SmartSecure

Sicherheit als Service

Aryaka SmartSecure wurde als Ergänzung zu SmartConnect mit SD-WAN-Sicherheit als Managed Service entwickelt.

- In der Filiale wird über eine Zugriffs-Firewall als Managed Service innerhalb des ANAP der ein- und ausgehende Verkehr kontrolliert, während eine optionale NFV-basierte Tier-1-Firewall umfassenden L7-Schutz bietet.
- Durch die **Aryaka-Zonen** wird dies auf das LAN ausgedehnt, mit horizontaler Sicherheit durch eine Standortsegmentierung mit richtlinienbasierten Zugang. Gemeinsam trennen diese beiden Funktionen den WAN-Verkehr zu Aryaka und ins Internet vom LAN-Verkehr, sowohl intern als auch in der DMZ.
- Der ANAP unterstützt auch **VRF-basierte Mikrosegmentierung**. Dadurch wird die Mandantenfähigkeit ermöglicht.
- Aryaka SmartSecure erweitert auch die Sicherheit weiter auf die Cloud, durch Aryakas Ökosystem von Sicherheitspartnern – einschließlich **Zscaler, Palo Alto Networks und Symantec.**

Die wichtigsten Funktionen

1.
Cloud-Sicherheit

Sicherer, lokaler Internet-Breakout wird durch Palo Altos Prisma Cloud Security Suite, Symantecs Web Security Service und Zscalers Cloud Security ermöglicht. Dadurch werden alle Ports und Protokolle ohne zusätzliche Geräte geschützt.

2.
Mikrosegmentierung

Die Mikrosegmentierung erweitert die Funktionalität der ANAP-Zonen. Vor Ort sorgen VLANs für lokale Segmentierung für interne und DMZ-Zonen. Die Mikrosegmentierung erweitert diese Funktion über das gesamte Aryaka-Kern-Netzwerk, mithilfe einer BGP-gesteuerten, vereinfachten VRF-Funktionalität.

3.
Virtuelle Firewall

Aryakas ANAP unterstützt NFV-Funktionalität für zusätzliche vom SDN bereitgestellte Dienste. Wir arbeiten mit mehreren Tier-1-Sicherheitsanbietern zusammen, um unseren Kunden eine Auswahl zu bieten. Die Verwaltung von physischen Firewalls ist Teil der SD-WAN-Implementierung und wird ebenfalls unterstützt.

4.
Sicherer Fernzugriff

Der sichere Fernzugriff von Aryaka ist das erste clientlose SD-WAN, das den softwaredefinierten Fernzugriff ermöglicht. So werden sowohl die Leistung am Standort als auch die Leistung von Cloud-/SaaS-Anwendungen für entfernte und mobile Mitarbeiter erheblich verbessert, ohne dass zusätzliche Hardware oder Software-Clients nötig wären.

5.
Aryaka-Kernschutz

Parallel dazu bietet das private Kernnetzwerk von Aryaka partitionierte Konnektivität für alle Unternehmen, mit verschlüsselten Daten und Schutz vor DDoS-Angriffen. Innerhalb der Filiale haben Unternehmen Zugriff auf Syslog- und Netflow-Logging, und auf Netzwerkebene bietet das MyAryaka Cloud Portal eine zentrale Ebene für Dienstkonfiguration, Überwachung und Status.

6.
Edge-Firewall

Der ANAP verfügt über eine virtuelle zustandsorientierte Firewall, die für den Zugangsschutz für ein- und ausgehenden Verkehr sorgt, sowie über eine Zonenfunktion, mit der der Standort segmentiert und der horizontale Datenverkehr innerhalb der Filiale gesichert wird. ANAP ist auf Secure Access Service Edge (SASE) ausgerichtet, eine sich entwickelnde Technologie, und bietet eine Auswahl an Edge- und Cloud-Sicherheit.

Implementierungsmöglichkeiten

Fernzugriff

Der sichere Fernzugriff ist eine optionale Funktion für globale und regionale Implementierungen

Aryaka + Zscaler

Ein Unternehmen kann die ergänzenden Cloud-basierten Sicherheitsdienste als Service von Zscaler benutzen, wobei Aryaka den Verkehr entsprechend lenkt.

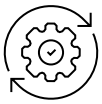
Aryaka + Palo Alto

Remote-Mitarbeiter können über die Prisma Cloud Security Suite von Palo Alto auf Aryaka zugreifen. Hierdurch werden die Authentifizierung und Beschleunigung ermöglicht.

Vorteile durch Aryaka SmartSecure

SD-WAN-Sicherheit als Managed Service

Mit WAN-Sicherheit als oberste Priorität bietet Aryaka SmartSecure Unternehmen eine sichere End-to-End-Infrastruktur auf der ersten und mittleren Meile sowie bis in die Cloud.



Einfacher Betrieb

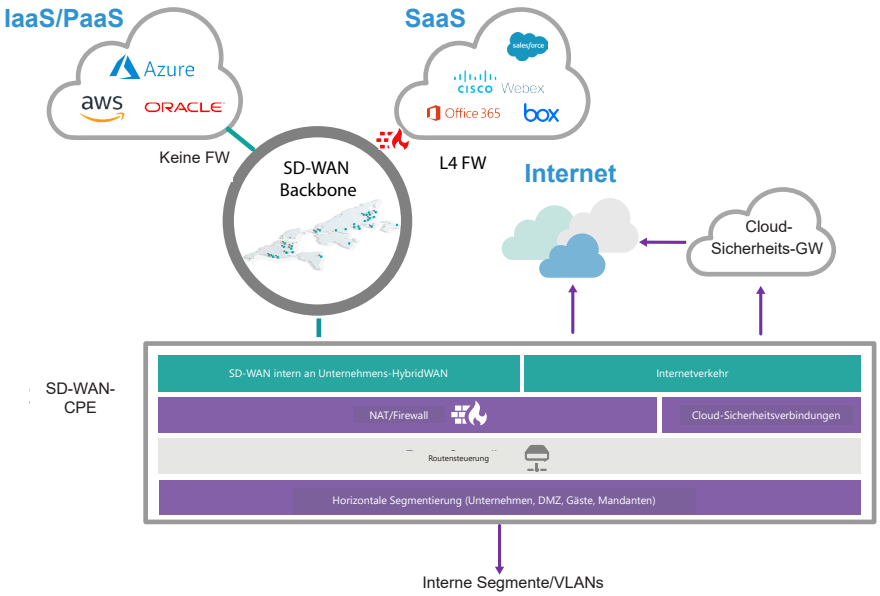
Mit dem End-to-End-SD-WAN als Managed Service bietet Aryaka Sicherheit für die Edge und die Cloud mithilfe unserer Tier-1-Partner. Darüber hinaus bleibt die Komplexität des Systems so vor dem Unternehmen verborgen.

Niedrigere Gesamtbetriebskosten

SD-WAN-Sicherheit hilft Unternehmen, den maximalen Ertrag aus ihren SD-WAN-Investitionen zu erzielen und gewährleistet den Schutz vor externen Bedrohungen sowie die Integrität von Unternehmensdaten überall auf der Welt.

Aryaka's SmartSecure ist auf die sich entwickelnde Secure Access Service Edge (SASE-Architektur) ausgerichtet. Unsere Sicherheitsangebote decken sowohl die Filiale als auch die Cloud ab und bieten Unternehmen die Wahl, wo sie ihre Sicherheitsmaßnahmen einsetzen möchten, je nach individuellen Anforderungen. Ein weiterer wichtiger Faktor ist, dass wir ein einziges Betriebsmodell und einen einzigen Satz von Funktionen planen, der beide Domänen abdeckt.

			Global	Regional
SmartSecure	Edge-Grundelemente (Firewall, Mikrosegmentierung)	ANAP-basierte Firewall für horizontalen sowie ein- und ausgehenden Zugriff; Filialen-Mikrosegmentierung und Mandantenfähigkeit	Inklusive	Inklusive
	Virtuelles Firewall-Hosting und Virtuelle/physische FW-Verwaltung	NFV-FW über ANAP und Verwaltung physischer und virtueller Unternehmensfirewalls	Optional	Optional
	Cloud-Sicherheitsverbindung	In der Cloud gehostete Sicherheit auf Grundlage der Filialkapazität (klein/mittel/groß)	Inklusive	Inklusive
	Sicherer Fernzugriff	Globales ExtraNET, globales VPN oder BYO-VPN-Konzentration	Optional	Optional



Sicherer Fernzugriff

Beschleunigen Sie die Anwendungsleistung für entfernte/mobile Mitarbeiter mit dem ersten clientlosen SD-WAN. Aryakas sicherer Fernzugriff bringt erhebliche Steigerungen der Anwendungsleistung, sowohl am Standort als auch über die Cloud/SaaS für entfernte und mobile Mitarbeiter, ohne dass zusätzliche Hardware oder Software-Clients nötig wären.

Bis zu 3-mal schnellerer Fernzugriff

Produktivität erhöhen- Komplexität und Kosten reduzieren

Für externe und mobile Mitarbeiter

- Beschleunigung der Leistung von Vor-Ort- und Cloud-/SaaS-Anwendungen
- Konstanter schneller Zugriff auf Daten, Sprach- und Videoverbindungen von überall auf der Welt
- Weniger Verbindungsunterbrechungen
- Vorhandener VPN-Client kann benutzt werden — keine zusätzliche Software erforderlich

Für die IT-Abteilung

- Vereinfachung der VPN-Infrastruktur und Kostensenkung
- End-to-End-Netzwerk- und Anwendungssichtbarkeit
- Erhöhte Sicherheit für den Fernzugriff
- Weltweite Implementierung innerhalb weniger Stunden, ohne Änderung der Sicherheitsrichtlinien

Aryaka-Sicherheitsarchitektur

Das Aryaka-Privatnetzwerk bietet echte mandantenfähige Datenpartitionierung mit virtualisierten Rechen-, Netzwerk- und Speicherressourcen. Der daraus resultierende private Backbone bietet mehr Sicherheit als die MPLS-Dienste der Konkurrenz, bei denen der Kundenverkehr nicht verschlüsselt wird. Das umfasst dedizierte PoPs in gesicherten Rechenzentren, dedizierte Layer-2-Verbindungen, Verschlüsselung mit IPSec, Schlüsselverwaltung und DDoS-Schutz. Das setzen wir über unsere hochentwickelte Orchestrierungsplattform um, damit Ihre Benutzer gesicherten Zugriff auf Ihre wichtigen Anwendungen und Daten haben, von überall und zu jeder Zeit.

Aryaka betreibt ein robustes Sicherheitsprogramm, das international anerkannten Sicherheitspraktiken entspricht.
SOC 2: SSAE-16-Berichte über Aryakas Richtlinien und Prozesse
Cloud Controls Matrix (CCM)
Consensus Assessments Initiative Questionnaire (CAIQ)
ISO27002 Framework
Netzwerk-Scanberichte von Drittanbietern auf Anfrage innerhalb von 48 Stunden verfügbar

Über Aryaka Networks

Aryaka bietet den branchenführenden Dienst für globale End-to-End-SD-WANs als Managed Service für die Cloud-First-Ära. Unsere einzigartige Technologie integriert Multi-Cloud-Konnektivität, Anwendungsoptimierung, Sicherheit, Management auf der letzten Meile und Transparenz in einer SLA-gesteuerten, ausschließlich auf Betriebskosten ausgelegten Lösung, die unübertroffene Flexibilität und verbesserte Gesamtbetriebskosten für globale Unternehmen bietet.

MEHR ERFAHREN: info@aryaka.com