SECURE ACCESS FOR THE HYBRID WORKPLACE

KEY NETWORK INFRASTRUCTURE CONSIDERATIONS

EXECUTIVE SUMMARY

Recent events underscore the need to support a hybrid approach to enable knowledge-worker productivity, both inside and outside the office. To ensure a consistent and secure application experience for all users, IT directors need to rethink network design to ensure consistency of IT operations as well as ease of management. Infrastructure providers offer many tools to enable flexible access, but the choices are many, and businesses of all sizes need guidance.

Enterprises require an integrated approach that tightens functionality to support scalable, reliable, and secure networking. Integration also delivers simplification and ease of management. Specifically, what tools are needed to facilitate secure access within the campus, branch, and work from home? Is it time to upgrade to Wi-Fi 6? Should 5G private cellular networking be a consideration? Can automation play a key role in ensuring a higher quality of service? Why are assurance, analytics, and security so important? There is a multitude of software-defined wide-area networking (SD-WAN) solutions from which to choose – which is the best fit? The mix of tools used may vary among key verticals such as education, healthcare, and brick and mortar retail by workload requirement, but they all play an important role in supporting ubiquitous connectivity. There are only a few networking infrastructure providers that can provide a complete solution.

This paper explores key network infrastructure considerations that deliver an optimal mix of hardware, software, and SaaS to support consistent, secure access across hybrid work environments, including Wi-Fi 6, 5G, wired infrastructure, security, automation, assurance, analytical tools, and SD-WAN. We also provide our opinion of Cisco Systems' ability to deliver these capabilities, based on its broad portfolio, exceptional research and development investments, and deep experience supported by a considerable number of deployments across multiple industries.

Wi-Fi 6 Considerations

Is it time for enterprises consider the upgrade path to Wi-Fi 6? The simple answer is yes. Wi-Fi 6's improvements over prior wireless standards are compelling. It offers improvements in latency and throughput, greater device support, improved power management, and robust security.

Wi-Fi 6 delivers a significant increase in performance. Roughly speaking, throughput is an astounding twenty times faster, and latency is three times lower than previous Wi-Fi standards. In remote work scenarios, Cisco's Wi-Fi 6 solution, in particular, is exclusively able to dynamically select the optimal channel that mitigates interference in congested areas such as apartment complexes, hotels, and popular co-working spaces. In campus deployments, Wi-Fi 6, combined with location-based and proximity services, will support a safe return to the office with density monitoring. The new wireless standard is also poised to dramatically accelerate the digital transformation occurring in education with augmented and virtual/mixed reality applications, healthcare with massive IoT biometric sensor integration, and hospitality for improved guest management.

Wi-Fi 6 also delivers greater device support through a significant power management improvement as well as stronger encryption to harden network access. The latter is especially compelling for remote access as well as higher education environments in which students utilize several devices for in-person and distance learning. Wi-Fi 6 can support more connected devices in healthcare environments to facilitate video-intensive care such as telemedicine and remote monitoring at scale while ensuring Health Insurance Portability and Accountability Act (HIPAA) patient data compliance with improved security. Considering the significant improvements in performance, device support, and security, Wi-Fi 6 should be part of any plan to support business resiliency for hybrid work spanning campus, branch, and work from home.

5G, on the other hand, promises to deliver ultra-low latency and significant throughput performance gains over LTE, unlocking transformative uses cases across many industries. There is high interest in deploying 5G cellular infrastructure within the enterprise back-office to complement Wi-Fi carpeted deployments. Private networking, by definition, allows a select number of devices to communicate with one another. The integration of 5G into private enterprise network topologies promises to enable the next industrial revolution, often referred to as Industry 4.0, delivering smart automation, manufacturing, warehousing, and logistical capabilities.

Will 5G be the ultimate demise of Wi-Fi? Certainly not. Instead, use cases will drive a blend of both connectivity options. 5G and Wi-Fi 6 are truly better together. Case in point, Wi-Fi 6 is architecturally better equipped to integrate with public and private 5G networks to facilitate an improved roaming user experience. Mobile 5G is undoubtedly a game-changer, but Wi-Fi will also continue to evolve beyond Wi-Fi 6, providing a highly scalable, cost-effective networking solution for most front-office operations.

Wired Infrastructure Considerations

Although connectivity to the end device is most-often untethered today, critical wired networking infrastructure encompasses routers, switches, and fiber optics that weave together an essential support backbone for enterprises. Wired infrastructure is a critical component in supporting both campus and remote workers, given it is inherently more secure and provides robust segmentation. Wired infrastructure within campuses also facilitates an emerging “smart” building trend that will enhance higher degrees of automation and operational control and tighter integration between IT and OT environments. Purpose-built switches are designed to power and manage a variety of IT, OT, or IoT devices and sensors. They can enable visibility, control, and automation through the integration with artificial intelligence (AI) and machine learning (ML). Smart building solutions can facilitate a safer return to the office by monitoring the density of employees and automatically triggering actions such as closing meeting room doors and sanitizing areas when safety thresholds are surpassed.

Another compelling point in support of strong campus wired infrastructure is remote workforce access. The implementation of critical policy, routing, segmentation, and monitoring, consistently across campus and remote work environments is dependent on the robustness of a given network’s wired architecture. Security is also a major consideration. The reality is that without the proper zero-trust security foundation within campus infrastructure, it is not possible to extend critical identity-based policy and segmentation to distributed remote workforces.

Enterprises should not overlook the importance of a robust wired infrastructure. Enterprises of all sizes should inventory current deployments and determine critical upgrades to support both campus and remote worker access and productivity.

Automation for Scalability and Resilience

Is it time for enterprises to finally trust automation? The answer is yes. They have little choice. Historically, enterprise network operators wanted the "easy" button to deploy automation, easing the transition to full automation, while service providers have long

embraced automation to ensure a high quality of service and to avoid subscriber churn. Recent events, including shelter-in orders and an increase in remote work, have accelerated work from home and compel enterprises to embrace network automation. The benefits of automation include faster new device provisioning, network self-healing, and improved compliance and configuration management among other capabilities. Consequently, automation should be a strategic consideration for any hybrid workplace networking deployment.

THE VALUE OF NETWORK ASSURANCE AND ANALYTICS

Assurance provides a network operational baseline and ensures that a given network's desired state is realized and maintained with some degree of automated corrective action for self-healing. Assurance also measures the impact of network change on security, compliance, availability, and quality of service through continual policy verification.

Analytics involves collecting and analyzing data to improve visibility, performance, reliability, and security. Analytics often applies automation elements – such as device provisioning and orchestration – that eliminate network operators' needs to perform mundane tasks. Employing analytics frees IT staff to support more strategic endeavors for lines of business, such as new application delivery and other productivity enhancements.

How do assurance and analytics work hand-in-hand? The combination establishes a critical network operational baseline through the integration of assurance, analytic software engines that examine traffic patterns, application performance, and network events. Artificial intelligence and machine learning also facilitate a more efficient aggregation of large volumes of data across many network devices. Such platforms include data from switches, routers, Wi-Fi access points, IoT, and headless devices and sensors. Benefits tied to the synergies between assurance, analytics, and automation for both network operators and employees include:

- Identifying potential issues before they occur
- Implementing corrective actions and remediation with limited IT operator involvement
- Isolating potential security vulnerabilities and preventing damaging breaches that result in remote user access issues
- Continual fine-tuning of network performance for an improved user experience
- Identifying significant operational savings for IT staff

SD-WAN AND THE RISE OF SASE

SD-WAN revolutionizes how network operators support distributed branch locations, remote knowledge workers, and enhanced business productivity. SD-WAN's power lies in its ability to improve performance, ensure application consistency, and reduce cost dynamically through software. However, the number of SD-WAN offerings is overwhelming, and it is often difficult for network operators to make an informed decision. One size does not fit all. Thus, enterprises should consider a platform's ability to support cloud management for simplicity and scalability as well as topology complexity for segmentation and advanced routing needs. What is needed is a fully integrated solution combining robust connectivity and security. Secure Access Service Edge (SASE) delivers both software-defined connectivity at scale and robust security tools in a cloud-delivered service model. The benefit to enterprises of all sizes is the ability to support user access dynamically and securely regardless of location.

CALL TO ACTION

To emerge successful in the "new normal," network operators must rethink the overall approach to supporting connectivity for telecommuters and traditional office environments. Integration is key to building a robust connectivity platform that simplifies deployment, ongoing management and delivers higher levels of security, scalability, reliability, and enhanced user experience. IT professionals should also consider a number of important elements when planning any network for hybrid work. These include Wi-Fi 6, 5G, wired infrastructure, security, automation, assurance, analytical tools, and SD-WAN as integral to the network architecture of the future.

It is Moor Insights & Strategy's opinion that Cisco is well-positioned to deliver the necessary set of tools to facilitate consistent, secure access across hybrid work environments. The company's deep capabilities evidence this for all of the tools, infrastructure, and solutions referenced in this research paper. The following two customer deployments in education and health care exemplify Cisco's capabilities to support secure access in hybrid work environments.

San Jose State University:

"The Cisco Catalyst access points and switches provide a robust and flexible wireless solution that has enabled us to provide a collaborative digital learning experience across our diverse environment with support for more than 25,000 concurrent devices. It's amazing how leveraging our existing Cisco wireless

network infrastructure investment, combined with the Cisco DNA Spaces platform, enabled us to quickly create a safer environment based on real-time, data-driven decisions and analytics."

Shai Silberman, Director of Network Services, San Jose State University

Adventist Health:

"With the help of Cisco DNA Center installed in our central data center, we are able to manage our entire Cisco Catalyst 9000 switches and Wi-Fi 6 access points. It supports more than 80,000 employees as well as patients and guests within our 54 hospital campus systems throughout nine states. In addition, we are using Cisco's AI endpoint analytics application as the centerpiece of our security strategy. Its unprecedented visibility and insights to endpoints keep our healthcare network secure and compliant with HIPAA regulations."

Ed Vanderpool, Senior IT Manager, Adventist Health

To learn more, visit www.cisco.com/go/dna.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR
Will Townsend, Senior Analyst at Moor Insights & Strategy

PUBLISHER
Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
This paper was commissioned by Cisco Systems. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.