APP NOTE

BRING YOUR OWN DEVICE (BYOD)

Enable Secure and Controlled Access to Cloud and Digital Workspaces from Personal Endpoint Devices

As economies and companies emerge from the pandemic, embracing the new way of work is key to restoring a "new normal" that includes business continuity as a key element going forward. A hybrid model of combining working from anywhere with days in the office is proving to be a popular choice for many organizations and people.

Another important player in the future of work is the gig economy. Many organizations hire temporary staff or contract experts to address surges in business or spearhead specialized projects. These "guest users" require temporary and controlled access to the company apps and workspaces.

This widely distributed and disparate workforce creates a number of challenges for IT teams and puts a strain on IT resources. With worldwide chip shortages impacting the supply of new endpoint devices, many companies are experiencing lengthy delivery times for new PCs, laptops and thin clients. One way to circumvent this challenge is to enable employees to work on their personal device or any compatible x86-64 device in a "bring your own device" (BYOD) model. However, the recent spike in ransomware attacks targeting users at the endpoint has placed even more emphasis on the importance of securing the edge.

Let's take look at how IGEL can enable a controlled and secure BYOD solution.
VIEW THE WORK VIDEO

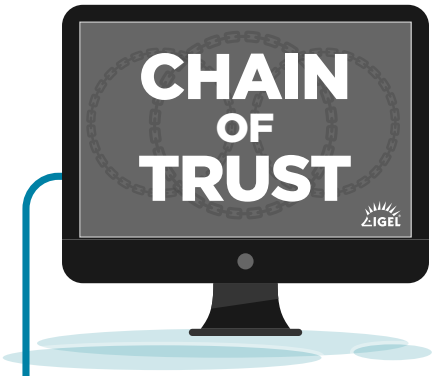
Why is IGEL the best endpoint OS partner for companies embracing a BYOD or Use Your Own Device (UYOD) model?

IGEL OS IS SIMPLE

Enabling a BYOD or UYOD strategy with IGEL is quick and easy to deploy, even remotely. Any compatible x86-64 device—on the corporate network or remote—can be set up in minutes. IGEL's UD Pocket, a highly portable USB stick solution, enables workers to temporarily turn their device of choice into an IGEL OS-powered endpoint. They simply plug it into their device and then connect to the IGEL Cloud Gateway via the Internet and they are up and running! **WATCH THE PROCESS**

IGEL OS IS SECURE

Across all industries, the flexibility and simplicity of IGEL OS and the UD Pocket offers a quick and secure solution. Based on Linux and structured as a modular, read-only, tamper-resistant firmware base, IGEL OS has an extremely small attack surface and a broad array of security-focused features designed to minimize exposure and prevent attackers from infiltrating your organization by infecting the most popular entry point: the network edge. IGEL enables secure access to cloud workspaces from end to end. IGEL's complete "chain of trust", which verifies all boot-up processes from the endpoint UEFI to the destination VDI host or cloud workspace, applies even to remote or temporary endpoint devices and offers added confidence for IT endpoint administrators.



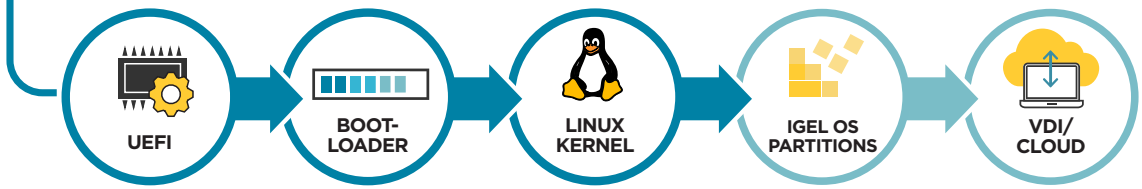
THE IGEL CHAIN OF TRUST

- Ensures all components of your VDI/cloud workspace scenario are secure and trustworthy
- As each component starts, it checks the cryptographic signature of the next, only starting it, if it is signed by a trusted party (e.g. IGEL, UEFI Forum)
- If a failure condition at any step is detected, the end-user is alerted, and IT can take appropriate action.

THE PROCESS

1. The software-related IGEL Chain of Trust starts at UEFI.
2. UEFI checks the bootloader for a UEFI Secure Boot signature.
3. Bootloader then checks the IGEL OS Linux kernel.
4. If the OS partitions' signatures are correct IGEL OS* is started, and the partitions are mounted.
5. For users connecting to a VDI or cloud environment, access software software checks the certificate of the connected server.

**IGEL OS 11.03 or later*



For those end-users running IGEL OS via the UD Pocket on their personal devices, once they have completed their work, they need only remove the UD Pocket to return to the native environment. All underlying apps and files remain untouched. The ease of control, even from remote locations, makes the UD Pocket a simple BYOD solution. If a personal device is lost or stolen, the IT admin can easily disable the UD Pocket with IGEL's unified management console, the Universal Management Suite. **VIEW THE SECURITY INFOGRAPHIC**

A WIN-WIN SOLUTION

Give people the flexibility they desire by enabling them to work securely from any location on their device of choice. Studies have shown this increases user satisfaction and productivity. A managed and secure BYOD strategy benefits the organization with significant savings by delaying or bypassing hardware refresh cycles that come around every three or four years. By enabling existing and personal endpoint devices to continue to run with more than enough processing power and resources needed for lean, efficient IGEL OS, the disruption and cost of buying new hardware can be avoided while reducing carbon footprint.

IGEL offers the essential components needed to enable a secure BYOD and UYOD strategy for remote access to company apps and workspaces from personal devices.

IGEL OS

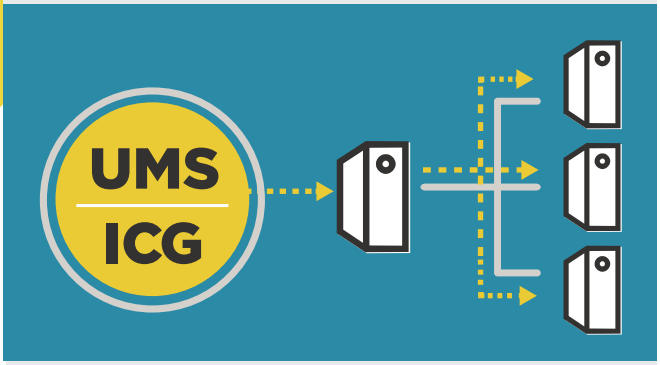
A platform-independent Linux-based next-gen endpoint operating system designed for simple, smart, and secure endpoint control and optimization. It allows access to cloud services, server-based computing applications or virtual desktops, and provides outstanding audio, video, interactive graphics, and unified communications.

IGEL UD Pocket

A portable and powerful USB pluggable endpoint solution. No larger than a paper clip, the UD Pocket is essentially “IGEL OS on a stick” and offers secure high performance for remote mobile and guest workers. The UD Pocket boots IGEL OS from a PC, laptop or any compatible x86-64 CPU based endpoint device.

Universal Management Suite (UMS)

A single management and control solution for just a few to up to 300,000 distributed IGEL OS powered endpoint devices. Purpose-built to simplify complex enterprise environments, UMS supports diverse operating systems, databases and directories. The UMS server can be located on the corporate network or in the cloud.



IGEL Cloud Gateway (ICG)

Enables full UMS management and controlof IGEL OS-powered endpoints located “off-network” in remote locations including home offices, remote campuses, or for mobile “road warrior” workers. It extends the reach of UMS without requiring a separate VPN connection to ensure strong management and control of all your IGEL OS-powered endpoints, regardless of their location.

CONCLUSION

As workforces become more disparate and distributed with full-time, part-time, and guest workers, and with sustainability top of mind for responsible business practice, IGEL has emerged as an ideal endpoint OS partner in these times of agile working. IGEL customers can benefit from a unified, coordinated end user computing solution on any compatible device that enables secure and productive working that is quick and easy. With an emphasis on secure and powerful unified communications and collaboration, IGEL delivers a great user experience for end-users be they employees, guest users or temporary staff, while giving both IT administrators and the CFO peace of mind.

Experience more about how IGEL OS and the IGEL UD Pocket support BYOD and business continuity with secure, controlled access to company apps and desktops from personal endpoint devices: IGEL.COM/UDPOCKET/

IGEL is a registered trademark of IGEL Technology GmbH. All hardware and software names are registered trademarks of the respective manufacturers.
Errors and omissions excepted. Subject to change without notice. ©2020 IGEL I 85-EN-24-1 I
WEEE-Reg.-Nr. DE 79295479 I WEEE-Reg.-No. UK 5613471

IGEL
next-gen EDGE OS
for cloud workspaces