# SmartSecure（智能安全）

安全即服务

**Aryaka SmartSecure（智能安全）**旨在通过托管软件定义广域网 (SD-WAN) 安全即服务技术为 SmartConnect（智能连接）提供进一步支持。

- 在分支机构，Aryaka 网络访问点 (ANAP) 中的接入防火墙可提供“南北向”控制，而基于 NFV 的可选配一级托管防火墙则可提供全面的 L7 层安全防护。
- **Aryaka Zone** 通过基于策略的访问对站点进行分段，进而可将其扩展为具备“东西向”安全性的局域网 (LAN)。整合这两种功能后，便能将广域网 (WAN) 流量从内部和非管制区域 (DMZ) 的 LAN 流量划分到 Aryaka 和互联网。
- 此外，ANAP 还支持**基于 VRF 的微分段**，进而支持多租户。
- Aryaka SmartSecure（智能安全）还会通过 Aryaka 安全合作伙伴生态系统（包括 **Zscaler、Palo Alto Networks 和 Symantec**）为云端扩展安全性。

## 核心功能

### 1. 云安全

通过 Palo Alto 的 Prisma 云安全套件、Symantec 的网络安全服务和 Zscaler 的云安全服务实现安全的本地互联网分流，无需借助设备即可保护所有端口和协议。

### 2. 微分段

微分段增加了 ANAP 的区域功能。虚拟局域网 (VLAN) 在站点为内部和 DMZ 区域提供局部分段。微分段可通过支持边界网关协议 (BGP) 的 VRF 轻量级功能将其扩展到整个 Aryaka 核心网络。

### 3. 虚拟防火墙

Aryaka 的 ANAP 支持 NFV 功能，可提供其他 SDN 交付服务。我们正在与多个一级安全供应商合作，以便提供多样化选择。同时，我们还会为 SD-WAN 部署中的物理防火墙管理提供支持。

### 4. 安全远程访问

Aryaka 的安全远程访问服务是首个实现软件定义的远程访问的无客户端 SD-WAN。该服务能够为远程和移动办公人员大幅提升本地和云 / 软件即服务 (SaaS) 应用程序的性能，而无需使用额外的硬件或软件客户端。

### 5. Aryaka 核心防护

与此同时，Aryaka 专用核心还能为所有企业提供分区连接，进而加密数据并防止分布式拒绝服务 (DDoS) 攻击。在分支机构中，企业可以访问 Syslog 和 Netflow 日志，而在网络级别，MyAryaka 云门户会提供一个单独的窗口，用于进行服务配置、监控和健康状况诊断。

### 6. 边缘防火墙

ANAP 包含虚拟状态防火墙和“区域”功能，前者可提供南北向的访问保护，而后者可提供站点分段以保护分支机构内的东西向流量。ANAP 与不断发展的 Secure Access Service Edge (SASE) 保持一致，可提供多种边缘和云安全功能。

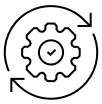
## 部署选项

| 远程访问 | Aryaka + Zscaler | Aryaka + Palo Alto |
| --- | --- | --- |
| 安全远程访问是实现全球部署和地区部署的可选功能 | 企业可以利用 Zscaler 基于云的辅助安全即服务，并通过 Aryaka 适当引导流量。 | 远程办公人员可通过 Palo Alto 的 Prisma 云安全套件访问 Aryaka，该套件提供身份验证和加速功能 |

## Aryaka SmartSecure （智能安全）为用户带来的优势

### 托管 SD-WAN 安全服务

Aryaka SmartSecure（智能安全）将 WAN 安全性放在首位，无论是在第一公里、中间一公里还是云端，均能为企业提供端到端的安全基础架构。



### 简化运营

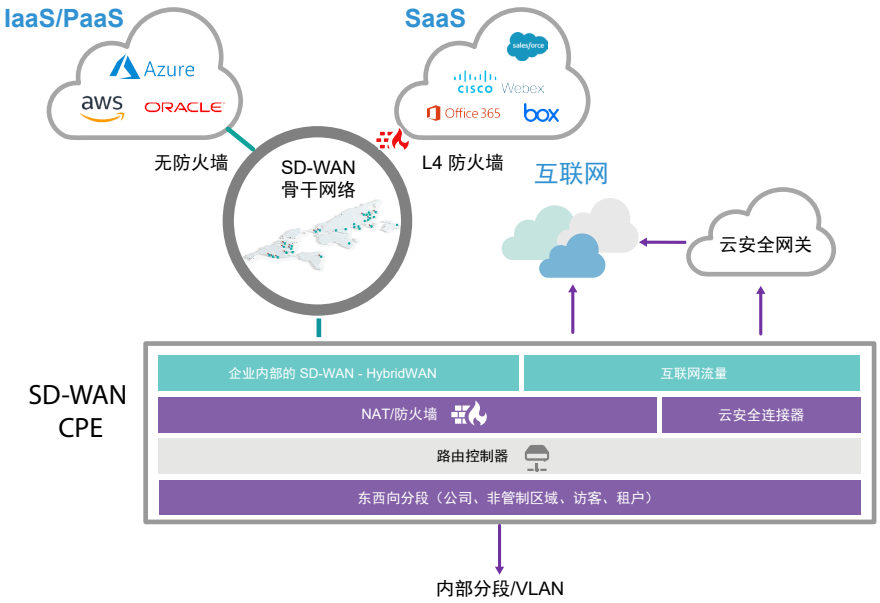
Aryaka 端到端托管 SD-WAN 包含边缘和云安全服务，该服务可充分利用一级合作伙伴，进而为企业隐藏复杂操作。

### 减少 TCO

SD-WAN 安全服务有助于企业从 SD-WAN 投资中获得巨大回报，保护企业在全球各地免受外部威胁，同时确保企业数据的完整性。

**Aryaka 的 SmartSecure（智能安全）**与不断发展的 Secure Access Service Edge (SASE) 架构保持一致。我们的安全产品覆盖分支机构和云端，可让企业根据个人需求自由选择部署其安全服务的位置。 重要的是，我们设计了可覆盖两个领域的单一运营模型和功能集。

| | | | 全球 | 地区 |
| --- | --- | --- | --- | --- |
| **SmartOptimize（智能优化）** | 边缘必需服务（防火墙、微分段） | 基于 ANAP 的 N-S 和 E-W 访问防火墙；分支机构微分段和多租户支持 | 已加入 | 已加入 |
| | 虚拟防火墙托管和虚拟 / 物理防火墙管理 | ANAP 上的 NFV 防火墙，以及企业物理和虚拟防火墙管理 | 可选 | 可选 |
| | 云安全连接器 | 基于站点容量（小型 / 中型 / 大型）的云托管安全功能 | 已加入 | 已加入 |
| | 安全远程访问 | 全球 ExtraNET、全球 VPN 或 BYO VPN 集中器 | 可选 | 可选 |




## 安全远程访问

利用第一个无客户端 SD-WAN，为远程 / 移动办公员工加速应用程序性能。Aryaka 的安全远程访问服务能够为远程和移动办公人员大幅提升本地和云 / 软件即服务 (SaaS) 应用程序的性能，而无需使用额外的硬件或软件客户端。

**将远程访问速度提升高达 3 倍**
提高生产力 - 简化操作，减少成本

### 面向远程和移动办公员工

- 同时加速本地和云 /SaaS 应用程序性能
- 无论天涯海角，均可快速获取一致的数据、语音和视频
- 减少断开连接的次数
- 使用现有的 VPN 客户端，无需安装其他软件

### 面向 IT 人员

- 简化 VPN 基础架构并减少成本
- 获取端到端网络和应用程序可见性
- 提升远程访问安全性
- 数小时内即可完成全球部署，无需更改安全策略

## Aryaka 安全架构

通过虚拟化计算、网络和存储资源，Aryaka 私有网络可提供真正的多租户数据分区。相比无法加密客户流量的竞争对手 MPLS 服务，由此产生的私有骨干网安全性更高。该网络包含以下安全服务：位于安全数据中心的专用入网点 (PoP)、L2 专用链路、互联网安全协议 (IPSec) 加密、密钥管理和分布式拒绝服务 (DDoS) 保护。我们通过先进的业务流程平台来管理该网络，以确保您的用户可随时随地访问重要的应用程序和数据。

**Aryaka 维护着一项可靠的安全方案，该方案符合国际公认的安全惯例要求。**
SOC 2：针对 Aryaka 政策和流程的 SSAE-16 报告
云控制矩阵 (CCM)
共识评估调查问卷 (CAIQ)
ISO27002 框架
可根据要求在 48 小时内提供第三方网络扫描报告

### 关于 Aryaka 网络

Aryaka 率先推出全托管端到端全球 SD-WAN 服务，以满足云优先时代的网络需求。借助独家技术，我们在 SLA 驱动的解决方案中集成了多云连接、应用程序优化、安全性、最后一公里管理和可见性服务，该解决方案仅需支付运营费用，可为全球企业提供超一流敏捷性并减少总体拥有成本 (TCO)。

**了解详情：** info@aryaka.com