TOP REASONS WHY IGEL HELPS STREAMLINE OPERATIONS AND IMPROVE SECURITY IN MANUFACTURING

The manufacturing and logistics industries face intense competition and a growing demand from their workforce for mobile access accelerated by the COVID-19 pandemic. The IT infrastructure you select plays a critical role in securing the most vulnerable entry point for malware — the network edge. It should also improve overall operational efficiency while creating a secure and lean manufacturing environment. This is especially true for user endpoint devices attached to the network, either on a corporate LAN or via the Internet.

IGEL OS, IGEL's next-gen edge OS for cloud workspaces, helps ensure the highest levels of connectivity by supporting a broad range of applications and interfaces. With IGEL OS, these apps and interfaces can be easily customized for user-specific requirements, whether in production, quality assurance, or in the warehouse.

1. **Secure, user-friendly access** – the IGEL Shared Workplace feature enables secure, personalized use of shared devices in administration, back-office, and on the shop floor based on user/department policies and profiles.

2. **Device security via minimal "footprint" OS** – IGEL OS is read-only for tamper resistance and modular, in that only the features needed by any particular end-user are presented to them. This minimizes the firmware "footprint" on any given user endpoint device which in turn reduces the malware attack surface of that device.

3. **End-to-end security** – the IGEL chain of trust ensures all components of your VDI/cloud workspace scenario, starting from select IGEL hardware or UEFI, are secure and trustworthy. Each discrete step validates the cryptographic signature of the next, only starting if it is signed by a trusted party (e.g., AMD Secure Processor, UEFI Secure Boot, IGEL OS).

4. **Frequent software releases** and additional fixes as necessary enable you to always stay current with the latest feature enhancements and security features of our technology partners.

5. **Safe and compliant** – while working with IGEL OS, no data is stored on the endpoint device — even if people use their own PC or notebook with an IGEL UD Pocket, all data is stored in the cloud/VDI and not on the user's private hardware. Your network edge is more secure, and compliance with key security requirements like GDPR becomes easier.

6. **Cost savings** – hardware independent IGEL OS runs on any compatible x86-64 device, expanding endpoint device choice for company environments with different and even specialized form factor requirements. By converting x86-64 endpoint devices to IGEL OS, you can quickly extend the life of existing hardware, regardless of manufacturer, or easily assign a license to another device. This can sharply reduce capital expenditure (CAPEX) and operational expenditure (OPEX). IGEL OS also runs on the Arm-based NComputing RX420(IGEL) device in Citrix environments.

7. **Highly connected** — a broad technology partner ecosystem of more than 100 leading partners ensures fast and seamless integration of authentication tools, logistics devices, unified communications, printing, USB management technologies, and more.

8. **Easily integrated** – IGEL OS is customizable. Corporate branding or unique screensavers for corporate messaging can make endpoint devices look and perform exactly as desired in accordance with an organization's requirements.

9. **Expanded productivity** – IGEL OS delivers a great user experience for graphics-intensive applications and unified communications. It gives design engineers the multimedia performance they need, and supports offloading of Microsoft Teams via Citrix Workspace App, Cisco Teams VDI and JVDI, Zoom, and a broad range of headsets whose firmware can be updated via the IGEL Universal Management Suite (UMS).

10. **Easy management and control** – the UMS centralizes endpoint management and control of devices in administration, office, manufacturing, logistics, or at-home locations. The IGEL Cloud Gateway (ICG) enables full management and control of remote, distributed user devices that are "off network" — not on the corporate LAN. A high degree of standardization of back-office workstations requires minimal management effort for server-based or cloud workstations.

11. **Easy, efficient updating and troubleshooting** – endpoint device updates are simple via zero touch deployment and drag-and-drop profiling. IT managers are spared the time-consuming and error-prone patching typical for Windows endpoints. The IGEL UMS also offers extensive support and troubleshooting capabilities, including secure shadowing of remote off-network devices via the ICG feature. This eliminates the need for on-site IT support and minimizes interruption of revenue-impacting systems.

For the above reasons, IGEL can help manufacturing and logistic companies of all types and sizes to improve operational efficiency and create a lean, secure manufacturing environment while protecting critical confidential data. All while saving significant money in both capital and operating expenses.

REQUEST A DEMO
IGEL.COM/GET-STARTED/TRY-FOR-FREE/

IGEL
next-gen EDGE OS
for cloud workspaces