Home IoT Devices, Remote Work Drive New Revenue Streams for Broadband Operators

New cybersecurity solutions for home networks need to address consumer privacy and security concerns without compromising internet experience.

By Vikram Venkatasubramanian / *Nandi Security*

It's 2023 – the start of the post-pandemic era – and multiple macro and micro trends are happening simultaneously and forcing a sea change for people in cybersecurity. Let me list a few of the biggest factors driving the change:

- In the current tricky geopolitical environment, adversaries are in open warfare, and new threats are emerging.
- The pandemic created new social trends, such as people and jobs moving out of big cities and emerging models of remote and hybrid work.
- There has been an explosion in the number of home IoT devices, including wearables and embedded devices such as connected pacemakers.
- The emergence and commoditization of artificial intelligence is the technological equivalent of an F-5 tornado.
- A substantial level of public awareness around privacy issues exists because of multiple high-profile cases against big tech companies.

Society will experience strong positives and negatives because of each of these, but let me focus on the impacts for cybersecurity – in terms of both threats and tremendous opportunities.

THE REMOTE WORK FACTOR

Remote and hybrid work is fundamentally powered by broadband and tools that leverage the presence of broadband in homes. Knowledge workers realize the benefits of lower costs in smaller towns and cities around the U.S. Many employers are eager to offer flexibility as a work-life balance benefit because knowledge workers are increasingly in demand, especially in technology, AI, robotics and drug development. Though the migration out of big cities is slowing, hybrid work is here to stay.

Broadband providers are no strangers to constant, daily, high-volume attacks from Russia and China on their subscribers' homes. Thousands of homes have been hacked, and devices such as cameras, routers and other home IoT devices have been converted into botnets. Broadband providers have battled these issues for some time already.

As the attack surface of connected homes continues to increase in terms of apps, devices and internet-connected services that people use every day, enterprises have no option but to view connected homes as nebulous extensions of their corporate networks. This is already an issue for security leaders at enterprises. The HP Wolf Security report released in March 2023 identified that 36 percent of enterprise security leaders are concerned about employees' unsecured home networks – and privacy threats are the most significant security concern.

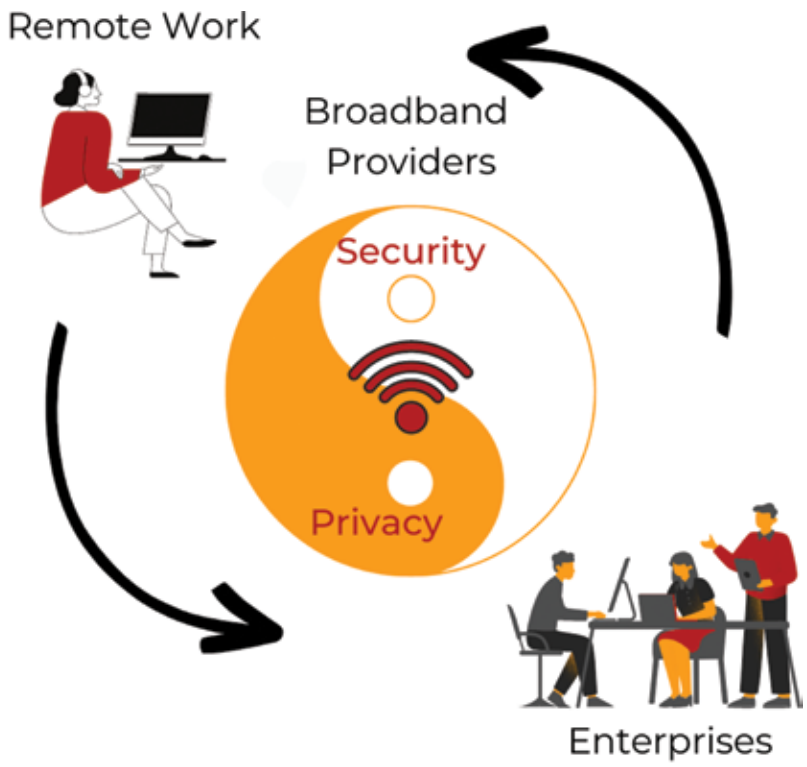
REAL CYBERSECURITY THREATS

The bad guys didn't wait for research reports and data to emerge on market trends. They acted and continue to work in very significant ways – the impact affects everyone's daily lives. In December 2022, the cybersecurity company LastPass, which makes a commercial password manager, was breached. The vector of attack? Well, you guessed it – a home IoT device, a music system in the home of an employee working remotely.

Once inside the home network, it accessed an employee's corporate laptop – moving laterally in a home network with no segmentation policies or internal firewalls is very easy – and entered the corporate network! And just like that, the worlds of enterprise cybersecurity, consumer cybersecurity and broadband collided.

But wait, what was that sound the collision made? It sounded more like a knock of opportunity than a doomsday bell. Let me rephrase what this article identifies so far:

- Consumers want lifestyles with strong work-life balance.
- Consumers demand privacy and security.



There is a massive opportunity in being a trusted security vendor to home users over the next decade.

- The enterprises that hire people are eager to offer them the perks of remote work, privacy and security.
- The enterprises that hire people see the same privacy and security as risks and are looking for solutions.
- The risks are *real* and already being exploited by threat actors.
- The glue that connects them all today is broadband service providers.

OPPORTUNITY BECKONS

The stage is set, and the situation is ripe for a win-win opportunity for broadband providers. The average U.S. home today has 20 connected devices, and the U.S. smart-home market is projected to grow 10.2 percent through 2027. The average home today has more computing, storage and networking power than an average enterprise did even a decade ago, but the cyber posture of homes stays constant.

The Broadband Equity, Access, and Deployment (BEAD) Program provides funding for rural broadband providers and increased the incentive to connect unserved and underserved communities with high-speed broadband. But let's be realistic: there isn't clarity yet on the size of the allocation a specific broadband service provider will get. Further, once connectivity is enabled, broadband service providers are still left with the question of where revenue growth will come from once all the fiber has been installed with BEAD Program money.

Value-added services and differentiation will be critical to long-term strategic plans. Every home that comes online, irrespective of geographic location, is moved to the frontline of the U.S.'s cyber borders with connectivity.

The ARPU growth opportunity and the differentiation in cybersecurity are independent of the BEAD Program opportunity and can be acted on now. This is not a new concept in the industry. Several rural broadband companies have seen the same trend in the physical security market and already offer solutions for physical home security. Offering cybersecurity to the home is a natural extension of that model into innovative home cybersecurity and privacy.

Home internet consumers are at the center of this issue because the solutions envisioned need to address their privacy and security concerns and not compromise their internet experience. Cybersecurity needs to be comprehensive across all devices, apps and services used in homes and adaptable to changes; e.g., consumers may change apps, employers, devices, home routers and even homes.

There is a massive opportunity in being a trusted security vendor to home users over the next decade, mainly because this opportunity for broadband service providers is not limited to *only* the areas they cover with fiber nor to *only* subscribers of their broadband service. The length of fiber coverage does not bind the ARPU growth opportunity for the first time and allows broadband providers to compete with lower-cost services in their regions.

Nandi Security saw this trend coming several years back and invested in products and business models to enable broadband providers to provide cybersecurity and privacy protection to smart/connected homes with no capex to reduce risk and ensured that budget constraints are not a barrier. Nandi continues to invest in expanding the cybersecurity capabilities of products so providers can add additional layers of security and services to homes and small businesses inside and outside their current coverage areas.

Vikram Venkatasubramanian is the founder and CEO of Nandi Security, an online privacy and security company focused on protecting intelligent homes and home IoT devices from privacy and cyber threats.