

SOPHOS



# Come passare alla SD-WAN con Sophos: sei casi di utilizzo

# Introduzione

In un mondo sempre più connesso, le organizzazioni distribuite sono ormai molto comuni. La capacità di connettere uffici diversi, superando grandi distanze geografiche per scambiare informazioni e inviare applicazioni, ha rivoluzionato il modo di fare affari per le aziende, la formazione per le scuole e l'assistenza medica per i pazienti.

Indipendentemente dal settore di competenza o dalle dimensioni, le organizzazioni distribuite hanno molte esigenze in comune, che includono la necessità di: condividere i dati, inviare applicazioni cloud e SaaS e implementare comunicazioni e transazioni tra le sedi remote e la sede centrale. Proteggere tutti questi sistemi contro minacce informatiche quali ransomware, malware e tentativi di violazione è indispensabile. Le organizzazioni distribuite vogliono anche la libertà di connettere nuove sedi e aggiungere rapidamente nuove app e servizi. Gestire tutte queste strutture può richiedere diverso tempo, e per questo è importante disporre degli strumenti necessari per orchestrare tutti i sistemi. Anche i costi possono rappresentare un problema, in quanto si accumulano nel tempo.

Finora, la soluzione tradizionale utilizzata dalla maggior parte delle organizzazioni è stato il Multiprotocol Label Switching (MPLS): una tecnica di routing nata quasi due decenni fa. L'MPLS offre vantaggi che vanno oltre la semplice connessione di sedi geograficamente distribuite. Ad esempio, indirizzando i pacchetti da un nodo della rete a un altro nodo, seguendo il più breve percorso disponibile, MPLS offre un'ottima qualità del servizio (QoS) per applicazioni sensibili alla latenza che operano in tempo reale, come nel caso delle comunicazioni audio e video. Tuttavia, presenta anche degli svantaggi. Il passaggio al cloud computing rende obsoleti i servizi quali l'MPLS, che effettua il backhaul del traffico, indirizzandolo attraverso un data center. Inoltre, l'MPLS non è disponibile ovunque. Tuttavia, il motivo principale per cui le organizzazioni distribuite stanno abbandonando l'MPLS sono i costi. L'emergere di tecnologie alternative quali la SD-WAN (software-defined wide area networking) permette alle organizzazioni di impostare e connettere nuove sedi, scambiare informazioni e inviare applicazioni rapidamente e a un costo minore rispetto all'MPLS.

La SD-WAN è, fondamentalmente, una tecnica di overlay che viene sovrapposta a un'architettura WAN già esistente. Può utilizzare qualsiasi servizio di trasporto, incluse le connessioni DSL, via cavo, 3G/4G/LTE e persino MPLS, per reindirizzare il traffico sulla WAN in maniera intelligente dall'origine alla destinazione, con pochissimo (o nessun) rischio di latenza, instabilità o perdita dei pacchetti. L'obiettivo è garantire un'ottima esperienza utente, mediante l'elevata qualità del servizio. A sua volta, i maggiori livelli di QoS favoriscono l'aumento della produttività. Per quanto riguarda la distribuzione, la SD-WAN offre alle organizzazioni varie opzioni. I vendor specializzati in tecnologie SD-WAN offrono soluzioni ricche di funzionalità, ma il prezzo dell'appliance, unito a una gestione ininterrotta e alla mancanza di un sistema di protezione integrato, si traduce in costi proibitivi. Pertanto, sono sempre più numerose le organizzazioni che desiderano integrare opzioni SD-WAN nel proprio firewall.

## Il passaggio alla SD-WAN

La diffusione della SD-WAN è in crescita, secondo Gartner, che prevede un tasso di crescita annuale composto (CAGR) del 59% nel 2021, il che la porterebbe a diventare un mercato da 1,3 miliardi di \$. Siccome offre alle organizzazioni distribuite una vasta gamma di vantaggi estremamente convincenti a un prezzo inferiore, la SD-WAN contribuisce a rendere il passaggio a questa tecnologia un processo semplice ed economico. Di seguito elenchiamo alcuni dei motivi principali.

**Riduzione delle spese:** se da un lato l'MPLS merita ancora un posto all'interno della rete per alcune esigenze specifiche, trasferire tutte le connessioni alla SD-WAN aiuta a risparmiare. La SD-WAN sfrutta servizi internet e a banda larga disponibili al pubblico che sono molto più economici, riducendo quindi i costi operativi (OpEx). Inoltre, se si sta considerando un upgrade del proprio dispositivo periferico WAN, è possibile ridurre le spese di capitale (CapEx), acquistandone uno che integri la tecnologia SD-WAN.

**Una performance delle applicazioni costante e affidabile:** le applicazioni lente possono essere la rovina di qualsiasi organizzazione. La SD-WAN consente di utilizzare varie connessioni ad alta velocità dello stesso ISP, oppure di ISP diversi, per mantenere una performance delle applicazioni rapida e sempre disponibile sulla WAN, tutto a un costo minore rispetto all'MPLS. Inoltre, offre i controlli necessari per limitare le app non essenziali e indirizzare più rapidamente il traffico verso quelle più importanti, in base a criteri che possono essere definiti.

**Maggiore flessibilità:** con un abbonamento al servizio MPLS, si rimane "bloccati" con lo stesso provider fino al termine del contratto. La SD-WAN garantisce invece la flessibilità di aggiungere e rimuovere ISP, approfittando delle offerte di provider locali, che potrebbero avere tariffe ancora più convenienti. Inoltre, è anche possibile utilizzare l'MPLS tra la sede centrale e le filiali più grandi, ma la SD-WAN per le sedi più piccole.

**Maggiore agilità:** le organizzazioni in crescita hanno bisogno di poter includere rapidamente nuove sedi e applicazioni, per poter soddisfare l'aumento della domanda. Siccome è una overlay, o rete virtuale, la SD-WAN permette di aggiungere rapidamente altre sedi e di accelerarne la distribuzione. È anche possibile incrementare la larghezza di banda per adattare la struttura alla presenza di nuove sedi, oppure durante gli orari caratterizzati da picchi di utilizzo di Internet.

## Sophos SD-WAN: un valido aiuto per le organizzazioni

Indipendentemente dal tipo o dalle dimensioni di un'organizzazione, Sophos offre un valido aiuto per impostare una rete distribuita e protetta che utilizza la tecnologia SD-WAN per connettere la sede centrale con le sedi remote e le filiali. Con Sophos è possibile limitare le spese e ridurre il costo totale di proprietà (Total Cost of Ownership, TCO), sostituendo l'MPLS con servizi internet meno cari, eliminando allo stesso tempo hardware superflui. Abbiamo integrato la SD-WAN nei nostri XG Firewall, incluse le appliance hardware, software e virtuali. Ora è possibile usufruire di tutti i vantaggi di un vendor di sicurezza leader di settore, per proteggere la trasmissione di informazioni di natura sensibile, pur mantenendo costantemente alti livelli di performance e disponibilità per applicazioni cloud quali Office 365, Salesforce, G Suite, Microsoft Azure e altre, sia nella rete locale che globale.

## I vantaggi dei Sophos XG Firewall con SD-WAN

I Sophos XG Firewall che eseguono la più recente versione del firmware XG Firewall possono usufruire di molti dei vantaggi offerti dalla SD-WAN.

**Riduzione dei costi:** grazie all'integrazione della SD-WAN in tutti i Sophos XG Firewall, non occorre acquistare un prodotto SD-WAN a parte. Inoltre, la sostituzione di tutte le connessioni di rete MPLS con servizi Internet meno costosi contribuirà a diminuire le spese.

**Massima protezione:** disponibili come opzioni hardware, software, virtuali e cloud, i firewall next-gen leader di settore Sophos XG Series garantiscono massima protezione contro malware, ransomware, intrusioni e altre minacce che incombono sulla rete distribuita.

**Xstream:** XG Firewall offre un approccio innovativo al modo di identificare i rischi, proteggere i sistemi dalle minacce e rispondere agli incidenti, senza che ne risenta la performance. La nostra architettura Xstream per XG Firewall utilizza un'architettura esclusiva per l'elaborazione dei pacchetti, in grado di garantire livelli estremi di visibilità, protezione e performance.

**Distribuzione "Branch-in-a-Box":** creazione e distribuzione di soluzioni SD-Branch personalizzate per ogni sede remota, con i nostri esclusivi ed economici dispositivi periferici RED, oppure con i nostri dispositivi desktop a moduli XG Firewall. Includono SD-WAN, funzionalità di sicurezza e di rete affidabili, nonché opzioni LTE e wireless ad alta velocità, tutto in un'unica appliance hardware gestita centralmente.

**Continuità aziendale:** è possibile garantire l'operatività delle organizzazioni, grazie a connessioni ridondanti dagli stessi (o altri) ISP, per gestire routing e failover, nonché per preservare la sessione in caso di interruzioni del servizio WAN.

**RED:** i Sophos SD Remote Ethernet Devices (SD-RED) sono dispositivi economici che consentono di ridurre ulteriormente le spese. L'appliance SD-RED inoltra il traffico cifrato dalla sede remota a un firewall locale o centrale, che analizza i dati alla ricerca di minacce, prima di inoltrarlo a Internet.

**Sincronizzazione:** il sistema di Synchronized Security, un'esclusiva Sophos, abilita la condivisione di informazioni in tempo reale tra i prodotti Sophos all'interno della rete distribuita con il nostro Security Heartbeat™, per consentire la risposta automatica agli incidenti di sicurezza.

**Ottimizzazione della performance delle applicazioni:** a differenza dell'MPLS, che penalizza la performance effettuando il backhaul del traffico dalla sede remota al data center aziendale, per poi inoltrarlo a Internet, la SD-WAN elimina gli intasamenti e la latenza connettendosi direttamente a Internet, per un accesso più rapido alle applicazioni cloud.

**Maggiore agilità:** aggiunta rapida delle sedi remote, senza bisogno di tecnici in situ, grazie alla distribuzione zero-touch di Sophos. I nuovi servizi e le nuove applicazioni cloud possono essere inclusi velocemente nell'intera infrastruttura di rete.

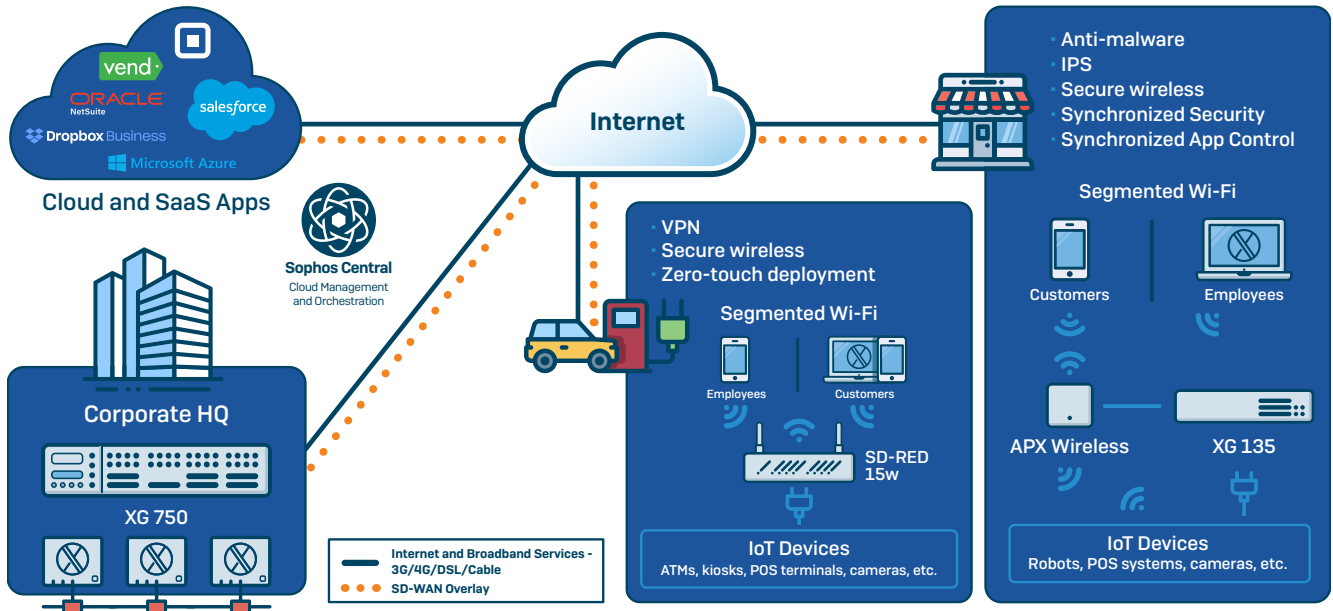
**Migliore visibilità e controllo sulle applicazioni:** livelli mai raggiunti prima di visibilità sull'utilizzo delle applicazioni nella rete. Sophos Synchronized SD-WAN, una funzionalità di Synchronized Security, sfrutta gli elevati livelli di chiarezza e affidabilità dell'identificazione delle applicazioni di Sophos Synchronized Application Control per identificare il 100% delle applicazioni sconosciute, elusive e personalizzate. Questo consente di attribuire priorità alle app utili e bloccare quelle indesiderate. Le applicazioni che precedentemente non venivano identificate possono essere aggiunte alla SD-WAN con policy di routing, per un livello di controllo sul routing delle applicazioni al di fuori della portata degli altri firewall.

**Orchestratura di tutti i sistemi:** massima efficienza di coordinazione e automazione della rete, per mezzo delle nostre potentissime API. La rete distribuita può quindi essere gestita da qualsiasi luogo con Sophos Central: la piattaforma Sophos basata sul cloud per la gestione unificata.

## Casi di utilizzo Sophos per la SD-WAN

È possibile distribuire dispositivi Sophos XG Firewall e SD-RED nei seguenti casi di utilizzo, per connettere in maniera sicura le sedi remote e le filiali con una sede centrale.

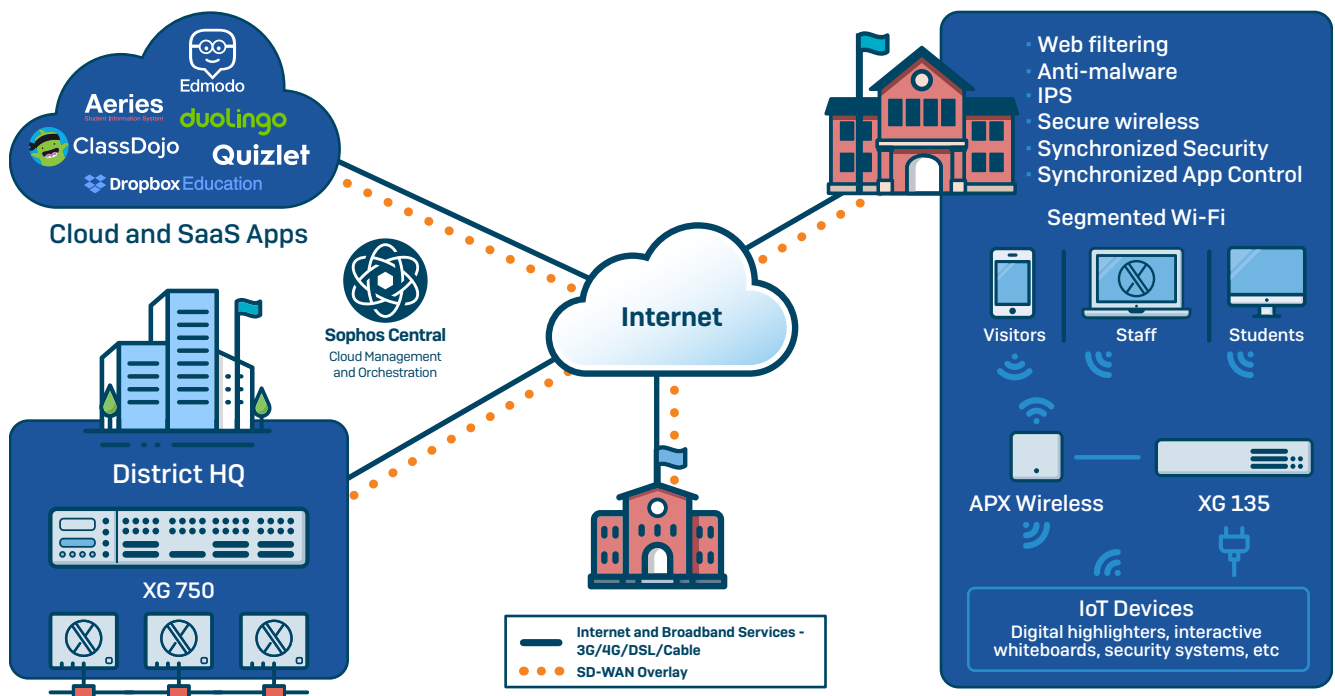
### 1. Vendita al dettaglio



**Descrizione:** catene di vendita al dettaglio con vari negozi o franchising, che scambiano dati finanziari e personali dei clienti per mezzo di transazioni presso il negozio oppure on-line.

- Connessione dei negozi di franchising e dei dispositivi abilitati a Internet sia all'interno che all'esterno della rete, inclusi POS, totem multimediali, segnaletica digitale e dispositivi IoT
- Protezione della trasmissione di informazioni di natura riservata sui clienti dai POS alla sede centrale
- Aggiornamento delle nuove tecnologie POS, quali i pagamenti con dispositivi mobili e coupon digitali
- Accesso a Internet per i clienti tramite una rete Wi-Fi isolata dai sistemi a cui accedono i dipendenti
- Conformità alle disposizioni normative PCI DSS [U.S.A.] e GDPR [UE]

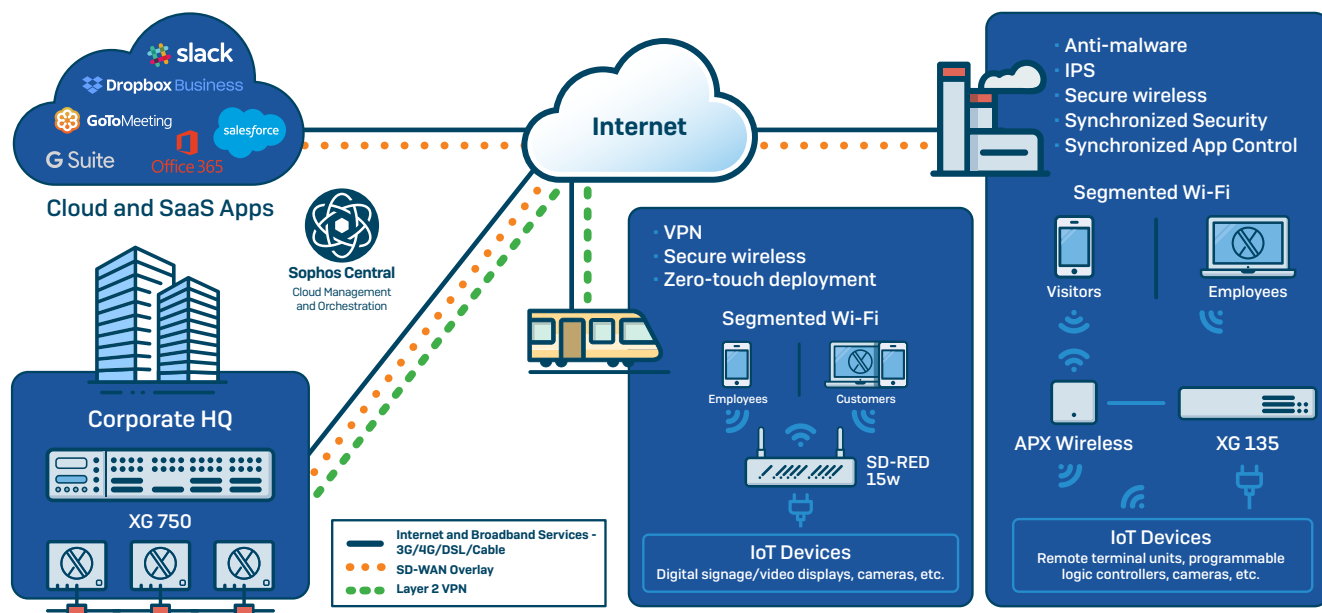
## 2. Istruzione



**Descrizione:** asili, scuole primarie e secondarie individuali o distretti scolastici, consolidati in un unico distretto per fornire servizi di istruzione per alunni e studenti.

- Connessione di scuole e sedi centrali nei distretti scolastici degli istituti primari o secondari
- Scambio sicuro di dati relativi all'istituto, informazioni personali degli studenti e transazioni finanziarie
- Gestione della crescita continua del numero di nuovi dispositivi (personali o forniti in dotazione) che accedono alla rete
- Aggiornamento delle tecnologie e applicazioni didattiche presenti nella rete, in base alle ultime evoluzioni
- Conformità alle disposizioni normative CIPA (U.S.A.)

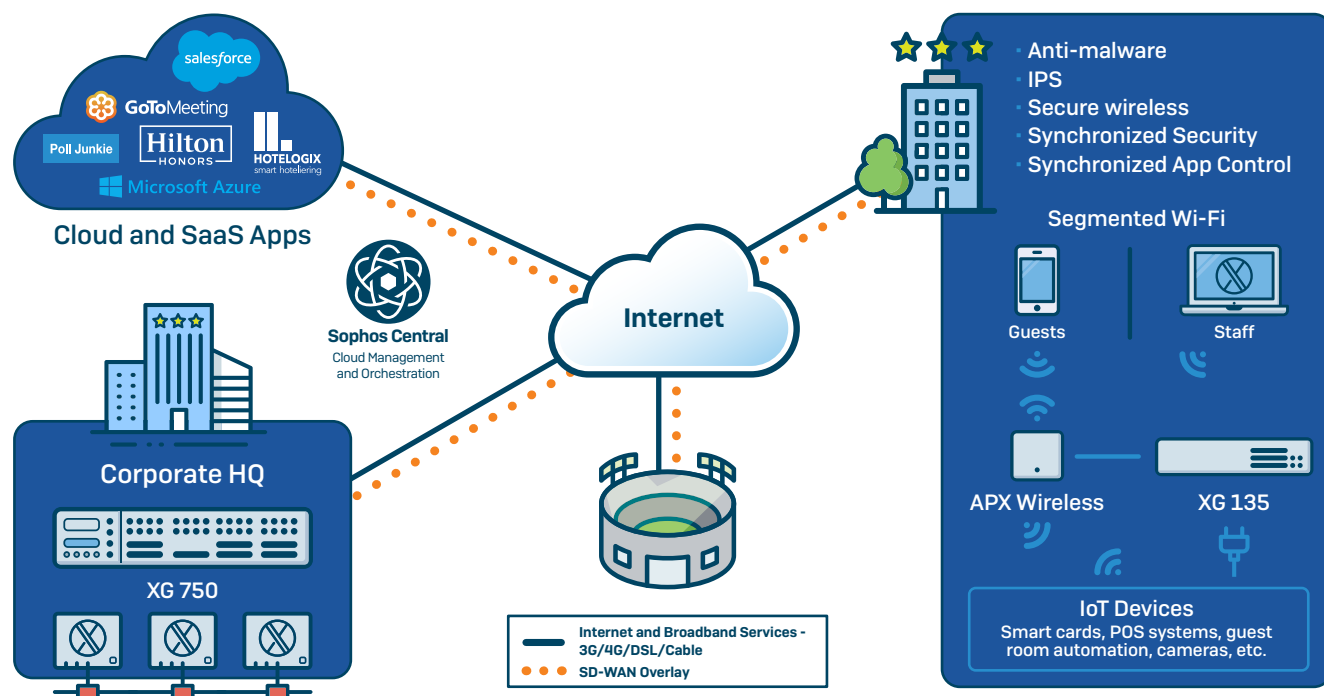
### 3. Sistemi di controllo industriale, dispositivi remoti e veicoli



**Descrizione:** organizzazioni quali industrie manifatturiere, servizi pubblici, trasporti, edilizia e altre, che utilizzano tecnologie (ad es. SCADA), dispositivi remoti (ad es. sistemi di videosorveglianza) o veicoli pubblici con il servizio Condivisione Connessione Internet (ICS) a sostegno di infrastrutture essenziali.

- Connessione sia tra sedi statiche (fabbriche, stazioni, impianti) che veicoli (autobus, treni, velivoli) continuamente in viaggio tra la sede centrale e le varie destinazioni
- Protezione dei dati raccolti da sensori e strumenti presso le sedi remote, e delle relative informazioni che vengono trasmesse a un host centrale
- Aggiornamento costante delle tecnologie POS e dei dispositivi IoT presenti sulla rete
- Protezione delle transazioni finanziarie e accesso a Internet e contenuti in streaming (ad es. musica e film) per i clienti
- Distribuzione di dispositivi Sophos SD-RED presso ciascuna sede e su ciascun veicolo, per una soluzione economica e zero-touch che consente di abilitare la connettività SD-WAN tra le sedi

## 4. Hotel e settore alberghiero

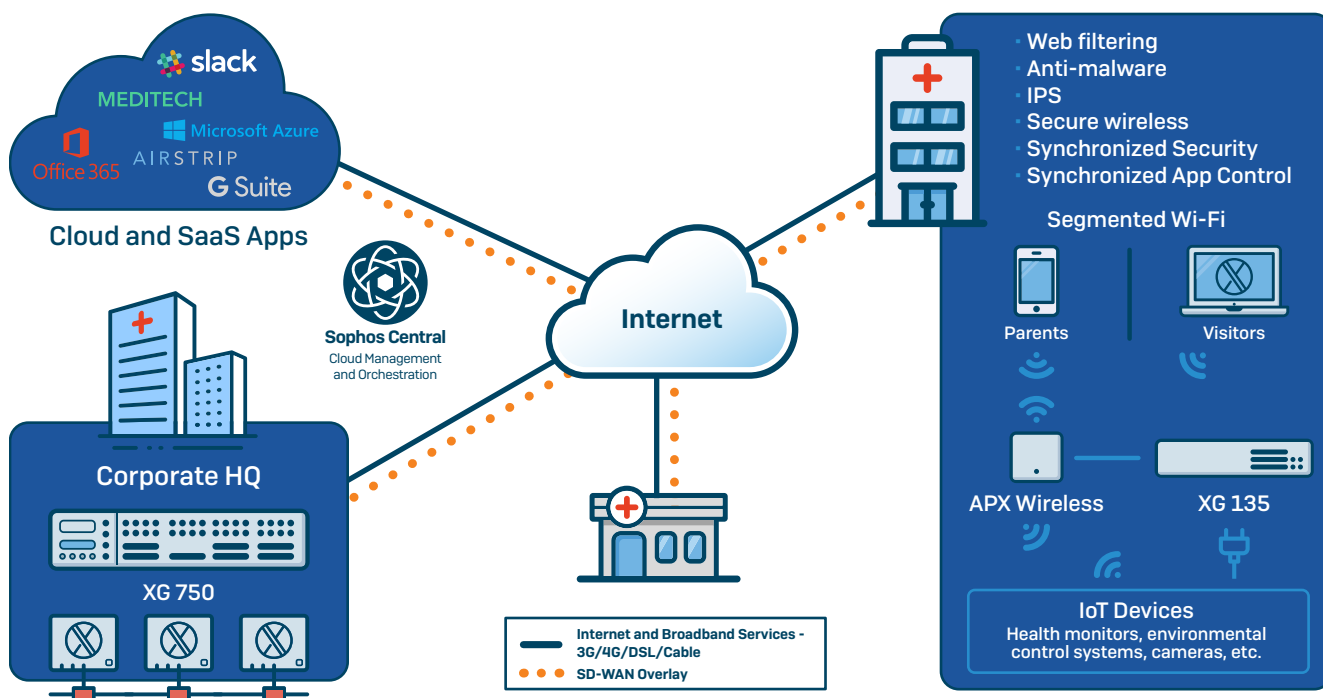


**Descrizione:** catene locali e globali di hotel/motel e operatori dell'accoglienza/organizzazione eventi, che offrono alloggio e servizi di intrattenimento.

- Connessione degli hotel e/o delle strutture di accoglienza e dei locali adibiti a eventi, per condividere informazioni riservate sugli ospiti e per abilitare servizi tra ciascuna struttura e la sede amministrativa
- Fornitura di servizi quali accesso Wi-Fi, chiavi digitali, contenuti in streaming e televoto in tempo reale per ospiti e clienti
- Aggiornamento dei sistemi, per tenere il passo con il crescente numero di dispositivi intelligenti che si connettono alla rete
- Protezione delle informazioni di natura riservata su ospiti e clienti e delle transazioni finanziarie contro gli attacchi
- Conformità alle disposizioni normative PCI DSS (U.S.A.) e GDPR (UE)



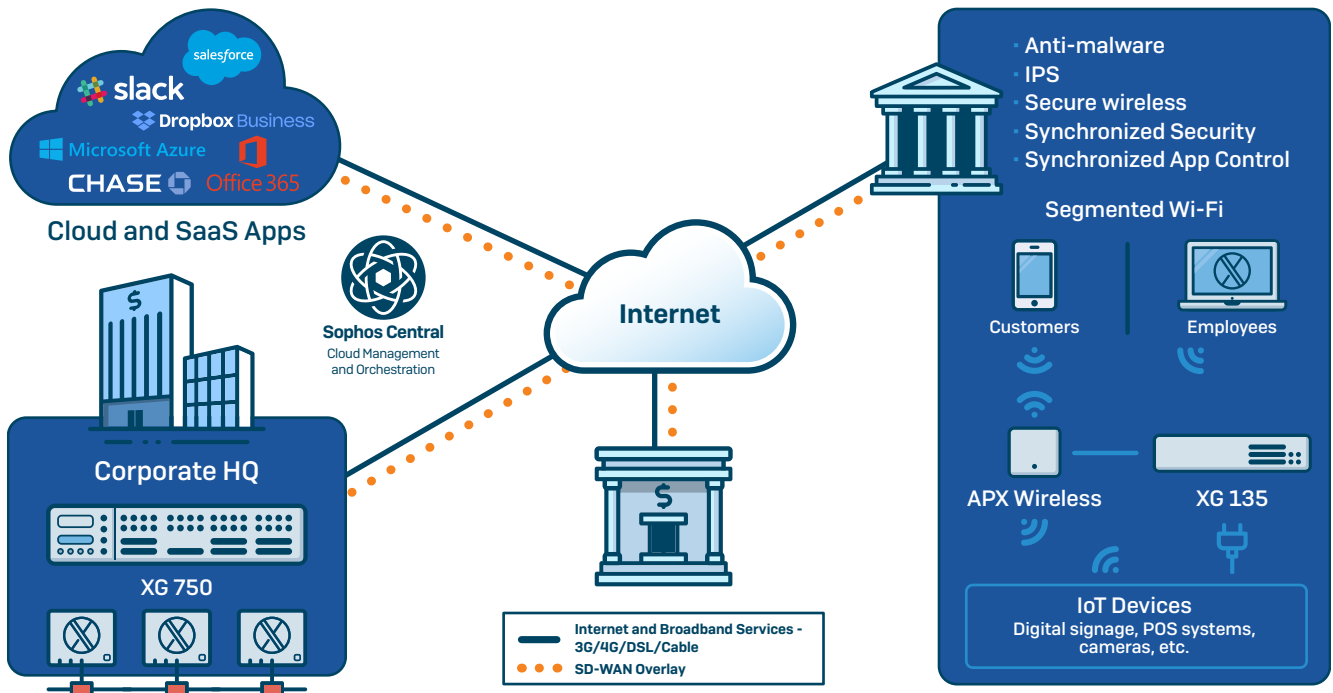
## 5. Sanità



**Descrizione:** un insieme di cliniche, ambulatori medici e strutture sanitarie che utilizzano varie reti e tecnologie diverse per fornire servizi sanitari.

- Connessione delle strutture sanitarie pubbliche e private, per condividere informazioni mediche di natura critica
- Aggiornamento dei sistemi, per tenere il passo con il crescente numero di dispositivi medici e IoT connessi
- Implementazione dell'utilizzo di nuove tecnologie e applicazioni sanitarie sulla rete, quali la telemedicina
- Aggiunta rapida di nuove strutture sanitarie oppure uffici a una rete, con la distribuzione zero-touch
- Conformità alle disposizioni normative HIPAA (U.S.A.) e GDPR (UE), che richiedono la trasmissione sicura delle informazioni elettroniche sanitarie protette (ePHI)

## 6. Finanza



**Descrizione:** Istituzioni quali banche, cooperative di credito e agenzie di intermediazione, che offrono servizi finanziari ad aziende e singoli individui.

- Connessione delle sedi locali, regionali e nazionali, per condividere ogni giorno grandi quantità di informazioni di natura sensibile sui clienti
- Protezione dei dati personali, delle informazioni aziendali e delle transazioni finanziarie contro le minacce informatiche
- Aggiornamento dei sistemi, per tenere il passo con il crescente numero di dispositivi IoT quali bancomat e telecamere di videosorveglianza
- Implementazione di nuove tecnologie e applicazioni all'interno della rete, quali internet banking, firme elettroniche, firme digitali, segnaletica digitale e video
- Conformità alle disposizioni normative PSD2, PCI DSS (U.S.A) e GDPR (UE)

## Conclusione

Quello delle reti distribuite è un panorama in continua evoluzione. Tecnologie obsolete quali l'MPLS, che un tempo connetteva organizzazioni con varie sedi diverse situate a grandi distanze le une dalle altre, non sono più la soluzione ideale. Al giorno d'oggi, le organizzazioni si affidano sempre maggiormente alla SD-WAN, che offre maggiore flessibilità e controllo sulle applicazioni, nonché uno straordinario livello di agilità, tutto a un costo di gran lunga inferiore.

I Sophos XG Firewall con funzionalità SD-WAN abilitano la connessione con sedi remote e filiali, l'invio di applicazioni cloud e SaaS essenziali e la condivisione di dati e informazioni, tutto con l'orchestrazione dell'intero sistema dal cloud grazie a un'unica soluzione. Inoltre, offrono la certezza e la sicurezza di una protezione a cura di un'azienda leader nel settore della cybersecurity.

Per maggiori informazioni sulla SD-WAN e sui Sophos XG Firewall, visitare: [www.sophos.it/sd-wan](http://www.sophos.it/sd-wan).

Per maggiori informazioni  
sulla SD-WAN e sui Sophos XG  
Firewall, visitare:  
[www.sophos.it/sd-wan](http://www.sophos.it/sd-wan).

Vendite per Italia:  
Tel: (+39) 02 94 75 98 00  
E-mail: [sales@sophos.it](mailto:sales@sophos.it)