

FAQs on Remote Worker Connectivity

Q. Why do we need more security now than we did before?

A. The need for better security is greater because the threat is greater. With so many stay-at-home orders in place, more people are working from home now — many of whom have never worked in such a way before. Cybercriminals have stepped up attacks in response to the phenomenon created by this virus, specifically targeting people whose job situations have changed because of COVID 19.

Q. Is improved security really worth the extra cost? How can I justify the expense?

A. If you think security is expensive, consider the cost of a data breach. According to a 2019 report, the average cost of a corporate data breach is \$3.9 million. In the healthcare industry it's even worse—\$6.4 million per data breach. The cost of improving corporate security with Digi remote-work solutions is only a tiny fraction of that.

*2019 Cost of a Data Breach Report, Ponemon Institute LLC, 2019, <https://www.ibm.com/security/data-breach>

Q. I don't understand why we should invest in routers or extenders for our remote workers. Isn't VPN good enough?

A. VPN alone doesn't give you all the centralized security, management, and control you require to match your current network. There are major security advantages with a Digi router or extender that are simply not available to PC-based VPN. With Digi enterprise cellular routers and extenders like the Digi EX15 and 6310-DX, corporate IT staff can extend and enforce critical security policies to the edge of the network. They can remotely configure devices with Digi Remote Manager and encrypted VPN tunnels between remote work environments and the corporate network. Additionally, PC-based VPN typically only enables remote access to centralized resources, while local Internet browsing still uses the local connection. This is a risky scenario for home-based employees.

Q. Digi is known for protecting IoT devices. Do you know how to protect laptops and tablets as well?

A. The same Digi devices protecting the integrity and security of the electrical grid and other critical infrastructure worldwide effectively protects computer assets in the home. In addition to personal work devices, Digi Remote Manager software provides IT organizations with centralized management of security configurations, no matter where end users are working — whether in field offices or at the kitchen table.

Q. Don't my employees have their own security protections in place at home?

A. Home Wi-Fi routers with consumer-grade features are just not secure enough to protect corporate assets. Without enterprise-caliber security, your company is open to the type of security disasters you've been working so hard to prevent: virus infections, malware, and ransomware. Plus, consumer-grade connections often lack content blocking / filtering capabilities. This is a critical consideration for the work-at-home environment, where family members and visitors might obtain access to an employee's computer, or where others may use unsecured computing hardware on the same network as the employee.

Q. What are some more of these "enterprise-level" features you're talking about with Digi solutions?

A. Here's a short list:

- Centralized management: With Digi Remote Manager, IT groups have the ability to centrally secure, manage, and monitor 1000s of devices. You can "open" or "close" the network down to the individual employee level.

- Content and site filtering and blocking: You can blacklist and whitelist content with source-based routing so only approved sites are accessible—an added benefit for homes with children.
- Enterprise DNS filtering services like Cisco Umbrella are also integrated directly into Digi devices.
- Enterprise-grade firewall
- Support for VPN tunnels with multiple VPN tunnel options: IPsec, GRE, and OpenVPN
- MAC address binding allows your company to control exactly which devices are connecting to the network.

Q. Some of my employees live on the outskirts of our metropolitan area. What can Digi do for them?

A. Connectivity can be an issue for people living in outer suburbs or rural areas or even in a large building. Power-over-Ethernet (POE) on Digi LTE extenders allows remote workers to isolate the best signal reception in their work environment and then run a single cable back to their home office.

Q. I work for a medium-sized business. Are cyber criminals even interested in my company?

A. Yes, they are. Small and medium-sized businesses or “SMBs” (under 1,000 employees and under \$1 billion in annual revenue) are prime targets for cyber criminals precisely because these companies often skimp on IT security. Attacks on SMBs are often proportionally more costly than attacks on large enterprises. In fact, cyberattacks can be fatal to a small or medium-sized business.*

**The Denver Post*, October 23, 2016, <https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/>

Q. We’re a school district with a lot of budget pressures. Why should we spend money on security?

A. Public institutions like school districts and municipalities are being increasingly victimized by cyber criminals, especially via ransomware. From a criminal’s point of view, these institutions represent an ideal target because they combine vulnerability with (supposedly) deep pockets. Budget constraints force public entities to make careful decisions around their technology expenditures. Fortunately, school districts of certain composition may be eligible for substantial discounts on communication services. They can also obtain grants to help pay for equipment and infrastructure. Meanwhile, millions of teachers and students are now in remote-study situations, and in dire need of connectivity and access to school resources. Cellular connectivity and enterprise security are a critical investment for school staff and students.

Q. What happens when the need for all this remote work is over? What happens after I’ve invested all this money in remote worker security?

A. COVID-19 won’t be the last global pandemic and we may find ourselves back in this situation again in the future. Once the current crisis is under control, the cost advantages of the work-from-home model will remain with us. Cost pressures of office rents and building maintenance will only continue their increase as time progresses. Meanwhile, cellular connectivity with enterprise security is one of the best long-term investments a company can make. Updating security protocols and firmware is easier and cheaper in the long run when completed centrally, leveraging Digi Remote Manager. Finally, the Digi CORE® Plug-In LTE Modem helps customers to future proof solutions by allowing upgrades to newer modules without replacing the primary cellular router or extender.