NITEL-CONNECT SD-WAN **PLAYBOOK**

ABOUT **NITEL**

Nitel is a leading next-generation technology services provider. We **simplify the complex** technology challenges of today's enterprise organizations to create seamless and integrated **managed network solutions** that propel their organizations forward. Because we solve customers' complicated IT challenges, they can operate with **greater productivity and security**, and in turn have the freedom to focus on other critical business issues.

EXECUTIVE SUMMARY: THE NITEL-CONNECT STORY

It is difficult to discern differences between the dozens of SD-WAN solutions available today. However, those that rely exclusively on the internet are still susceptible to latency, packet loss and jitter, disrupting the cloud applications that have become critical to today's businesses.

A select few SD-WAN providers mitigate internet variability by using their own private networks and endpoint hardware, but they lack flexibiliity and can be expensive. Other solutions gateway traffic to POPs, but then rely on the internet's middle mile to get traffic to their destination.

The new Nitel-Connect SD-WAN platform makes our private, high-speed nationwide MPLS network available to every SD-WAN deployment, without an MPLS contract.

Nitel-Connect provides private-network consistency and prioritized cloud access, but with the flexibility of different SD-WAN endpoint and security providers. This means customers can get customized, high-performing SD-WAN solutions at a lower price.

THE PROBLEM

- SD-WAN is marketed to IT departments as a do-it-yourself or DIY solution, but businesses have found managing multiple internet circuits with endpoint security to be difficult
- SD-WAN is marketed by many providers as an MPLS replacement, but internet-only SD-WAN lacks private network reliability
- Internet-only SD-WAN solutions increase the chances of erratic middle-mile behavior causing sub-optimal cloud, video, and voice experiences
- Introducing public internet into enterprise WANs increases exposure to security risks
- Hybrid SD-WAN (MPLS and internet); the emerging solution that guards against erratic internet behavior by using MPLS for latency-sensitive traffic is more costly and more difficult to manage than internet-only SD-WAN
- Big carrier SD-WAN solutions often use a single endpoint hardware provider and run exclusively with their own broadband, offering little in the way of flexibility or circuit diversity

SUMMARY CONTINUED

THE SOLUTION:

- Nitel-Connect SD-WAN includes access to our high-speed nationwide MPLS network to deliver a hybrid SD-WAN as a service, delivering a level of redundancy (the carrier-grade Nitel network design), predictability (of a private network), diversity (over 1,000 internet providers) and performance (optimized capacity management) that other SD-WAN providers will find difficult to match
- Interconnects into Canada and South America extend private-line reliability throughout the continent
- Our SD-WAN endpoint technology providers; Barracuda, Cisco, Versa, and VMware ensure that businesses get the security, visibility and control capabilities to match their business and budget requirements

  All solutions have flexible on-premises (integrated) or cloud-based security options

  - Cloud-based security can lower the cost of multi-site deployments by reducing the number of required endpoints
  - Decoupling security from the SD-WAN technology provides the opportunity for “best of breed” deployments while enabling the option for customers to manage their own security
- Direct and peering connections to public cloud and UCaaS providers ensure optimal SaaS, IaaS and VoIP experiences
- Supported from our US-based network operation center, Nitel-Connect is a fully- managed, OPEX-friendly, uniquely flexible hybrid SD-WAN service that can be customized to bring digital transformation to businesses of any size or budget

BENEFITS

- Private network reliability
- Business internet affordability
- Priority cloud access
- World-class security monitoring and management

THE EMERGING NETWORK VISION

In late 2019 Gartner, seeing the increased complexity of enterprise computing, developed a framework called Secure Access Service Edge (SASE) to describe a converged network and security management solution. The intent is to consolidate various security solutions, along with SD-WAN, into a single solution that is easy to manage, highly scalable and supports all types of edge devices and users.

SASE is based on a foundation of 5 core capabilities:

Network Routing	Identity/Remote Access	Threat Detection & Protection	Cloud Enablement	Web Threat Detection
SD-WAN	Zero Trust Network Access (ZTNA)	Next Generation Firewall (NGFW)	Cloud Access Service Broker (CASB)	Secure Web Gateway (SWG)

Nitel-Connect's technology choices provide the flexibility to design secure, SASE-aligned solutions, based on each company's specific needs, that deliver predictable performance and user experience:

Network Routing	Identity/Remote Access	Threat Detection & Protection	Cloud Enablement	Web Threat Detection
Industry-leading SD-WAN solutions: • Barracuda • Cisco • Versa • VMware	ZTNA Secure Remote Worker User-based VPN	Cloud-based and integrated NGFW Managed Threat Detection	Cloud Connection Service Cloud On-Ramp	Integrated Secure Web Gateway

Nitel-Connect is a fully-managed SD-WAN platform that i**ncludes private-network access** with **multiple endpoint hardware and security options.** This **unmatched flexibility** means companies of any size can easily and affordably realize the power of SD-WAN **without sacrificing predictability, all in SASE-aligned solution.**

NITEL-CONNECT SD-WAN PLATFORM

- Private Network Predictability
- Business Internet Affordability
- Priority Cloud Access
- World-Class Security Monitoring and Management

NITEL-CONNECT PROVIDES A PRIVATE, HIGH-SPEED ALTERNATIVE NETWORK TO THE VARIABILITY OF THE INTERNET

There is a near-universal desire to rearchitect wide area networks away from private connections to those with optimal cloud connectivity. With the promise of being more affordable and flexible, SD-WAN (software-defined wide area networking) has become the go-to solution for meeting next generation network requirements.

SD-WAN combines different networks into a single virtual WAN on which traffic can be prioritized to business needs. The two most common underlay networks are internet (fiber, broadband, LTE, DSL, satellite) and private MPLS networks.

> **The most significant challenge to SD-WAN adoption are designs that rely solely on the internet.**

SD-WAN solutions that rely solely on the internet increase the likelihood that latency, jitter and packet loss will disrupt cloud, voice and video applications. These are rare occurrences when using private networks.

These transmission errors were often thought to occur during last-mile connectivity. In fact, they are marginalized by the relatively short distances of last-mile connections. It is the internet long-haul or “middle-mile” that accounts for the most disruptive internet variables.

> **SD-WAN providers claiming to provide a replacement for private networks lack the most critical component to a consistent, safe and resilient WAN: a network.**

NITEL-CONNECT: EXTENDING THE REACH OF SD-WAN

SD-WAN has succeeded in bringing great value to the network edge, managing cost, performance, and availability. But for most SD-WAN solutions, that's where the control ends, and the unknowns of the internet's middle-mile begins.

The **Nitel-Connect SD-WAN** platform extends control *beyond* the network edge by making our private, high-speed network available to every SD-WAN deployment, **without expensive MPLS service contracts.**

Nitel-Connect minimizes the middle-mile variability that plagues internet-only SD-WAN solutions. Moreover, once connected to our nationwide network, customers gain better-than-Internet access to public cloud and voice services and can be easily onboarded to Nitel's cloud-based security solutions.

HOW IT WORKS

- Prior to implementation, Nitel sales engineers will analyze customers' traffic requirements
- Optimal routes will be decided based on all available routes, which include:
    - **Over the Nitel Network:** Traffic is sent to Nitel's closest POP (or "point of presence," a Nitel data center at the edge of our nationwide network), where it is then routed over Nitel's private network to the Nitel POP closest to its destination (a customer's local branch or a cloud-based IaaS, SaaS, or UCaaS provider)

      Traffic destined for Canada or South America is routed to a partner network in the destination country
    - **A Nitel-Peered or Direct-Connect Destination:** from the Nitel POP, traffic will be routed privately to cloud providers that are peered with Nitel
    - **Directly to the Internet:** non-critical traffic can be routed directly to a local internet connection

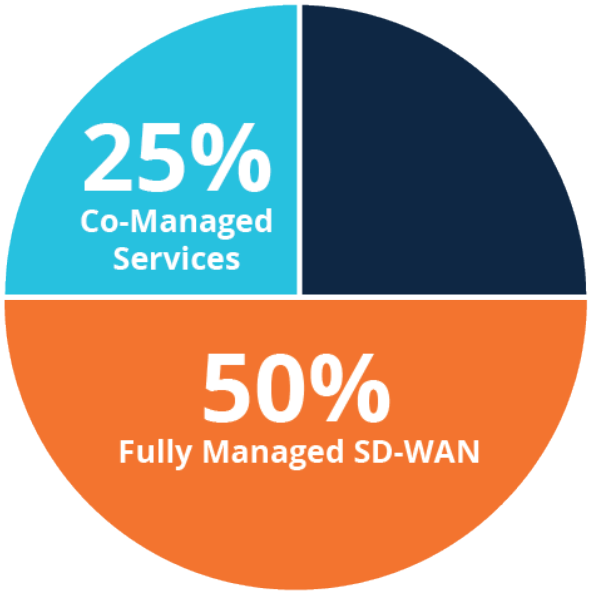
Nitel believes that SD-WAN should be flexible, adapting to WAN needs as they change**. Nitel offers four different endpoint hardware solutions**:

- **Barracuda Networks:** Full-featured SD-WAN with integrated security, aggressively priced
- **Cisco SD-WAN:** Full-featured SD-WAN with integrated security, intelligent cloud pathing, and advanced VPN segmentation for meeting the most demanding WAN requirements
- **Versa Networks:** Comprehensive SD-WAN with powerful data analytics and network insights
- **VMware**: Complete SD-WAN solution featuring application aware routing and cloud on-ramp support.

THE VALUE OF MANAGED SD-WAN

While SD-WAN makes traffic management over multiple circuits possible, deploying and managing the underlying WAN infrastructure is not easy. IT departments still have to manage an array of WAN equipment, including routers and load balancers, firewalls, and more. From a management perspective, it could be argued that SD-WAN and cloud connectivity has made IT's job more difficult.

A 2018 Frost & Sullivan survey indicated that complexities around how software-defined WANs impact underlying networks and services are driving 50% of enterprises to prefer fully managed SD-WAN, while another 25% opt for co-managed services.

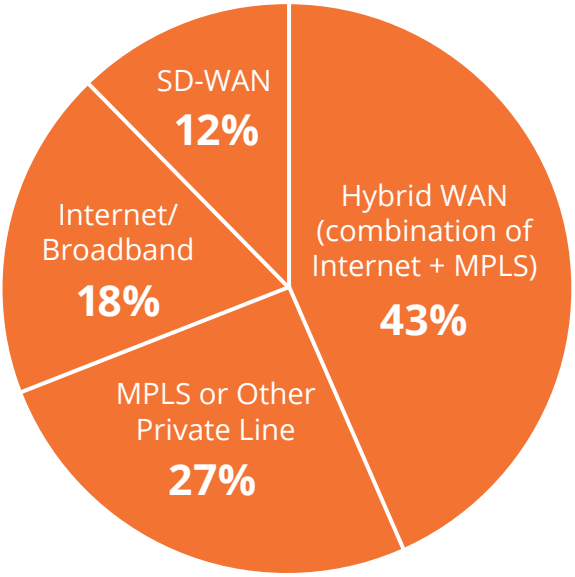


Nitel-Connect SD-WAN provides customers with a fully managed SD-WAN as a service (SDWaaS) platform consisting of multiple on-premise (endpoint) hardware options (Barracuda, Cisco, Versa, and VMware) with integrated, on-premise or cloud-based security options. This is complimented by Nitel's hallmark ability to deliver diverse access from over 1000 transport vendors to over 8.5 million commercial buildings in 42,000 ZIP codes. Nitel monitors all connections and firewalls and maintains optimal connections between sites and providers.

HYBRID MADE EASY

Hybrid SD-WAN blends the predictability and performance of MPLS with affordable internet access, allowing transport costs to be aligned with traffic priority and cost reduction. The growing interest in hybrid SD-WAN accounts for concerns of using SD-WAN solutions that rely solely on the internet. However, while SD-WAN is a complex DIY solution, hybrid SD-WAN is even more so.

Nitel-Connect SD-WAN is a redundant, resilient, hybrid SD-WAN available as a monthly service with none of the management headaches that come with self-managed networks.



Hybrid SD-WAN deployments are the most popular enterprise WAN types currently deployed. (IBM-sponsored study, Fall 2018)

DIGITAL TRANSFORMATION AND GETTING TO THE CLOUD

A recent survey indicated that 50% of small and medium-sized businesses with $5 to $100 million in revenue are budgeting for public cloud access. The majority of U.S. enterprises already rely on cloud services. The transformative capabilities can be significant (see inset below). Many businesses feel cloud adoption is necessary to compete.

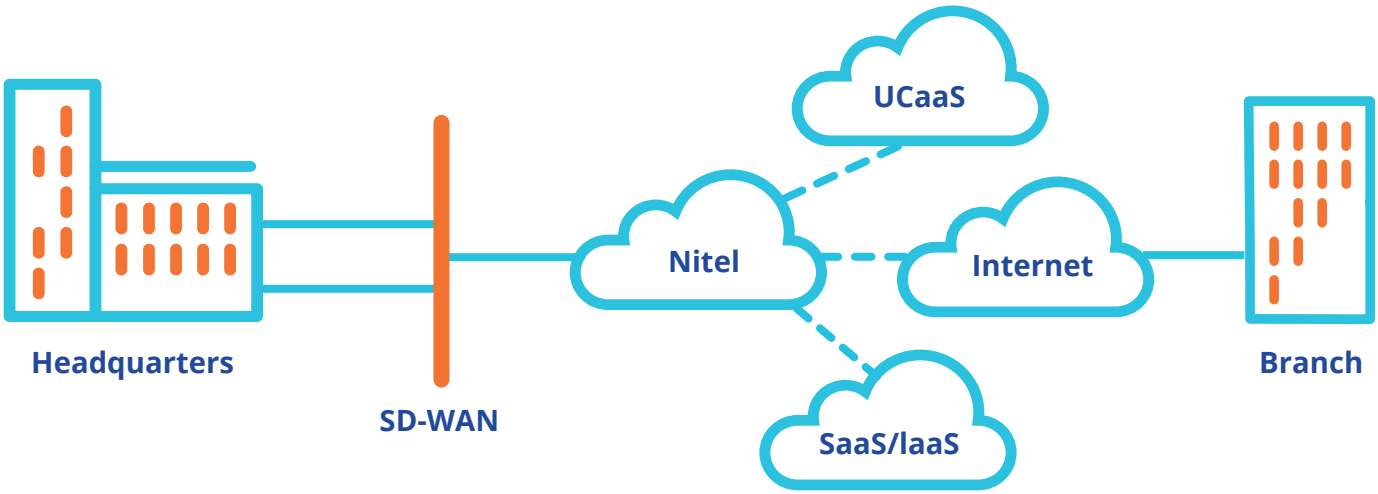
DIGITAL TRANSFORMATIONS
Real-World Benefits of SD-WAN

- **5X** improvement in Office365 performance
- **Accelerated** public cloud migration
- **12-fold** improvement in change control time
- **Connect seamlessly** and securely with critical business partners
- **100%** application uptime
- **4X** improvement in application latency
- **Significant reduction** in operating expenses
- **Rapid deployment** of multisite retail wireless access

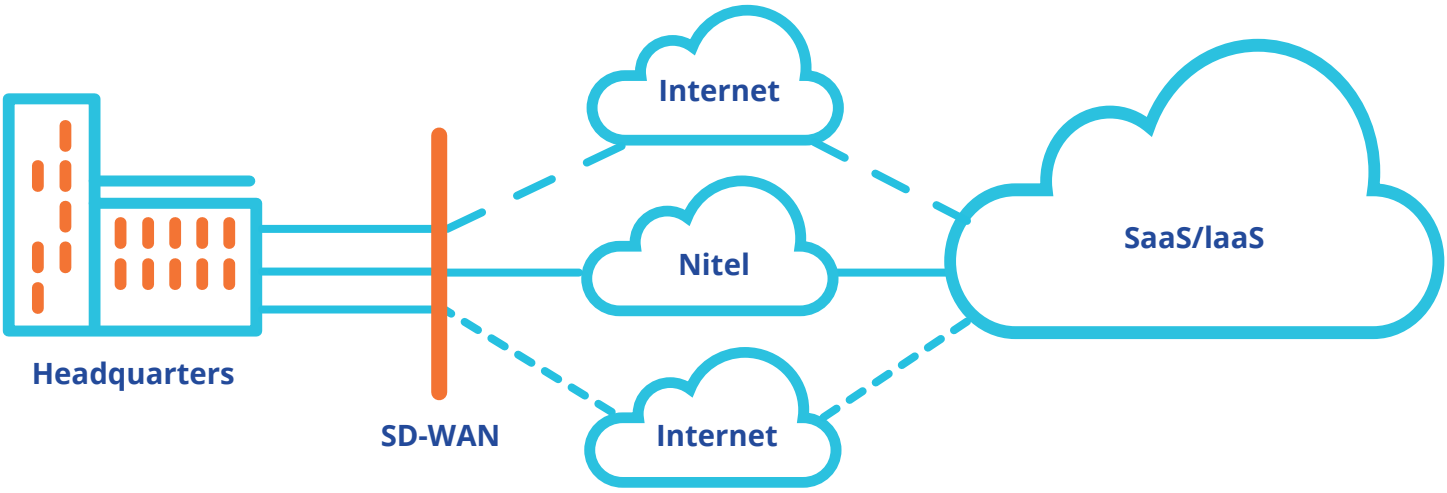
SD-WAN enables path optimization or direct access to the cloud, without first having to route traffic back to a central location to access the internet.

Nitel-Connect provides three better-than-internet options to public cloud providers.

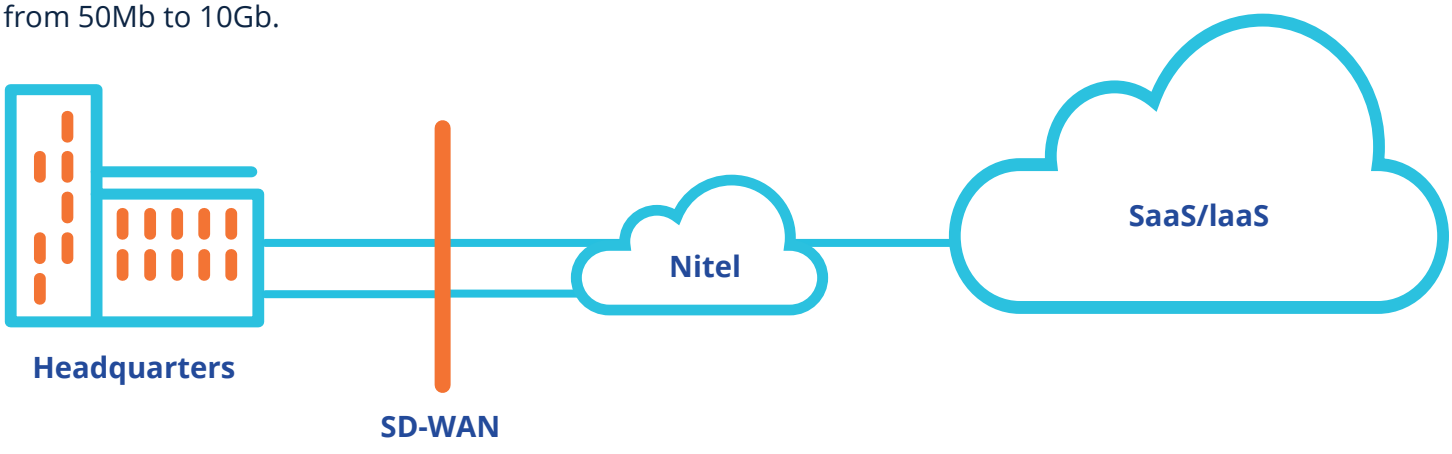
Leveraging the Nitel Network: As an alternative to the internet's middle mile, traffic can be routed to one of Nitel's seven POPs, over the Nitel network, then exit at the Nitel POP closest to its destination.



Cisco on-ramp, available with VMware or Cisco Advantage, actively monitors multiple paths to cloud destinations, including paths over the Nitel network, automatically routing traffic over the optimal path.



Nitel Cloud Connect provides a direct connection to leading public cloud providers at speeds ranging from 50Mb to 10Gb.



NITEL-CONNECT: THE PATH TO ENHANCED SECURITY

Internet access is essential for cloud connectivity and WAN-cost reduction, but more security is required. Nitel-Connect SD-WAN supports integrated (on-premises), or cloud-based security options. This means adopting new security does not have to happen at the same time new WAN technology is being adopted.

Nitel Managed Security Services: Organizations are moving away from perimeter-centric approaches, placing more value on detection and response. Practically speaking, this can be a daunting DIY undertaking, especially when budgets are tight. Nitel's optional Managed Security Services compliments the preventative nature of integrated security and firewalls. These real-time cyber threat intelligence services are proven to minimize security risks while automating the cumbersome task of firewall log review required for HIPAA and PCI compliance.

NITEL-CONNECT, COMPLIANCE, & MANAGED SECURITY SERVICES

In today's sophisticated threat landscape, traditional preventative (firewall) security is challenged. The need for advanced detection-centric security is becoming essential, especially in retail and health care industries. Further, the analysis of log and event information from devices and applications, essential for PCI and HIPAA compliance.

Nitel-Connect opens the door to Nitel's Managed Threat Detection (MTD) Services, which automates the analysis of log data required for PCI and HIPAA compliance. Automated analysis of firewall and device logs hunts for known threats, unusual behavior, and suspicious activity. Human analysis is called in when needed for advanced threat identification and triage.

Nitel-Connect makes Managed Threat Detection affordable by supporting cloud-based firewalls. Multiple sites can use a single cloud firewall, reducing MTD deployment costs.

THE BENEFITS OF NITEL-CONNECT SD-WAN

The Predictable Connectivity of MPLS

- While many providers point to SD-WAN as an alternative to more expensive MPLS, SD-WAN cannot be an MPLS replacement unless it can provide the predictable connectivity of MPLS
- Nitel-Connect SD-WAN routes select customer traffic to Nitel's nationwide network, avoiding the unpredictability of the internet's middle mile and leading to a more consistent experience for voice and cloud application use

Enhanced Security and Compliance

- While the Cisco and Barracuda endpoint options each offer robust, integrated security, Nitel-Connect SD-WAN also supports cloud-based solutions from Barracuda, Cisco, and Palo Alto
- Data protection is enhanced for traffic routed over Nitel's private network
- Nitel has partnered with Trustwave, a Gartner Magic Quadrant leader for global threat intelligence and incident response, for Managed Security Services, which can easily be added to most configurations
- The Trustwave partnership allows companies to access a level of expertise that would otherwise be elusive
- At its most affordable level, MTD-Compliance offloads the cumbersome task of firewall log review, which is an essential component of HIPAA and PCI compliance
- The transition to managed SD-WAN is an ideal time to onboard managed security services

Agility

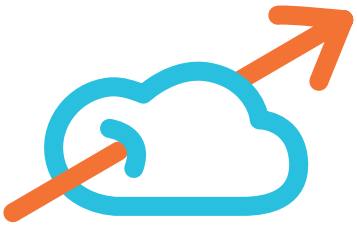
- Nitel's North American network and access vendor relationships with over 1,000 providers enable customers to set up a new sites and add new services quickly
- Once connected to the Nitel network, deploying new network security, unified communications, and other products are faster and more affordable

Value

- Regardless of the endpoint provider chosen, all Nitel-Connect SD-WAN customers benefit from access to Nitel's North American network, which adds MPLS-like predictability to their WAN at no additional charge
- Both Barracuda and Cisco include security as part of the base features
- With over 1,000 transport vendors, Nitel can deploy right-sized network connections at every site, more easily matching budget and technical requirements

Express Routing to Cloud and Voice Providers

- Nitel has built an MPLS network with 100% uptime and direct connections to leading cloud and voice providers
- Not only does headquarter and branch traffic benefit from delivery over the Nitel network but so do SaaS, laaS and VoIP services



Flexibility

- Most SD-WAN providers restrict users to a single technology provider
- Nitel Connect SD-WAN supports Barracuda, Versa Cisco, or VMware SD-WAN endpoint technology; each with its own strengths and price points
- Nitel allows businesses to connect to cloud services, scale bandwidth and add security services as needed, on a per-site basis
- Nitel offers a wide variety of on-premise and cloud-based security options including those from Barracuda, Palo Alto and Cisco
- For customers who already own Cisco compatible routers, Nitel will work to leverage their investment into new SD-WAN deployments

Managed Security and Network Functions

- Bundled pricing with Managed Threat Detection, managed next-gen firewall, web application firewalls, Al-based anti-phishing and other network services, both physical and virtual, helps maximize ROI and peace-of-mind

Scalability

- The Nitel network, coupled with Nitel's flexible endpoint hardware upgrade policies, means the size and scope of customers' services can be scaled up without the time and hassle associated with self-managed SD-WAN solutions

SECURE ACCESS SERVICE EDGE: THE EMERGING NETWORK VISION

THE SHIFT TO DECENTRALIZED NETWORKS

Prior to the rise in cloud computing, the traditional network model was centralized, with applications and data concentrated in data center locations, and branch offices connected through dedicated links. Internet traffic was also routed through the data center, where a company's security infrastructure resided. In this scenario, where most network activity was within the company's private domain, it was relatively easy to manage traffic routing and maintain the security of applications and users.

The rise of cloud-based applications and infrastructure has inverted the traditional model, with the majority of network traffic now external, destined for internet-based services such as Salesforce and Office 365 or infrastructure providers such as Amazon Web Services. In parallel, the remote workforce has grown significantly. This evolution of the traditional security perimeter creates challenges for organizations to secure their network using traditional approaches.
This decentralized network has created five underlying challenges

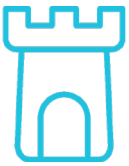
NETWORK ROUTING

Efficiently routing traffic between HQ/branches/ remote users/cloud

IDENTITY & REMOTE ACCESS

Providing appropriate access from remote users to internal resources

THREAT DETECTION & PREVENTION



Network threat detection and prevention

CLOUD ENABLEMENT

Providing direct, source access from remote users to cloud resources.

WEB THREAT PROTECTION

Protection from web access-related threats

In late 2019 Gartner, seeing the increased complexity of enterprise computing, developed a framework called Secure Access Service Edge (SASE) to describe a converged network and security management solution. The intent of SASE is to consolidate various security solutions, along with SD-WAN, into a single solution that is easy to manage, highly scalable and supports all types of edge devices and users.

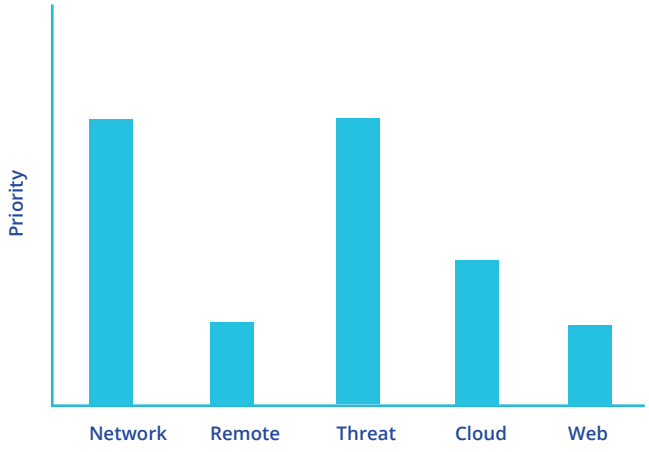
SASE is based on a foundation of core capabilities to address key challenges:

Network Routing	Identity/Remote Access	Threat Detection & Protection	Cloud Enablement	Web Threat Detection
SD-WAN	Zero Trust Network Access (ZTNA)	Next Generation Firewall (NGFW)	Cloud Access Service Broker (CASB)	Secure Web Gateway (SWG)

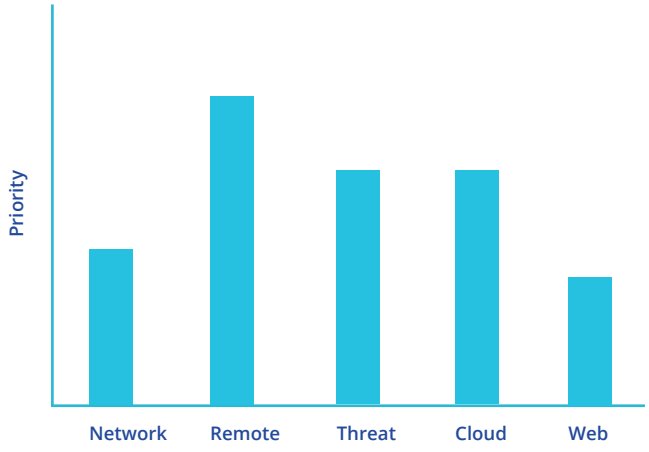
NITEL-CONNECT DELIVERS SASE

SASE is a vision for what the network will become in terms of converged capabilities and management, but it is built on a collection of existing underlying technologies. SASE is a framework, not a standard and as such, is not easily addressed using specific products or technologies. In addition, each company has unique requirements— prioritizing the elements of SASE to best meet their needs. For example, a hospital group with multiple locations and mostly on-site employees may prioritize SD-WAN capabilities, while a software company with many remote workers and a heavy reliance on cloud services may prioritize remote access and cloud enablement capabilities. The right solution goes beyond individual technologies to build an all-inclusive, SASE-aligned strategy to guide network evolution.

Example: Hospital Group
Most in-office workforce,
in multiple branch offices



Example: Software Company
Remote workforce, cloud-first
computing approach



Nitel-Connect's technology choices provide the flexibility to design secure, SASE-aligned solutions, based on each company's specific needs, that deliver predictable performance and user experience:

Network Routing	Identity/Remote Access	Threat Detection & Protection	Cloud Enablement	Web Threat Detection
Industry-leading SD-WAN solutions: • Barracuda • Cisco • VMware • Versa	ZTNA Secure Remote Worker User-based VPN	Next Generation Firewall (NGFW) Managed Threat Detection	Cloud Connection Service Cloud On-Ramp	Integrated Secure Web Gateway

PRIVATE NETWORKS ARE KEY TO DELIVERING THE SASE "SERVICE EDGE"

As users become more geographically distributed, a good user experience will depend on providing optimal access to the resources they need, with a minimum of latency. Nitel-Connect includes a nationwide private network that brings the network to the user, regardless of location. SD-WAN solutions which rely solely on the internet or utilize public clouds as the SASE service edge, cannot deliver a predictable experience.

Nitel-Connect provides flexibility and predictability in a SASE-aligned strategy:

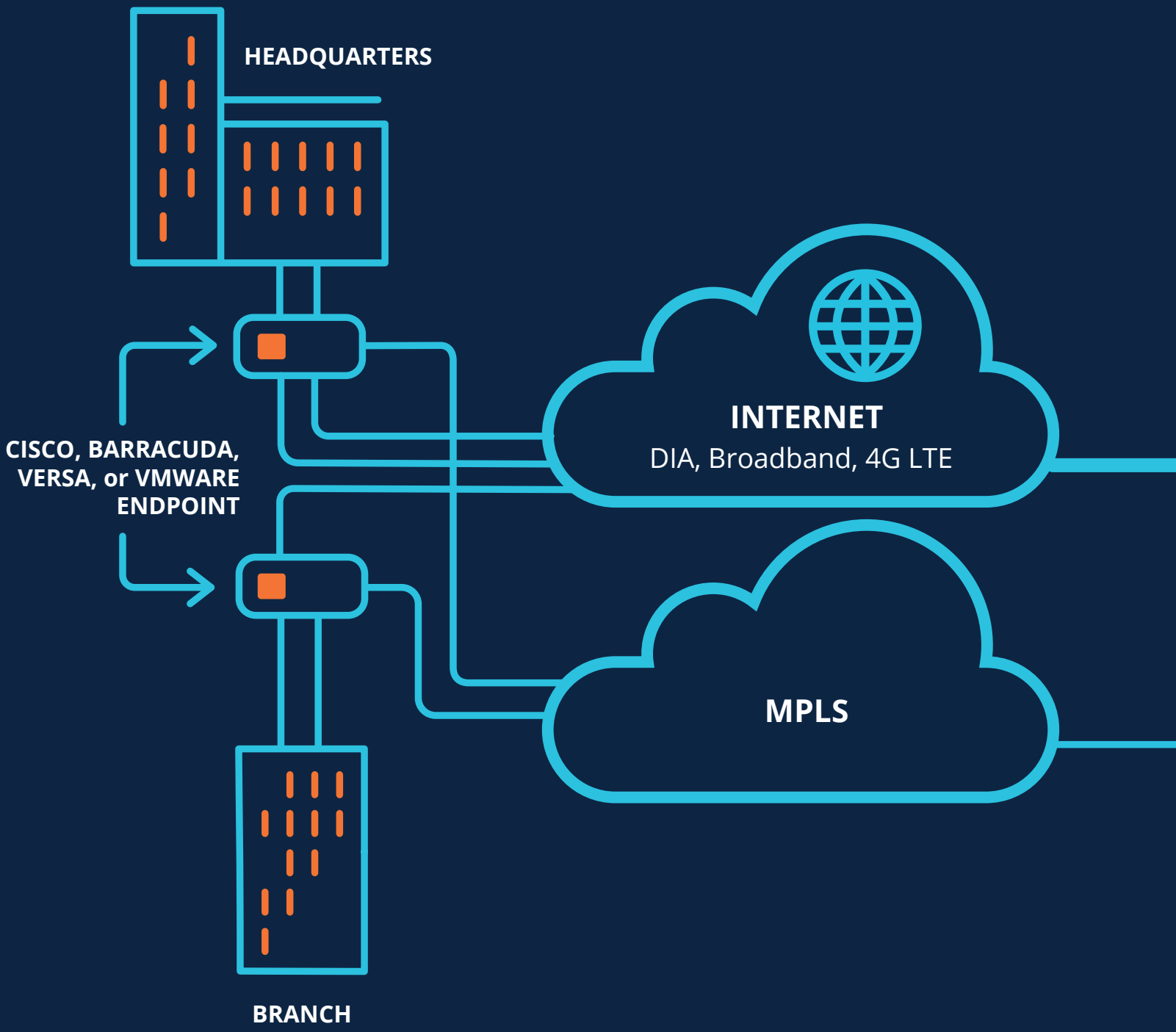
- Technology choices – Flexibility to find the right solution for your company, from leading network and security vendors, all with SASE evolution strategies.
- Private, nationwide network – Reliable, predictable user experience, regardless of location
- Expert managed services – Simplified management through Nitel managed services

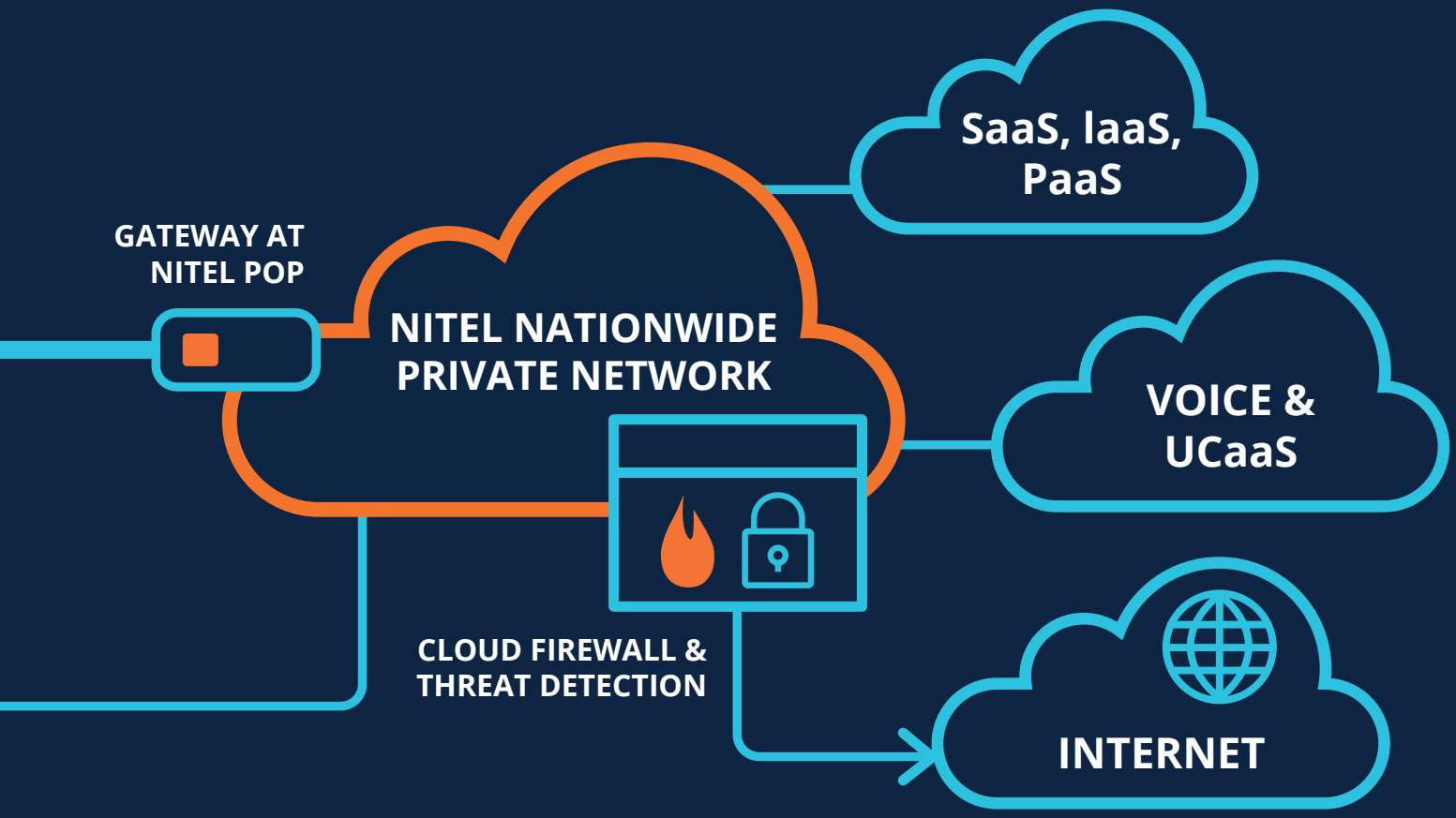
NITEL
NETWORK FACTS

DISCOVER HOW THE NITEL NETWORK PLAYS A CRITICAL ROLE IN EVERY NITEL-CONNECT OPPURTUNITY

Carrier-grade MPLS backbone with 100% uptime since its inception	Nitel's carrier-grade network is the product of a highly redundant design that has delivered 100% MPLS uptime since its inception.
Strategically located dual-core POPs	Every North American business is milliseconds away from a Nitel POP, each with multiple, high-powered Cisco ASR 9900 edge routers in high-availability mode. Each router can handle 32 Tbps of traffic and is capable of handling the full load of POP traffic.
Peering with multiple tier-1 internet providers	Nitel peers with multiple Tier-1 internet backbone providers for ingress and egress at each POP giving traffic a direct path to every major internet network.
10 Gbps multipath connections between POPs	All Nitel POPs are interconnected with high-speed 10 Gbps connections. Should a connection be lost, traffic is instantly routed to another POP. Built for the future, the network can easily scale to 100Gbps and beyond.
Highly interconnected – over 190 NNIs	Nitel's North American network fabric offers the ability to route traffic privately from branch locations to the Nitel network edge, without touching the internet.
Priority voice and cloud connections include: AWS, Azure, Nextiva, RingCentral, Jive, Microsoft (Skype), and Momentum	Think of these as express lanes to the cloud and VoIP solutions customers rely on. Customers with Nitel-managed links can avoid the public internet with priority access to top providers from any of our POPs.
Extensive national and international reach	Nitel has partnerships with over 1,000 transport vendors, access to over 42,000 ZIP codes and the ability to connect to over 8.5 million commercial buildings. Traffic destined for Canada or South America is routed to a partner network in the destination country.

NITEL-CONNECT SD-WAN




SaaS, IaaS,
PaaS
GATEWAY AT
NITEL POP
NITEL NATIONWIDE
PRIVATE NETWORK
VOICE &
UCaaS
CLOUD FIREWALL &
THREAT DETECTION
INTERNET

ADDRESSING BUSINESS DRIVERS WITH NITEL-CONNECT SD-WAN

The top drivers of SD-WAN deployments are the **operational efficiencies gained by simplification of WAN management, cost savings from leveraging more affordable internet bandwidth (bandwidth optimization), improved productivity of cloud applications through higher performance connectivity and improved cloud connectivity.** With the latter comes an increased need for improved security. Below describes how Nitel-Connect SD-WAN addresses these common business drivers.

WAN SIMPLIFICATION

The Problem:
SD-WAN technology makes managing multiple WAN connections possible, but not necessarily easy. Coming from a managed service where everything done for you, to integrating MPLS and internet, transitioning to the cloud and bolstering security, is no small task.

A Q4 2018 Frost & Sullivan survey cites these complexities as the reason that 50% of enterprises prefer fully managed SD-WAN while another 25% prefer co-managed services.

The Nitel Solution:
Nitel provides a fully managed service that takes care of every aspect of the WAN environment: connectivity, deployment, security, and maintenance that offers significant benefits over self-managed SD-WAN solutions:

- **Flexible Co-Managed Option:** Nitel's co-managed option keeps our network experts at the ready should they be needed.
- **No Vendor Hardware Lock-In:** Nitel offers multiple hardware solutions with flexible upgrade options.
- **Fast Deployment:** Nitel's nationwide network and relationships with hundreds of last-mile vendors make for fast deployments.
- **Offload Administrative Functions:** Simplify vendor management by consolidating North American internet service providers on a single bill.
- **Lower Ownership Costs and CapEx:** The cost of achieving and maintaining a hybrid SD-WAN network is prohibitive to most businesses.

BANDWIDTH OPTIMIZATION

The Problem:
Increased use of cloud applications requires high-bandwidth, low-latency connectivity to cloud providers. Broadband is fast and affordable, but can also subject cloud connections to jitter and packet loss, compromising real-time communications (video and UCaaS/VoIP) and application performance.

The Nitel Solution:
Nitel addresses the need to optimize bandwidth in two ways. First, Nitel's MPLS core network is part of every Nitel-Connect SD-WAN deployment. This ensures select traffic gets as close to its destination as possible without being subjected to the unknown congestion and security issues of the internet's middle mile.

In addition, the Nitel network interconnects privately to the major cloud and VoIP providers at every POP.

Unlike most SD-WAN solutions, Nitel provides a real WAN as part of its solution; a high-speed, highly secure nationwide private network, available to every Nitel-Connect SD-WAN solution at no additional charge.

IMPROVED CLOUD CONNECTIVITY

The Problem:
The traditional approach of routing traffic to a data center adds too much latency to cloud-destined traffic. Many SD-WAN vendors promote the ability to prioritize cloud traffic by placing a virtual device in a cloud data center. This can be complicated, expensive and difficult to maintain.

The Nitel Solution:
Nitel provides both optimized routing of cloud traffic and direct cloud connections, without requiring more appliances. Application-based policy routing is complemented with intuitive dashboards and analytics that help track application performance.

SECURITY

The Problem:
SD-WAN offers optimized or direct connections to cloud applications and services. However, this means more internet use and more exposure to risk. SD-WAN technology providers' integrated security offerings can be inflexible.

For organizations with just a few sites, integrated security is an excellent choice.
For organizations with many sites, this may be cost-prohibitive.

The key is flexibility.

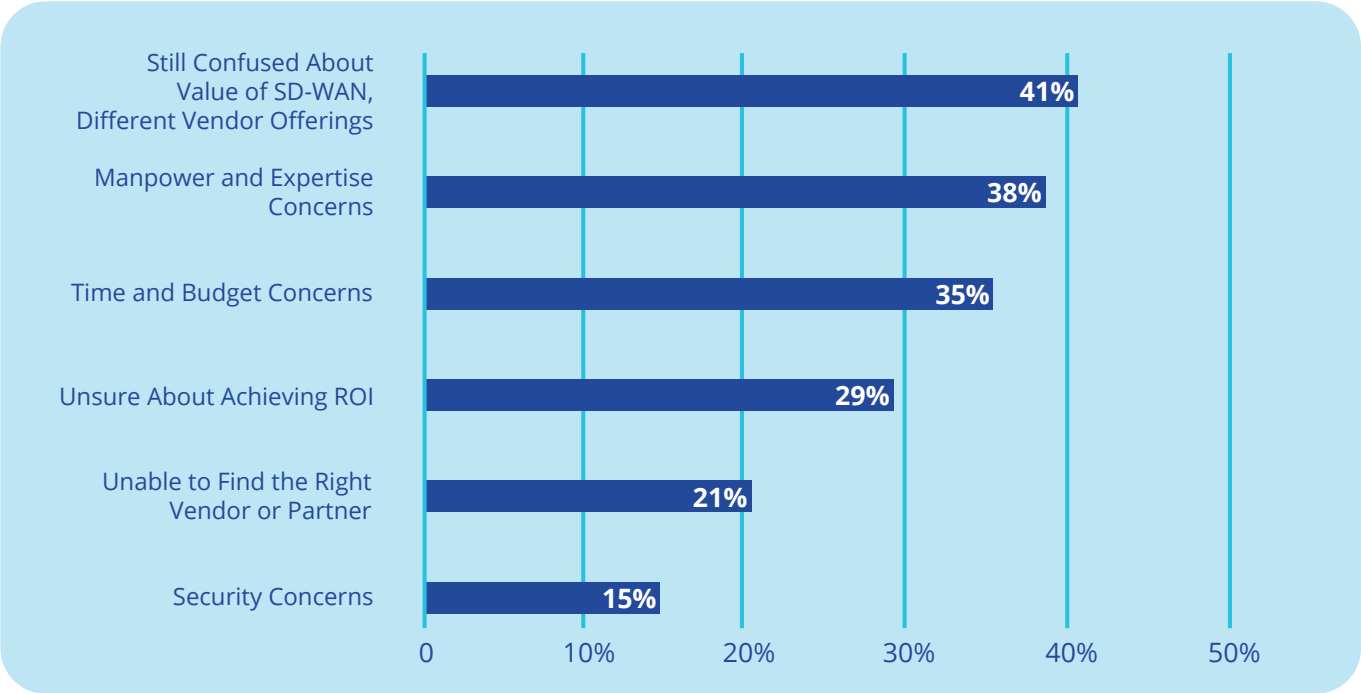
The Nitel Solution:
Cisco and Barracuda endpoint options include integrated next-gen firewalls as part of the base features. Embedded security protects data passing to and from branch locations to the cloud, guarding against debilitating security attacks that could originate from compromised connections and applications.

Nitel-Connect SD-WAN can also be decoupled from security, meaning customers have the option to bypass the integrated security and opt for cloud-based solutions at Nitel POPs. This regional-based approach allows for a more cost-effective deployment of Nitel's Managed Security Services.

Select configurations of Nitel-Connect support VPN segmentation, allowing encrypted traffic types to be kept separate from each other. This can be a compelling feature in verticals such as healthcare, retail and finance. Here, the extra layer of encryption between traffic types mitigate risk against hackers and back-door attacks through third-party vendors.

Optional Managed Threat Detection offers 24x7 real-time, global threat intelligence.

OVERCOMING ADOPTION CHALLENGES



Flexible technology partners and Nitel network integration in every Nitel-Connect deployment helps address concerns about value. A managed SD-WAN addresses concerns in SD-WAN adoption, manpower and expertise. **IBM-sponsored study, Fall 2018.**

The combination of private-network reliability, flexible hardware options, and unmatched access diversity delivered in a fully-managed service mean Nitel can help companies of any size overcome many of **the common concerns in adopting SD-WAN**:

Lack of experience in managing and maintaining SD-WAN

This one may not be immediately visible as many organizations may not readily admit to their lack of understanding of SD-WAN technology. **That is the inherent appeal of a fully managed SD-WAN service**. Nitel provides all the SD-WAN and security expertise needed to deliver a secure, high-performing, next-generation WAN environment.

Interoperability Challenges

Nitel specializes in deploying a mix of internet mediums, including fiber, cable, DSL, LTE, and fixed wireless, in addition to private MPLS, and aggregating them into a seamless WAN fabric across branches and to the cloud.

Cyber attacks, data breaches, and security concerns

SMBs typically lack in-house network security expertise. SD-WAN can magnify the skill gap. Nitel brings significant security expertise to every SD-WAN design and deployment. Our partnership with Gartner Magic Quadrant leader Trustwave for managed security services further adds to the level of security expertise we can provide.

Increase visibility and predictability

Nitel SD-WAN solutions provide app-aware routing with deep packet inspection (DPI), application visibility, and routing. And by carrying select traffic across Nitel's private network, middle-mile variability is replaced with more consistent, predictable performance.

A recent hardware or network purchase

Nitel will work to onboard existing, compatible routers, security, and network circuits wherever possible.

SD-WAN is not for us

One of the most significant barriers to selling SD-WAN is approaching a prospect with a single solution. Not all SD-WAN solutions are the same. Some have strengths in security. Others in providing flexible topologies and segmentation. One of the benefits of Nitel-Connect SD-WAN platform is the wide array of SD-WAN options and solutions we support.

NITEL-CONNECT:
SD-WAN ENDPOINT TECHNOLOGY

It's rare to find two organizations that have the exact same WAN requirements. One organization may require their WAN to connect to a data center. Another that uses IaaS may need to prioritize branch-to-cloud applications. Still, others may find comfort in solutions that support its existing router and security platforms. For this reason, Nitel supports multiple SD-WAN endpoint solutions, enabling deeper conversations and an opportunity to better align with customer needs.

Collectively, Barracuda, Cisco, Versa, and VMware address a wide variety of WAN requirements, providing nearly every type of business a path to Nitel-Connect SD-WAN. Each solution can be sized from a handful of employees to thousands, and from bandwidths as low as 50 Mbps up to 10 Gbps. Each offers integrated next-generation security features, or they can leverage Nitel's cloud-based security.

Barracuda®

The Barracuda Networks SD-WAN solution offers comprehensive SD-WAN features integrated with next-generation firewall and highly resilient VPN technology. Optional Advanced Threat and Malware Protection with sandboxing provide additional protection against potential threats.

WHAT SETS BARRACUDA APART

- **Cost-Effective SD-WAN Deployments -** Barracuda delivers robust SD-WAN features with built-in WAN optimization and Microsoft Azure Cloud traffic optimization.

- **Integrated Next-Generation Security -** Full control and visibility of application traffic with application detection, user-identity awareness, SSL interception, built-in live reporting and optional unified threat management.

- **Remote User VPN -** Reliable multi-transport VPN tunnels, WAN Optimization, and application-based prioritization enhance user experience when accessing remote applications both in the cloud and in private data centers.

EXAMPLE CUSTOMERS

- Businesses looking for the best value per dollar in an SD-WAN solution
- Businesses with a high number of locations and challenging deployment budgets
- Businesses seeking integrated security
- Businesses that place importance on remote user VPN access

HARDWARE AND PACKAGING

Barracuda SD-WAN is deployed as part of the company's highly-regarded next-gen CloudGen Firewalls and can be deployed as a physical endpoint or as a virtual appliance embedded with laaS providers. Physical and virtual models are available for small branch offices (25-75 users) as well as large headquarters and data centers (7,000 to 15,000 users). Optional integrated WiFi is available on select models.

LICENSING

Barracuda SD-WAN is not licensed based on bandwidth; throughput is dictated by the model of the Barracuda CloudGen selected.

SD-WAN

- **Advanced Threat and Malware Protection combines** gateway-based malware and virus protection with Advanced Threat sandboxing, protecting against network breaches and advanced malware attacks such as zero-day exploits and ransomware.

- **Advanced Remote Access** provides a customizable and easy-to-use portal-based SSL VPN as well as sophisticated Network Access Control (NAC) functionality and CudaLaunch, which provides mobile workers secure remote access through the firewall.

ADVANTAGES

- Aggressively priced
- No bandwidth license required
- Integrated next-generation firewall out of the box

Cisco SD-WAN provides advanced routing, segmentation and security capabilities for interconnecting enterprise networks with exacting requirements. Advanced VPN segmentation capabilities include support for individual VPN topologies within IPSec tunnels, optimizing network traffic while allowing sensitive traffic from different lines of business or application segments to be isolated and secured.

Integrated security capabilities include application-aware enterprise firewall, globally backed intrusion prevention, malware protection with sandboxing, and reputation-based URL filtering. Cisco Umbrella offers integrated DNS protection that blocks malicious websites before a connection can be made.

Cisco SD-WAN is being offered in two license tiers: DNA Essentials and DNA Advantage. Cloud onRamp, a feature of DNA Advantage, provides real-time path optimization across both local internet and the Nitel network to ensure a predictable experience to SaaS providers.

WHAT SETS CISCO APART

- **Advanced Segmentation -** Deploy multiple WAN segmentation topologies over a single IPSec tunnel. This provides robust network protection against outside attacks through the secure separation of multiple application segments.

- **Available, Real-Time Cloud Path Optimization -** Optional Cloud onRamp continuously measures the performance of SaaS applications through all permissible paths and atomically routes traffic over the optimal path in real-time.

- **Deployed on highly-regarded Cisco ISR/ASR routers -**Cisco's SD-WAN solution can be installed on select Cisco Integrated Services Routers (ISRs) and Aggregation Services Routers (ASRs). Nitel will work with customers to leverage their existing Cisco routers into their new Nitel-Connect SD-WAN environment**.**

EXAMPLE CUSTOMERS

- Organizations valuing high levels of customization
- Businesses embracing the cloud
- Businesses already using Cisco

HARDWARE AND PACKAGING

All Cisco SD-WAN endpoint hardware offers the same basic SD-WAN functionality. Key differences between the device platforms relate to the inclusion of integrated next-generation security features and port density.

The highly regarded Cisco router lineup offers a range of endpoint solutions from lower-cost options that are ideal for leveraging cloud-based security, to more powerful models that support Cisco's full integrated security stack.

The flexibility of Cisco endpoints allows SD-WAN to be cost-effectively priced and packaged for small businesses through Fortune 100 enterprises.

LICENSING

Cisco SD-WAN endpoint hardware is available with two license tiers; DNA Essentials and DNA Advantage. Cloud onRamp and advanced VPN segmentation require DNA Advantage. Cisco SD-WAN licenses are priced by required bandwidth tiers at each location.

ADVANTAGES

- Cisco market share and brand recognition
- Proven Cisco router platforms
- Powerful VPN segmentation and Cloud onRamp (Advantage tier only)
- Intelligent path optimization to SaaS providers via Cloud onRamp
- 50+ Fortune 500 deployments with over 40,000 devices shipped

The Versa Networks SD-WAN solution delivers a rich set of highly scalable software-based capabilities ideal for large enterprises, including carrier-grade NAT and load balancing. Near-real-time analytics and historical reports provide deep visibility into network and application performance. An integrated KVM hypervisor supports third-party VNFs, enabling greater flexibility in services.

The solution allows for secure tunnels to be dynamically created between locations with any topology. Through application-aware routing and the ability to identify more than 2,500 specific applications, Versa SD-WAN can carefully map different applications across diverse connections based on business policy and app-specific SLAs.

WHAT SETS VERSA APART

- **Industry-Leading Analytics -** Versa features rich data visualization tools and a real-time, big data analytics engine that provides deep visibility and control, base-lining, correlation, and predictive capabilities.

EXAMPLE CUSTOMERS

- Organizations valuing deep insights on network and application performance

HARDWARE AND PACKAGING

- Versa SD-WAN is deployed as software on certified, Intel-based servers and appliances.

ADVANTAGES

- Holistic environment management with deep analytics

VMware SD-WAN enables enterprises to securely support application growth, network agility, and simplified branch implementations while delivering high-performance, reliable branch access to cloud services, private data centers, and software as a service (SaaS) based enterprise applications. VMware SD-WAN is built on software-defined networking principals to address end-to-end automation, application continuity, branch transformation, and security from the data center and cloud to the edge.

Nitel-Connect will offer VMware SD-WAN at the Premium license level. Premium includes VMware SD-WAN Gateway Services:

- Cloud Gateway Services for SaaS
- Cloud VPN
- Cloud Gateway Services for non-VMware sites

WHAT SETS VMware APART

- **Optimized routing.** VMware SD-WAN Dynamic Multipath Optimization™ aggregates multiple links and steers traffic over optimal links to other VMware SD-WAN Edges.

- **Simplified management.** Including straightforward operations and one-click service insertion.

- **Efficient branch deployments.** VMware SD-WAN Edge devices can host virtual network functions, simplifying deployment of network services.

EXAMPLE CUSTOMERS

- Expanding enterprises adding new sites or applications
- Businesses with many (hundreds or thousands) sites
- Businesses embracing the cloud

HARDWARE AND PACKAGING

VMware SD-WAN is deployed on VMware Edge platforms.

LICENSING

VMware SD-WAN requires a license based on bandwidth capacity. Nitel offers VMware SD-WAN at the Premium license tier.

ADVANTAGES

- VMware has strong name recognition and is consistently rated as a “Leader” in Gartner’s Magic Quadrant ratings
- Managed on-ramp to the cloud
- Management of branch deployments

NITEL-CONNECT SD-WAN
ENDPOINT FEATURE COMPARISON

Nitel Managed SD-WAN Services		Barracuda	Cisco	VMware	Versa
Nitel nationwide private network	Provides performance predictability by reducing middle-mile latency. Included with all Nitel SD-WAN deployments at no additional charge	●	●	●	●
Voice service provider peering	Improves voice quality by optimizing connections to leading service providers	●	●	●	●
Award-winning customer support	24/7 NOC support from Nitel's multiple Stevie Award-winning team	●	●	●	●
Network management options	Nitel offers fully managed SD-WAN solutions. Customers can also choose to co-manage their network	●	●	●	
SD-WAN Features		**Barracuda**	**Cisco**	**VMware**	**Versa**
Simultaneous use of multiple uplinks (transports)		●	●	●	●
Dynamic bandwidth detection		●	●	●	●
Performance-based transport selection		●	●	●	●
Available gateways		●	●	●	●
Application-aware traffic routing		●	●	●	●
Adaptive session balancing across multiple uplinks		●	●	●	●
Traffic replication (forward error correction)		●	●	●	●
Application-aware WAN		●	●	●	●
Traffic shaping and QoS		●	●	●	●
Full, partial, and hub & spoke topologies		●	●	●	●
Cloud on-ramp with path optimization			● w/ Advanced	●	
VPN segmentation			●	● Network Segmentation	
High availability		Active/Passive	Active/Active	Active/Passive	Active/Active
Portal-based analytics		Site-wide	Network-wide	Network-wide	Network-wide

Security Features	Barracuda	Cisco	VMware	Versa
Integrated stateful firewall with packet inspection and forwarding	●	●	● with Palo Alto	●
Integrated next-generation firewall	●	●	● with Palo Alto	
IDS/IPS (UTM)	●	●	● with Palo Alto	
Antivirus and web filtering	●	●	● with Palo Alto	
Sandboxing and advanced malware protection	●	●	● with Palo Alto	
Application control and granular application enforcement	●	●	●	●
URL filtering	●	●	● with Palo Alto	
Interception and decryption of SSL/TLS encrypted applications	●	●	● with Palo Alto	
NAT (SNAT, DNAT) PAT	●	●	●	●
Cisco Umbrella DNS protection (included with Nitel-Connect SD-WAN)	●	●	●	●
Active directory integration	●		●	

SELLING TO THE C-SUITE

C-suite or other senior-level executives hold the majority of the decision-making power in a B2B sale. As such, understanding how Nitel-Connect helps executives reach their goals can be helpful.

Goals/Motivation	Positioning
CEO • Drive Business Growth	• Improved customer and employee experience through new and/or more efficient use of cloud and WAN solutions
CIO • Increase productivity through enhanced voice, SaaS and IaaS experiences • Protection against increasingly sophisticated cyber attacks • Guarantee business continuity • Optimal use of IT staff	• Reduced latency in SaaS and IaaS performance • More efficient WAN topologies • Prioritization and visibility of application usage • Redundant, resilient, private network/internet hybrid SD-WAN with available active/active architecture and multiple cloud access points • Fully managed threat detection and firewall options for entire WAN • Fully-managed service with US-based NOC, 30-second call response and dedicated account manager
CTO • Utilize new technologies to improve business, IT and customer experiences • More easily meet compliance requirements	• Adding new applications that will improve customer experience • Confidence that application performance will be sufficient and seamless • Automated firewall log management helps meet compliance requirements
CFO • Reduce CAPEX & OPEX • Protection against increasingly sophisticated cyber attacks	• Potential reduction in bandwidth costs • Reduce IT support for branch locations • Fully-managed OPEX service • Lower risk of cyber-attack damage via MTD
CMO • Improve customer experience • Develop brand loyalty	• Ability to efficiently access top marketing and CRM SaaS applications • Ability to provide applications that improve customer experience

QUALIFYING QUESTIONS

The following are questions to help understand if a prospect might be a good fit for Nitel-Connect SD-WAN.

Qualifying Question	Explanation of Fit
Are you migrating applications to the cloud?	SaaS and IaaS cloud application traffic that is forced to backhaul through the data center before reaching the Internet provides poor user experiences. Nitel-Connect allows for traffic from a particular branch to be segmented and then directly connected to the cloud via the Internet, over the Nitel network, or more efficient connections available from within Nitel's network.
What are your top critical applications? How do you know you have enough bandwidth to support those apps?	Cloud and video conferencing apps require significant bandwidth. Nitel-Connect blends affordable broadband connections with private-network reliability. The Nitel network is available as an alternate path to the Internet for critical traffic, and at no additional cost. Applications can then be prioritized based on their importance to the business in their use of available bandwidth.
Do customers/visitors require secure, direct Internet access?	Select configurations of Nitel-Connect with Cisco SD-WAN have the ability to isolate application traffic within a single IPSec tunnel. This lowers the potential impact of a security breach should one occur.
Are remote workers accessing or transmitting highly sensitive data?	Select configurations of Nitel-Connect with Barracuda feature highly secure remote access options through desktop and mobile clients, as well as via clientless VPN portal with no user limit.
Do you foresee expanding the number of branches needing WAN connectivity?	• Nitel can provide and manage nationwide access from over 1,000 providers • Every business is close to one of Nitel's North American POPs, delivering fast access to the Nitel network, cloud and UCaaS providers • Nitel can deploy and configure branch locations quickly and efficiently • Once on the Nitel network, customers can add products and services with ease
What kind of redundancy has been built into your network?	• Every deployment of Nitel-Connect SD-WAN includes access to Nitel's private network for select traffic. The Nitel network provides an alternate path to the unknowns of the internet's middle mile. • Nitel's network is designed for redundancy and has never had an unscheduled outage. • Nitel is also able to provide extensive last-mile diversity and high-availability endpoint hardware