5 ways remote access is changing the tech world

Trends such as the Internet of Things (IoT), 24/7 business cultures, and evolving technologies mean that the way we work is changing rapidly, and businesses are increasingly sharing resources and collaborating in order to get ahead. Some are unaware of the role remote access plays within these developments, when it can provide a strategic foundation to support our changing technology landscape.

With this in mind, RealVNC has outlined some of the most prominent ways that remote access tools will impact businesses in the next 12 months.

1. Breaking down internal silos
   Remote access transforms conventional office activities
   • Departmental training  • Remote working  • IT resource sharing

   Businesses across a wide range of sectors are recognizing the competitive advantages of information and resource sharing, and we are seeing more collaborative business environments emerge. This is essential in today’s very competitive markets. Together with other technologies, secure remote access software is transforming office activities that are often inefficient, such as training, remote working and sharing resources. Staff are empowered to access resources and talent from the whole business, regardless of location.

   For example, construction firms such as Arup are using remote access technology to facilitate a resource sharing and staff training revolution. They enable engineers and other experts to ‘remote into’ systems, apps and devices in order to share resources, and to help and train colleagues in distant offices from anywhere.

   Remote access software allows employees to participate in real-time support or training given by department experts based in any location, and enables staff to ‘remote in’ to office PCs or servers from laptops, tablets or even mobile phones. With traditional business silos breaking down, companies are able to maximize their capital investments and reduce ROI, while removing traditional corporate barriers that hamper business efficiency.

   Organizations increasingly solve problems and develop innovations by crowdsourcing the best information and skills from the best sources across their network. Using remote access is no longer ‘just an IT support tool’, it can enable collaboration across an entire organization.

2. Creating an interconnected business ecosystem
   Remote access is a strategic technology for business optimization
   • Improves business efficiency  • Enable new revenue models  • Reduce travel costs

   The interconnectivity of different businesses within a larger ecosystem is developing momentum. It is quite normal to see businesses physically share office space, or place IT resources in the cloud. Companies can no longer operate in isolation or they risk being left behind in an increasingly competitive ecosystem. As this trend progresses, tools to work with partners or to help customers must become more creative, without compromising security. A greater need for connecting business processes to partners, suppliers and customers means that tools like remote access will be called upon to deliver secure connectivity between businesses, and directly with customers.
For example, remote access is used by service providers and vendors to access their systems in a controlled and secure fashion, ensuring systems stay tuned, updated and resistant to downtime risks. In another scenario, organizations can grant their customers remote access to resources such as training and test environments. This virtually eliminates the expense and cost of training travel, while improving customer service.

Managed Service Providers can also use this connectivity strategy to securely access their customers' IT resources and provide proactive and rapid support. Data center software company iQuate, for example, is using remote access technology to enable customers to access their training servers remotely and securely through encrypted connections.

There are many ways remote access technology enables innovation in an interconnected business environment. In the medical sector it is used to support distant training. A trainee doctor could remotely access an MRI screen, while the consultant talks through the scan. Scientists from different teams and partner businesses could remotely monitor experiments and critical systems from anywhere in the world.

We have seen strong adoption of remote access as a strategy to support collaboration between organizations in technology and engineering companies with high value propositions and mission critical software infrastructure.

3. Enabling an on-demand world

Remote access enhances real-time B2B and B2C connectivity

- Real-time connectivity
- Global access and control
- Meet performance expectations

In both our business and private lives, we have a growing expectation for instant access to information and resources. It is no longer acceptable for the content we receive to be delivered in anything other than real-time. This expectation is driven by advancements in database and software applications, and the availability of super-fast networks including 4G, and soon 5G. The ‘On-Demand Economy’ is growing - consumers today want their needs to be met instantly, and expect businesses to be ‘always on’. The expectation will only increase with emerging Artificial Intelligence, Virtual Reality and Machine Learning technology.

In the next 12 months, remote access will play a vital role in supporting our real-time world. By its very nature, remote access enables business to see and control geographically-distributed devices in real-time. Employees and IT staff are increasingly using remote access to maintain and service their critical IT estates, even on devices that do not have the software pre-installed.

As organizations feel more pressure to meet the expectations of a real-time economy, having a reliable way to deliver real-time support and management across an ever-growing range of devices and applications will be key to survival for many businesses.

4. Balancing connectivity and security

Remote access supports risk mitigation and compliance obligations

- Encrypted transfer and access security
- Central management
- Audited accountability

Security is a major concern for all businesses today. Recent large-scale hostile attacks on corporate assets illustrate just how exposed some businesses can be, and with the explosion of new devices and users, the security risk multiplies. Securely managing rapidly growing numbers of increasingly complex devices, and controlling the people that can access them, is critical to a larger security strategy.
A secure remote access platform can play a big part in mitigating the risk that comes with distributed devices, and in the next 12 months there will be more demand for end-to-end encryption and multi-factor authentication from businesses demanding a safely-managed device estate.

With the proliferation of privacy regulations like General Data Protection Regulation (GDPR) and industry-specific compliance requirements such as PCI DSS and HIPAA, controlling access to data and resources is increasingly important. A secure remote access strategy can help to ensure that only authorized individuals can access restricted information. Seeking out tools with robust security standards that specifically address the compliance considerations relevant to your industry should therefore be a priority.

Remote access is increasingly used to centrally manage a distributed estate of diverse devices, reducing the number of people involved in the device maintenance and management process and limiting the need for onsite support. An audited central management strategy mitigates the security risks inherent with large support teams, while actually lowering maintenance costs, improving uptime and enhancing estate efficiency.

5. Building innovation directly into products

Remote access enables advanced product connectivity

- Greater device uptime
- Cost efficient remote maintenance
- Improve customer service

Just as the adoption of remote access is increasing within and between companies, we are seeing a significant trend in the integration of remote access software directly into products. This OEM integration model is part of the growing IoT phenomenon, providing high value products with real-time connectivity to reduce the cost of maintenance, improve support efficiency and enhance customer service.

One good example is aging ATMs that have been in operation for many years. Financial institutions are dealing with legacy systems where the support for old operating systems has ceased. Because the operating systems are out of date, security is at risk, modern applications cannot run, and upgrades are extremely expensive, demanding hours of onsite service time.

To address this situation, the banking sector is starting to put remote access capabilities directly into ATMs, for remote diagnostics, management and central OS upgrades. They can leverage their investment by using the same technology to support customers with on-screen annotations and advice, improving the customer experience and putting the human element back into a predominantly automated operation.

A secure remote access strategy is helping financial institutions reduce the cost of operating their ATM estates through more efficient central management and fewer onsite service calls, while improving customer service at the same time.

This trend extends well beyond the banking sector. We are seeing a growing trend for the integration of real-time remote access into a wide range of “smart” devices, to cut the cost of management and support. Other sectors include retail, fleet management, manufacturing, consumer electronics and healthcare; in short, any environment with valuable devices that demand high uptime and reliable operation.