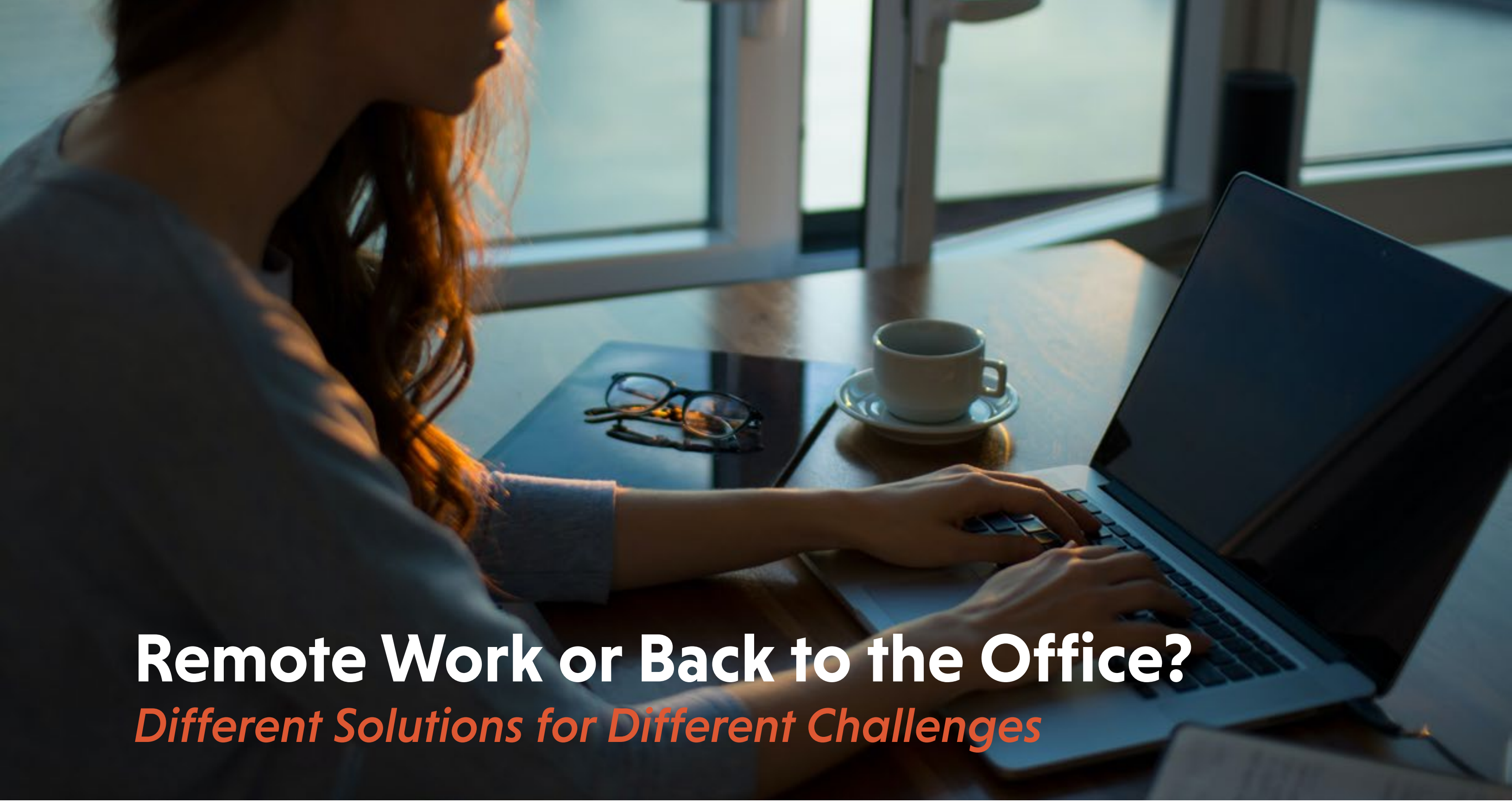

Remote Work or Back to the Office?

Different Solutions for Different Challenges

CHALLENGE

By now, it's very clear that it will take a long time – if ever – for the workplace to function as it did before COVID-19 hit. That's certainly true for the federal government, which has spent the past few months trying to determine the best options for its employees and the government as a whole.

For most organizations, there are three basic options, each with its own set of challenges:

Remote working indefinitely

While this option protects employees' health, it can impact productivity and security. On the productivity front, connectivity becomes key. Without reliable connectivity, employees can't effectively do their jobs. And because employees are working from home, often on their own devices, it can be much more difficult to ensure that agency data and other resources are secure. Managing a large work-from-home group also can complicate user and network management. It can be very difficult to manage both wired and wireless networks in addition to all of the users and devices connected to those networks.

Returning to work

Even if employees return to the office, they won't be returning to normal. Their workspaces will be further away from each other, making it harder to collaborate. Some employees will have lingering concerns about health and safety. Agencies have to find ways to prevent potentially compromised employees and visitors from entering the premises. These constraints will require some form of contact and location tracing, visitor management and health monitoring. A more modular environment also may require some rethinking of traditional network and security infrastructure.

There will be a lot of circumstances agencies need to understand, such as how employees move and gather in a facility, how to notify others when someone violates social distancing requirements, and how a person can notify others when they become infected.

A hybrid model

Many agencies and private organizations are considering a hybrid model, where employees work a few days at home and a few days in the office each week. While this is a worthwhile option, it creates challenges in both the remote work scenario and the new office environment.

SOLUTION

Each scenario comes with key connectivity requirements.

If keeping employees at home, agencies must be sure that employees can work securely and productively. That requires secure Wi-Fi access. One way to provide this capability is by having remote access points drop-shipped to each employee's home. Plugging in. these self-configuring, plug-and-play devices provides a secure tunnel back to the home office. Additionally, everything will look the same to employees as it did in the office.

"The network will look the same, their laptops will respond the same way, and workers can even plug their VoIP phone into one of the ports to get the same experience as they did in the office," explained Paul Kaspian, worldwide product marketing manager for enterprise security at Aruba, an HPE company.

Because users and their devices are geographically dispersed, it's also important to find a way to ensure full visibility, monitoring and security. Kaspian recommends adding an AI-powered platform that can not only see all devices on the network but also troubleshoot issues; monitor and manage wired, wireless and WAN devices; and quickly deploy network services as needed. It's also important to include technology that uses role-based policies to strengthen security.

Agencies planning on bringing employees back to the office have different requirements. One of the most important is the ability to perform contact and location tracing. One of the most effective ways to do that is by collecting data from wireless access points via either Wi-Fi or Bluetooth Low Energy (BLE) to understand where they are.

"If you triangulate users using Wi-Fi triangulation, you can figure out that Paul is within 10 meters of Brian," Kaspian said. "If Paul tests positive, you can plug him into the tool, and it will tell you that he spent three hours in close proximity to Brian. That gives you the information to make good decisions."

Bluetooth technology can enable agencies to take things up a few levels. Attaching Bluetooth tags to employee ID or Common Access Cards, for example, will not only tell you employees' locations but also where people are congregating. Using this type of "heat mapping,"a department head can visually see whether too many people are currently gathering in the fourth-floor break room, allowing the department head to immediately disperse the crowd and notify the facilities staff to ramp up cleaning protocols in that area. Aruba's Bluetooth-based solution, comprised of Aruba Meridian software, BLE-enabled Aruba tags, and BLE-enabled wireless access points, is one solution.

With the right technology, there are many other ways to make work facilities safer. One idea is contactless visitor management, which allows visitors to pre-register and automatically generate visitor Wi-Fi credentials. Another is video and AI-based health monitoring, which uses contactless thermographic solutions to measure the forehead temperature of groups of people simultaneously. Additional use cases can be enabled utilizing Aruba's extensive partner ecosystem of solutions.

STATS

80%

Up to 80% of the Defense Department (DoD) workforce is authorized to return to the office.

#1

Employees said sub-par connectivity is their top challenge while working from home.

70%

of federal employees who have been teleworking during the pandemic say they are more productive.

47%

of those currently working remotely say that the ideal situation would be working from home 1–4 days per week, with the rest of the time spent in the office.

TIPS FOR SUCCESS

Data is key.

"There are so many ways you can use data to improve both remote work and the new office reality," Kaspian said. For example, a network management platform like Aruba AirWave or Aruba Central can collect data that allows agencies to steer people in the right direction within a building, helping preserve social distancing. Health and safety teams can also use that data to pinpoint higher use areas that they need to disinfect more frequently.

It's not as complicated or expensive as you might think.

Most agencies, in fact, already have the infrastructure they need, like remote access points, wireless controllers and network management systems. If you do need to spend some money, the required technology is very affordable. Many agencies have been using the Coronavirus Aid, Relief and Economic Security (CARES) Act funding to fill in the gaps.

Choose a vendor with deep integrations for more options.

Aruba, together with its partners, provides innovative tools to monitor social distancing and group sizes, generate contact tracing trees, touchless visitor management, and video and AI-based health monitoring.

ABOUT AFFIGENT

Affigent is a turnkey IT solutions provider dedicated to helping agencies modernize their IT infrastructure while simultaneously improving security and delivering mission-serving solutions faster and at a lower cost. As a subsidiary of Akima, Affigent is owned by an Alaska Native Corporation, and offers customers the flexibility and agility of working with a small business, while also receiving support from a global enterprise with decades of experience working with the federal government.

To learn more about how Affigent and Aruba can provide cutting-edge solutions to address your agency's challenges, please visit www.affigent.com.

Affigent
AN AKIMA COMPANY

aruba
NETWORKS

govloop