# The Limits at the Edge: Six Remote Network Challenges

The events of early 2020 have seen organizations scrambling to quickly enable their workforces to be productive outside the corporate office. In these highly distributed environments, the boundaries of the network edge extend all the way to employees' homes. While rapid responses were necessary in the moment, and a good first step, these measures revealed major shortcomings in user experience and put a significant strain on IT.

## Read on for six network challenges experienced by remote workers and IT.

**USER PAIN POINT 1**

### "I can't get—or stay—connected."

When VPN technology was developed in the Nineties, it was designed to provide a subset of corporate apps to a subset of mobile, remote or branch users. In today's new normal, all the users are on the VPN, distributed across many devices and locations, accessing applications on-premises and across various SaaS and IaaS providers. This increased network traffic pushes the VPN past its capacity, as activity bumps up against capacity and licensing limits, and leads to congestion, random disconnects or rationing.

**Bottom Line:** No one can get their job done and productivity plummets.

**U.S. BUSINESS VPN USAGE SKYROCKETS**

VPN

Extra **3 hours** a day on business VPNs

Since March 11, global VPN usage has shown a massive spike. Workers in the U.S. are spending an extra 3 hours a day on business VPNs, the highest jump worldwide.

Source: IT Security Guru.

**USER PAIN POINT 2**

### "My apps don't perform like they should. I'm not getting anything done!"

Business-critical apps in a home office are up against compounding performance challenges:

- Last-mile connections to users' homes are notoriously oversubscribed and congested.
- VPNs are overloaded by more traffic than they were designed for.
- Some legacy apps were designed for clients in proximity to a server on the LAN. These apps may not perform well when remote.
- Without priority handling, business apps must compete with all the other neighborhood network traffic, including video conferencing and content streaming.
- Enterprise cloud and SaaS apps may take unnecessary trips back to the corporate network.

**Bottom Line:** When employees can't get the application performance they need to do their jobs, they not only get frustrated but the business suffers.

**FIERCE COMPETITION FOR BANDWIDTH**

**90+** Days

**10.3** Trillion MB of Data

Throughout the first 90+ days of the COVID response, Verizon networks carried 10.3+ trillion MB of data—leaving business-critical apps to contend with a massive flow.

Source: Verizon.

**USER PAIN POINT 3**

### "I've got too many passwords to remember...plus, I have to log in over and over."

Accessing apps from home often requires more frequent or more stringent authentication. Combine this with the new productivity apps, like video conferencing and chat, that organizations are rolling out to enable remote collaboration, and you've got a recipe for proliferating credentials—one more thing users have to juggle to get the job done.

**Bottom Line:** A frustrating, unproductive end-user experience. This frustration is passed on to IT via tickets, which can quickly overload help desk resources.

**HELP DESK OVERLOAD**

Help desk tickets: **1/3** are password reset requests

Password resets represent the highest proportion of help desk tickets, coming in at 1/3 of all requests.

Source: Security Boulevard.

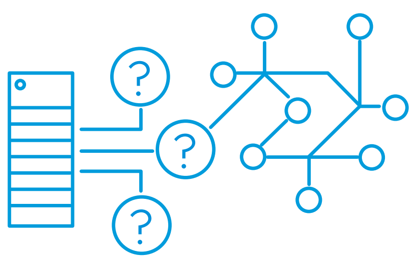
**IT PAIN POINT 1**

### "We don't know who's accessing what."

Traditional monitoring and security tools require devices to be on the corporate network.

**Bottom Line:** Lack of visibility into users and the corporate resources they access raises multiple security red flags.

**OFF-NETWORK DEVICES REMAIN A MYSTERY WITH TRADITIONAL TOOLS.**



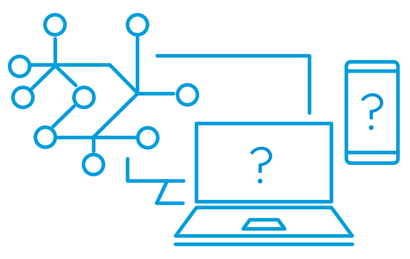
**IT PAIN POINT 2**

### "We can't be sure our devices—and data—are still secure."

As current events sharply accelerate the transition to remote working, employees are exchanging and sharing data from a variety of unmanaged personal devices to get their jobs done. But with endpoints no longer behind the corporate firewall and web filtering, IT has much less visibility into device compliance. It's difficult to push updates to corporate-managed devices when they're off-premises. On top of that, home office users introduce the risk of business apps and data being shared with other users on the network.

**Bottom Line:** Outdated devices accessing your network for the sake of employee productivity increase the attack surface—and your risk of a breach.

**DATA EXCHANGE VIA UNMANAGED DEVICES INCREASES EXPOSURE—AND RISK.**



**IT PAIN POINT 3**

### "Our OS and app updates take forever over the VPN."

When large patches and updates are pushed from the corporate network over the Internet via an overloaded VPN instead of over the LAN, they have to travel over a much slower connection to the users' devices at home. These bottlenecks mean that routine patches and app updates that take minutes to deliver on a local network can take significantly longer.

**Bottom Line:** The more IT time and resources are spent on routine maintenance, the less there is available for digital transformation and innovation.

**RESIDENTIAL NETWORK TRAFFIC BOTTLENECKS**

**32%** Increase in Comcast residential upstream traffic growth

**30-40%** Increase in VPN traffic

VPN

Comcast, operator of the largest residential Internet network in the U.S., saw a 32% increase in upstream traffic growth and 30–40% increase in VPN traffic from March to May 2020.

Source: Comcast.

# Take the next step toward optimizing your network edge.

VMware enables today's distributed workforce to do their best work, wherever they are.

Learn more about how VMware Future Ready™ Workforce solutions bring the corporate network to the remote employee in a secure and scalable way.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VMW-CL-REMOTEFIRST-USLET-20200702-WEB
7/20