WORKING FROM ANYWHERE

How to create an effective hybrid working environment that works for employees and your organisation, with software-defined solutions, intelligent collaboration, and a zero-trust access model.

At a glance

- A changed environment – a different response
- A strategic trend with new urgency
- Business drivers and challenges
- Ensuring Secure Connected Digital Workplace
- Tata Communications's solutions for working from anywhere

A CHANGED ENVIRONMENT – A DIFFERENT RESPONSE

Organisations today find themselves in a very different environment to that of even just one year ago. They now face an immediate business imperative to become digital first to sustain themselves in the market. They need the ability to rapidly adjust to changing circumstances, and a key element of this is enabling their employees to work from anywhere.

Working from anywhere allows employees to create continuous value through a seamless, secure, and connected workplace experience at home, on the move, and in the office. This has become the new priority for most enterprises globally.

While the ability to work from anywhere promises great benefits, it can also bring with it many technology challenges. To overcome these, we believe organisations need to take a different approach, focusing on delivering a seamless user experience - with corporate grade security and performance – to any location.

This paper describes these challenges and puts forward our perspective on how to overcome them using smarter technologies and a holistic and pragmatic approach.

A STRATEGIC TREND WITH NEW URGENCY

Working from anywhere has been a growing trend for several decades, which has become much more mission-critical since the pandemic.

Gartner forecasts worldwide public cloud end-user spending to grow 18% in 2021. The proportion of IT spending that is shifting to cloud will accelerate in the aftermath of the COVID-19 crisis, with cloud projected to make up 14.2% of the total global enterprise IT spending market in 2024, up from 9.1% in 2020.

The growth in Software as a Service (SaaS) productivity and collaboration platforms is also a good barometer of flexible working patterns. The number of active users of Microsoft Office 365 had been growing steadily by about 10-20 million per month in the four years to the end of 2019. Then, in just one month, April 2020, it suddenly jumped by 58 million to 258 million. Teams now has 75 million daily active users, compared to 20 million before the pandemic.

Although SaaS remains the largest market segment and is forecast to grow to $117.7 billion in 2021, application infrastructure or platform as a service services (PaaS) are anticipated to grow by a higher margin at 26.6%. The increased consumption of PaaS is driven by the need for remote workers to have access to high performing, content-rich, and scalable infrastructure to perform their duties.

These trends are expected to become long-term, with three quarters of companies planning to make remote working permanent following COVID-19.

BUSINESS DRIVERS AND CHALLENGES

Organisations are pursuing a work-from-anywhere strategy for a number of reasons. They see that it will make them more resilient to disruption, give them greater flexibility and scalability, and the ability to respond positively to unforeseen changes.

Having a good proportion of the workforce regularly working away from the office brings the potential for significant reductions in facilities costs and the opportunity to cut energy consumption and carbon footprint. Many organisations are taking the opportunity to consolidate and revamp their offices and to make remote working a permanent option. Flexible working is also a factor in attracting and retaining talent in a competitive labor market.

But implementing a work-from-anywhere strategy also brings its share of business challenges. One of the biggest is ensuring regulatory compliance. For example, banking transactions have to be auditable and high value transactions have to be checked by another person to avoid fraud. If a contact centre agent is working from home, the bank needs to find new ways of managing this process to ensure compliance.

Organisations also face the business challenge of keeping systems secure to avoid data theft or interruption to business. They need to balance delivering a seamless user experience with keeping it governable. On top of this, special measures are required to keep employees engaged and productive while they are working remotely, and to ensure good communication and support for remote workers. And organisations need to rethink how to maintain their employee brand and cultural identity across a distributed workforce.

ENSURING A SECURE, CONNECTED, DIGITAL WORKPLACE

To provide an effective and sustainable working from anywhere model, and improve employee experience in a secure, connected, digital workplace, we believe there are a number of critical factors and steps to consider and address.

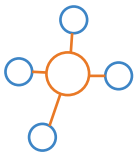
Some providers will tell you that all you need to enable working from anywhere is their technology product. Others may try to convince you that you need a full-scale consulting exercise first.

Given that working from anywhere is an urgent as well as an important priority, we advise our customers adopt a pragmatic approach that is neither wholly bespoke nor vanilla. From experience, we believe steering a course between full consultancy and off-the-shelf, established, proven solutions is the most effective. Start rolling out the industry proven solution in steps, and then improving, extending, and building on the reliable foundation created, is a fast, low risk, and cost effective way to deliver business value.

When beginning this process, we recommend focusing on the following areas:

SEAMLESS EXPERIENCE

To deliver a truly seamless work-from-anywhere experience it is key that employees can use similar processes and authentication to access applications from different locations. Ideally, we would recommend creating just one way of logging on that is transparent to the user regardless of where they are.



PRODUCTIVE COLLABORATION

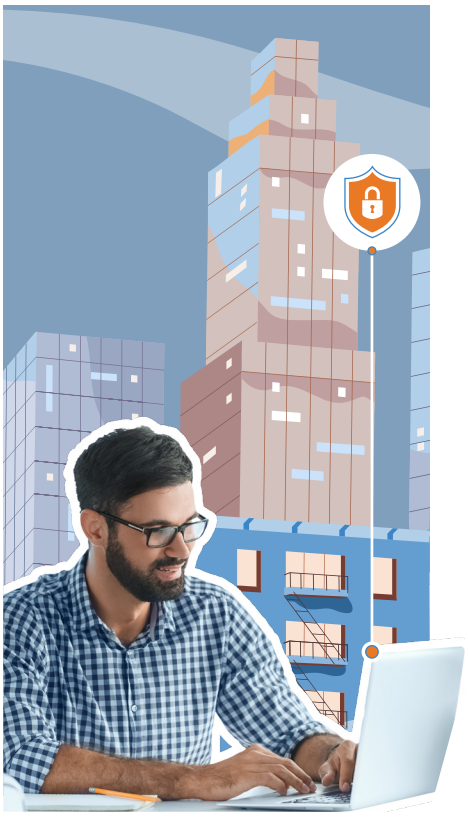
While collaboration service providers like Microsoft Teams, Cisco Webex, and Zoom have introduced many easy-to-use features such as text scripting and online translation to facilitate employee, partner, and customer collaboration, you will need a robust infrastructure to support these real-time applications. You should also consider how to ensure access to the same materials, systems, and databases from any location without users experiencing any variation in accessibility, performance, or speed.

MAKING THE INTERNET FIT FOR BUSINESS.

True working from anywhere will often involve the use of the public internet to access corporate critical applications and systems. This means you should consider and address any potential performance issues that may arise during the access of these applications via the internet.

MAKING THE INTERNET SECURE FOR BUSINESS: ACCESS WITH A ZERO-TRUST MODEL

Remote-workers accessing corporate applications and data over untrusted networks can lead to security issues. You need to ensure you can deliver secure, seamless, remote access to core enterprise applications over untrusted networks, and strike the right balance between ensuring security and not making access too difficult. Using a software-defined, Zero-Trust Access (ZTA) model is more secure, more reliable, and more flexible than connecting via a VPN – and gives a better user experience to people working from anywhere.



Ideally, ZTA should have multiple layers of security:

- two-factor authentication
- data is transmitted over a dark network, invisible to hackers
- micro-segmentation of data means it can be sent over multiple networks so hackers can't intercept it
- it has no inbound ports, so the firewall doesn't allow any inbound traffic at all
- movable attack surface, meaning if the network provider is attacked it can move transmission to another network
- look for zero-trust host access and zero-trust application access, which are safer when working from anywhere

We believe that ZTA is important to secure working from anywhere. If a home worker uses a personal laptop to access enterprise resources, one option is to use a VPN client with username/password or two-factor authentication. However, any security vulnerability on the laptop can still pose a risk to the enterprise network. VPNs have other inherent disadvantages: they don't connect users directly to resources but go via concentrators, the corporate network, and then to the relevant clouds. If the VPN is hosted on a firewall that constitutes a single point of failure, and if the firewall fails, it affects application performance.

By contrast, software-defined ZTA solutions give specific application access to a user on a specific device. The user downloads the app from an app store and an administrator grants selective access. The laptop works as normal for everything else as the ZTA is only invoked when using specific applications.

However, when considering a ZTA model endpoint protection, identity and access management, cyber threat and data protection should also be reviewed to ensure frictionless sign on and access given how ZTA works. For example, if an employee's identity is authenticated but the employee appears to be in a strange location, or the device does not have the correct security posture, then access will not be validated or authorised.

MAKING THE INTERNET EFFECTIVE FOR BUSINESS: APPLICATION PERFORMANCE

Ensuring consistent high performance from remotely-accessed applications and services over public internet connections can be challenging. The public internet is a contended, best-efforts network often with no quality-of-service guarantee. This can make it difficult to assure remote user experience when they are using applications hosted in the corporate data centre, public cloud, or consumed as a SaaS service – especially if these applications carry voice data.

We have found that using software-defined application WAN helps with experience optimisation in this situation. People working from home using Citrix or Windows virtual desktop have often found these platforms can seem slow to respond. We recommend looking for solutions that reduce time lag, delivering superior user experience by only optimising the relevant applications, and by using AI-powered dynamic routing to find the best network path behind the scenes. This approach connects individuals directly to the cloud, giving a better response than VPNs for the reasons noted above.

In addition, you could also choose to deploy an SD-WAN edge device in home offices and remote offices to allow intelligent path selection, as well as the zero-trust access, to improve site availability. At the same time, having the Wi-Fi managed in a way to ensure business traffic has higher priority and consumes more available bandwidth can avoid congestion due to any non-business traffic at the same location.

EASE OF DEPLOYMENT

While making the internet secure and effective is key to enabling an infrastructure that is fit for working from anywhere, the speed in deployment is important given the heightened need to enable remote working. We recommend making services available from an online portal. Finding a service provider that offers a digital customer journey from quote to delivery will mean you can manage ordering and delivery of all the elements you require entirely online. Any ZTA solution should be simple to administer because you can configure multiple connections to multiple applications on multiple clouds once centrally, rather than having to configure and maintain multiple connections. Also, remember to include mobile devices in any deployment, making all these advantages available to people using cell phones and tablets to work from anywhere. ZTA solutions are simple to operate and generally don't require an IT expert to operate them and we suggest looking for a ZTA solution that can be configured by the line-of-business to ease adoption.
Software-defined ZTA solutions also help control costs, as they don't require hardware purchase or long implementation projects.

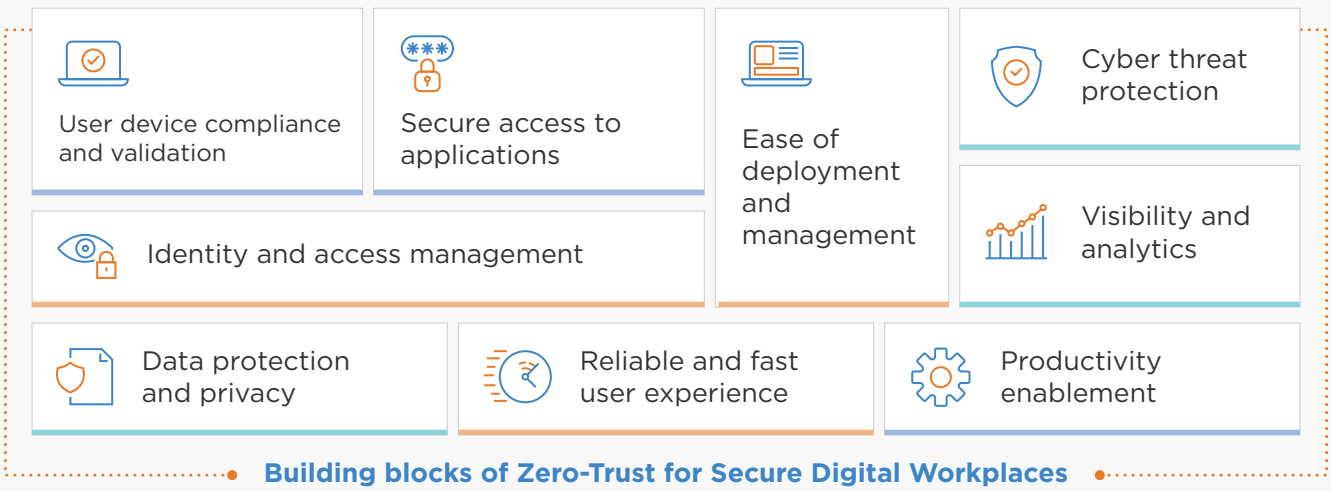
WORKING FROM THE OFFICE

The office is still an important work location and working from anywhere should include enabling working from a corporate office location. We believe that office settings will be connected very differently from how they used to be, with agile, pay-as-you-go access and availability, rather than the fixed bandwidth options of the past. In order to meet with the contingent requirement, enterprises should look for capacities such as network-on-demand and should consider a change of routing policy management with a real-time online self-service portal, allowing the modification on the fly. It would be good to also think about how you will be providing a contactless and safe workplace for employees to comply with prevailing public health regulations and the network requirements this may raise.

VISIBILITY

Your organisation needs visibility of application and network performance at all times. If, for example, it suffers a DDoS attack, you need to be able to react in real time to throttle bandwidth or deny access to protect applications, data, and systems. With working from anywhere you also now need to monitor the entire user experience, through access, log-on, application or platform performance, and network responsiveness for all applications wherever they are hosted – evolving from network performance monitoring to digital experience monitoring.

SECURE ACCESS ENABLED BY ZERO-TRUST MODEL



TATA COMMUNICATIONS' SOLUTIONS FOR WORKING FROM ANYWHERE

Tata Communications offers the whole range of technologies and services required to implement a secure, high-performance, and cost-effective work-from-anywhere policy.

Zero-trust access: NetFoundry This software-defined solution gives connectivity to cloud in minutes. It can yield performance optimisation, 40-70% cost savings, and has five layers of security.

Automatic connection to a greater choice of points of presence and less backhauling of data significantly improve responsiveness. Granular segmentation controls access for every application, user, and device. And it features continuous trust verification to enforce central security policies when working from anywhere. Bundled into a physical device that provides dual connectivity, the NetFoundry software also supports broadband with Wi-Fi backup.

In September 2020, Gartner recognised NetFoundry as one of the few providers offering full SASE.

RAPID REMOTE WORKING SOLUTION FOR CRITICAL NATIONAL INFRASTRUCTURE ORGANISATION

Tata Communications implemented a secure remote working solution based on NetFoundry for 300+ employees of a power generation company in less than six hours. No hardware procurement or installation was involved, and two data centers were connected in a few minutes. The ZTNA solution gives three times faster application performance than a VPN and is 30% cheaper.

Endpoint Detection & Response (EDR). Identify, isolate, and remove endpoint threats in real time.

Global VPN, IZO™ Private Connect, and IZO™ SD-WAN. Secure access to the corporate network, with reliable and fast user experience.

Identity & Access Management. Identity checks to provide governed access to applications with multi-factor authentication.

Secured Internet Gateway. A gateway to inject public routes over a private network.

Virtual Desktop Interfaces. Virtual environment with policy enforcement by business need on Azure or AWS.

Collaboration platforms. Choose from Cisco webex to enable meetings, calling, messaging, and team collaboration, or Microsoft Teams to connect, communicate, and collaborate in real time with audio and web conferencing.

Services. Tata Communications offers full implementation, and managed services and co-managed services to meet different business needs.

ABOUT TATA COMMUNICATIONS

Tata Communications is a digital ecosystem enabler that powers today's fast-growing digital economy.

The company enables the digital transformation of enterprises globally, including 300 of the Fortune 500 – unlocking opportunities for businesses by enabling borderless growth, boosting product innovation and customer experience, improving productivity and efficiency, building agility, and managing risk.

With its solutions-orientated approach and proven managed service capabilities and cutting-edge infrastructure, Tata Communications drives the next level of intelligence powered by cloud, mobility, Internet of Things (IoT), collaboration, security, and network services.

Tata Communications carries around 30% of the world's internet routes and connects businesses to 60% of the world's cloud giants and 4 out of 5 cell phone subscribers.

The company's capabilities are underpinned by its global network, the world's largest wholly owned subsea fiber backbone, and a Tier-1 IP network with connectivity to more than 200 countries and territories.

Tata Communications Limited is listed on the Bombay Stock Exchange and the National Stock Exchange of India.

Source:

1. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021 https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021
2. Microsoft Office 365 usage statistics, The XYZ, https://www.thexyz.com/blog/microsoft-office-365-usage-statistics/
3. Gartner, COVID-19 Bulletin, April 2020
4. Maturity of Completely Consolidated SASE Solutions (restricted distribution report), Gartner 2020

For more information, visit us at www.tatacommunications.com

Contact us