PANORAMICA DELLA SOLUZIONE

# Sicurezza Aruba edge-to-cloud

## Adozione dell'edge e trasformazione WAN sicure

### L'EVOLUZIONE DELLA RETE: L'ESPANSIONE DELL'EDGE E DEL CLOUD

La crescita dell'edge a causa dell'aumento del numero di lavoratori da remoto e dei dispositivi IoT ha fatto emergere nuove sfide in termini di onboarding, visibilità e sicurezza. Nel frattempo, la continua migrazione delle applicazioni sul cloud ha modificato l'approccio alla pianificazione delle reti e, conseguentemente, ai requisiti di sicurezza, visto che le reti tradizionali non erano state progettate per un mondo basato sul cloud. La maggiore complessità delle reti e l'insorgere di nuove minacce creano nelle organizzazioni la necessità di un approccio end-to-end olistico, che assicuri sicurezza e conformità dall'edge, dove risiedono i nuovi dispositivi, gli utenti e gli uffici delle filiali, al cloud, che ospita le applicazioni e i dati critici e che richiede dunque altissimi livelli di protezione, prestazioni e disponibilità.

### ARUBA ESP (EDGE SERVICES PLATFORM) CON SICUREZZA EDGE-TO-CLOUD

Aruba ESP è l'unica architettura che permette alle organizzazioni di implementare un'architettura di rete end-to-end comprendente WLAN, switching, SD-WAN e AIOps, il tutto con soluzioni di sicurezza integrate. Con l'aggiunta della sua nuova piattaforma SD-WAN EdgeConnect, Aruba può ora aiutare i suoi clienti a sfruttare i vantaggi offerti dalle funzionalità dell'SD-WAN leader nel settore senza correre rischi grazie a funzionalità di sicurezza Zero Trust e SASE.

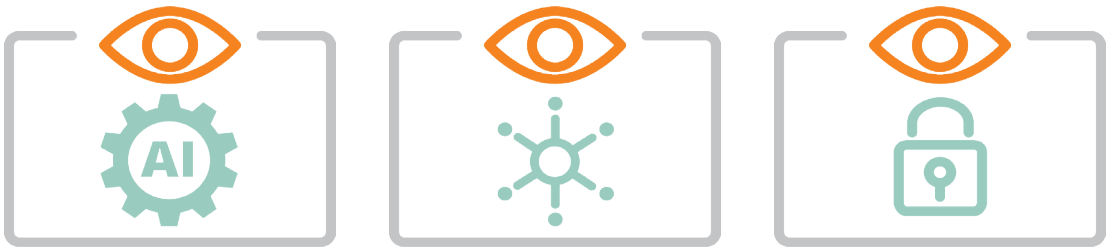
### LA SICUREZZA NELL'EDGE: VISIBILITÀ COMPLETA E SEGMENTAZIONE ZERO TRUST

L'adozione di un numero sempre crescente di dispositivi IoT e il significativo aumento di utenti da remoto hanno reso davvero ardua la sfida della completa visibilità di tutti gli utenti e dispositivi connessi alla rete. E, in assenza di visibilità, è difficile applicare i controlli necessari per mettere l'edge in sicurezza. L'automazione, il machine learning basato sull'IA e la possibilità di identificare rapidamente i tipi di dispositivi diventano essenziali. Aruba ClearPass Device Insight sfrutta una combinazione di tecniche di scoperta e profilazione attive e passive per rilevare l'intero spettro dei dispositivi che sono connessi o cercano di connettersi alla rete, inclusi i dispositivi d'uso comune come portatili e tablet. La differenza rispetto agli strumenti tradizionali sta nella sua capacità di vedere e riconoscere anche i nuovi dispositivi IoT che sempre più pervadono le reti di oggi.

Aruba ClearPass Policy Manager consente la creazione di politiche di accesso basate sul ruolo che permettono ai team IT e della sicurezza di rendere operative le migliori pratiche applicando i ruoli e i privilegi d'accesso a essi associati all'intera rete, indipendentemente dal fatto che si tratti di un'infrastruttura wireless o cablata o che ci si trovi in una filiale o nel campus. Una volta profilati, ai dispositivi viene automaticamente assegnata la politica di controllo degli accessi più opportuna e il loro traffico viene separato

### ARUBA ESP (EDGE SERVICES PLATFORM)

La prima piattaforma del settore con un sesto senso basato sull'IA per automatizzare e proteggere




**AIOps**
Informazioni dall'IA | Networks Analytics Engine
Informazioni sull'esperienza utente
Informazioni sui dispositivi

**Infrastruttura unificata**
Wi-Fi | Switching | SD-WAN
Cloud | 5G | Data lake comune

**Sicurezza edge-to-cloud**
Segmentazione dinamica | Applicazione delle politiche Zero Trust
ClearPass | Orchestrazione della sicurezza del cloud

Figura 1: La sicurezza edge-to-cloud è uno dei pilastri di Aruba ESP

da quello degli altri dispositivi tramite le funzionalità di segmentazione dinamica di Aruba. L'applicazione è garantita dal Policy Enforcement Firewall (PEF) di Aruba, un application firewall completo e integrato nell'infrastruttura di rete di Aruba. Inoltre, ClearPass condivide ora con le appliance dell'SD-WAN di EdgeConnect la telemetria basata sull'identificazione, così da offrire una segmentazione ancora più granulare.

## SICUREZZA DELLE FILIALI E PROTEZIONE DALLE MINACCE UNIFICATE

Le funzionalità di protezione dalle minacce di Aruba difendono la rete da una miriade di minacce, inclusi i tentativi di phishing, gli attacchi DoS (denial of service) e i sempre più frequenti attacchi ransomware. In sinergia con Aruba Central, ClearPass Policy Manager e il Policy Enforcement Firewall, i gateway SD-WAN Aruba supportati mettono in atto misure di prevenzione e rilevamento delle intrusioni (IDS/IPS) basate sull'identità. Le funzionalità IDS/IPS basate sull'identità effettuano ispezioni del traffico basate sulla firma e sugli schemi sia sul traffico delle LAN delle filiali (est-ovest), sia sul traffico dell'SD-WAN (nord-sud) che passa per il gateway, offrendo così un servizio di sicurezza di rete a livello delle filiali integrato. Il dashboard di sicurezza avanzato di Aruba Central offre ai team IT la visibilità totale della rete, metriche multi-dimensionali sulle minacce, informazioni sulle minacce e strumenti di correlazione e gestione degli incidenti. Gli eventi delle minacce vengono inviati ai sistemi SIEM e a ClearPass per essere bonificati.

## ORCHESTRAZIONE DELLA SICUREZZA DEL CLOUD E SECURE ACCESS SERVICE EDGE (SASE)

Man mano che le organizzazioni procedono alla migrazione di buona parte delle loro applicazioni sul cloud, diventa sempre più essenziale che le soluzioni SD-WAN e di sicurezza si adattino a questa trasformazione. Modernizzando le proprie infrastrutture WAN e di sicurezza, i clienti possono ottenere vantaggi significativi sia in termini di networking sia di sicurezza. La soluzione EdgeConnect di Aruba offre le migliori funzionalità SD-WAN insieme a un'orchestrazione

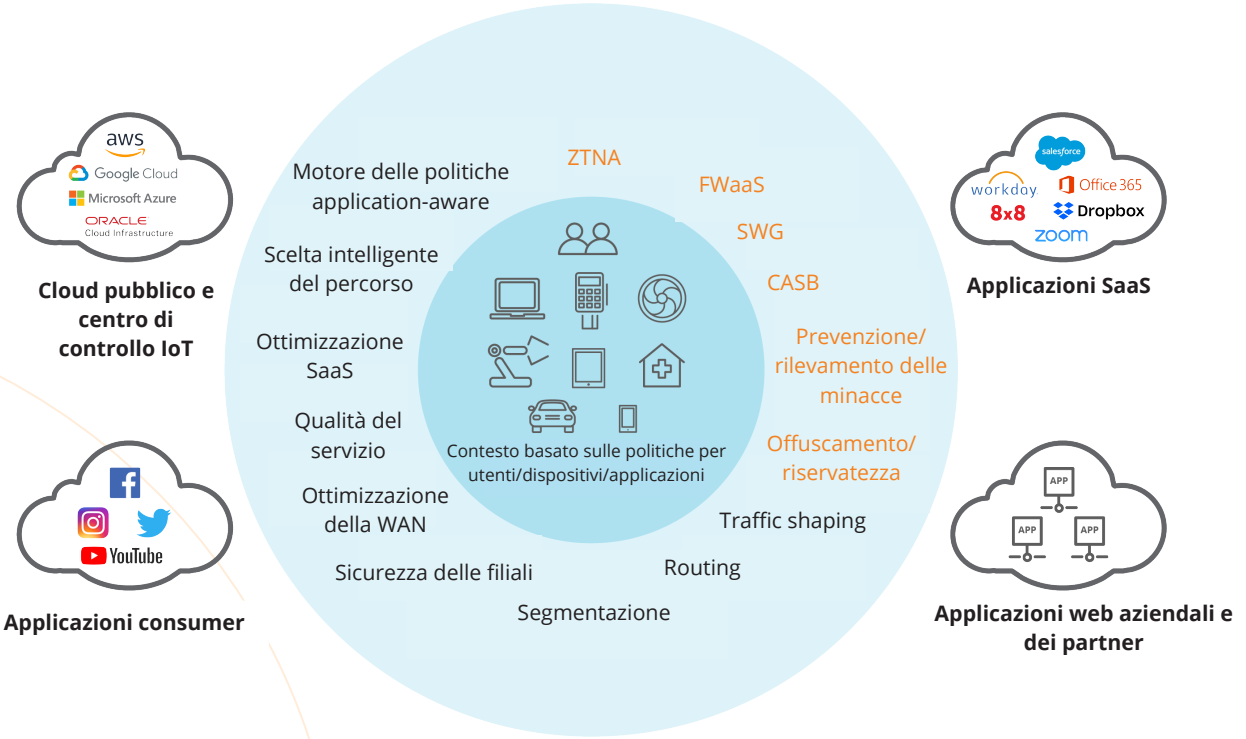



**Figura 2: Una soluzione SASE è indispensabile per supportare le iniziative di trasformazione digitale aziendale come la strategia cloud-first e il soddisfacimento delle esigenze di mobilità dei lavoratori. In un'architettura SASE robusta, delle funzionalità WAN complete operano in sinergia con delle funzionalità di sicurezza di rete complete per soddisfare le esigenze di accesso sicuro e dinamico di utenti, dispositivi e applicazioni proprie delle aziende digitali.**

integrata con le soluzioni dei migliori fornitori di sicurezza per il cloud. Questo riduce in modo significativo lo sforzo di integrazione dei servizi di sicurezza del cloud nell'infrastruttura di rete e di sicurezza già esistente. Integrando questi servizi di sicurezza basati sul cloud, le organizzazioni possono proteggere nel modo più efficace la propria infrastruttura ospitata sul cloud.

## ARUBA CENTRAL: INFORMAZIONI SULLE MINACCE DA TUTTA L'INFRASTRUTTURA

Aruba Central è una potente soluzione di rete in grado di offrire una semplicità d'utilizzo senza eguali, considerata la complessità delle reti odierne. Console di gestione e orchestrazione di Aruba ESP, Aruba Central fornisce un unico pannello di controllo da cui supervisionare ogni aspetto delle LAN, cablate e wireless, delle WAN e delle VPN di campus, filiali e postazioni remote. Esso include un dashboard di sicurezza avanzato comprendente avvisi IDS/IPS, informazioni sulle minacce e strumenti di correlazione e gestione degli incidenti.





SO_ArubaEdgetoCloud_SK_040921 a00112725enw.