IGEL OS is:

SECURE BY DESIGN
IGEL OS has built-in security to protect your endpoints and to safeguard your business. Security is at the core of development with a dedicated security team focusing on multi-layer integrations for secure VDI, DaaS, and cloud-delivered digital workspaces.

Moreover, since IGEL OS is designed specifically for access to cloud-delivered digital workspaces and nothing else, it offers zero "overhead" within its firmware footprint, unlike in a general-purpose OS like Windows.

READ-ONLY AND TAMPER-PROOF
IGEL's operating system and software reside on read-only storage partitions that cannot be changed. Additionally, they are cryptographically signed and validated at every boot to make sure that they have not been tampered with.

ENCRYPTED
Partitions or sensitive sections in the OS are secret coded to further secure critical data and features. IGEL OS offers an AES XTS-plain 64 encryption mode option. This requires users to enter a pass phrase after booting. This extra level of refinement helps to further decrease the endpoint's attack surface.

MODULAR
The IT admin can easily remove unnecessary features and network services in the OS via the management console. Features, apps, and data can be assigned and visible based on user role – as easy as selecting a check box.

IGEL OS offers:

A SMALL ATTACK SURFACE
IGEL OS is small and efficient with the option to turn interfaces and network services off. This and the fact that no business data is stored on the device, minimizes the attack surface, and deters hackers.

IGEL CHAIN OF TRUST
IGEL's verification sequence is initiated at boot-up to ensure end-to-end system integrity. A sequence of cryptographic signature verifications starts on the device UEFI or system-on-chip* to unlock each step of the boot-up process, from the endpoint device up to the digital workspace VDI host or cloud.

*depending on device SOC

The chain of trust thus ensures that every time the IGEL OS-powered device boots, none of the firmware and software in the startup sequence have been altered.
If indeed the chain of trust detects a failure condition at any step, the end-user is alerted, and IT can take appropriate action.

A MATURE ECO-SYSTEM
Multi-layer approach to endpoint security with integrated technologies from partners verified by the IGEL Ready program ensures continual compatibility with IGEL OS and adds an extra layer of security on the endpoint device.

BIOS UPDATES VIA LINUX VENDOR FIRMWARE SERVICE
IGEL OS supports the LVFS BIOS update mechanism. If the BIOS of your device is distributed via the LVFS you can access it through IGEL Universal Management Suite (UMS). Learn more on the **IGEL Knowledge Base**

IGEL Management via the Universal Management Suite (UMS) offers:

ENCRYPTED TRANSPORT LAYER SECURITY (TLS) TUNNELS
TLS tunnels ensure connections and file transfers from the UMS management console to the endpoint device are secure.

CENTRALIZED AND CRYPTOGRAPHIC UPDATES
Firmware updates from the UMS are validated by IGEL OS before installing on the target endpoint(s). IT admins can easily and quickly roll out firmware and security updates from one console to thousands of endpoints in a network-friendly manner.

SECURE SHADOWING
The IGEL Cloud Gateway feature enables IT personnel to securely shadow a remote endpoint device for troubleshooting purposes. For example, a helpdesk engineer can take over the endpoint device's keyboard and mouse. The UMS console, or alternatively, an external VNC viewer, establishes a secure connection to the UMS server. The UMS server then establishes a TLS tunnel to the device which is verified by a one-time-password issued by the UMS and sent to IGEL OS on the target device to grant permission. In addition, each and every secure shadowing session is logged by the UMS.

SECURE BROWSER MANAGEMENT
IGEL secure browser mode enables secure access to select cloud apps and services by setting up a kiosk or single-purpose "appliance" on any IGEL OS-powered endpoint. **LEARN MORE**

STREAMLINED AND SECURE PATCHES
IGEL OS firmware updates and patches are minuscule in terms of size and frequency when compared to Windows. In addition, IGEL OS updates are distributed by a network-friendly "buddy update" technique to accelerate the process and minimize bandwidth consumption. A high availability extension ensures simultaneous update of endpoints in large environments from the UMS console.

USB PORT CONTROL
An IT administrator can manage USB ports (e.g., enable or disable) on an IGEL OS powered endpoint via the management console. USB management and USB access control software partners are "IGEL Ready" for seamless functionaility with IGEL OS.

MULTI-FACTOR AUTHENTICATION
IGEL OS contributes to access control via a selection of integrated PKCS11 libraries that support authentication and single sign-on technologies with the use of almost all smart card readers and biometric solutions that enable multi-factor authentication, adding another layer of security to prevent breaches, even in the event of loss or theft of the endpoint device.

Security Hygiene at IGEL

VULNERABILITY MANAGEMENT

Vulnerability Management is the complete process of finding security vulnerabilities in software which are rated and prioritized. IGEL produces fixes and discloses information about them. IGEL practices vulnerability management through ongoing assessment and bug fixes in days, rather than weeks.

SECURE SOFTWARE DEVELOPMENT (SECURE SDLC)

The software (or system) development lifecycle (SDLC) contains all the activities needed to produce a finished software product at each stage, from the design via the coding up to the release.
IGEL conducts secure SLDC which complements this process with security activities at every stage, with design review, threat modeling, secure coding guidelines, security testing and much more.

REGULAR INDEPENDENT SECURITY ASSESSMENT THROUGH PEN TESTING

Software developers create software for a purpose, they tend to see how it is supposed to work, not how it can be mishandled or abused, e.g., view someone else's data. Therefore, it is important to have the security of a software product tested by an external expert. This is often called penetration testing (or "pen testing") or security assessment. The experts carrying out such a test try to make the software do things it shouldn't or allow users to conduct unintentional actions and then write a confidential report on their findings.
IGEL's products are independently tested.

SECURITY BULLETINS / CUSTOMER COMMUNICATIONS / ISN

IGEL Security Notices (ISNs) are email alerts sent by IGEL's security management team to inform our customers about critical and high security vulnerabilities in IGEL products should they occur.
ISNs tell customers what the vulnerability is, what IGEL product versions are affected, what can be done to mitigate the risk until a fixed version is available, and what product version fixes the vulnerability.
All ISNs are available in the **IGEL Knowledge Base.** Bookmark them today or subscribe to the IGEL security announcement mailing list.

REQUEST A SECURITY DEMO WITH AN IGEL EXPERT