WHITE PAPER

NETWORKS EVOLVE TO SUPPORT A CHANGING WORLD

New technologies deliver secure connections and build business resilience.

EXECUTIVE SUMMARY

Organizations have become more reliant on networking to help achieve both critical and aspirational objectives as they have struggled to maintain control, visibility and security amid a massive shift to remote work. These types of challenges are now not unusual, nor are they likely to be temporary. They have become the norm — defining features of the future of work, an environment which is decidedly a hybrid of both remote and in-person models.

To address these changing circumstances, organizations are looking to automation solutions to improve the speed and quality of their network performance and security and, ultimately, the achievement of business priorities. Two such solutions, software-defined WAN and intuitive management platforms, enhance visibility and facilitate management, no matter how dispersed an organization's employees may be.

Remote work has irrevocably altered the cybersecurity landscape as well, requiring network strategies that address these new threats and vulnerabilities. Secure access service edge, next-generation firewalls and multifactor authentication are the baseline. Zero-trust approaches will reinforce security controls and policies through network segmentation, identity-based access and other best practices. Additionally, advanced wireless capabilities, including Wi-Fi 6, Wi-Fi 6E and public and private 5G, will create new opportunities while augmenting security.

Organizations and their networks evolve and adapt in tandem, with capabilities and limitations that are frequently interdependent. As organizations move their networks forward, they strengthen their resiliency against future crises and build a solid foundation for business success.

The Changing Demands on Network Technology

As the pandemic begins to subside, organizations are preparing for yet another chapter of change. Instead of seeking a return to normalcy, we are entering an era of redefinition — in essence, creating the future of work as we go.

The pandemic has forced organizations to grapple with pivots and disruptions that, in many cases, will leave a lasting mark on their teams, operations and society as a whole. Remote work, remote learning, telehealth and other forms of virtual collaboration will require not a central hub but a cohesive, coordinated assembly of microhubs, connected by networking technology. The top two considerations as organizations address their changing needs are connectivity and security.

Home networks, in particular, have become an extension of office networks. These new "microbranches" challenge organizations to maintain productivity and enforce cybersecurity in new ways, while providing an effective experience for employees and customers. Virtually overnight, some IT staffs have gone from connecting a few dozen locations through controlled connections to connecting hundreds or thousands of locations. They're tasked with ensuring employees have high-quality access to important applications while contending with the vagaries and competing traffic of employees' home networks and the variable quality of their local internet access.

Cybersecurity has been a more difficult and urgent problem to solve. The loss of control over and visibility into remote employees' activities is especially problematic, as cyberattackers also have adapted to the pandemic. As they evolved their strategies to match new vulnerabilities, reports to the FBI's Internet Crime Complaint Center increased by 300 percent. Many attacks were successful, with cybercriminals stealing troves of valuable data in some cases. In addition to the increase in the volume of attacks, both the variety and the scale of attacks have also jumped. For example, ransomware may become doxware, with attackers threatening to sell or release stolen data if their demands are not met.

The question facing organizations now is how to provide secure, seamless wireless connectivity anywhere, regardless of device or location. With the network footprint now extended across the internet, organizations must rely on the endpoint to be able to connect, manage, monitor, maintain and secure connectivity moving forward. In this environment, automation and identity-based access are the way to achieve, at scale, the dynamic responsiveness required to safely provide a path to connectivity among all of an organization's microbranches.

It has become clear that most organizations will retain some level of remote work beyond the pandemic, with many adopting hybrid work as a permanent feature of operations. Even those that elect to locate employees onsite, either primarily or exclusively, should be prepared to shift to remote operations, even temporarily, in the event of a future crisis.

A Hybrid Future

Organizations recognize these realities and are aligning their investments accordingly. As leaders prepare their teams for hybrid work, PwC research shows many plan to increase their investment in tools for virtual collaboration (72 percent), IT infrastructure to secure virtual connectivity (70 percent) and training for managers to oversee a more virtual workforce (64 percent).

Even those investments that specifically focus on the in-person environment reflect the hybrid nature of future work and will include a networking component, such as conference rooms with enhanced virtual connectivity (57 percent) and hoteling applications (50 percent).

Only 20 percent of business leaders worldwide believe their organizations will emerge from the pandemic stronger than they were before, PwC's Global Crisis Survey 2021 reports. Some

of these organizations succeeded where their competitors failed — leveraging a profound crisis in ways that ultimately yielded positive outcomes — because of their commitment to enhanced technology. In a hybrid business environment, networking infrastructure is the framework that makes these outcomes attainable and allows organizations to bring remote colleagues together in meaningful ways.

"Resilience Pioneers," in PwC's terminology, are "innovative, tech-driven and able to adapt to changing conditions." As a result, they were already ahead of the game, while their peers struggled to keep up. It is certain that, when the next crisis arrives, organizations that follow their lead will be in the best position to demonstrate true business resilience.

3

The number of days per week that an employee needs to be in the office to maintain organizational culture, once COVID-19 is not a concern, according to a survey of U.S. executives[1]

The Evolution of Network Technology

It remains true that the vast majority of network configurations are done manually. That is quickly becoming untenable in the dynamic, complex landscape in which organizations now operate. The footprint has become too large and too sprawling. The solution, automation, will advance rapidly over the next few years, offering more opportunities for organizations to integrate a variety of new technologies, including artificial intelligence and machine learning, into their networks.

SD-WAN

SD-WAN is compatible with 21st-century workflows in a way that traditional WANs are not. Unlike the old hub-and-spoke model, SD-WAN has the ability to elevate performance by allowing microbranches to connect directly to the application, cloud or data center they need. These solutions directly address the connectivity challenges organizations face in relation to mobility, cloud computing and the Internet of Things (IoT).

Greater demands on networking, combined with increased complexity of management, often move organizations toward software-defined solutions that can better accommodate these requirements. Centralized control lets administrators establish policies and manage an entire network from a single, unified tool. Simplification and streamlining enhance efficiency, agility and accuracy. Equally important, SD-WANs improve performance by utilizing multiple transports, routing traffic in the most efficient way based on customized application and performance policies.

The prioritization of critical application traffic also improves the user experience. When users are dispersed, SD-WAN's centralization makes it easier to deliver high-quality connectivity. System-level policies can be pushed down to microbranches, with traffic among work sites, clouds and data centers flowing along optimal paths.

Network Automation

Increasingly, the defining features of network management are dynamism and complexity. As organizations identify opportunities to shift away from manual processes, they will find that automation of end-to-end network policies enhances the security posture and alleviates burdens on IT staffers, who can then focus on other work.

Software-defined networking (SDN) leverages automation to simplify and standardize network configuration, with administrators deploying policies and best practices across network devices. Establishing network policies at a high level gives administrators more consistency in network performance and control, while allowing the solution to handle the bulk of repetitive implementation work.

Intent-based networking (IBN) leverages automation in a similar way, gathering telemetry data from the various network components to create an in-depth view of network health and performance. With the added application of machine learning, IBN can analyze vast amounts of telemetry data to measure the effect of network and security policies on applications and the end-user experience.

IBN is well-suited to remote work because it brings an AI-driven, data-informed approach to performance: measuring certain types of traffic and identifying patterns to optimize the user experience. These controls, and the resulting insights they provide, help administrators deliver consistent, business-enhancing performance in a constantly changing environment.

Users' At-Home Connectivity

One of the challenges of remote work is the immense variation in employees' home networking environments. In response to this, organizations can apply strategic variation in the network services they provide to these remote employees. The homogenous managed network has given way, in many cases, to tiered services that more closely align two key concerns — security and performance — with the nature and business criticality of users' work.

Virtual private networks (VPNs) remain a viable solution for many employees. Organizations may choose to augment VPNs with digital experience monitoring, allowing them to understand how remote workers and devices interact with company applications and services.

Certain user groups require higher levels of connectivity and security, like those supported by organization-secured access points, Wi-Fi routers or software-defined WAN (SD-WAN) routers. Customer-facing employees also warrant attention.

In addition, organizations should be mindful of the employee experience, especially as new norms and expectations settle around remote work. Increasingly, remote workers may expect their employers to equip them with high-quality internet. Organizations may also face questions of equity should one employee's experience differ significantly from another's as a result of home network quality.

Source: [1]pwc.com, US Remote Work Survey, Jan. 12, 2021

Network automation is especially valuable in multicloud environments. Automation effectively raises the ceiling on the network efficiency and performance that organizations can achieve, allowing them to take full advantage of the attributes of the cloud. From a security perspective, network automation adds consistent control and improved visibility to provide secure access between the cloud and end-user devices.

Together, SDN and IBN improve network and security policy management, while providing validation that the network is performing to expectations.

Wireless Networking

Device density has become a driving force on par with or greater than the focus on wireless coverage. When looking at the latest wireless networking standards, 5G and Wi-Fi 6, it's important to recognize that they are not either/or propositions. For many organizations, 5G and Wi-Fi 6 are complementary, with use cases suited to both. High-density environments, such as healthcare, higher education and manufacturing, will see the most gains in performance and efficiency.

Organizations that have tried, without success, to fix performance by adding wireless access points (APs) may find the answer in Wi-Fi 6. Often, the problem with wireless is efficiency, not speed. Wi-Fi 6 has three key features that make it a better fit for today's high-density environments:

- Multi-user, multiple input, multiple output (MU-MIMO) allows an AP to communicate with several devices simultaneously, rather than sequentially, via separate spatial streams.
- Orthogonal frequency-division multiple access (OFDMA) also facilitates multiuser access, subdividing channels to allow more devices to communicate at once.
- Target Wake Time (TWT) reduces power consumption and extends battery life by enabling APs and stations to "sleep" at designated times.

Wi-Fi 6 aligns with the mobile-first model that is shaping lines of business, if not entire organizations. Healthcare providers, for example, anticipate a long-term expansion of telehealth, which will require wireless connectivity that can handle data-intensive transmission of sensitive images, video and patient records. Wi-Fi 6 also offers better security for operations like these: WPA3, the newest security standard, provides better encryption and authentication.

Wi-Fi 6E will change the game further by significantly increasing the number of available channels. Organizations seeking to take advantage of Wi-Fi 6 and 6E will need to understand where they will and won't be able to do so. For instance, Wi-Fi 6E capabilities extend only to devices that are compatible with the 6GHz spectrum. In addition, while 6E will add even more bandwidth, compatible wireless access points may also be more expensive because they have more radios.

Careful alignment of device and infrastructure upgrades, particularly with an eye toward opportunities to maximize specific operational areas, can position organizations to achieve the desired outcomes at the right time.

Organizations that rely on outdoor connectivity, video-intensive applications and IoT will see major gains with 5G mobile broadband. High-speed connectivity, expanded bandwidth and ultralow latency will improve existing use cases and facilitate exciting new ones, from augmented reality to remote surgery.

While IoT devices allow for more efficient and sophisticated workflows, they also deliver one of the most valuable assets an organization can have: data. As 5G pushes IoT to new heights, organizations will be able to leverage new types of data-driven analysis and deploy automation in new ways. Private 5G deployments can enhance indoor wireless coverage for manufacturing and warehouse applications and provide another failover option for wired connections.

Citizens Broadband Radio Service (CBRS) will expand the options even further, allowing organizations to establish private 4G/5G networks on the 3.5GHz spectrum.

Network Security

Even before the pandemic, the traditional IT perimeter had expanded to such an extent that the analogy of a "perimeter" no longer fit. Now, the focus is on the edge and zero trust. Segmentation and identity-based access enforce policies and determine who can get to certain types of data, while preventing issues in home and business networking environments from affecting each other in undesirable ways.

Secure access service edge: SASE is an architectural framework that finds the edge at the device-to-cloud intersection and protects users, endpoints and data wherever they are located.

Hybrid Work Is Here to Stay

More than half (56 percent) of the U.S. workforce could work remotely part or full time, according to a Global Workplace Analytics estimate, and many employers agree. A PwC survey of U.S. executives indicates that hybrid work is poised to become the norm, with only 17 percent of respondents saying their organizations will resume full-time onsite work after the pandemic.

Higher morale and broader talent recruitment are two big drivers. Financially, even partial remote work could save companies up to $500 billion each year in real estate and other costs, Global Workplace Analytics estimates. That's in addition to brick-and-mortar expenses such as janitorial services and transit subsidies.

Some organizations may reduce their physical footprints, while others may expand them to accommodate social distancing. Central locations that can house all employees at certain times may work for some organizations, and others will find multiple, dispersed sites a better fit. Many organizations may continue to experiment into the near future.

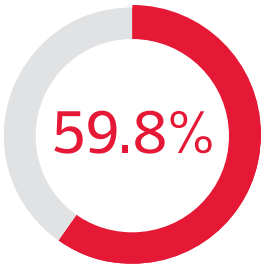
What is certain is that new work patterns will involve numerous variations on in-person and virtual collaboration — all raising new requirements and challenges for network connectivity.

SASE brings together several core technologies, such as network security functions and software-defined networking, in ways that allow for continuous, responsive oversight. SASE's dynamism, for example, lets IT teams modulate access based on contextual, granular insight into users' behavior. Real-time identification of behavioral anomalies, paired with appropriate data governance, enable security to remain consistent even as users engage with mobile- and cloud-first environments.

SASE does require solid data management and governance programs. Defining security in terms of data and users means that organizations must be clear on which data assets exist, where they reside and who should have access — the latter based on least-privilege principles.

Software-defined perimeter (SDP): Organizations may also implement this approach to secure remote access to both cloud-based and on-premises applications, using a unified platform to manage security policy.

For remote work, SDP offers more precise, granular control than broader-based solutions, such as VPNs, segmenting network access based on identity and device. It also delivers a better experience on mobile devices. For organizations pursuing a zero-trust approach, SDP is an essential component, requiring stronger authentication and limiting exposure.



The percentage of business continuity professionals who said IT resilience contributed the most to the success of their organizations' pandemic response[2]

Next-generation firewalls (NGFW): NGFWs bring powerful analytics to inbound and outbound traffic both in the data center and on the network edge. Organizations require advanced tactical defenses now more than ever given the massive surge in attacks that has accompanied the pandemic. Centralizing NGFW management by deploying the same firewall engine across the network increases consistency, streamlines change management and facilitates visibility and response as administrators manage events, analytics and reporting.

Cloud-delivered firewalls (CDFW) as a Service: CDFWs bring capabilities similar to those of an NGFW into the "as a service" model, which enables organizations to protect users, endpoints and data with the same level regardless of location. Connecting a CDFW service to an SD-WAN branch enables organizations to scale their security efforts without the need for expensive security hardware at multiple, smaller locations.

Multifactor authentication: Finally, organizations should be integrating MFA throughout their networking environments. A periodic review of critical business applications to ensure they are secured by MFA is warranted, particularly in light of recent operational changes.

4 Guiding Questions About Your Network

Many organizations are driven by a focused need when they embark on a major networking initiative, but the ramifications of any new approach will expand broadly. A good starting point to ensure that an initiative ultimately addresses all the important and interrelated outcomes is to identify and understand the nature of the problems the organization seeks to address.

The process of clarifying current and desired capabilities can surface challenges and opportunities that, in turn, can inform the alignment of technology with business objectives. Start with the following questions about your organization:

1. Who needs to be involved in the networking project to address applications, cybersecurity and business needs? What other stakeholders exist?

2. Can you provide consistent network performance for your employees, wherever they are, while maintaining corporate security policy, posture and compliance requirements? Is your remote work experience great or merely adequate? Does this affect employees' effectiveness? Can you support it operationally?

3. As you shift toward a post-pandemic environment, are your campuses capable of handling a new connection paradigm? Have capacity requirements changed? Are there additional Internet of Things devices, coverage areas or office space issues that affect networking infrastructure in new ways?

4. Do you have the same level of visibility into cloud-based and on-premises environments, mobile, and microbranch and in-person employees to make informed application performance decisions?

Network Strategies for the Modern Era

Three principles should guide organizations' networking strategies as they navigate the next phases of pandemic response and recovery: zero-trust security, automation and resilience. These are interrelated, with each representing a holistic objective that organizations should aspire to. They serve as targets, providing constancy and direction when so much else in the business environment continues to change.

Zero Trust

The stringency of zero trust — trusting no user or device until it has established identity and authorization for access — is appropriate for today's security environment. Authenticating users to access the network and then allowing free rein is an insufficient approach when attackers can exploit so many potential vulnerabilities. Perimeter-based authentication no longer works when the perimeter is fluid, shifting continuously among clouds, branches and microbranches.

Zero trust addresses these realities through the following measures:

Source: [2]The Business Continuity Institute and FortressAS, "The Future of Business Continuity and Resilience," September 2020

- Segmenting the network in ways that reinforce security controls and policies
- Strengthening identity and access management with MFA, role-based access control and other tactics
- Implementing least-privilege controls throughout the network, blocking unnecessary traffic in and between segments
- Deploying application inspection technology to inform contextual controls
- Analyzing activity across network and cloud services with security information and event management tools

Automation

Given the current complexity of networking, it may be surprising that nearly all network changes are still made manually. Too often, these processes lead to configuration errors and inconsistencies. These, in turn, result in security vulnerabilities, degraded performance, improper application of policies and procedures, and outages. Automating the vast scope of work required to manage and optimize a network minimizes these outcomes while freeing staff to focus on business-enhancing initiatives.

Network assurance tools improve visibility across the network, gathering telemetry data and compiling it into a clear, concise format that helps staff identify and address problems. Coupled with detection and response tools, they also provide a powerful boost to security, augmenting the work of IT staff by using AI and machine learning to analyze logs, flag priority alerts and block attacks before they infiltrate the network any further.

Resilience

The organizations that are most likely to thrive after the pandemic are those that approach the disruption and uncertainty they have faced as enduring characteristics of the modern business environment. It is telling that even among organizations that developed crisis response plans prior to 2020, many had not prepared specifically for a pandemic, and certainly had not anticipated such an extended disruption.

These outcomes, together with the negative consequences that have befallen so many organizations, attest to the absolute necessity of IT infrastructure that enables resilience — no matter what it may encounter. The seeds of the next crisis may already be taking root. Before it emerges, networking teams have a rare opportunity to conduct post-crisis reviews and to strategize about the best ways to leverage advanced networking and security technology for the future of work. Whatever it may bring, a commitment to build technological resilience is the most effective way to achieve business resilience.

CDW: We Get Networking

Partnering with CDW gives you access to our expertise, state-of-the-art tools and strong relationships with technology vendors. These relationships, together with our scale, allow us to assemble the best solutions for each organization and to facilitate their deployments.

We provide varying levels of support, depending on the needs of each organization:

- **Advisory services:** Prior to purchase, consultation with our solution architects helps organizations to identify business goals and the technical solutions to achieve them.
- **Assessments:** These range from deployment planning to full-scale assessments that help organizations improve and optimize existing solutions.
- **Implementation:** This service may be a pilot, a white-glove rollout or anything in between.

We offer three levels of managed services to help customers derive the most benefit from their networking investments:

- Bronze — Monitoring, alerting and reporting
- Silver — Bronze managed services with minor software upgrades
- Gold — Silver managed services with maintenance, troubleshooting, reactive remediation and incident management

CDW Can Design, Orchestrate and Manage a Comprehensive Infrastructure Strategy

CDW's simple, smart, scalable and flexible services portfolio provides a fully automated and managed infrastructure across your entire network, whether on-premises, hybrid or in the cloud.

DESIGN for the Future
Consult with our team of technology experts to plan a solution that fits your unique needs and optimizes business impact.

ORCHESTRATE Progress
CDW Amplified™ Infrastructure services help you build and deploy your custom infrastructure utilizing best practices.

MANAGE Operations
Our world-class, certified staff monitors and manages your infrastructure 24/7/365 to ensure operational efficiency and security.

Sponsors

aruba a Hewlett Packard Enterprise company

cisco Partner

Extreme networks

NETGEAR BUSINESS

Learn more about how CDW can help your organization optimize its network connectivity.