



Using Network and WiFi Analytics to Help with Workplace Safety

Part of the Driving Digital Agility content series: Insights and strategies to pivot to digital business, navigate new work environments, and manage changing customer expectations.

Managing the return to work is going to be a complex, cross-functional, risk and operations management exercise. Companies and organizations of all sizes and industries are planning for the unprecedented challenges of returning to work in a way that ensures a productive and safe work environment for their employees and customers. New social distancing at work guidelines are being planned and will likely be in place for the foreseeable future. Employee health and safety are the primary concerns, but employee health issues can significantly impact the health of the business as well.

Business leaders need to consider monitoring processes and technologies that balance maintaining safety with respect for the privacy and work habits of their employees. As such, organizations of all sizes can leverage their computer and communication networks to enable such automated monitoring processes. In many cases, these network monitoring tools may already be in place and only require IT teams to configure settings and generate the reporting. Because of this, IT has a new leadership opportunity to work across their business to determine the best technology to support the new safety measures. For further safety management, organizations may decide to deploy additional hardware or software solutions.

Working Cross-Functionally and Using Technology for Scale

IT teams and technology solutions have a special, and perhaps unexpected, role to play in providing answers to the many new challenges businesses are facing when considering transitioning to working on premise. IT leaders have the opportunity to work cross-functionally as they've never done before to help address business continuity and workplace safety challenges. Employee safety to limit infection risk will be a common goal for HR, facilities, operations, risk management, IT, and executive teams. And in order to do this at scale, companies of all sizes need to leverage technology that enables, and then monitors, the new processes they are putting into place.

To be performed at scale, the following processes will need to be enabled through technology:

- **On-premise employee scheduling:** Mix of office and working from home (WFH) to limit risk of exposure
- **Controlled access:** To premises as well as to equipment, systems, and applications
- **Active monitoring:** Know where employees are throughout each day
- **Ability to contact trace:** If and when an employee tests positive to isolate further exposure

How to Use Network Monitoring for Employee and Workplace Safety

Unlike ever before, employee presence on premises - whether in offices, manufacturing facilities, retail stores, hospitals, or education institutions - will need to be tracked to limit the number of people in a space. Additionally, companies will need to preserve these records for potential contact tracing if an employee is identified as virus-positive. For many companies, limiting the number of people on site may mean adopting rotating shifts or extended hours in order to enable the required physical distancing. Network monitoring can help automate these new processes.

Many companies will likely manage this through devices that monitor access to premises such as keycards and time cards. However, if these systems aren't already in place, you can capture this data with actual on-premise device monitoring on the company network.

IT teams can also use network monitoring to determine where, when, and who is logging in and logging out. Device tracking, e.g. of desktops, laptops, tablets, phones, and system terminals, as well as keycards systems that are all connected to the company network, through network log-in monitoring can provide the additional reporting to help HR and business leaders ensure safety for everyone. Knowing who was at the office and at what times can ensure compliance with policies and allow for re-tracing if needed.

WiFi Solutions Can Help in Unexpected Ways

To enable contact tracing, IT can further configure networks to segregate certain areas of the premises, e.g. WiFi area 1, WiFi area 2, etc, which provides visibility into movement within specific areas on premises. IT reports can then help trace contacts and isolate who may have been exposed in certain areas. Network monitoring technologies and [software-defined wide area networks \(SD-WAN\)](#) can be configured to enable such networks, visibility, and reporting.

Guest WiFi log-in is another way to monitor non-employee presence. As companies get back to a more regular rhythm of business, non-employees like vendors, contractors, clients, and cleaning crews will also be entering the building. These WiFi areas can also monitor their location through the guest WiFi device recognition, including cell phones.

Access and Presence Monitoring through Other Technology Solutions

Not leveraging technology could result in cumbersome and ineffective manual processes. There may be unique problems for companies with larger workforces or multiple interpersonal touchpoints, such as in manufacturing, warehouses, retail, hospitals, educational institutions, or personal services. Such organizations may enable other simple and inexpensive technology solutions that are then connected to company networks for presence and access monitoring and workplace safety purposes. Some video systems can provide daily analytics reports on foot traffic, if necessary. Phone system reports may be another way to retrace and monitor office presence for employees working from the office.

Conclusion

For most businesses, going back to the workplace will be a slow and thoughtful process. The considerations are unprecedented and no one knows quite what to expect. It will be inefficient, if not impossible, to manage such processes manually. These unique challenges require innovative thinking and necessitate technological support that is scalable and automated. Businesses will need to plan and operate cross-functionally like they've never done before.

In many cases, depending on the policies business leaders are adopting for their employees, this means using technology systems that are already in place, in new and different ways. Business, HR and IT leaders will need to

leverage existing and new company policies to balance efficiencies, new processes, and employee privacy for the common good.

To get more information on how your networks and network monitoring tools can enable your organization's employee safety talk to your IT team or your [Comcast Business Customer Service or Sales Rep](#).

For more information on how businesses can use technology to navigate new work environments and expectations, explore the rest of our "Driving Digital Agility" blog series.

[READ MORE](#)