SOLUTION BRIEF

EMPOWERING WORKER MOBILITY WITH IGEL

Enable anywhere productivity securely and efficiently with IGEL's next-gen edge OS for cloud workspaces

The nature of remote work has changed dramatically over the last decade. Once reserved for business travel and special situations, remote work is now integral to how most businesses operate. In fact, in a recent survey of full-time workers in the U.S., nearly two-thirds reported that they work at home at least one day per month, and thirty percent work remotely on a full-time basis.

Embracing remote work unlocks numerous benefits for both companies and their employees. It gives employers access to a much broader pool of high-quality candidates, reduces facilities costs, and improves employee retention. Meanwhile, workers with the ability to work remotely at least part of the time often find that they are both happier and more productive with their work.

Advances with high-speed Internet availability and remote collaboration tools have made supporting remote work much easier. However, implementing and maintaining secure endpoints at hundreds, thousands, or even tens of thousands of untrusted remote locations remains a major IT challenge.

Simplify Endpoint Deployment and Management

IT teams charged with supporting remote workers often face a difficult choice when it comes to endpoint deployment. Issuing company-owned PCs to remote employees is extremely costly across several dimensions. Beyond initial hardware cost, remote Windows devices are notoriously difficult to patch and secure. They are also prone to day-to-day support issues that are difficult to diagnose and resolve remotely.

Meanwhile, allowing remote access to corporate systems from unmanaged personal devices comes with its own perils. While operating system patching and management headaches are eliminated, the company loses any ability to support employees when technology issues negatively impact their productivity. Unmanaged personal devices also represent a major security risk, as the IT teams have little ability to detect and defend against malware that could compromise sensitive corporate data.

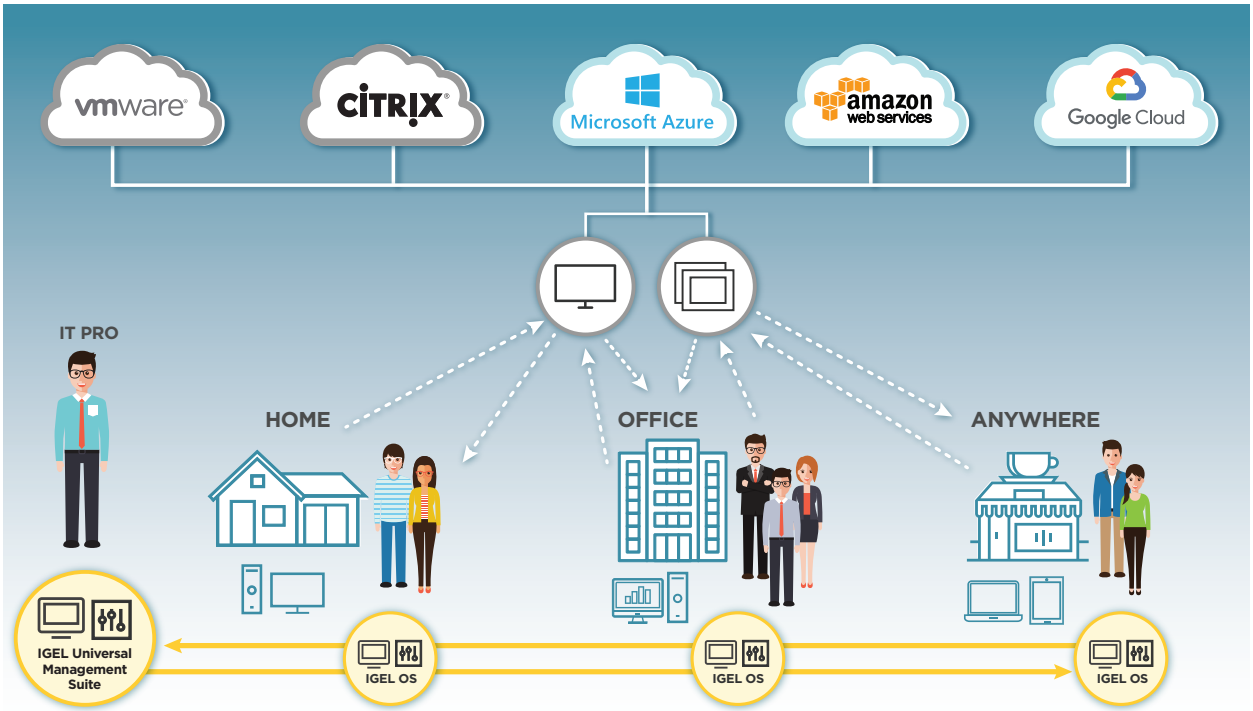
Providing users with simple and reliable remote access to the corporate environment is another major obstacle to remote work. While virtual private networks (VPNs) made this much more practical, they are often complex and costly to scale, prone to user experience friction, and not suitable for IT-initiated device management and support activities.

[1] OWL Labs / Global Workplace Analytics State of Remote Work 2019 report.

Simplifying Remote Work with IGEL

IGEL combines powerful, centralized endpoint management and control with a lightweight, software-defined endpoint operating system called IGEL OS to enable secure remote access to desktops and applications running in the data center or the cloud. IGEL OS was designed for remote management and has a much smaller footprint than a traditional Windows operating system.

IGEL OS can be deployed in multiple ways to serve as a secure endpoint using either company or employee-owned hardware. With IGEL OS in place, employees enjoy a responsive and familiar desktop experience, while IT teams benefit from simpler, centralized management of Windows and streamlined endpoint management using the IGEL Universal Management Suite (UMS).



Provisioning Secure Endpoints

IT teams supporting remote users have the flexibility to deploy IGEL OS in several ways to optimize manageability and security while minimizing hardware costs. Organizations that prefer to deploy dedicated company-owned devices to remote users can install IGEL OS directly on any 64-bit x86 device with a 1 Gigahertz processor and 2 Gigabytes of RAM or greater. This includes the ability to repurpose existing PC hardware extensively using turn-key device conversion technology. This platform-independent software approach can result in huge endpoint hardware savings as the classic “hardware refresh” cyle is either significantly delayed or eliminated altogether.

IGEL OS also enables previously untrusted employee-owned endpoints to be used for business purposes securely and reliably. IGEL’s UD Pocket USB boot devices make it possible for users to boot a personally owned PC into a secure instance of IGEL OS that is fully isolated

and completely independent from the locally installed personal operating system. Personal endpoints using UD Pocket devices can be configured and managed in exactly the same way as a company-owned endpoint, while maintaining the user's ability run a separate personal OS when they are not using the device for business purposes.

Simplifying Remote Access and Management

While IGEL OS can be used with most enterprise VPN technologies, organizations with a large population of remote users can deploy the integrated IGEL Cloud Gateway (ICG) software to dramatically simplify device onboarding, remote access, and ongoing endpoint management. ICG can be deployed on-premises in an organization's Internet-facing DMZ environment or in the public cloud.

Once in place, ICG enables zero-touch onboarding of endpoints running IGEL OS and frictionless ongoing remote access for users. The two-way communication between IGEL UMS and Internet-connected endpoints running IGEL OS also simplifies and accelerates IT-initiated endpoint updates and configuration changes with no action required by the user.

Optimizing User Experience and Support

By shifting Windows OS execution to data center or cloud environments with robust computing resources and providing rich local support for peripherals and multi-media, IGEL eliminates the performance and user experience trade-offs that remote users have endured in the past.

IGEL OS includes over 80 integrations with leading end user computing technologies, supporting both general and industry-specific needs. In addition to a myriad of software drivers and protocols and peripheral devices, this includes support for integrated user experience measurement and optimization technologies that IT teams can use to proactively measure and optimize remote desktop performance.

When remote users require support, IT teams can perform a wide array of endpoint configuration changes with ease from UMS. As more complex troubleshooting needs arise, they can also connect to remote devices through ICG and perform secure remote shadowing of user activity on the local endpoint.

The work-from-home and remote working trends will only continue to gain momentum as a new generation joins the workforce. People now ***expect*** to be able to work, play, and connect from virtually anywhere, and those companies that best embrace the new mobile/remote work paradigm will be best positioned for future success. Where endpoint security, fulfilling user experience, and comprehensive IT management are all key organizational priorities, IGEL OS and UMS software can serve as key enablers in your move to cloud-hosted work experiences. From any cloud, and from ***anywhere***.

Download IGEL Workspace Edition to Get Started Today

Are you looking for ways to make worker mobility simpler and more secure? **Download IGEL Workspace Edition for free** to experience the simplest, most cost-effective, and most secure way to deliver VDI and DaaS desktops to your users.

Your IGEL Workspace Edition download will include 3 IGEL OS licenses and complete access to IGEL UMS for management, all of which are free to use for up to 90 days.

20191106