



Software Testing in a Post Pandemic World

The global COVID-19 pandemic has changed the landscape of work. With more employees working from home, companies had to quickly transform their digital infrastructure to accommodate the trend and support remote work. Even after the pandemic is over, the changes will be long-lasting. Moving forward, software companies need to have the digital infrastructure as well as the policies and procedures in place to enable their workforce to work efficiently and safely no matter where in the world their employees are.

TABLE OF CONTENTS

- 3 Software Testing in a Post Pandemic World
- 3 IT Leads the Way in Remote Work
- 5 Remote Testing Makes Sense
- 6 Remote Testing Requires Expertise
- 7 Putting It All Together

SOFTWARE TESTING IN A POST PANDEMIC WORLD

In the history of commerce, remote work is nothing new. Traveling salesmen have been part of the commercial landscape well before automobiles and telephones were commonplace technologies. Farmers used "[commission men](#)" to sell their livestock at the stockyards of America. A commission man was a remote agent who represented a farmer who was hundreds of miles away.

The same was true for insurance agents which have been a vital part of companies such as the Travellers and Prudential insurance companies, both of which go back centuries. The insurance agent traveled to the home of the policyholder to pick up the monthly premium payment. Many worked from home.

Yet, while remote work was possible for some, most employees were required to work at the place of production. Assembly line workers went to the factory. Lawyers went to the law office. Doctors went to the hospital. The notion of someone being able to do production work for a company, in real-time yet reside half a continent away from that company's plant or office was the stuff of fantasy. Then, computer technology changed it all.

If you were to go to a travel agent's office in 1975 to book a flight from Los Angeles to New York City, that agent would use the same [SABRE](#) reservation system to make the reservation that an employee at an airline used. All were connected to the same computer system no matter their physical location. The same was true for banking. A teller in an uptown branch of a bank used the same computer system as a loan officer at the downtown branch. The workforce was distributed and remote, but for security reasons, they tended to work in a location owned by the company.

IT LEADS THE WAY IN REMOTE WORK

Today, given the prevalence of ubiquitous, secure networking due to the emergence of the Internet along with the growth of mobile technologies such as lightweight laptops, cellphones, wireless connections, and handheld tablets, most employees can work from anywhere as long as there is an adequate corporate infrastructure to support sophisticated remote work. Information technology (IT) has long had a history of supporting a distributed workforce. Also, many technology companies have embraced the philosophy of the Results-Only Work Environments (ROWE) which stipulates that a company ought not to be concerned about where employees are or what

they are doing as workers are meeting the expectations of their job. As a result, working from home, or the gym for that matter has gained wider acceptance.

Still, for employees outside of IT, remote work was more the exception than the rule. But, now that the COVID-19 pandemic is upon us, anybody who can work remotely, is working remotely. As shown in the diagram below in Figure 1, according to the websites, [Statista](#) and [Clutch.co](#), since the outbreak of COVID-19, nearly half the US workforce is working remotely.

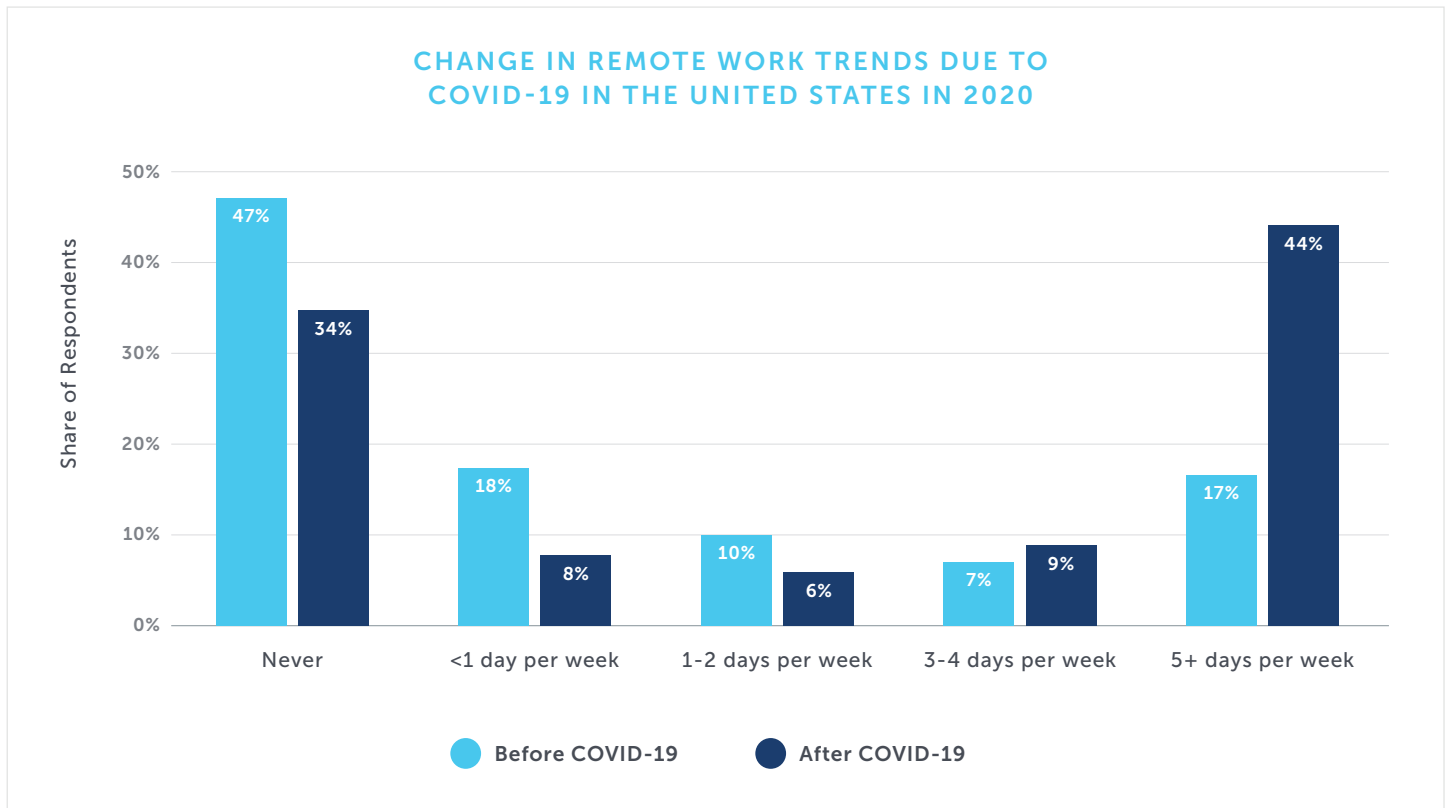


Figure 1: As reported by Statista, working remotely is gaining wider acceptance.

As remote work becomes a commonplace norm, and COVID-19 still affects us on a global scale, more companies will adopt the practice. The ramifications of this trend are far-reaching.

First, the growth of remote work is forcing companies to re-evaluate long-held core beliefs about the cost of doing business. The conventional wisdom of continuing to pay the expense of massive office complexes is coming into question. Even something as traditional as the interview process is subject to revaluation. In the past, the, "1 phone screen, 3 in-office interview" process was the norm, but today the trend for many companies is to do everything via video conference. The cost and time savings are apparent.

In addition to embracing remote workers from a policy point of view, there are also tactical factors to consider. This is especially evident in terms of how technology companies utilize their digital infrastructure to get work done, particularly around testing.

REMOTE TESTING MAKES SENSE

Historically, software testing has been a challenge from an environmental perspective. Before the rise of the Internet, companies had to go through a great deal of effort to set up a product or system for testing. The test machines need to be standardized as did the operating systems. Then the application(s) needed to be loaded in followed by any testing utilities that needed to be present. Finally, the whole test environment needed to be connected to test data, and testers, as well as testing software, needed to be given access to the test environment. This process could take days, particularly when working with very big data sets. If something went awry, the whole process needed to be done over. It was an arduous undertaking. Remember, back in those days, a company owned its testing environment and that environment was in-house. Testers and test environments were typically in the same building, if not the same floor of the given building.

The rise of the Internet and machine virtualization made setting up and provisioning the test environment easier. The Internet and machine virtualization made it so dynamic environments could be run in remote data centers and reprovisioned on demand. Test and test designers working in New York City could execute their work on systems that were housed in Chicago. This sort of separation became commonplace.

Eventually, as data centers and testing demands became generic, testing services such as Sauce Labs emerged. These testing services absorbed the mundane tasks for test setup, hardware and software provisioning, and even execution. The cost benefits were hard to ignore.

Yet, up until recently, most testers and test designers still congregated in a common physical location. Then, as mentioned above, COVID-19 struck. The response to the crisis was increased social distancing that has resulted in staff working from home. While it was both nice and usual to have test personnel working at the same physical location, current events have shown that it's no longer a necessity. Thus, remote work is fast becoming a norm that will continue to trend upward well after the threat of COVID-19 subsides. Yet, such transformation will have challenges, particularly for technology companies that intend to have a remote workforce using cloud-based testing platforms such as Sauce Labs. The most prominent of these challenges is security.

REMOTE TESTING REQUIRES EXPERTISE

Anybody who has worked in a cloud environment for any amount of time knows the enormous amount of detail that goes into creating a secure computing environment. It's not just a matter of creating a password to go with a username and then granting access to a given resource based on that credential pair.

One application can utilize a myriad of server-side constituent services. Each of those services will be used in a particular way and, thus, will have a security configuration that is special. Working in this environment requires a very particular type of expertise. Some businesses have it, many don't. This is why there are so many companies that are specialized in managing cloud services. It's hard work. And, in terms of cloud-based testing services, the work is even harder.

There can be any number of real devices, emulators and simulators provisioned to the given testing platform. And, the given platform will need to work with a variety of other services and data sources. Managing all this can be mind-boggling. Now, add in the extra burden of having test personnel needing to access the test platform from anywhere in the world using any one of a variety of devices; anything from a laptop computer to a smartphone to an Internet appliance. The security risks have just risen dramatically. Whereas a company could have a good deal of control when all the employees are in the same physical location doing testing, remote work pushes the envelope beyond the capabilities of most companies.

Fortunately, top-tier companies such as Sauce Labs are SOC 2 (Service Organization Control) certified, providing customers with a modicum of assurance as to how they handle security controls. As organizations increasingly rely on cloud- and SaaS-based technologies to implement their agile and DevOps initiatives, SOC 2 certification provides a crucial layer of independent security controls validation, one that is especially critical for organizations in highly regulated industries dealing with highly sensitive customer data.

PUTTING IT ALL TOGETHER

The [first case of COVID-19 was reported](#) on November 17, 2019. According to [Bloomberg News](#), as of January 28, 2021, there have been over 2 million deaths due to the virus. Vaccination programs are underway. Yet, when the pandemic will come to a controllable end is unknown.

In the meantime, cautionary measures will still be in force. People who can work at home will continue to work at home. Cutting edge tech companies plan to support remote work even after the pandemic passes. Twitter plans to allow its employees to [work at home forever](#). According to a [new survey from Conference Board](#), 77% of responders expect an increase in the number of employees working from home at least 3 days a week. COVID-19 has accelerated a trend that was slow before the onset. Today, the number of employees working from home has skyrocketed.

As more employees work from home, companies will need to transform their digital infrastructure to accommodate the trend. Today the modern tech worker uses a larger number of cloud-based services that proliferate over the internet. Just getting access to a company's internal network is no longer sufficient. A more robust approach will be needed.

The benefit of using a cloud-based testing platform is that companies can support a widely distributed, remote workforce at a fraction of the cost of one that's homegrown. As mentioned above, the benefit is hard to ignore, particularly as remote work becomes more the norm rather than the exception in the post-COVID-19 world.

For those companies that earn their keep from software, testing processes and practices will need to adjust to the age of the remote worker. Some companies will revert to old ways of doing business once COVID-19 passes. Most won't. In the years to come, forward-thinking software manufacturers will have the digital infrastructure as well as the policies and procedures in place to enable their workforce to work efficiently and safely no matter where in the world their employees are. It's not a nice to have. In the post-COVID-19 world, it's essential.



ABOUT SAUCE LABS

Sauce Labs is the leading provider of continuous testing solutions that deliver digital confidence. The Sauce Labs Continuous Testing Cloud delivers a 360-degree view of a customer's application experience, ensuring that web and mobile applications look, function, and perform exactly as they should on every browser, OS, and device, every single time. Sauce Labs is a privately held company funded by TPG, Salesforce Ventures, IVP, Adams Street Partners, and Riverwood Capital. For more information, please visit saucelabs.com.



saucelabs.com/signup/trial

FREE TRIAL