INFO BRIEF

A MODERN, SECURE ENDPOINT ARCHITECTURE FOR VIRTUAL DESKTOPS AND CLOUD WORKSPACES

IGEL's next-generation endpoint architecture is secure by design and equipped to deliver an unparalleled user experience

The legendary performance, quality, and reliability of IGEL's endpoint devices make it the hardware platform of choice for many of the world's most demanding end user computing environments. Now, with the introduction of its next-generation endpoint hardware design architecture, IGEL sets an even higher standard for virtual desktop and cloud workspace security and user experience.

IGEL's latest hardware designs combine an innovative, end-to-end security framework, modern and legacy connectivity options, and powerful remote management capabilities to optimize both user productivity and IT efficiency.

Premium, Eco-Friendly Hardware Design

The new IGEL hardware design features a more compact and sleek form factor, resulting in up to a 50 percent volume reduction from the previous generation of IGEL endpoints. A more modern industrial design includes premium elements like ergonomic power by touch. An included removable footrest and industry standard VESA mounting options provide deployment flexibility.

IGEL's latest hardware designs also feature a new, eco-friendly manufacturing process, including a chassis constructed from 30 percent recycled plastic.

End-to-End Security

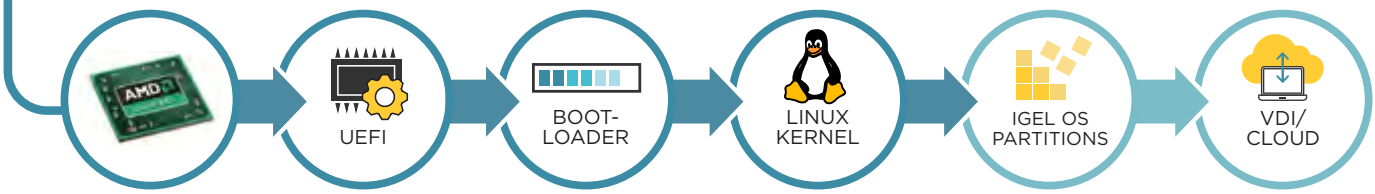
IGEL's next-generation architecture combines AMD Secure Processor hardware-based security with an extensive set of OS-level security measures to ensure system integrity at all times. The IGEL architecture is uniquely capable of providing an end-to-end "chain of trust" from the endpoint processor or UEFI process to the destination server or cloud platform. This innovative security framework validates each discrete step of the endpoint boot and workspace execution processes.

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)

The Process

0. On the new AMD-driven endpoint models UD3 and UD7 a dedicated security processor checks the cryptographic signature of the UEFI
1. Other IGEL devices: Chain 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 (starting with IGEL OS 11.03), IGEL OS is started and the partitions are mounted
5. For users connecting to a VDI or cloud environment, access software such as Citrix Workspace App or VMware Horizon checks thecertificate of the connected server



In addition to protecting the integrity of the system boot and workspace execution, the IGEL architecture is also designed to mitigate security risk on an ongoing basis. IGEL OS operates in a read-only manner and is configured to include only the modules that are necessary to support specific use cases. This unique security architecture, along with IGEL's proactive approach to security updates, minimizes the endpoint attack surface.

Modern Connectivity Options

IGEL's latest hardware designs provide an optimal blend of modern connectivity options and backward compatibility with legacy peripherals. This includes USB Type-C[1] and USB Type-A ports with support for superspeed USB 3.2 Gen. 1 connectivity. WiFi and Bluetooth connectivity with two integrated diversity antennas for optimized performance is also available as an optional add-on.

These modern connectivity options are available alongside more traditional options like serial and DisplayPort connectors for maximum flexibility. An integrated smart card reader[1] can also be included as an optional addition for use with extensive third-party software integrations that are available with IGEL OS.

Optimized for Remote Management

IGEL next-generation hardware endpoints come pre-installed with IGEL OS, which was designed for secure and efficient remote endpoint management at enterprise scale. IGEL OS works in concert with the IGEL Universal Management Suite (UMS) to enable simple, smart, and secure management and control of virtual desktops and cloud workspaces. IGEL endpoints and third-party hardware running IGEL OS can be provisioned, managed, and updated from a single management interface with drag-and-drop simplicity. Additionally, IGEL endpoints situated off the corporate network (e.g., home call center worker) can be fully managed and controlled by the UMS, including secure shadowing of these devices for helpdesk purposes via the IGEL Cloud Gateway (ICG) feature.

[1]USB Type-C and optional integrated smart card reader are presently available on the IGEL UD3 model.

Get Started Today!

IGEL's latest hardware endpoint offerings, the UD2 and UD3, showcase the design, performance, and security advantages of IGEL's next-generation design architecture.

UD2

Performance and security in a slim, cost-effective footprint that addresses many common virtual desktop and cloud workspace usage models.

Learn More

UD3

A secure, high-performance endpoint with an integrated WiFi option, SuperSpeed USB (3.2 Gen 1 Type-C), and support for up to two 4K monitors running at 60 GHz.

Learn More

REQUEST A FREE EVALUATION UNIT to see first-hand how the new IGEL hardware architecture can support advanced endpoint computing requirements and optimize user experience.

DOWNLOAD IGEL WORKSPACE EDITION for free to see how easy it is to convert your existing devices to IGEL OS and manage them alongside your best-of-breed IGEL endpoints.

IGEL
next-gen
EDGE OS
for cloud workspaces

Visit us online at **igel.com**

Revolutionary in its
Simplicity

20200201