

The Secure Endpoint OS for Healthcare Now and Next

Deliver uninterrupted care with the modern healthcare endpoint OS built for preventative security.

IGEL Endpoint OS: Built for Healthcare

IGEL Endpoint OS removes the endpoint management and security challenges that healthcare providers face today. A preventative approach to security, simplified endpoint management and reduced costs support healthcare organizations in the frictionless delivery of patient information to clinicians. IGEL partners with essential care delivery peripherals and platform providers to support VDI and application virtualization, DaaS, speech mics, signature pads, badge-tap technologies, printers, scanners, EMR/ EPR workflows, and other critical clinical and administrative functions.

Simplicity for Care Providers

IGEL Endpoint OS delivers the fast, always-on access care providers need. Fast boot and connection times put patient information at the providers fingertips. Integration with Imprivata authentication and single sign-on support 'tap, turn, treat' workflows where the focus is on the patient, not the technology. Long standing partnerships with Citrix, Microsoft and VMware deliver the desktop roaming and fast user switching capabilities critical to security, compliance and a focus on patient care.

Simplicity for IT

Endpoint management consumes a disproportionate amount of IT resources and budget – particularly when environments use application virtualization and VDI, such as healthcare, 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 required, and hardware refresh cycles are extended by up to 100%.

Key Features

- Integration with Imprivata Tap and Go workflows
- Support for leading EHR / EPR vendors
- Preventative Security Model minimizes endpoint downtime

Key Benefits

- Improved resilience to cyber-attacks
- Reduced endpoint total cost of ownership
- Clinicians focus on the patient, not technology

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 healthcare 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 Citrix, Imprivata, 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

- ✦ [Success Story IGEL and LG Team to improve the digital experience for KALEIDA health](#)
- ✦ [Case Study Pennine acute hospitals NHS trust invests 5M to upgrade IT infrastructure, refreshing its EUC estate using igel](#)
- ✦ [Solution Brief Secure clinician access to AZURE VIRTUAL DESKTOP and WINDOWS 365 Cloud PC](#)

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