SOLUTION BRIEF

IGEL

The Secure Endpoint OS for Government Now and Next

Meet the mission with the modern government endpoint built for Zero Trust and reduced costs.

IGEL Endpoint OS: Built for Government

IGEL Endpoint OS enables government agencies to deliver secure workspaces to distributed field offices and facilities. The IGEL Preventative Security Model supports Zero Trust endpoint security, eliminates data leakage at the endpoint and supports hybrid ways of working whether at home, distributed offices, or field locations. IGEL OS supports sustainability goals while reducing operational costs.

Simplicity for Government Workers

IGEL OS delivers the secure, fast, user experience that government employees need. Support for laptop, desktop and thin client devices enable users to have the right device for their use case – be that a role that requires mobility or a home-based call centre worker. Wide ranging support for peripherals ensure that the headsets, scanners, printers, and cameras that are a necessity for a great customer experience work flawlessly.

Simplicity for IT

Endpoint management consumes a disproportionate amount of IT resources and budget – particularly when environments use application virtualization and VDI, such as government, that move the applications and workloads away from the endpoint. IGEL Endpoint OS is designed for VDI, DaaS, secure browsing and SaaS environments. The IGEL OS footprint is small reducing the size and frequency of updates, security and management agents are not needed, and hardware refresh cycles are extended by up to 100%.

Key Features

- Support for 90meter authentication
- Preventative Security Model minimizes endpoint downtime
- Broad device format support fits any agency use case

Key Benefits

- Improved resilience to cyber-attacks
- Reduced endpoint total cost of ownership
- Contribute to IT sustainability goals

Reduce Ransomware and Malware

IGEL's transformative Preventative Security Model supports Zero Trust security initiatives and removes vulnerable endpoint attack vectors. The hardened IGEL OS eliminates local data storage, is read-only and encrypted. A secure boot process tied to the hardware ensures the endpoint platform has not been tampered with ensuring a known good state with a simple reboot. The combination of non-persistent desktops with IGEL OS deliver one of the most robust end-user compute architectures available today.

Savings

IGEL OS modernizes the government endpoint for the cloud. CAPEX costs are reduced by enabling the purchase of less powerful laptops, desktops and thin clients. Costs are further reduced by extending the lifecycle of a device, replacing the existing operating system with IGEL OS. OPEX costs are greatly reduced by eliminating costly and time-consuming management and security agents simplifying the test, update, manage, monitor, troubleshoot lifecycle.

Comprehensive Support

IGEL offers 24/7 technical support, a dedicated technical relationship manager (TRM) and the IGEL Academy education portal. Integrations with 90meter, Citrix, Microsoft, and VMware deliver support for the latest, most secure digital clinical workspaces. The active IGEL community has more than 11,000 members and is an opportunity to learn, share and engage with customers, partners and industry experts.

Resources

- Case Study UP-AND-RUNNING IN 10 MINUTES WITH IGEL IN LIMBURG MUNICIPALITY
- Customer Video Spotlight CITY OF TIGARD SAVES TIME FOR LARGER PROJECTS
- Customer Video Spotlight SCOTTISH GOVERNMENT AGENCY ENABLES "ANYWHERE" COMPUTING WITH CITRIX AND IGEL
- Solution Paper ENDPOINT SECURITY AND CONTROL FOR U.S. FEDERAL GOVERNMENT

For more information or to register for trial access,
please visit www.igel.com/get-started/try-for-free.

Visit us at igel.com

IGEL