epsilon a kt company

Integrated Security with SD WAN

Enable Cloud-delivered Security as part of your WAN transformation

Overview

Epsilon partners with Zscaler, a leader in cloud-hosted security services – using its Zscaler Internet Access™, to provide a superior security solution for cloud-first enterprises. It is a centrally orchestrated cloud-hosted security service complemented by application-aware and business driven Aruba EdgeConnect™ SD WAN edge platform. The solution provides a powerful secure access services edge (SASE) that protects an enterprise from threats whilst enabling high application performance, enhancing user experience and delivering cost efficiencies.

Centrally managed and supporting a full security stack, including next-generation firewall, access control, Intrusion Prevention System (IPS), sandboxing, Unified Threat Management (UTM), URL filtering, Data Loss Prevention (DLP), Cloud Access Security Brokers (CASB), remote browser isolation, and more. Zscaler delivers identical protection for all users and consistent policies and policy enforcement across hundreds or even thousands of sites — without the need to buy, deploy or manage any security appliances.

Cloud-hosted security services coupled with the application-aware, business intent driven Aruba EdgeConnect platform, streamline WAN edge infrastructure at the branch. Enterprises no longer need to deploy expensive, complex-to-manage next-generation firewalls at every branch location. Additionally, Epsilon's SD WAN service is underpinned by Epsilon's global network fabric, enabling Enterprises to securely connect to their digital infrastructure and cloud services.

Epsilon's Integrated Security helps enterprises to address:

Rising cloud migration trend for applications, driving the need for a new Wide Area Network (WAN) approach model with strong security measures

•

Challenges when migrating applications via direct connection to cloud-hosted and SaaS applications over the internet

•

The chance of threats and vulnerabilities exposure from increased attack surfaces, with real protection focus on branch locations without the deployment of robust security measures

•

Complex security requirements with users' needs to access their applications anywhere

•

Expensive MPLS bandwidth and latency additions that negatively impairs applications performance resulted from a legacy hub-and-spoke architecture

•

High costs associated with backhauling of internet-bound traffic to headquarters site for inspection

Features

Threat Prevention – a set of features that enhance an organisation's defence against threats or content, such as malicious code, bot attacks, etc.

- Proxy (SSL Inspection) - Find threats where they hide with full and unlimited inspection of SSL traffic at scale.
- Intrusion Prevention System (IPS) - Deliver full threat protection from malicious web content, such as browser exploits, scripts, and identify and block botnets and malware callbacks.
- Cloud Sandbox - Block zero-day exploits by analysing unknown files for malicious behaviour, and easily scale to every user regardless of location.
- DNS Security - Identify and route suspicious command-and-control connections to Zscaler threat detection engines for full content inspection.

Access Control – ability to dictate the users' access. Access control policies in-place to ensure users are authentic and authorised with the appropriate access.

- Cloud Firewall - Full DPI and access controls across all ports and protocol. Applications and users aware.
- URL Filtering - Block or limit website access based on a user or group across destinations or URL categories.
- Bandwidth Control - Enforce bandwidth policies and prioritise business-critical applications over recreational traffic.
- DNS (Domain Name System) Filtering - Control and block DNS requests against known and malicious destinations.

Data Protection – protect data loss or leakage, providing the same level of protection for data in-motion across locations and unified data at-rest protections across SaaS and public cloud applications.

- Cloud DLP With EDM - Easily scale DLP across all users and inside SSL. Improve detection by fingerprinting structured data with Exact Data Match (EDM).
- Cloud Access Security Broker (CASB) - Prevent data exposure and ensure SaaS compliance with out-of-band CASB. Discover and control unknown cloud apps with inline CASB.
- Cloud Security Posture Management (CSPM) - Extend data protection into AWS, Azure and SaaS. Monitor and mitigate app misconfiguration along with compliance reporting and violation remediation.
- Cloud Browser Isolation - Eliminate exposure to risky web content and data exfiltration by separating browsing activity from the end user device.

Key Differentiators

Full Inline Content/SSL Inspection
Inspect ALL your traffic, with no compromises.

•

Cloud-delivered Security
Any threat detected anywhere in Zscaler cloud is immediately blocked for all customers.

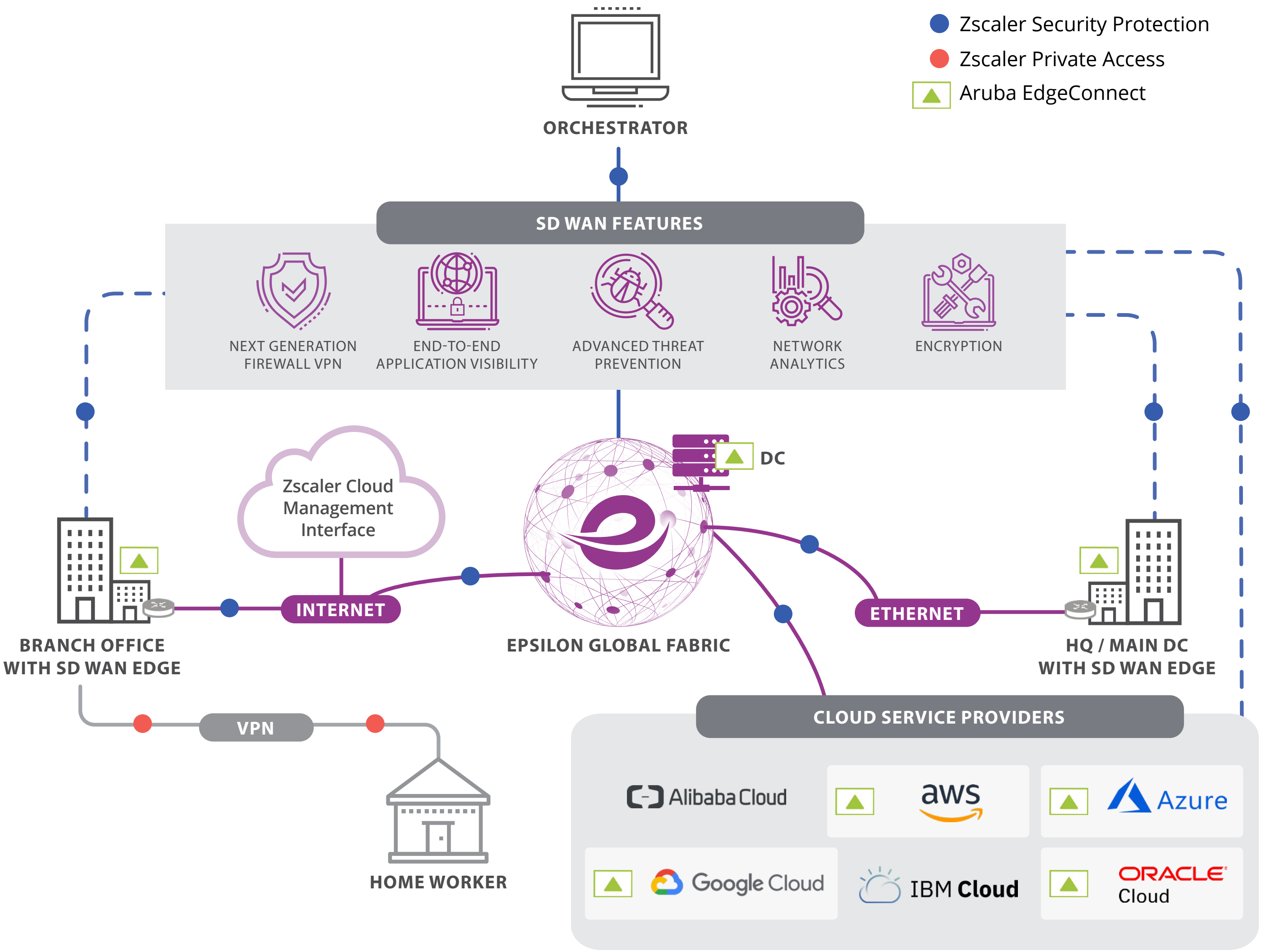
•

Daily Threat Updates
Get automatic updates far beyond what could be accomplished with appliances.

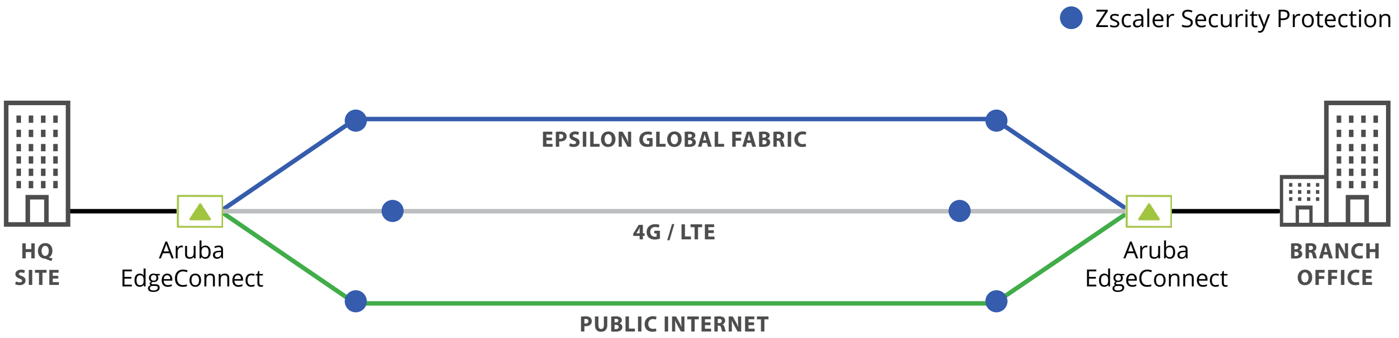
•

More Than 40 Industry Threat Feeds
Find and stop more threats with a platform that consumes more than 40 third-party threat feeds across open source, commercial, and private sources.

Overview Diagram



Zscaler Workflow Diagram



Benefits

Embed secure access services edge (SASE) into your architecture
Delivers the full benefits of the cloud – greater business agility and simplified IT operations.

Ensure fast, secure access to business-critical applications
Prioritisation of business-critical applications delivers the highest quality of experience to users.

Deliver consistent business and security policies globally to all users
Automated security and cloud application updates ensure optimal network and security policy enforcement across all locations.

Simplify day-to-day management
Let Epsilon's team managing the day-to-day operations – make changes easier, minimise human errors, and enable faster troubleshooting.

Centralise management and agility
Centrally managed policy configuration and administration eliminates device-by-device configuration. It results in agility, consistent, granular, end-to-end security policy enforcement.

Fully automated onboarding
Seamless integration between Zscaler and Aruba. Fully automated IPsec tunnel configuration between Aruba EdgeConnect SD WAN appliances and proximity-based ZIA Public Service Edge PoP eliminates the time-consuming task of manually defining IPsec tunnels at every branch site.

Why Choose Us?

Global Connectivity
Our extensive infrastructure around the world gives you the ability to connect whenever and wherever you need, bundled with high security and optimal speed efficiency advantages.

One-stop Provisioning
We offer a full suite SD WAN solution deployed over public or private networks with integrated security, enabling customers to enjoy highly secured network without the need to manage multiple vendors.

Seamless Orchestration
Our centrally orchestrated solution eases the maintenance work for your IT team and improves your productivity in the long run.

Customer-Centric
Our team of global experts provide you a complete managed service experience with real time technical and operational support 24/7.

Simple Solution
We help you reduce complexity in every touchpoint in terms of security and cost budgeting, you can focus on expanding your business with easy cloud migration on all your applications.

> "Epsilon's cloud-native security solution enables enterprises to move their security stack to the cloud, allowing them to easily scale protection to all offices or users, regardless of location, and seamless integration with SD WAN."

Aden Li
Product Manager
Epsilon

Contact Us

APAC
+65 6813 4020

UK
+44 207 096 9600

EMAIL
info@epsilontel.com