

Internet Access



Lessons for
future business
continuity

Humans are wired to connect. We live in a digital age that allows us to stay connected through email, texting, smartphones and social media. But even with the world at our fingertips, we weren't prepared for 2020.


The simple human interactions we took for granted were quickly replaced with food delivery, Zoom calls and online meetings. But we found ways to connect and collaborate while the world was forced to isolate. Why? Because humans are also wired to adapt. The question is: Can the same be said about your network? If our networks weren't nimble before the pandemic, we've learned the lesson—and value—of being flexible and prepared for anything.

The need for nimble..... 4

The future of work rides on network resilience..... 8

A proactive partner keeps you prepared for anything 11

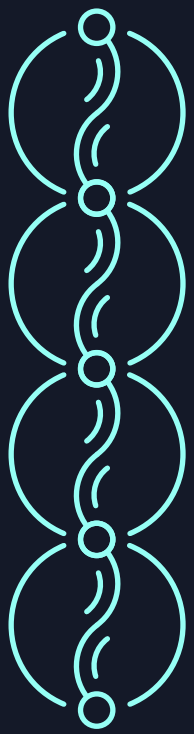




36% of companies said they were unprepared for the shift to remote work.¹



– NAVISITE



THE NEED FOR NIMBLE

Business-as-unusual is a bandwidth hog

When the global pandemic hit, we adapted—especially in the way we conducted business.

At first, skipping the morning commute and being “professional” from the waist up seemed like luxuries. But working from home soon presented a unique set of challenges. Video meetings using apps like Zoom and Microsoft Teams became the collaboration method of choice. As a result, unreliable internet connections became a huge issue. Many homes had two parents teleworking and children remote learning, which placed high demand on networks and throttled bandwidth at peak times when everyone was online.

But in the rush to transition their teams to remote work practically overnight, many businesses were unable to ramp up bandwidth in time. No wonder 83% of organizations found the transition moderately, very or extremely challenging.²

Once a word reserved for high-tech conversations, “bandwidth” refers to how much internet use a network can support at once. A classic analogy used to explain bandwidth is a highway: if the interstate was designed to accommodate a set number of cars moving from point A to point B during any given hour, adding more lanes to the highway would increase bandwidth and allow more cars to pass through. The more people connecting to the network, and the more use of bandwidth-hungry applications like video conferencing vs. phone calls, the more congested the network gets. And all that congestion can lead to slowdowns or activity starting and stopping—none of which is good for business.





THE NEED FOR NIMBLE

A perfect storm for network security

Remote working uncovered a range of vulnerabilities in our business networks. IT managers and partners are faced with a wider web of security concerns in our work-from-anywhere society. A Navisite survey² in late 2020 found that more than a third of respondents were unprepared for the shift to remote work. And the rush to get employees up and running from multiple locations likely took attention away from normal security protocols.

On the employee side, many were dealing with mental, physical and personal pressures on top of workloads and may have innocently overlooked protections like updating passwords, locking computers and updating software. As online activity increased on home networks, so did the use of VPN, WiFi and broadband, which exposed organizations to the threats of phishing, malware and DDoS attacks.



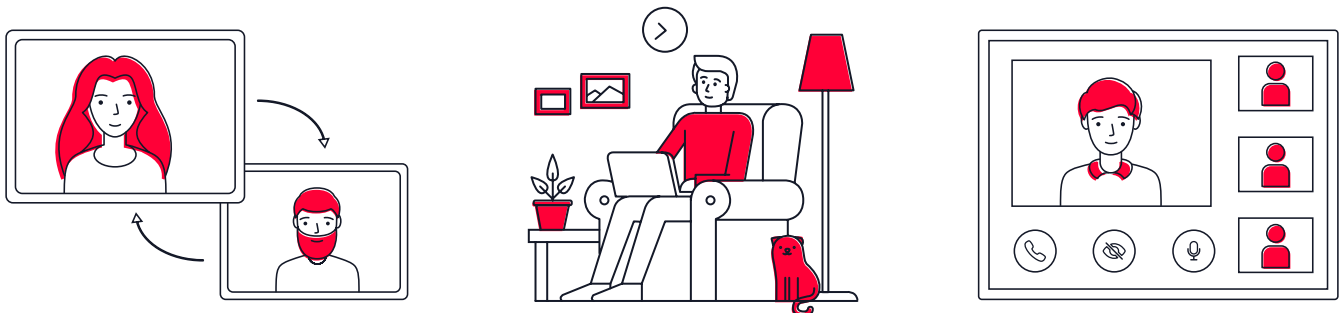
A Navisite survey² in late 2020 found that more than a third of respondents were unprepared for the shift to remote work. And the rush to get employees up and running from multiple locations likely took attention away from normal security protocols.

NEARLY TWO-THIRDS

of the businesses had to transition
over half of their workforce to
remote work practically overnight.

And 83% of those organizations
found this transition moderately,
very or extremely challenging.

– SECURITY INFOWATCH.COM SURVEY



The hazards of remote work

In April 2020, Sivan Tehila, founder of Cyber Ladies NYC, listed the three hazards of remote work.

Home WiFi security:

“As opposed to the office environment, where IT managers can control the security of all WiFi networks, employees’ home networks probably have weaker protocols, which allow hackers easier access to the network’s traffic.”

Phishing scams:

“Phishing attacks are widely recognized as the top cause of data breaches. Hackers can easily send seemingly legitimate, deceptive emails with malicious links and attachments. Once an employee clicks on this malicious link, a hacker can gain access to the employer’s device.”

Insecure passwords:

“Simple passwords are incredibly easy for hackers to crack, and if an insecure password is used across several platforms, it allows hackers to gain unauthorized access to multiple accounts in a very short period.”



Sure, these threats existed before working from home became prevalent, but the security stakes were definitely raised when the lines between work life and home life became blurred. Organizations were no longer shielded by the protection of their corporate LANs as personal and professional online activity inevitably blended.

Upwork Future Workplace reports that by 2025, 36.2 million Americans will work remotely. That’s up 87% from pre-pandemic levels,³ and businesses need to remain vigilant in securing their network and every device with access to it.

Being better prepared for change in the future is a must. As is the need for a nimble IT partner who comes to the table with innovative ideas and technological solutions—so you can be sure your company won’t be caught off guard by the next crisis.



Disruptive in a good way?

IT rose to the occasion in 2020 to keep businesses operational in the face of disruption. Now how do we take the lessons we learned and use them to keep business running smoothly in 2021 and beyond? How do we make sure our networks are secure, robust and resilient enough to support employees and ultimately customers?

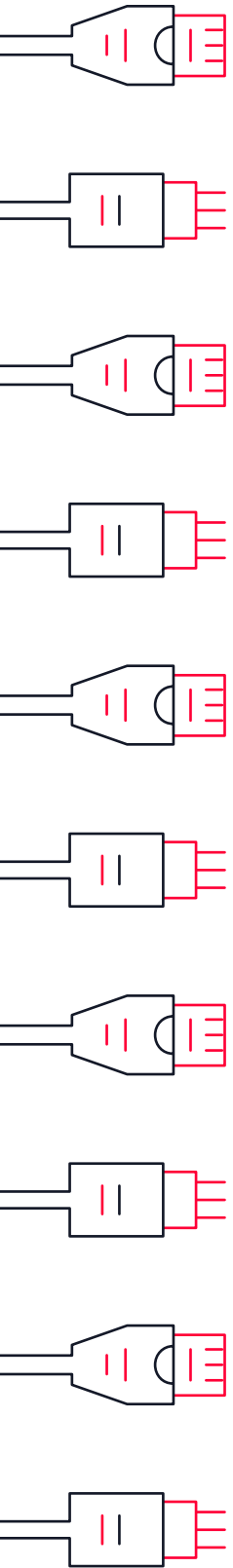
Now that many organizations have successfully adapted to remote working, a more flexible workspace will likely become the new normal. Many companies are heading toward hybrid work, a blended model where some employees return to the office and some remain working from home. A Gartner survey⁶ of company leaders found that 82% of respondents intend to permit remote working some of the time as employees return to the workplace. In a PwC survey⁴ of 669 CEOs, 78% agreed that remote collaboration is here to stay.



78%

agree that remote
collaboration is here to
stay for the long-term

– PWC



Flexible is the new constant



Business leaders are on the verge of major updates to give employees the flexibility to work when and where they want, along with the tools they need to equally contribute from wherever they happen to be. Many businesses are considering things like staggered or alternating work schedules and redesigning physical spaces to better accommodate hybrid work environments.

And because network connectivity is the backbone of productivity and allows businesses to stay functional, a much stronger, more secure network needs to exist. Optimizing the hybrid

workplace requires accelerating investments to support virtual collaboration and creativity, as well as for scheduling and safety. Dedicated Internet Access (DIA) allows reliable connections for remote workers and increases bandwidth speed and security. A network infrastructure that includes DIA will deliver consistent bandwidth and symmetrical download/upload speeds while maximizing business operations and minimizing slowdowns. It's a dedicated lifeline to the web, making it well suited for organizations with bandwidth-intensive or cloud-based applications.

Invisible threads are the strongest ties.

– FRIEDRICH NIETZSCHE

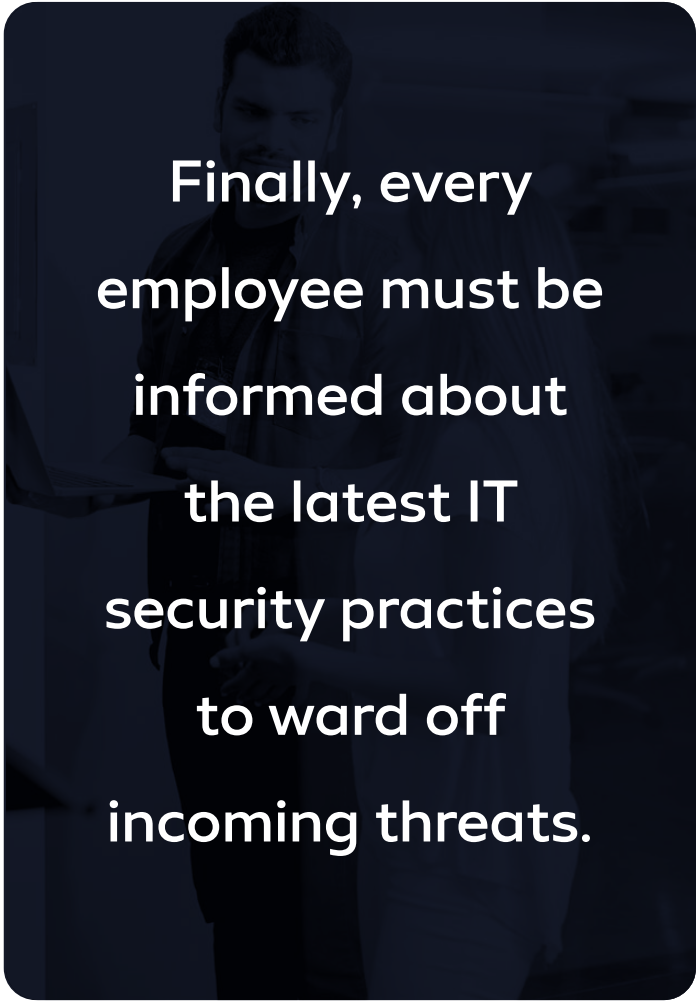
Visibility is valuable

In 2021, we learned that a remote workforce benefits from a flexible network. SD-WAN is a connectivity solution that uses software-defined networking (SDN) technology to control traffic over a wide area network (WAN). Built on a flexible combination of internet access, existing infrastructure and cloud technologies,

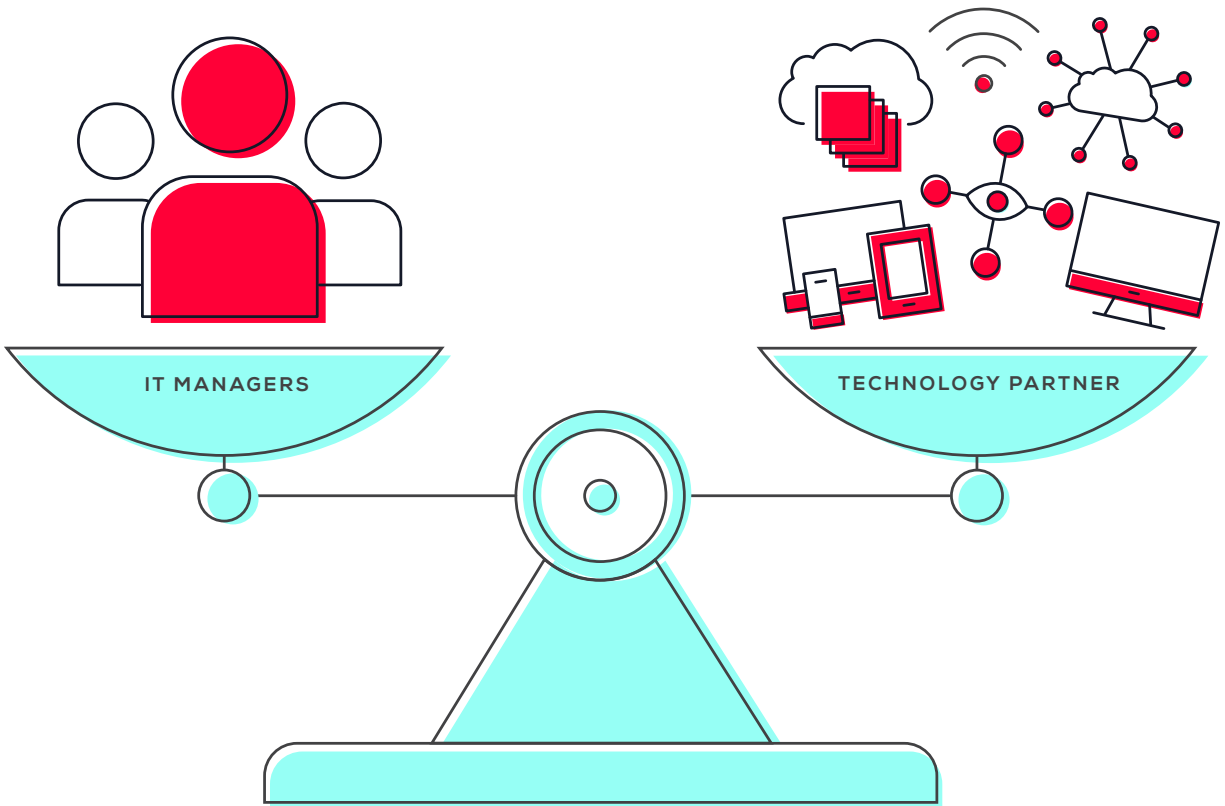
SD-WAN connects all of an organization's local area networks—such as primary sites, branch offices, headquarters and datacenters—from a central location. For example, during the pandemic, SD-WAN made it possible for IT personnel to manage networks remotely, supporting multiple employees, machines and office locations. With full visibility into network activity from one location, SD-WAN helps IT act quickly to prioritize bandwidth, deploy new applications and provide the best possible user experiences at all times.

Perhaps most important is protecting all of your business's valuable data from cyberattacks. Most businesses can't afford the consequences of a security breach. Firewalls block unauthorized access to your computer network by viruses, malware and hackers. They monitor data as it passes

between your computer, your server and the internet to make sure nothing harmful or unintended slips through. Having a managed firewall for your business will give you time to respond before the situation becomes serious—a remote firewall service team can help defend your organization from vulnerabilities 24/7/365.



**Finally, every
employee must be
informed about
the latest IT
security practices
to ward off
incoming threats.**



Heroic network measures

To make all of this happen, you need not only your IT managers—who've emerged as the unsung heroes of the pandemic—but also the right technology partner who can provide the tools, innovative thinking and resources to help your organization thrive, now and in the years ahead.

A proactive IT partner can make sure you:

- Connect and communicate across locations
- Securely send and receive files and information
- Protect the integrity of your systems and data
- Continue to serve your customers and keep your promises

Certainty after uncertain times



A PROACTIVE PARTNER KEEPS YOU PREPARED FOR ANYTHING

Business continuity hinges on the ability to connect. The good news is, we learned so much during COVID that connectivity is thriving. The main lesson learned is that we need to be more prepared. Having a business continuity plan—where your organization can maintain business functions or quickly resume them in the event of a major disruption—is a good place to start.

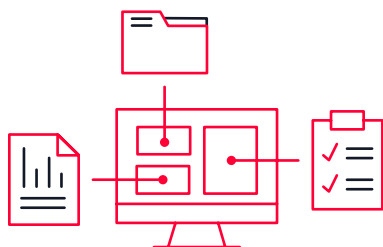
But even more important is making sure your IT plans are more proactive than reactive, and that your network partner can help your business evolve with the ever-changing landscape. With solutions that connect your teams, secure your most important data and are flexible enough to scale to your needs, your business can stay productive and efficient in uncertain times. And everything can be more digital and connected than ever before.

How much will reliable connectivity save you?

Calculate a real-time estimate today: enterprise.frontier.com/estimate

Sources

1. navisite.com/press-releases/navisite-research-finds-more-than-one-third-of-companies-caught-unprepared-to-support-large-scale-work-from-home-model/
2. securityinfowatch.com/cybersecurity/article/21154397/report-enterprises-caught-offguard-by-remote-work-cybersecurity-challenges
3. cnbc.com/2020/12/15/one-in-four-americans-will-be-working-remotely-in-2021-survey.html
4. pwc.com/gx/en/news-room/press-releases/2020/ceo-survey-covid-update.html
5. forbes.com/sites/carrierubinstein/2020/04/10/beware-remote-work-involves-these-3-cyber-security-risks/?sh=480ef65d61c4
6. gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time



Interested in more content like this?

Head over to our [blog](#) for the latest insights on Connectivity solutions.

Contact Us

Ready to discuss how to keep your network prepared for anything?

Give us a call.

888.603.1821

ENTERPRISE.FRONTIER.COM/
CERTIFIED-BUSINESS-ETHERNET

Frontier™