Frontier

Top priorities for your business continuity plan

As an IT leader, you might not be able to predict business disruptions. But by focusing on the right priorities, you can do everything in your power to make sure your teams, systems and technologies are prepared for what's ahead.

With the proper plan in place, you can move your company forward efficiently, productively and securely.

The IT Leader's guide to navigating unexpected change

The COVID-19 pandemic has posed and continues to pose challenges for IT leaders, employees and customers. A large-scale shift to remote and hybrid working means teams are more dispersed. The need to constantly adapt has forced leaders to work and manage in new ways, and rely on more devices and locations, escalating technology limitations and security concerns.

Being one step closer to a post-COVID world doesn't mean businesses are out of the water just yet. As companies adopt new platforms, applications and ways of working, they continue to face uncertainty, budget restrictions and unclear priorities.

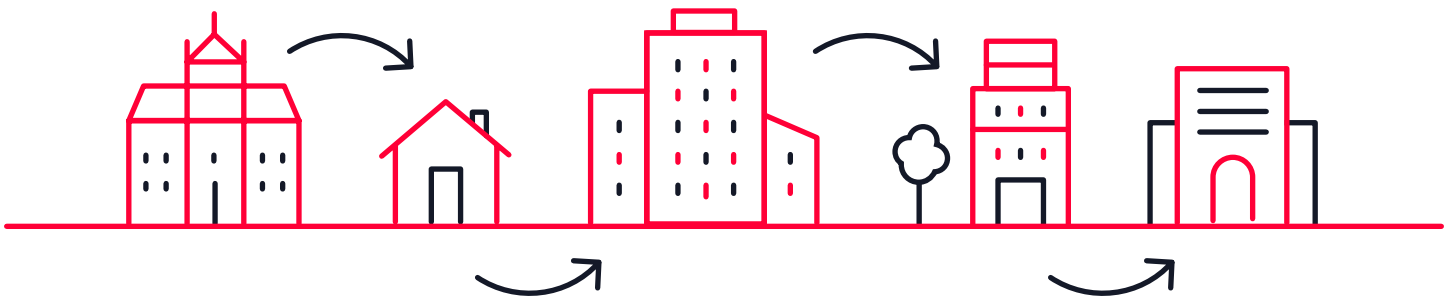And the question remains: How do you plan for the future when change seems to be the only constant?
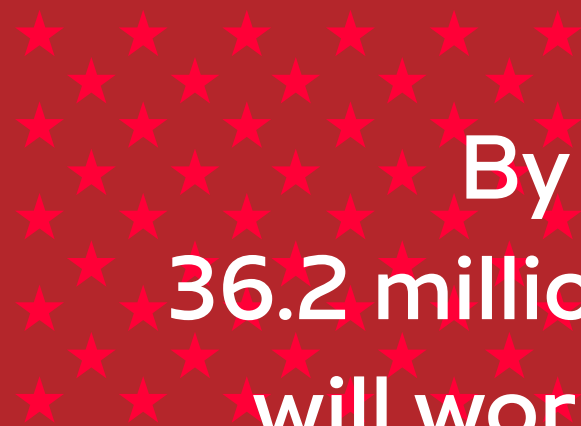
By 2025, 36.2 million Americans will work remotely, up 87% from pre-pandemic levels.

— UPWORK FUTURE WORKPLACE PULSE REPORT[1] —
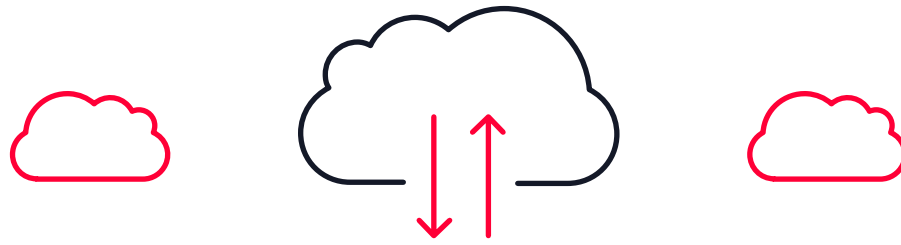
the **shift** to **hybrid** work

According to a "Future of Work Pulse Report" by Upwork[1], 36.2 million Americans will be working remotely by 2025—an 87% increase from pre-pandemic levels. For employees, having a choice of work environment means more flexibility. For employers, allowing some form of remote work helps attract talent, promote productivity and increase job satisfaction. It's no wonder a growing set of companies—including Amazon, Google, Microsoft, Twitter and more—have announced virtual collaboration is here to stay.

Working from any location provides a sense of freedom that many employees have never experienced. But working remotely also poses risks and challenges for teams and customers: Slow speeds and service interruptions. Getting on the same page from multiple locations. The vulnerability that comes with sharing sensitive data. Working across multiple apps and devices. How can IT leads provide the same access, stability and security when teams are virtually everywhere?

The risks of working remotely:

slow speeds and

service interruptions

+

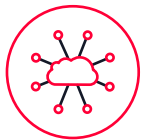getting on the same page

from multiple locations

+

the vulnerability that comes

with sharing sensitive data

+

working across numerous

apps and devices

KEEPING TEAMS AND CUSTOMERS CONNECTED

Break boundaries with cloud-based collaboration

When companies are expected to operate seamlessly from anywhere and everywhere, it's on you to set your teams up for success. But your role consists of more than reacting to IT problems. You hold the key to providing your teams the foundation they need to connect and communicate—so you can avoid future issues altogether.

Cloud-based collaboration bridges the gap between teams, devices and locations while giving people the flexibility to connect at home, at work and on the go. It provides increased mobility, real-time communication and 24/7/365 accessibility, so you don't have to sacrifice productivity when you implement work-from-anywhere policies.

Your network extends far beyond your internet access.

Instead of a single product, cloud-based tools are a collection of solutions that ensure your technology and teams work together through a simplified, reliable network. And here's the thing about your network: It extends far beyond your internet access.

Collaboration tools

Collaboration tools integrate chat, voice, conferencing, video and more through a single interface. With centralized control and fixed monthly rates, they allow you to add and adjust users and apps easily, from anywhere.

Trunk lines

Trunk lines connect you to a private network so no other data traffic interferes with your shared video, voice or apps. This helps ensure you have the bandwidth and security to share sensitive data without delay, even at peak usage times.

Call routing

Call routing uses built-in call recording and intelligence to centrally manage communication, which gives customer service agents the tools and support they need to personalize connections.

In supporting a hybrid workforce, it's not about where you work. It's about staying connected no matter the distance.

By designing a cloud-based solution that fits your teams' unique needs, you can take advantage of the right set of services to bring people closer from afar.
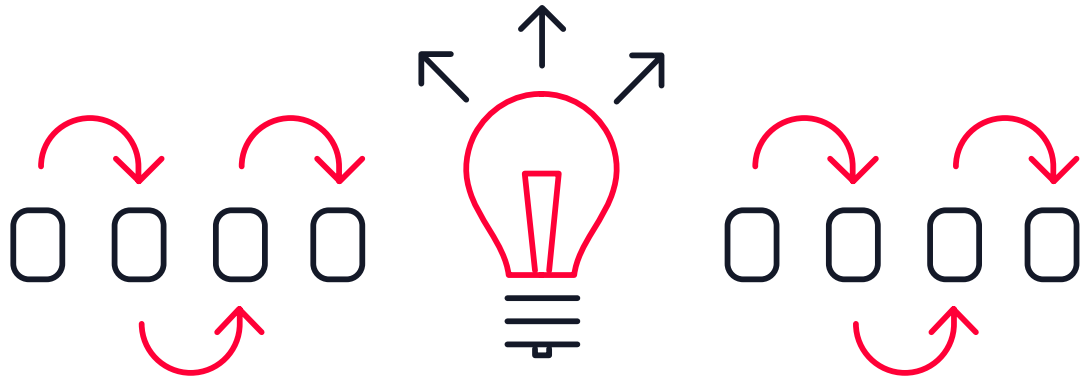
Transform your technology

In the virtual workplace, teams need to be able to adopt new norms and change the way they work to maintain (and improve) productivity, collaboration and innovation. This requires gathering information, devising solutions, adopting new approaches and refining outcomes—while minimizing downtime as much as possible. It becomes another story when employees are part on-site, part remote and bound by their technology's limitations.

On average, workers lose up to 32 days per year[2] toggling between the very apps meant to increase productivity. In addition, outdated systems and legacy technologies inevitably result in hardware failures, downtime, drained resources and unexpected expenses. While keeping old equipment may seem like a cost-saving measure, it requires more maintenance, labor and repairs, along with the costs of working with less-efficient technology.

> "
>
> What changes can you make right now that will have a lasting impact on the way your team works going forward? When people look for faster, simpler solutions to communicate clearly, the responsibility falls on IT to explore what's next—and often, that includes convincing company stakeholders to invest in the right tools and infrastructure.
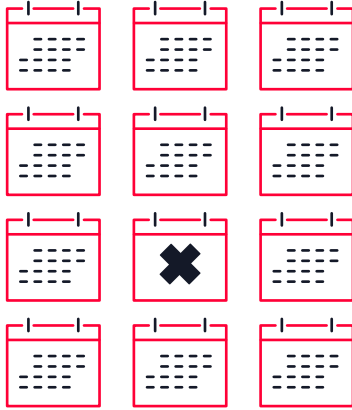
What changes can you make right now that will have a lasting impact on the way your team works going forward?

on average

workers lose up to

32 DAYS
per year

navigating between the very apps meant for productivity

Streamline decision making

Upgrading technology is essential for adapting to change. But doing so requires open communication, clear prioritization and buy-in from all key stakeholders.

CIOs and IT managers had essential roles in responding to the pandemic. That puts you in a great position to build support for upgrading the tools you need for the work-from-anywhere future. But more often than not, technology investments prioritize features requested by the business for the short term rather than critical infrastructure investments that allow companies to succeed in the future.

As beneficial as the latest tech trends may be, coworkers might not share your enthusiasm about the time it takes to adopt them. As an IT leader, it's your job to keep business running smoothly and to constantly innovate—and introduce the C-suite to new solutions they didn't know were possible. That's one tough task to incorporate into your daily to-do lists.
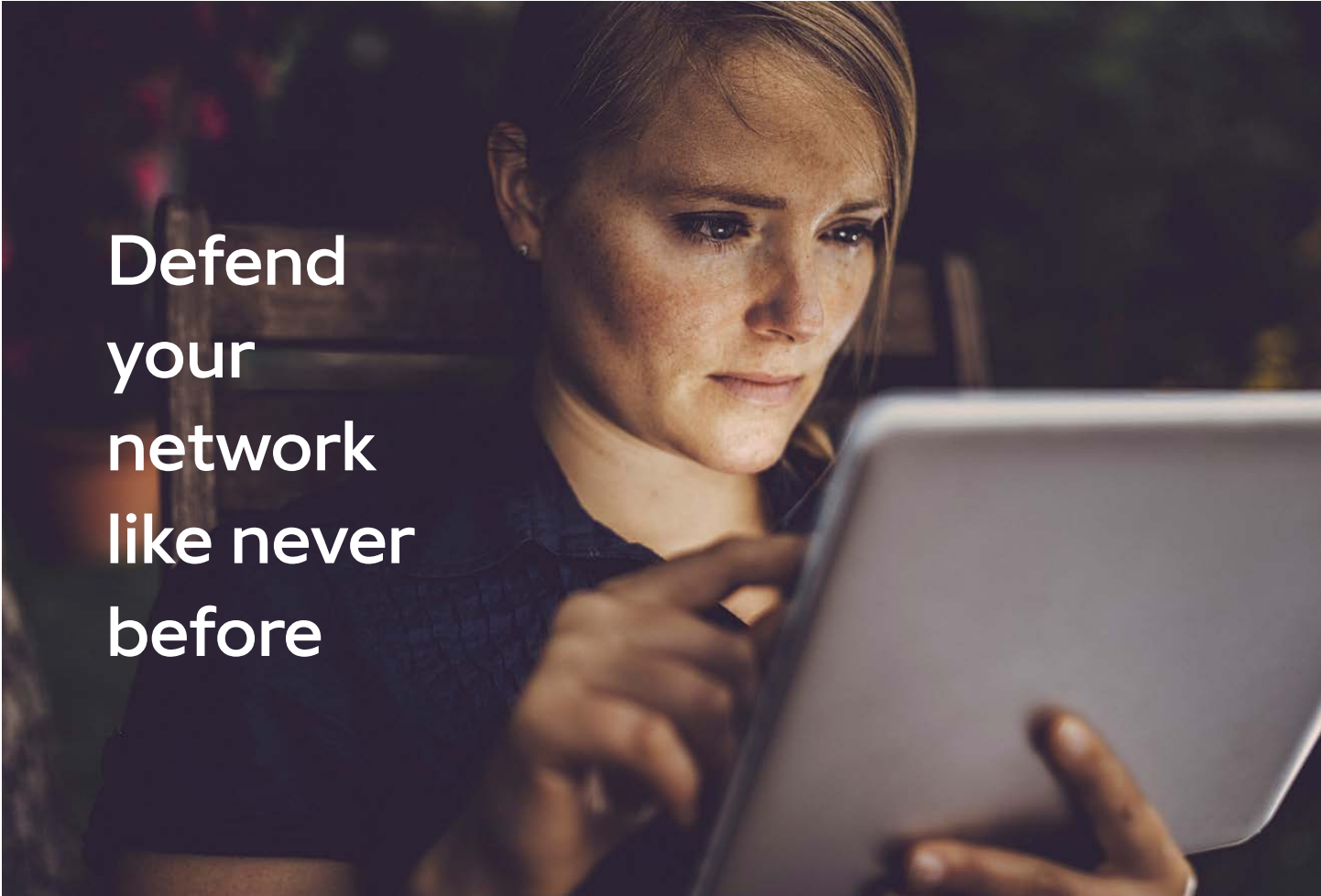
Improving technology at the highest level takes a collective-action approach—one that requires coordinated effort across the senior leadership team. When IT leaders communicate with their CEOs about the support they need for their teams, they can adopt an operating model that focuses on what people need to do their best work.

The process looks different for every business. But in every situation, to influence decisions, you need to build a case, highlight benefits, identify risks and create plans to mitigate those risks early on. Regardless of what you hope to push forward, you need to express this: Upgrading your technology allows your teams to communicate clearly, achieve a better workflow and ultimately be more productive. For stakeholders, that translates to saving time, hassle and cost.

In any decision-making process, it's expected that organizations will face silos. But by speaking with leaders and advocating for your people, you can create a foundation for more efficiency, communication and collaboration starting at the very top. When your executive team is on board with your vision, you can promote productivity for all.

Making security a priority

The state of cybersecurity

Security is always a top priority. And increased online activity means new opportunities for criminals. With teams relying on their own networks, working from home doesn't guarantee the same level of protection as an office environment. That's why device security is a top concern[3] for IT pros in today's remote and hybrid workplaces.

When teams are physically present in office buildings, they rely on firewalls to keep their data protected. But when workers are remote, they're relying on VPNs, which essentially lower the drawbridge to your internal network. So you need to shield external endpoints with proper security measures—and make sure you're set up with network monitoring that identifies if and when the system is under attack.

By extending your protections and monitoring from end to end, you can prevent threats from materializing and be more prepared for what's to come.

When it comes to the next opportunist, do you trust your employees to ignore dangerous hyperlinks and attachments? To only send sensitive data from company devices? Your biggest security threat isn't just your systems. It's also human error.

Defend your network like never before

The average cost of a data breach in 2020 was $3.86 million[4].

The average cost of a data breach in 2020 was $3.86 million[4]. But the cost of a breach is much more than monetary. It's lost data, strained resources, wasted time, compliance penalties and even risks to your company's reputation.

When your users are working from multiple locations, you need a fast and easy way to protect your data, secure reliable internet access and control the use of cloud-based apps. Here are a few hardware and security solutions that spotlight threats and mitigate issues if an attack does occur.

Managed Firewall   Prevention

Saves your network from all costs of a breach. With a dedicated security expert analyzing your network's vulnerabilities and defending your business from the inside out, you have the peace of mind you need to focus on your day-to-day priorities.

DNS-Layer Security   Prevention

Combines multiple security functions into one solution so you can extend protection from the corporate network to remote users and distributed locations anywhere. If employees try to visit websites marked as high-level risks, the connection to that address is halted immediately.

Business Continuity   Recovery

Ensures you have a disaster-recovery solution that kicks in instantly after an attack. It protects your organization from data loss and downtime, automates backup and recovery, and keeps your critical operations running.

Vigilance is key to security.

And in this case, vigilance isn't necessarily about bouncing back from setbacks, but being agile enough to predict potential issues and swiftly shift gears to stop them from materializing. And that requires visibility across your entire network, intelligence to uncover threats and protection to prevent phishing and malware attacks.

Over the next
12 months, industries
hit the hardest by the
pandemic are predicted
to see the greatest
losses to their
IT budgets[5].

MANUFACTURING

RETAIL

FINANCIAL SERVICES

HEALTHCARE

ENERGY

TRANSPORTATION

PROFESSIONAL SERVICES

HIGHER EDUCATION

PUBLIC SECTOR

Thrive under reduced budgets

Existing technical debt and old legacy technologies also contribute to your financial pressures. With reduced budgets and even more uncertainty ahead, what should IT leaders prioritize to adapt and move forward?

The good news is, digital transformation has the potential to dramatically reduce costs for industries across the board. In government agencies, for example, technology tools like the cloud, AI and data analytics can actually lower operating costs and improve efficiencies[6].

The Office of Inspector General within the US Department of Health and Human Services indicated that the department saves $5 for every $1 invested in using data to find fraud.

So it's not as simple as what IT leaders have to work with. It's how they're investing it for the future.

While hardware will still account for the largest portion of IT spending in 2021, money allocated to hardware budgets has started flowing into other areas.

IT spending in 2021

Hosted/Cloud Services

24%

Managed Services

16%

By prioritizing and spending intelligently, IT teams can avoid quick fixes and focus on long-term success.

Don't cut corners on connectivity

While half the battle of navigating through change is sorting through budgets and priorities, IT leaders can't afford to overlook the foundation their teams rely on most: connectivity.

After a year of abrupt change and operational setbacks, the need for seamless file sharing, chat, video and audio conferencing tools is more significant than ever. The more IT leaders adapt to managing remote and hybrid teams, the more we see increased investment in bandwidth expansion, network equipment and software that leverages cloud services.

Of course, networking doesn't look the same for every team or company.

Depending on your size, systems and needs, there are a variety of solutions to set you and your people up for success.

Internet access

Internet access over ethernet provides 99.99% availability, flexible speeds and greater security. So you can forget interruptions in service and prepare for increased bandwidth demands.
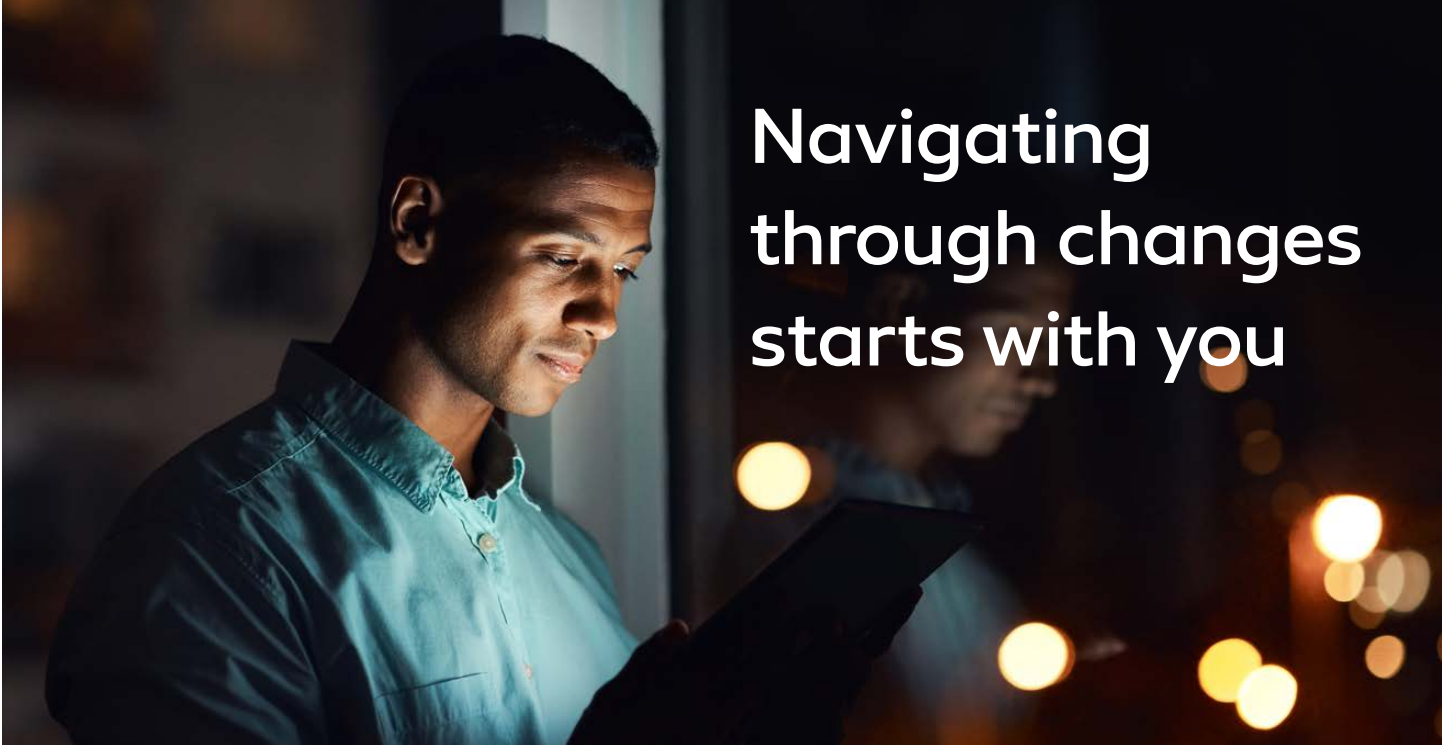
Multi-location connectivity

Multi-location connectivity lets your distributed team collaborate over a private network. You can share files, communicate instantly and conduct business securely from all locations.

Cloud connectivity

Cloud connectivity provides a reliable connection to all your data and apps from anywhere, while consolidating all platforms into a single dashboard.

Navigating through changes starts with you

Here's what we know:

Work-from-anywhere isn't going anywhere. Your security depends on your people as much as your systems. The best team is only as effective as its day-to-day tools. And when you find yourself at the center of change, your network is always worth the investment.

While we can't predict business disruptions, we can focus on what's in our control. By keeping teams connected, promoting productivity, making security a priority and protecting your ROI, you can plan, adapt and thrive through unexpected change. More important, you can address what's at the heart of it all: the need for humans to stay connected.

IT decision makers and business leaders everywhere are no longer waiting on the new normal.

They're creating it.

And key insights from the pandemic will help you prepare your teams for the future.
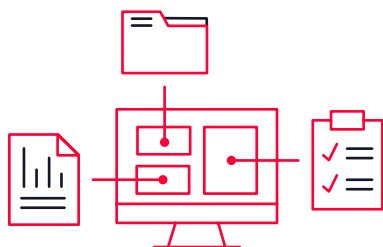
Frontier™

While we can't predict business disruptions, we can focus on what's in our control.

Are you ready to have the discussion about what's next for your teams, customers and business?

Sources

1. cnbc.com/2020/12/15/
   one-in-four-americans-will-be-working-remotely-in-2021-survey.html

2. forbes.com/sites/larissafaw/2018/03/05/
   workers-waste-32-days-a-year-due-to-workplace-efficiency-
   apps/?sh=37aed5f71d51

3. swzd.com/resources/state-of-it

4. ibm.com/security/data-breach

5. forbes.com/sites/louiscolumbus/2020/08/09/
   covid-19s-impact-on-the-future-of-it-budgets/?sh=53f6a198318b

6. deloitte.com/us/en/insights/economy/covid-19/state-budget-shortfalls.
   html

Interested in more content like this?

Head over to our **blog** for the latest insights on Unified Communications.

Contact Us

Ready to discuss what's next for your tech? Give us a call for an IT budget assessment.

888.530.2454

ENTERPRISE.FRONTIER.COM

Frontier™