

Jun 16, 2020, 09:00am  
EDT

# The Cloud Is The Backbone Of Remote Work



**Chris DeRamus** Forbes Councils Member  
Forbes Technology Council COUNCIL POST | Paid Program  
Innovation



*VP of Technology, Cloud Security Practice for DivvyCloud by Rapid7*



GETTY

Prior to the pandemic, many organizations required their employees to come into the workplace, whether it was for leadership, community, security or other reasons. COVID-19 caused organizations everywhere to quickly shift to remote work, regardless of their opinion before.

The shift was a matter of safety and public health, yet many companies that used to be against working from home realized that employees can be just as productive working remotely — even under the undesirable condition of having to follow stay-at-home orders and social distance. Working from home can even boost productivity; remote employees do not need to commute to and from work, so they can work from the comfort of anywhere in their dwelling, they can sleep in a little more than before, and more.

Boosted employee productivity and satisfaction are more than enough to have some companies continue to allow working from home once stay-at-home orders begin to ease up. To do this, enterprises will increasingly lean on cloud applications and services to allow remote workers to continue to be productive and access the corporate resources they need to do their jobs.

However, remote styles of work present new threats, and enterprises will quickly realize that security will move far past the traditional firewall perimeter. Instead, the identity of users in the cloud will need to be prioritized to ensure that the right employees have adequate levels of access to the resources they need, all while thwarting unauthorized access attempts and malicious insider threats.

## Business Benefits Of Remote Work

When implemented properly, remote work can [improve employee productivity](#) and [job satisfaction](#). Even prior to the pandemic, multiple businesses were already embracing or beginning to adopt flexible remote work policies to reap these benefits. In fact, the remote workforce [increased by 173%](#) since 2005. Additionally, employers can work with a larger pool of candidates with remote work policies since geographical location is not a barrier, and — a huge benefit for tech companies in particular — [over half of developers](#) say that being able to work remotely is a priority when looking for a job.

Some companies may even get rid of their offices completely or downsize to save on rent and associated costs. Companies that have had their business models disrupted by social distance and stay-at-home orders are especially likely to do this, as they have been hit hard financially from COVID-19. This will also save employees time and money, as on-site workers spend [over 200 hours a year](#) commuting to and from the workplace and various amounts on commuting expenses, such as buying gas or bus tickets.

## How The Cloud Supports A Remote Workforce

Cloud applications and services allow organizations to support remote workforces, regardless of their geographical location. For example, real-time communication platforms, such as Slack and Microsoft Teams, are invaluable for enabling real-time communications throughout an entire organization.

To best continue remote styles of work in the long run, companies need to take a closer look at how many (and which) cloud apps and services they're investing in. In order to work remotely, companies need employees to have access to corporate resources through cloud technologies, and major cloud service providers have recorded [higher sales numbers](#) to support this increased demand.

To put it simply, companies will need to prioritize spending on cloud security and governance tools, virtual desktop infrastructure (VDI) and other key instances that can securely support their remote workforce.

## Which Cloud Security And Governance Controls To Prioritize

Throughout this pandemic, many organizations that previously operated with an entirely on-site workforce have quickly realized that their security perimeter is no longer the traditional firewall. Once the stay-at-home mandates lift and organizations continue to support remote workforces, this will remain true. In fact, identity and access management (IAM) is and will continue to be the primary perimeter in cloud cybersecurity.

As such, companies will need to focus on IAM tools in their cloud infrastructure to ensure only authorized employees are able to securely access the corporate data, tools and resources necessary while thwarting unauthorized access attempts from cybercriminals. However, this is easier said than done.

Managing identities in the cloud is difficult since everything in it, from users to cloud services, all have an identity. To manage these identities at scale, organizations need to catalog the resources each worker should have access to in order to do his or her job. This should thwart any internal or external unauthorized access and over-privileged access attempts. For large organizations, this can be challenging, but with the proper IAM solution in place, organizations can have the confidence that workers will be able to do their jobs while malicious attempts will be thwarted.

The proper IAM solution must be able to protect an entire remote workforce, regardless of how large it may be. Manual processes would make this difficult, but by using IAM with automated monitoring and remediation capabilities, organizations can manage access and role management and identity authentication. This will also help enterprise security teams proactively navigate any identity-borne threats in the cloud environment.

## Moving Forward

While not every job or industry will ever be 100% remote, companies can still leverage cloud apps and services to continue enabling workers — both remotely and in the office. With a proper understanding of how to implement and support a remote workforce and the challenges that come with this, remote styles of work can be a win-win for employees and employers.

---

[Forbes Technology Council](#) is an invitation-only community for world-class CIOs, CTOs and technology executives. [Do I qualify?](#)

---

Follow me on [LinkedIn](#). Check out my [website](#).



**Chris  
DeRamus**

CTO and Co-Founder of [DivvyCloud](#). [Read Chris Deramus' full executive profile here....](#) **Read More**