TIP SHEET

TOP REASONS WHY IGEL OS IS IDEAL FOR SECURE GOVERNMENT END USER COMPUTING

Among the greatest challenges for IT teams working within government environments is providing end-users with productive, high-fidelity user experiences while at the same time offering strong endpoint security amid shrinking budgets.

Let's look at how IGEL can alleviate frequent government end user computing challenges and enable greater security and productivity while reducing budget constraints at the same time.

SECURITY AND COMPLIANCE

Strict compliance with national and international standards like GDPR to protect personal identifiable information (PII) is difficult to attain and manage.

1. IGEL OS is modular by design; unused features can be turned off, keeping endpoints as "lean" as possible to minimize the attack surface of the device. This, along with the read-only file system, makes IGEL OS even more tamper resistant. A secure browser can be configured for safe user access to web apps and cloud-based DaaS offers including Amazon Web Services (AWS) and Windows Virtual Desktop (WVD) from the Microsoft Azure cloud.
2. IGEL's complete "chain of trust" verifies each step of the boot-up process from the user hardware/ UEFI to the destination VDI host or cloud workspace delivered by Citrix, VMware, Microsoft RDP and WVD, Amazon WorkSpaces (PCoIP).
3. Multi-factor authentication plays an important role in controlling access. IGEL OS contributes to high-level access control via an integrated PKCS11 library that supports authentication and single sign-on technologies with the use of almost all smart card readers.
4. IGEL OS is secured to U.S. and European government standards and supports 3rd party technology that is approved for processing classified information up to and including SECRET, NATO SECRET, and SECRET UE/EU SECRET.
5. With secure shadowing using the IGEL Cloud Gateway (ICG) feature and Universal Management Suite (UMS), it is possible to manage and troubleshoot widely distributed endpoints including PCs, thin clients, and other x86-64 devices situated outside the corporate LAN.

OPTIMIZE USER EXPERIENCE AND IT BUDGET

Hardware replacement "refresh" is typically required every 3 or 4 years, which is extremely costly and disruptive.

1. Out-of-date hardware - PCs, laptops, and thin clients can be converted to an IGEL OS-powered endpoint within minutes. Lean, efficient IGEL OS runs on any compatible x86-64 device, so endpoint hardware refreshes can be significantly delayed or bypassed altogether. This minimizes disruption, unleashes IT budget, and supports green IT practices.

2. IGEL OS delivers a great user experience for unified communications. It supports offloading of Microsoft Teams via Citrix Workspace App, Cisco Teams VDI (with release of 11.04.100) and Zoom, and a broad range of headsets whose firmware can be updated via the Universal Management Suite.

3. IGEL's vast and growing technology partner ecosystem (100+) includes market leaders in unified communications such as Zoom and Microsoft Teams, single sign-on and digital signature, printer management, performance monitoring, optimization, and many more. The IGEL Ready technology partner program ensures IGEL OS stays current with the latest protocols, interfaces, and firmware versions to maintain streamlined interoperability for our customers.

SIMPLIFY CENTRAL MANAGEMENT AND CONTROL

IT administrators often struggle with time-consuming administration of dissimilar, complex, and slow management tools, especially in endpoint environments comprised of disparate vendor hardware and device operating systems. Managing and updating images and firmware by touching each endpoint is particularly tedious.

1. Quick and easy zero-touch deployment of IGEL OS with IGEL Universal Management Suite (UMS) software makes it possible for one administrator to optimize, image, and control up to 300,000 endpoints from a single console. Even those devices located across widely dispersed offices and homes using the IGEL Cloud Gateway (ICG).

2. Providing a high degree of standardization of all workstations requires minimal management effort for server-based or cloud workstations.

3. Drag-and-drop profiling, and a "buddy update" process minimizes bandwidth consumption, and avoids the time-consuming and error-prone patching typical for many dispersed Windows endpoints.

4. IGEL supports stringent identity & access management by supporting authentication tools like Common Access Cards (CAC) with Personal Identity Verification and SIPR tokens.

Lightweight and secure by design, IGEL OS offers a simple, smart, and secure solution that supports mission-critical functionality within government end user computing environments. Complex operational functions are standardized and streamlined. IT managers can shift their focus from ad-hoc issues to strategic plans. By reducing operational and capital expenses, cost-savings and allocated budget can be leveraged to fund further IT development projects.

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

IGEL
next-gen EDGE OS
for cloud workspaces