

Jim Rapoza

VP & Principal Analyst, IT



With the move to remote and hybrid workforces, businesses are seeing increasing challenges from employee devices that are accessing sensitive company networks. And one of the biggest pain points is the home network and router that is being used for work. As IT organizations look to overcome the security, management, and resource challenges that come with these “BYOD” routers, leading businesses are identifying a simple way to remove this challenge.

The Challenge of BYOD and Network Connectivity

Throughout the history of computing, there has been a tug-of-war between business and personal devices. For much of the first era of the PC and early smartphones, any device that touched company assets was provided to employees by the IT department.

Then, with the rise of powerful smartphones, many businesses tried to switch to a bring-your-own-device, or “BYOD” model, where employees could use their own device and IT would implement some controls over it. But this turned out to be a lose-lose idea, as employees pushed back on any control over devices with their personal data on them and IT struggled to secure and manage these devices.

Now, with the move to workforces that are heavily, or even 100% work from home, we are seeing a new twist in the troubles that BYOD can bring, namely the home networks that are now being used to access critical and sensitive company data and applications. And the problems for both employees and IT departments can be even bigger in this new BYOD struggle.

From an IT perspective, home networks often run on out-of-date routers with known issues, are poorly secured against rogue access, have a wide variety of potentially compromised devices on them, and are used by an employee’s family and friends. And from an employee perspective, giving IT control over a network that their family uses is a non-starter.

Aberdeen research shows that 56% of businesses have employees that are in hybrid or remote work environments.

These problems can only exacerbate the challenges that IT faces on a regular basis. According to recent Aberdeen research, the top IT challenges for businesses today include preventing security breaches, controlling budgets, and managing remote/hybrid workers. Dealing with BYOD home networks and routers only adds to these challenges.

Top IT Challenges

1. Risk of security breach – **49%**
2. Budget issues – **29%**
3. Cloud-centric infrastructure – **27%**
4. Move to remote/hybrid work models – **22%**

Eliminate the Risk of Bring Your Own Router with Standardized Connectivity

So, what is the best solution to overcoming the challenges of home networks being used to access company resources? According to Aberdeen research, the best outcomes and highest levels of benefits come from controlling all aspects of network access. In fact, businesses that do this are 4x more likely to lower security risks.

Just as the best way to remove the issues of *Bring Your Own Laptop* or *Smartphone* is to provide a managed, secured, and optimized company-issued device, leading organizations are finding that they can do the same thing when it comes to network connectivity. By taking advantage of advances in wireless networks (such as 5G), IT departments can deliver a powerful, managed, and secured company-provided router that is designed to be solely used for business purposes, leaving the employee's network for the family.

Businesses with increased control over network access are 4x more likely to see reduced security issues and risks.

With increased control over network access, businesses also gain increased management capabilities and visibility. In fact, Aberdeen research shows that businesses with strong control over network access are also 75% more likely to have a unified online management portal that provides IT with visibility and control over remote workers routers and business network connectivity.

Along with the benefits to improved security and management, IT departments that provide dedicated network connectivity through managed wireless routers are also able to overcome many of the other challenges that we identified for IT today. By reducing management and IT staff demands, along with potential varying costs to reimburse employees for home connectivity, these businesses can reduce costs both to the bottom line and to IT resources.

And gaining these benefits is a simple task for IT departments and businesses. By choosing high performing and reliable wireless business internet providers and easy to deploy routers, these organizations can remove the potential pain points of *Bring Your Own Router* and ensure reliable, cost effective and secure network access for all workers.

About Aberdeen Strategy & Research

Aberdeen Strategy & Research, a division of Spiceworks Ziff Davis, with over three decades of experience in independent, credible market research, helps **illuminate** market realities and inform business strategies. Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations, to **inspire** critical thinking and **ignite** data-driven business actions.

This document is the result of primary research performed by Aberdeen and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen.

18572