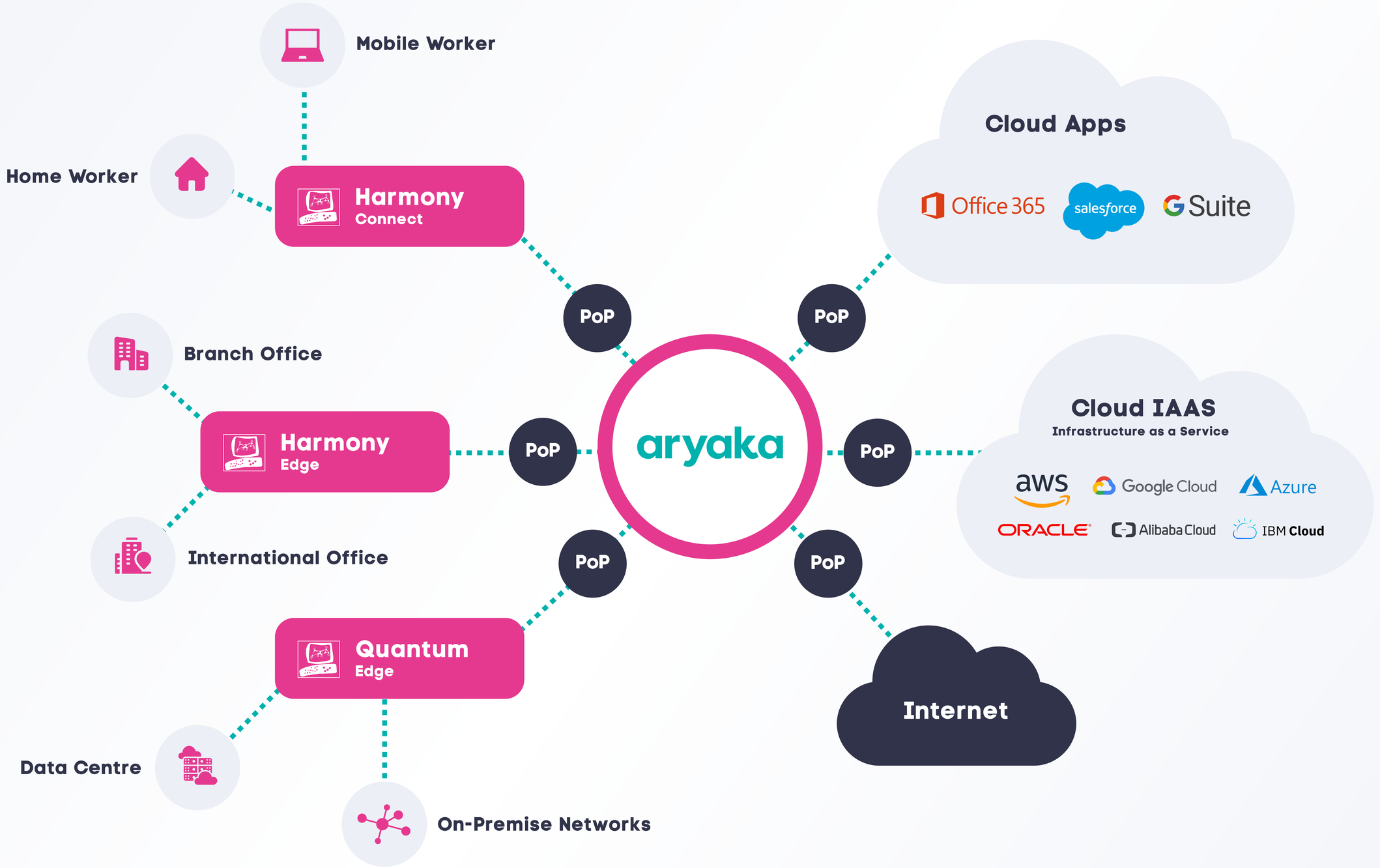
NSS top rated threat prevention with 100% cyber attack catch rate

Flexible

Deploy and protect in minutes in the cloud or on-premise

Efficient

Unified architecture reduces OpEx costs by up to 40% and CapEx by 20%


Mobile Worker
Home Worker
Harmony
Connect
Branch Office
Harmony
Edge
International Office
Quantum
Edge
Data Centre
On-Premise Networks
PoP
PoP
PoP
PoP
PoP
PoP
aryaka
Cloud Apps
Office 365
salesforce
G Suite
Cloud IAAS
Infrastructure as a Service
aws
Google Cloud
Azure
ORACLE
Alibaba Cloud
IBM Cloud
Internet

Use case #1

Security for the distributed enterprise

Challenge:

Enterprises leverage direct internet connections at remote locations, for guest Wi-Fi or cloud apps. This makes compliance challenging, and increase security defence complexity.

Solution:

The Aryaka Edge device directs all traffic via Check Point CloudGuard Connect, through Aryaka's global private network with integrated firewalls, encrypted tunnels and fortified security.

Benefits:

The combined solution does not require additional on-premises hardware, appliances or software and is easy and cost-effective to deploy and manage.

Use case #2

NGFW as a Virtual Network Function

Challenge:

Connecting branches directly to the cloud significantly increases security risks against sophisticated cyber attacks.

Solution:

With Aryaka SmartConnect, branch offices obtain secure and accelerated connectivity to any cloud service. CloudGuard Edge then protects branch offices on-premise with top-rated threat prevention deployed in minutes, managed by a unified platform.

Benefits:

Security is simplified with a single solution, integrated into the network connectivity that optimizes connections to the cloud.

e92cloud

Check Point SOFTWARE TECHNOLOGIES LTD

Check Point CloudGuard

Check Point CloudGuard Connect transforms branch cloud security by delivering enterprise grade security to branches as a cloud service, with top-rated threat prevention, quick and easy deployment, and unified management saving up to 40% in OpEx.

CloudGuard Connect protects against Zero Day attacks, with sandboxing, application and web filtering built in alongside advanced Threat Protection utilising intelligence from Check Point ThreatCloud. Designed to scale on-demand, branch on-boarding is fully automated with everything cloud-hosted so always up to date.

CloudGuard is available in two deployment options: Connect and Edge.

Check Point delivers real-time Advanced Threat Prevention for branch offices

- **Continuously up to date with the latest Threat Prevention**
- **Top-Rated Threat Prevention**
- **Protects from the latest Zero-Day and Gen V cyber attacks**
- **Leverages Real-time Threat Intelligence**

Edge for On-Premise

- **One click activation**
- **Lightweight on-premise VM**
- **Integration with Aryaka SD-WAN**

Connect for Cloud

- **100% Cloud Hosted**
- **APIs automate onboarding**
- **Transparent updates**

e92cloud

aryaka

Aryaka Cloud-First Managed WAN

Aryaka's Cloud-First ManagedSD-WAN enables enterprises with fast connectivity along with accelerated access to mission and business critical applications. Aryaka uses a global private network with built-in optimization and security capabilities that include a multi-layer security approach with a global private core network, delivering significantly faster application performance for enterprises, while integrating with Check Point CloudGuard for enhanced advanced security controls needed for web and cloud-bound traffic.

Unlike legacy connectivity solutions that take months to deploy, Aryaka's Global SD-WAN can be deployed within days. It is delivered as a service, so IT organizations can consume global networking services the way they would consume SaaS applications like Salesforce and Infrastructure-as-a-Service solutions like Amazon Web Services and Microsoft Azure.

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.
Lower TCO	Aryaka helps enterprises generate the maximum return on their SD-WAN investment.
Hybrid Workforce Enablement	Aryaka remote access solutions optimize the user experience for both remote and branch employees – anytime, anywhere, irrespective of changing traffic loads.
Flexibility and Elasticity	Aryaka delivers on the benefits of as-aService deployment to networking, allowing for on-demand self-service and elastic allocation of resources.
High Availability with 99.99% uptime	Aryaka combines complete visibility and predictive analytics to provide an always-on enterprise network platform.