SOPHOS

Making the Move to SD-WAN with Sophos: Six Use Cases

Introduction

Distributed organizations have become more common in today's connected world. The ability to link together sites spread over large geographical distances to exchange information and deliver applications has changed how businesses operate, schools provide education and hospitals care for patients.

Regardless of their industry or size, distributed organizations have many of the same needs. These include sharing data, delivering cloud and SaaS applications, and enabling communications and transactions between remote locations and headquarters. Securing each from cyber threats such as ransomware, malware, and breaches is critical. Distributed organizations also want the agility to bring up new sites and add new apps and services quickly. Managing it all can be time-intensive, so having the tools to orchestrate everything is important. So are the costs, which can add up over time.

The traditional solution used by many organizations has been multi-protocol label switching (MPLS), a routing technique that first came about almost two decades ago. MPLS offers benefits beyond just connecting geographically distributed sites. For example, by directing packets from one network node to another based on the shortest path available, MPLS provides high quality of service (QoS) for latency-sensitive real-time applications such as voice and video. However, there are drawbacks. The move to cloud computing means services such as MPLS that backhaul traffic through a data center are no longer the best solution. Also, MPLS isn't available everywhere. The biggest reason distributed organizations are moving away from MPLS, however, is the cost. The emergence of alternative technologies such as software-defined wide area networking, or SD-WAN, enables organizations to stand up new sites quickly, connect those sites, exchange information, and deliver applications at a significantly lower cost than they could using MPLS.

At its core, SD-WAN is an overlay technique that sits on top of the existing WAN architecture. It can leverage any transport service, including DSL, cable, 3G/4G/LTE, and even MPLS to intelligently steer traffic over the WAN from source to destination with minimal or no latency, jitter, or packet loss. The goal is to provide an exceptional user experience through high quality of service. The enhanced QoS, in turn, drives productivity increases. When it comes to deploying SD-WAN, organizations have several choices available. Pure-play SD-WAN vendors offer more feature-rich solutions, but the cost of the appliance combined with the ongoing management and lack of built-in security can be prohibitive. Increasingly, organizations are looking for integration of SD-WAN capabilities in their firewall.

The Move to SD-WAN

SD-WAN continues to grow in popularity according to Gartner, which forecasts a 59% compound annual growth rate (CAGR) through 2021 to become a $1.3 billion market. By providing distributed organizations with a range of compelling benefits at a lower cost, SD-WAN helps make transitioning to the technology easy and affordable. Here are some key reasons why.

Reduced expenses: While MPLS may still warrant a place in your network for certain needs, moving some or all of your connections over to SD-WAN will save you money. SD-WAN takes advantage of less expensive, publicly available internet and broadband services so your OpEx costs are greatly reduced. And, if you're looking to upgrade your WAN edge device you could lower your CapEx by purchasing one that integrates SD-WAN technology.

Consistent, predictable application performance: Slow-performing applications can doom any organization. SD-WAN enables you to utilize multiple high-speed connections either from the same ISP, or several, to ensure application performance over the WAN is consistently fast and available while still paying less than you would for MPLS. You also get the controls to throttle non-critical apps and route traffic faster over those that are more important based on your criteria.

Greater flexibility: When you sign up for MPLS service you are "locked in" with a single provider for the length of the contract. In contrast, with SD-WAN you have the flexibility to add and drop ISPs while taking advantage of local providers who may offer even lower rates. You can also use MPLS between headquarters and larger sites while smaller sites connect over SD-WAN.

Enhanced agility: Growing organizations need to add new sites and applications quickly to meet the increase in demand. Because it is an overlay, or virtual network, SD-WAN enables you to scale rapidly and speed the deployment of additional sites. You can also add more bandwidth to accommodate the new sites, as well as during periods of spike internet usage.

Sophos SD-WAN Can Help

No matter your organization's type or size, Sophos can help you build a secure distributed network that uses SD-WAN technology to connect your central site with remote and branch locations. With Sophos, you'll reduce expenses and lower your total cost of ownership (TCO) by replacing MPLS with inexpensive internet services while eliminating unnecessary hardware. We've integrated SD-WAN into our XG Firewalls, including hardware, software, and virtual appliance options. Now you can get all the advantages of a leading security vendor to protect the transmission of sensitive information while achieving consistent performance and availability for cloud applications such as Office 365, Salesforce, G Suite, Microsoft Azure, and others across your regional or global network.

Advantages of Sophos XG Firewalls With SD-WAN

Sophos XG Firewalls running the latest XG Firewall firmware version can take advantage of a broad range of SD-WAN benefits.

Lower your costs: With SD-WAN integrated into every Sophos XG Firewall, there's no need to add a standalone SD-WAN product. Replacing some or all of your MPLS network connections with less-expensive internet services will also reduce your expenses.

Maximize protection: Available in hardware, software, virtual and cloud options, Sophos' industry-leading XG series next-generation firewalls deliver maximum protection from malware, ransomware, intrusions, and other threats across your distributed network.

Go Xstream: XG Firewall brings a fresh approach to the way you identify hidden risks, protect against threats, and respond to incidents without taking a performance hit. Our Xstream architecture for XG Firewall utilizes a unique packet processing architecture that delivers extreme levels of visibility, protection, and performance.

Deploy Branch-in-a-Box: Create and deploy your own SD-Branch solution at each remote site with our unique affordable SD-RED edge devices or modular XG Firewall desktop devices. They come complete with SD-WAN, robust networking and security features, along with LTE and high-speed wireless options in a single hardware appliance that is centrally managed.

Achieve business continuity: Keep your organization up and running with redundant connections from the same, or different, ISPs to handle routing, failover, and session preservation in the event of potential WAN failures or outages.

Go SD-RED: Lower your costs even more with inexpensive Sophos SD-RED Remote Ethernet Devices. The SD-RED appliance forwards encrypted traffic from the remote site to a local or central firewall that scans the data for threats before it is sent to the internet.

Get synced: Sophos' unique Synchronized Security system shares real-time information between Sophos products across your distributed network via our unique Security Heartbeat™ for automated response to security incidents.

Optimize application performance: Unlike MPLS, which exacts performance penalties by backhauling traffic from the remote site through the corporate data center and then to the internet, SD-WAN eliminates bottlenecks and latency by connecting directly to the internet for faster access to cloud applications.

Become more agile: Bring up remote locations quickly without onsite IT personnel through Sophos zero-touch deployment. Add and deliver new cloud services and applications quickly across your entire network infrastructure.

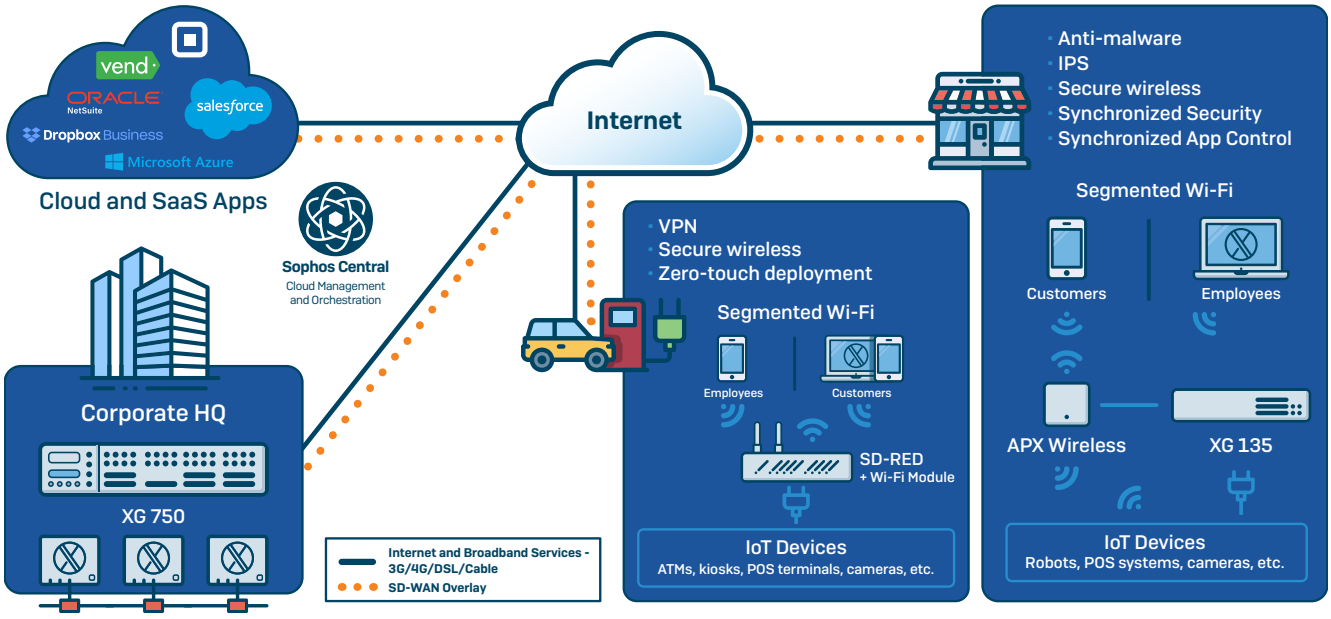
Improve application visibility and control: Get unprecedented visibility into application usage on your network. Sophos Synchronized SD-WAN, a Synchronized Security feature, leverages the added clarity and reliability of application identification that comes with Sophos Synchronized Application Control to identify 100% of unknown, evasive, and custom applications so you can easily prioritize the apps you want and block the ones you don't. Add these previously unidentified applications to SD-WAN routing policies for a level of application routing control and reliability that other firewalls can't match.

Orchestrate everything: Coordinate and automate your network functions more efficiently using powerful APIs. Then manage your entire distributed network from anywhere through Sophos Central, Sophos' cloud-based unified management platform.

Sophos SD-WAN Use Cases

Deploy Sophos XG Firewall and SD-RED devices in the following use cases to securely connect remote and branch locations with a central site.

1. Retail



Description: Retail chains consisting of multiple stores or franchises that exchange customer financial and personal data through in-store and online transactions.

a. Connect franchise stores and the internet-enabled devices inside or outside, including point of sale (POS) machines, kiosks, digital signage, and IoT devices

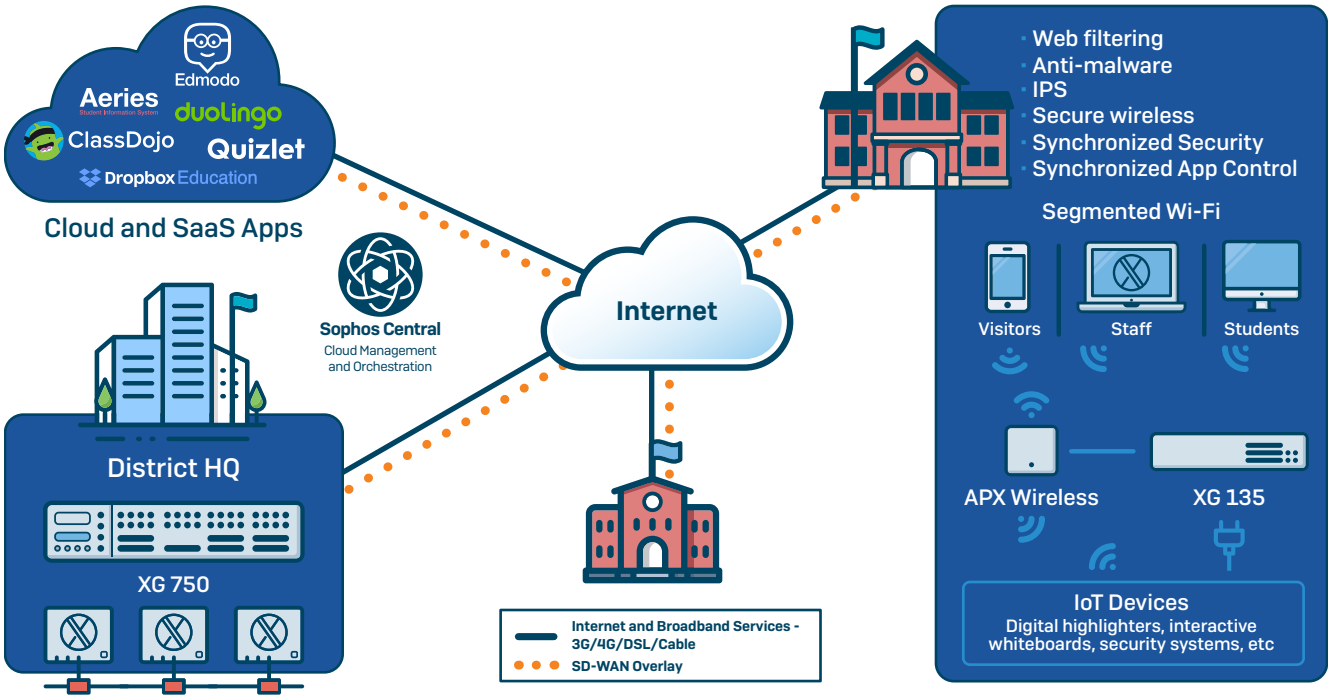
b. Secure the transmission of confidential customer information back to the central site from POS devices

c. Keep up with new POS technologies such as mobile device payments and digital coupons

d. Provide customers with internet access over Wi-Fi that is isolated from employee access

e. Comply with PCI DSS (U.S.) and GDPR (EU) regulatory mandates

2. Education



Description: Individual K-12, primary and secondary schools, or school districts, consolidated into a single district to provide student education.

a. Connect the schools and headquarters in your primary or secondary school district

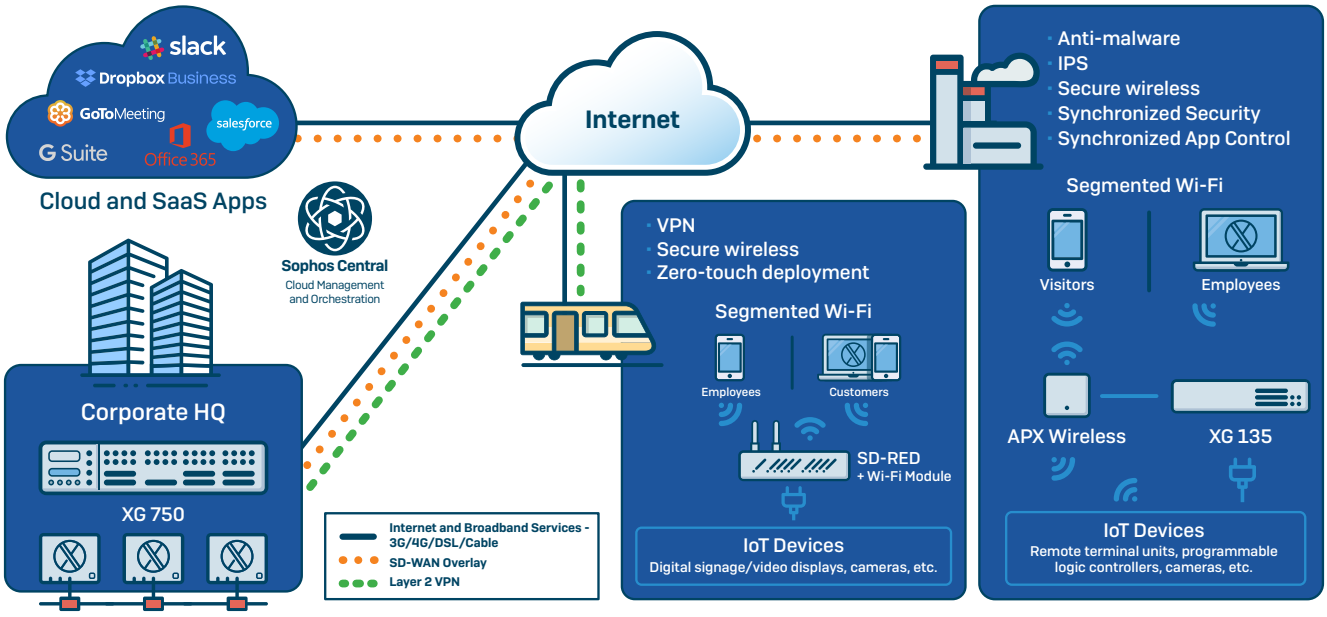
b. Securely exchange personal student and faculty information and financial transactions

c. Manage the continued growth of new devices accessing the network, both personal and school-issued

d. Keep pace with changing educational technologies and applications on the network

e. Comply with CIPA regulatory mandates (U.S.)

3. Industrial Control Systems, Remote Devices, and Vehicles



Description: Organizations such as manufacturing, utilities, transportation, construction, and others that use ICS technologies (e.g. SCADA), remote devices (e.g. CCTV) or public vehicles (e.g. rapid transit) to support crucial infrastructure.

a. Connect both static sites (factories, terminals, utility plants) and vehicles (buses, trains, airplanes) that continually travel between destinations to your central headquarters

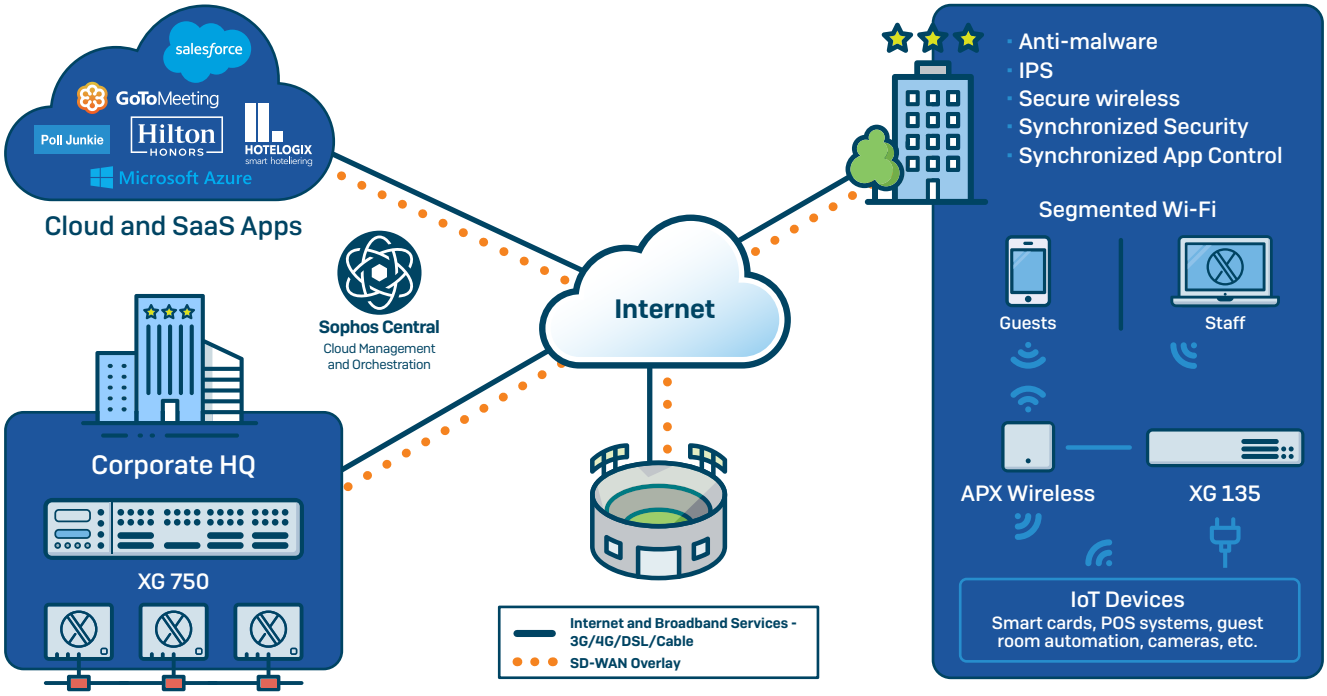
b. Secure data collected from sensors and field instruments at remote sites that is transmitted back to a central host

c. Keep up with constantly-changing POS technologies and IoT devices on the network

d. Protect financial transactions and provide internet access and streaming content (e.g. movies and music) to customers

e. Deploy Sophos SD-RED devices at each site and on each vehicle for an affordable, zero-touch solution to SD-WAN branch connectivity

4. Hotels and Hospitality



Description: Local and global hotel/motel chains and hospitality/event management organizations that provide lodging and entertainment services.

a. Connect hotel properties and/or hospitality and event venues to share confidential guest information and enable services between each property and corporate headquarters

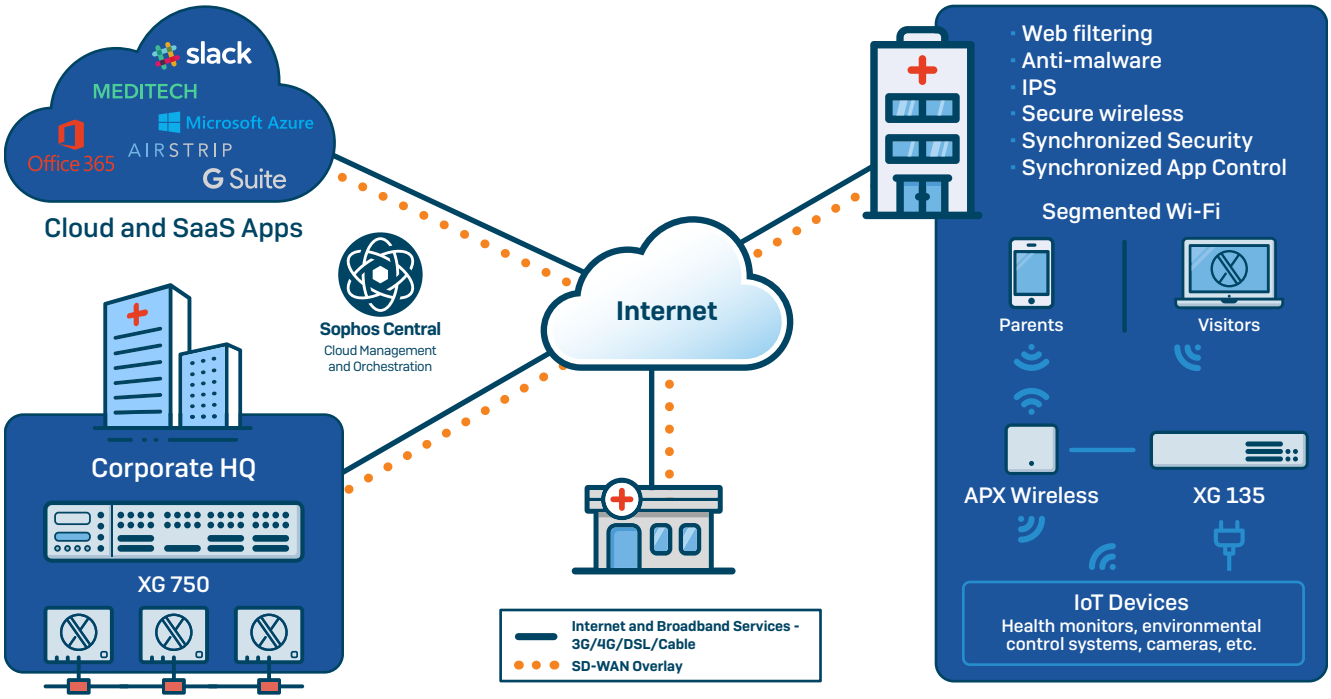
b. Provide services such as Wi-Fi access, digital room keys, streaming content, and real-time fan voting to guests and customers

c. Keep pace with the increasing number of smart devices connecting to the network

d. Ensure confidential guest/customer information and financial transactions are secured from attacks

e. Comply with PCI DSS (U.S.) and GDPR (EU) regulatory mandates

5. Healthcare



Description: A collective of hospitals, doctors' offices, and medical facilities using disparate networks and technologies to offer healthcare services.

a. Connect public and private healthcare facilities to share critical medical information

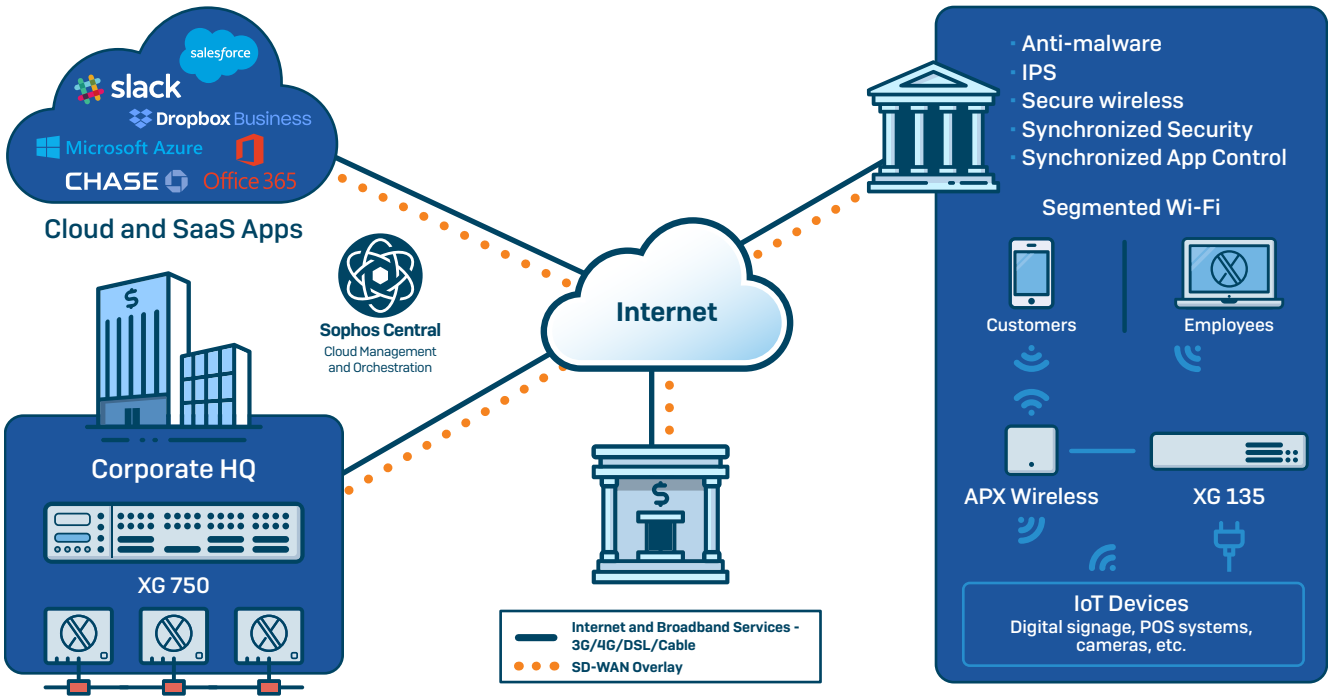
b. Keep up with the continued growth of connected medical and IoT devices

c. Enable the use of new healthcare technologies and applications on the network such as telehealth

d. Bring up new healthcare facilities or add existing offices to the network quickly using zero-touch deployment

e. Comply with HIPAA (US) and GDPR (EU) regulatory mandates that require secure transmission of patients' electronic protected health information (ePHI)

6. Finance



Description: Institutions such as banks, credit unions, and brokerage firms that provide personal and corporate financial services.

a. Connect local, state, and national branch sites that share large amounts of sensitive customer information each day

b. Protect personal and corporate data and financial transactions from cyber threats

c. Keep up with the continued growth of connected IoT devices such as ATMs and security cameras

d. Enable new technologies and applications on the network, such as mobile banking, e-signatures, digital signage, and videos

e. Comply with PSD2, PCI DSS (U.S.) and GDPR (EU) regulatory mandates

Conclusion

The landscape for distributed networks continues to evolve. Legacy technologies such as MPLS that once connected multi-site organizations across vast distances are no longer the best solution. Today's organizations are turning to SD-WAN which offers greater flexibility, more control over applications, and enhanced agility at a much lower cost.

Sophos XG Firewalls with built-in SD-WAN capabilities enable you to connect your remote and branch sites, deliver critical cloud and SaaS applications, and share data and information while orchestrating everything from the cloud, all in one solution. And you get the confidence of knowing you're protected by an industry leader in cybersecurity.

To learn more about SD-WAN and Sophos XG Firewalls, visit us at www.sophos.com/sd-wan.

To learn more about SD-WAN and Sophos XG Firewalls, visit us at www.sophos.com/sd-wan.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20-3-31 UC-NA (GH)

SOPHOS