Successful Network and Security Transformation Powers the Digital Enterprise

Executive Summary

Enterprises continue to embrace digital transformation with the intent to increase efficiency, enhance customer satisfaction, pursue new market opportunities, boost profitability and maintain a competitive edge. The cloud is integral to any successful digital transformation initiative. Why? Today, there are more applications running in the cloud than in traditional enterprise data centers, and the majority of these applications are being consumed as software-as-a-service (SaaS). Moreover, in the cloud-first world enterprises must ensure that applications are directly and securely accessible at any time, from any location using any device. They also want to ensure that the network consistently delivers the highest quality of experience to employees and customers. Finally, the explosion of mobile and IoT devices in the enterprise has dramatically increased the attack surface, exposing enterprises to security breaches that can compromise data and result in network downtime.

Today's corporate networks were never designed for the cloud and fall well short on delivering the agility and security required to address the requirements of digital transformation. It is critical that enterprises not only secure applications in the cloud but also protect users connecting to these applications across the network. At the same time, today's competitive business environment demands that enterprises deliver the highest quality of experience to customers through a network that maintains the performance and availability required to keep their business up and running.

> *To realize the full promise of the cloud and digital transformation, enterprises will need to transform both their WAN and security architectures — not just one or the other. A company may start with just one project, but it's important to make decisions knowing that to realize the true value of cloud investments, both aspects eventually must be addressed.*
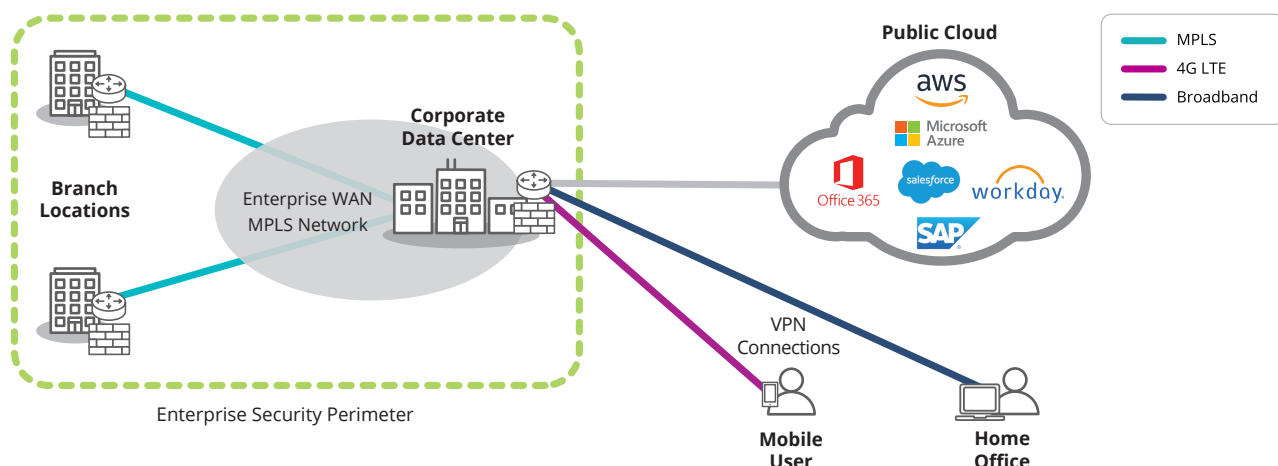
Figure 1: Traditional enterprise WANs and perimeter-based security approaches were not designed for the cloud. Backhauling all application traffic from branch locations to the data center impairs performance and delivers an inconsistent user experience. Additionally, remote access VPNs and branch firewalls also result in inconsistent user experiences and are increasingly ineffective in blocking vulnerabilities.

To realize the full promise of the cloud and digital transformation, enterprises will need to transform both their WAN and security architectures — not just one or the other. Companies have already made significant investments in their shift to the cloud so the ultimate challenge is how to achieve a multiplier effect on those cloud investments. The answer is to modernize enterprise WAN and security architectures. Therefore, the strategic imperative is to adopt a more intelligent, highly automated software-defined wide area network (SD-WAN) that can be seamlessly integrated with cloud-delivered security services.

An enterprise may start with modernizing its WAN or security, but to realize the true value of cloud investments, both aspects must be addressed. And it's equally important to avoid vendor lock-in by choosing technology solution partners that provide flexibility and freedom-of-choice. With transformed network and security architectures, enterprises can embrace new timely innovations to accelerate productivity, growth and profitability, all while containing costs and mitigating business risk.

Apps are delivered in the cloud — security should be too

Traditionally, all application traffic from branch locations would be backhauled over private MPLS services to the corporate data center for security inspection and verification (see Figure 1). This architecture made

sense when applications were hosted exclusively in the corporate data center. But with applications and services migrating to the cloud, this traditional network architecture falls short, mainly because it impairs application performance and delivers an inconsistent user experience as traffic destined for the internet first goes through the data center and the corporate firewall before reaching its destination.

Furthermore, with an increasing number of employees working outside of the corporate network and connecting directly to cloud applications, traditional perimeter-based security is insufficient. The cloud and SaaS have forever changed the way users connect and interact with applications. By transforming their WAN and security architectures, enterprises can ensure direct, secure access to applications and services across multi-cloud environments regardless of location or the devices being used to access them.

A cloud security solution is a cloud-delivered service that supports multiple network security functions that include secure web gateway (SWG), firewall-as-a-service (FWaaS), cloud access security broker CASB) and zero trust network architecture (ZTNA). Previously, these were each unique and dedicated on-premise functions, but can now be delivered from the cloud in a unified manner as shown in Figure 2. If an enterprise evaluates and deploys these security functions individually, it is likely that application performance will be negatively impacted due to induced latency and bandwidth bottlenecks.
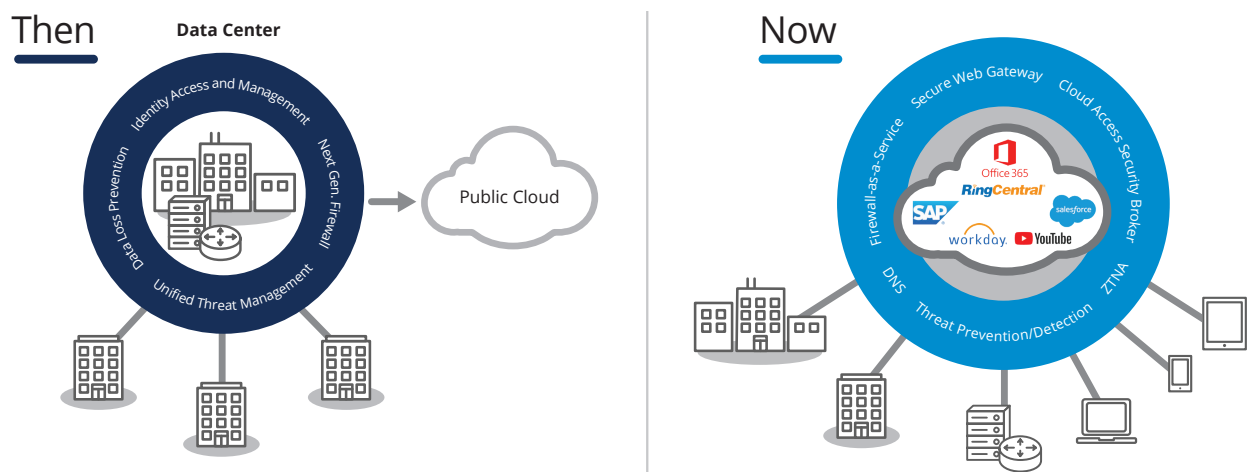
Figure 2: In the past it was all about securing the enterprise data center where applications were exclusively hosted. Now that applications have moved to and are being delivered from the cloud, enterprise perimeter-based security is becoming increasingly ineffective. It is imperative to think differently and move security to the cloud.

Early adopters of cloud-delivered security services often failed to implement an SD-WAN and therefore were unable to apply local internet breakout from branch sites and direct traffic to the cloud. Without the SD-WAN component, traffic is still backhauled to the data center. This defeats the purpose and negatively impacts application performance.

Adopting cloud-delivered security and SD-WAN still requires stateful firewall functionality at branch sites to block incoming threats, but eliminates the cost and complexity for on-premise, next-generation branch firewalls. As shown in Figure 3 below, using an advanced SD-WAN solution, enterprises can connect directly to the cloud via secure internet breakout using broadband internet connections. The intelligence to recognize whitelisted applications enables local breakout from the branch office to the nearest point of presence (PoP), eliminating latency and delivering the highest quality of experience for trusted SaaS and cloud applications such as Microsoft Office 365, 8x8 and RingCentral. Application awareness also provides the ability to send other internet-bound traffic first to a cloud-delivered security service for advanced inspection before forwarding to a SaaS provider. Advanced SD-WAN capabilities integrated with modern cloud-delivered security services ensures consistent policy enforcement and access control for users, devices, applications, and IoT.
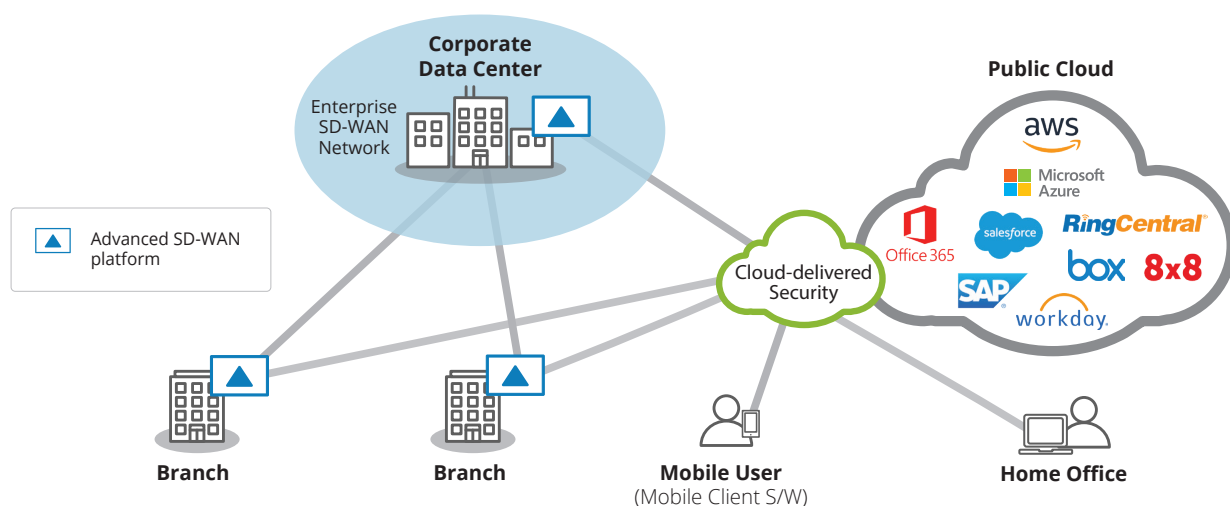

Figure 3: An advanced SD-WAN provides enterprises with a secure cloud on-ramp. Branch locations can use broadband connections and secure local internet breakout to directly connect to the cloud, optimizing application performance and user experience. The combination of SD-WAN and cloud security using a policy-based zero-trust network approach (ZTNA) ensures the WAN, users, devices and applications are secure.

This enables enterprises to enforce compliance, prevent downtime and mitigate the risk of data compromise associated with a security breach.

Securing enterprise IoT with SD-WAN

The proliferation of IoT across the enterprise network increases the attack surface, adding a new dimension of complexity. IoT devices are agentless and therefore are not able to utilize ZTNA architectures to protect them from vulnerabilities. As shown in Figure 4, by deploying an advanced SD-WAN platform at branch locations, enterprises can configure unique policies and granularly segment the network to enforce security for IoT endpoints. This ensures the network can operate without interruption while mitigating risks associated with breaches. An advanced SD-WAN platform also provides enterprises with additional flexibility to run third-party probes specifically for IoT security within the platform. By doing so, enterprises can use best-of-breed IoT security and network solutions without incurring the incremental cost or management complexity associated with operating separate dedicated appliances.

With the constantly evolving approaches to delivering network security and the intricacy of building complex networking solutions, it is important to evaluate best-in-class security and network solutions from vendors that have proven experience and focus. It is unrealistic to find a single vendor that can deliver best-in-class capabilities across both domains and enterprises shouldn't be forced to compromise with basic capabilities on either side.

With security being a top-of-mind concern due to a continuously evolving threat landscape, enterprises must retain the agility to quickly and cost-effectively adopt new security solutions without being locked into a single vendor solution. Having an independent network solution provides enterprises with the assurance and peace of mind to select and deploy the cloud security solutions that best align to their evolving business and security requirements.

By having the freedom of choice to select best-of-breed vendor solutions that unify SD-WAN and cloud security using automation, enterprises gain increased business agility and speed, while reducing complexity and cost by building a consistent security architecture that blocks the impact of cyberattacks. This ultimately enables enterprises to achieve a multiplier effect on their existing and ongoing investments in cloud applications and services.
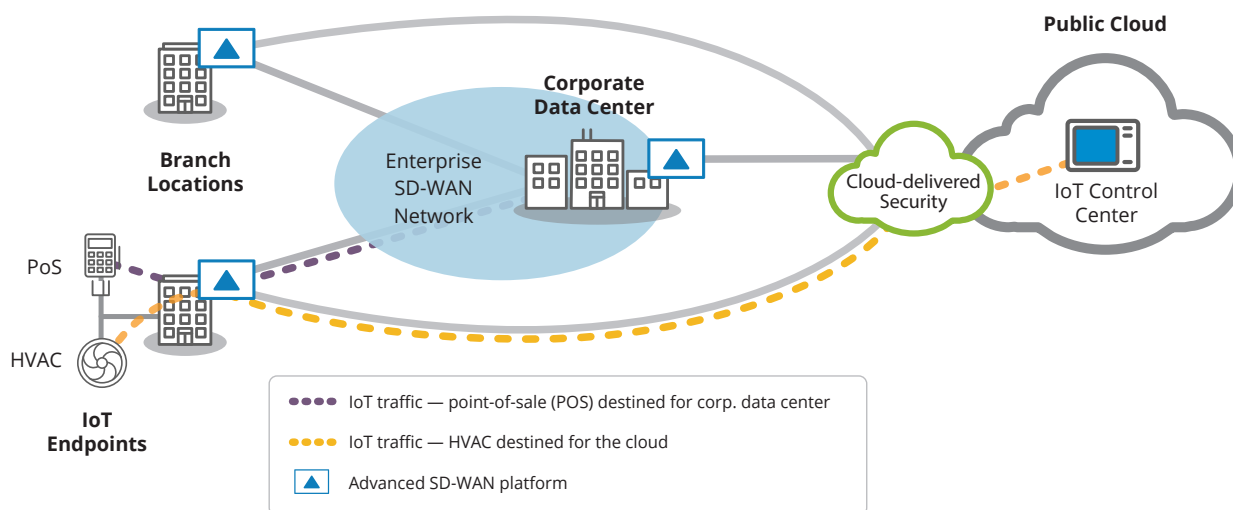

Figure 4: IoT endpoints are growing rapidly and pose new risks for security breaches. By using an advanced SD-WAN platform, enterprises can set unique policies and segment the network to very granular levels, ensuring traffic is sent to the correct destination including the cloud without any compromise or risk of exposure. In the diagram, all point-of-sale transaction data from the branch are destined to the enterprise data center, whereas the HVAC traffic is routed to an IoT control center in the cloud.

Network transformation is critical for digital transformation success

In addition to all the benefits of migrating to a modern cloud-delivered security architecture, there is tremendous value in transforming the network for a cloud-first enterprise. The traditional, router-centric WAN was never designed for the cloud. Enterprises must modernize their WAN architecture and rethink how to best architect their branch networks to improve the performance and security of cloud-based applications. Enterprises are increasing the use of cloud and SaaS, with a focus on delivering the highest quality of experience to users.

Network transformation encompasses providing a more efficient path and better experience between users and the cloud. As described previously, adoption of local internet breakout to cloud-hosted and SaaS applications directly from branch locations not only optimizes available bandwidth but also reduces any latency that can negatively impact user productivity.

Many organizations are transforming their network edge and embracing software-defined WAN to connect branch locations using broadband internet connections. SD-WAN provides application-driven intelligent path selection across WAN links (MPLS, broadband internet, LTE, etc.) based on centrally defined policies. The benefits of SD-WAN include:

> Providing cost-effective delivery of business applications

> Satisfying the requirements of the modern branch/remote site

> Accommodating SaaS and cloud-based applications and services

> Improving branch IT efficiency through automated service provisioning

> Meeting the demands of application SLAs

This directly results in greater enterprise productivity and business agility. Enterprises need a high-performance network, built on a highly available foundation that can support business critical applications reliably.

Security must never be an afterthought. The ability to support micro-segmentation capabilities and granular policy enforcement provides enterprises with the ability to secure their WAN, meet compliance requirements and defend against breaches.

Enterprises need agility to spin up new branches and dynamically adjust policy and security rules. The ability to propagate policy context is a critical requirement for branch automation. This makes the concept of an advanced SD-WAN solution, very attractive and can help enterprises eliminate the need for multiple appliances performing dedicated security functions and in turn, simplify and consolidate — or "thin" — their branch WAN edge architecture. An advanced SD-WAN edge platform enables enterprises to transform their WAN by unifying SD-WAN, routing, WAN optimization, segmentation and branch security in a single centrally managed platform.

Centralized SD-WAN orchestration and an application-specific approach ensures the priorities of the business are always reflected in the way the network behaves. Unifying the orchestration of network and security policies ensures that QoS and security are consistently applied and enforced to applications — or classes of applications — regardless of how or where they are being accessed. Application performance and security can be dictated by top-down business policies, not bottoms-up technology constraints.

An advanced SD-WAN continuously monitors the state of the network and applications, detects changing conditions and triggers immediate, automated real-time responses to eliminate the impact of brownouts, blackouts and security threat events. Furthermore, automating cloud platform connectivity with integrations via application programmable interfaces (APIs) simplifies IT operations providing enterprises with timely access to cloud-delivered security services, IaaS and SaaS.

Today's network requires end-to-end visibility, programmability, and automation to dynamically ensure performance, security, and the highest quality of experience required for multi-cloud environments. An intelligent WAN architected with best-of-breed SD-WAN and cloud-delivered security solutions advances digital transformation initiatives and enables

enterprises to evolve and embrace timely new innovations without limiting their productivity and growth, all while minimizing exposure to security risks.

Conclusion

As modern cloud-first enterprises continue to migrate applications from the data center to the cloud, they must embrace network and security architecture transformation to realize the maximum return from their cloud investments. Gartner coined the term SASE, or Secure Access Service Edge that moves the industry in this new direction. Setting aside for a moment what it's ultimately called, it is important that enterprises consider both WAN and security transformation as they architect a secure access service edge.

Ultimately, no single vendor will have the ability to truly deliver best-in-class network and security technologies across a single platform. With the continuously evolving threat landscape, enterprises must retain the agility to quickly and cost-effectively adopt new security solutions. Enterprises are well-served to evaluate platforms that offer the freedom of choice to integrate best-of-breed network and security solutions. By doing so, enterprises can avoid being locked-in to proprietary single vendor solutions or having to settle for basic features and capabilities.

An advanced SD-WAN platform that supports integrated application programmable interfaces (APIs) can bring new levels to automation to enterprises, providing the ability to connect to a variety of best-in-class cloud services, including security. It can support

the foundational security functions required at the branch and complement cloud-delivered security to deliver seamless end-to-end security policy enforcement across the entire enterprise. This enables enterprises that are not yet ready to completely transform both their network and security architectures with the opportunity to transition to modern, cloud-first WAN architecture at their own pace, without compromise.

Finally, for enterprises that may not be ready to retire branch firewalls and move completely to cloud-delivered security, it is important to find an advanced SD-WAN platform that offers the freedom-of-choice to support leading third-party unified threat management (UTM) software solutions running as an integrated solution in branch locations. This eliminates the additional cost and management complexity that would normally be incurred with separate dedicated appliances, but it also provides enterprises with the flexibility to deploy best-of-breed solutions, ultimately offering a smooth migration to a cloud-delivered security model.

As enterprises continue to make substantial investments in the cloud, considering the requirements for both WAN and security transformation will ultimately put them on the path to delivering the highest quality of experience to users, increase productivity and drive new revenue streams. Embarking on a thoughtful, no compromise WAN and security transformation journey will ultimately enable enterprises to achieve a multiplier effect from their existing and ongoing cloud investments.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com