INFO BRIEF

IGEL OS SECURITY

Comprehensive Endpoint Protection for the Secure Enterprise

Many organizations that adopt remote desktop session hosts, virtual desktops, and desktop-as-a-service models do so in part to reduce security exposure at the endpoint. Moving Windows OS execution from endpoints to centralized data center or cloud environments supports this goal in numerous ways. However, an OS footprint on the endpoint is still required to deliver remote application and desktop access and support local connectivity, display, and peripheral requirements.

IGEL OS is the next-generation edge OS for cloud and digital workspaces that was created with this specific purpose in mind. Based on Linux and structured as a modular, read-only and tamper-proof firmware base, IGEL OS has an extremely small attack surface and a broad array of security-focused features designed to minimize exposure and prevent attackers from infiltrating your organization through the most popular entry point: the network edge.

Security is central to the design and ongoing development of IGEL OS, and the tables that follow are a summary of its integrated security capabilities.

PRE-INSTALLED SECURITY	CAPABILITY
Modular partitions	Allows for specific features (e.g., Citrix Workspace, browser, ThinPrint, etc.) to be turned on or off on per-endpoint basis. Sensitive partitions are encrypted to further secure critical data and other features. IGEL OS 11.06.100 and subsequent versions, offers an AES XTS-plain 64 encryption option. This requires users to enter a pass phrase after booting. This modularization helps to further decrease the endpoint's attack surface.
Auto log-off	By combining a session type with an automatic log-off command, the device can log the user out of the last session. A username and password are required to log in again.
Pre-installed security features	Pure Kerberos-Ticket-Handling, based on username and password, with sophisticated "Two-Factor-Smartcard-Solutions" (smartcard and PIN) through a "three-party-constellation" • IGEL OS-powered endpoint devices • Active Directory infrastructure • Kerberos enabled service (s.a. Citrix XenApp or XenDesktop) Sophisticated rules and rights rollout management across the network on application level and for services. No local "Fake-Active-Directory".

PRE-INSTALLED SECURITY	CAPABILITY
VNC Secure Mode	Enables adherence with company compliance standards, including the following controls: • **Log** the shadowing • **Distribute** different shadowing permissions • **Define** shadowing groups and security levels • **Ban** VNC sessions between client to client (if it is integrated into the client desktop) • **Allow** only the IGEL shadowing or a 3rd party VNC client to communicate with the UMS console • **Ban** external/unknown 3rd party VNC clients in the whole network • Encrypted with TLSv1.2
Recycle bin	Deleted objects are moved to the recycle bin, where you can restore objects to the original point or delete objects permanently. Objects deleted by mistake can be restored.
High availability extension	The high availability extension enables new settings to be rolled out to several hundred devices at once in large environments. An upstream UMS load balancer takes over load distribution and ensures that each device can receive new settings at any time without overloading network capacity. More details on **Knowledge Base.**
USB management	USB management provides essential protection from security risks. USB devices such as pen drives, wireless controllers or printers can be used to steal data or to execute unauthorized software or even malware. To minimize the attack surface on an IGEL OS-powered endpoint, the USB ports can be deactivated. In IGEL Setup you can configure rules to block access to undesired USB devices. **A step-by-step guide is available on USB Access Control in Knowledge Base** IGEL USB-Management (basic function) is based on USB class, vendor/product-ID or by device UUID, with a very simplified access and denial mechanism. FabulaTech (extended function, requires optional server components from third party vendor) is based on protocols (RDP, Horizon, Citrix), and features depend on used protocol. DriveLock Thin Client Suite is based on virtual protocols, across each protocol with user dependent USB management enabling a very high safety standard.

IGEL Chain of Trust

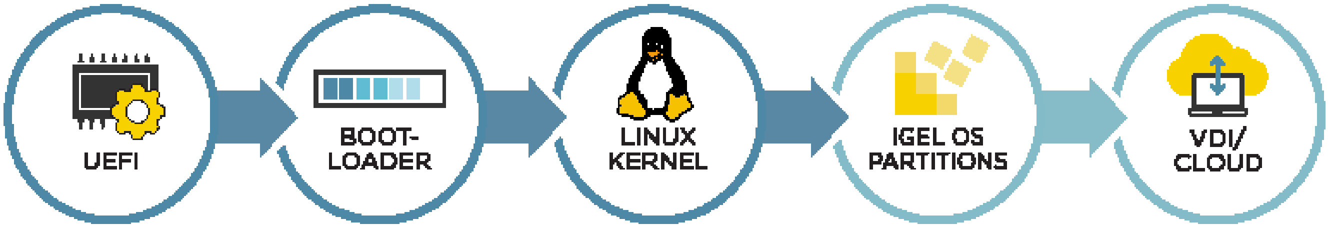
The chain of trust ensures that all components of your VDI/cloud workspace scenario are secure and trustworthy. A controlled boot sequence is initiated upon switching on the device. Each component checks the cryptographic signature of the next, and only starts it if it is signed by a trusted party such as IGEL or the UEFI Forum.
The IGEL chain of trust runs with IGEL OS on any compatible x86-64 device.

On IGEL OS-powered devices, the chain starts at the UEFI, which checks the bootloader for a UEFI Secure Boot signature. The loader in turn checks the Linux kernel of IGEL OS. If the signatures of the OS partitions on the hard disk are correct, IGEL OS is started and the partitions are mounted.

On IGEL UD3 and IGEL UD7 devices, this begins on the AMD hardware platform where a dedicated security processor checks the cryptographic signature of the UEFI.

If users connect to a VDI or Cloud environment, access software such as Citrix Workspace App or VMware Horizon checks the certificate of the server they are connecting to.

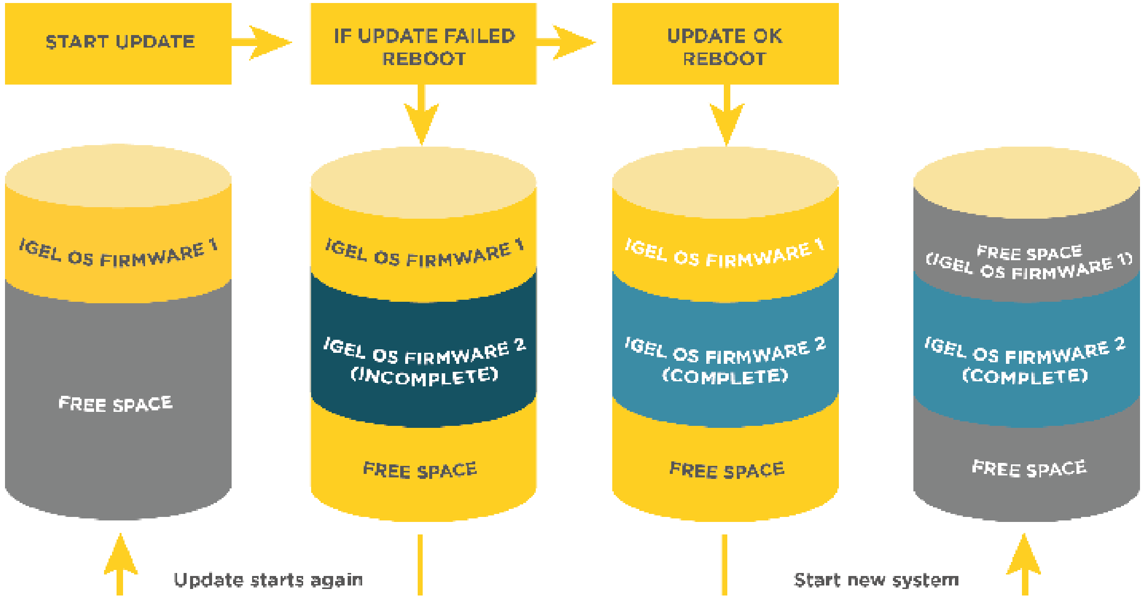
This chain ensures system integrity as it makes sure that none of the components in your environment have been tampered with – a great foundation for secure end user computing.



SYSTEM INTEGRITY	CAPABILITY
Partition confirmation checks	Signature checks on both update and boot processes for both system and user partitions detect tampering. If positive, the system will not boot. If any other partition is impacted, the system will boot with impacted modules deactivated.
Flash media cannot be mounted on any other device	IGEL uses its own partitioning system with compressed partitions that obfuscate data. Checksums of IGEL partitions avoid loading of modified code.
Protected configuration	Configuration is written to a dedicated and encrypted partition. IGEL OS 11.06.100 and newer, offers an AES XTS-plain 64 encryption option. This requires users to enter a pass phrase after booting.
Fail-safe firmware update	Firmware updates always finish completely while the device remains running and stays bootable. Critical updates are always processed in two phases to ensure success.
UEFI secure boot	IGEL OS bootloader signed by Microsoft (on behalf of UEFI Forum) on IGEL boots on systems with UEFI Secure Boot enabled. Only boot loaders signed with keys designated by IGEL or Microsoft keys approved by IGEL can load the operating system • IGEL generates and manages the cryptographic platform exchange keys which are included in the corresponding UEFI versions • A feature of IGEL UD2, UD3, and UD7 thin client endpoints • On IGEL OS11 “secure boot” mode is activated as the default value in the UEFI (BIOS)

SYSTEM INTEGRITY	CAPABILITY
Secure browser via AppArmor	Secure browser with restricted access to sensitive data with the following characteristics: • SSH key can’t be read or new keys added • IGEL configuration and firmware update scripts are not accessible • No view of configuration files • Java is completely disabled • No downloads • Access Yubikey: two-factor authentication
Ericom Shield	This tool executes web content in an isolated container on virtual browser and renders webpages as a safe interactive media stream for secure browsing.
Center of Internet Security (CIS) verification	Passed benchmarks for suite of CIS tests pertaining to safeguarding against cyber threats.

FAIL-SAFE FIRMWARE UPDATE PROCESS



INTEGRATED TECHNOLOGIES	CAPABILITY
Pre-installed VPN solutions	OpenVPN supported via VPN-based IGEL client management by IGEL UMS. NCP-e VPN client (optional NCP-e licensing) uses the universal IPsec client. Genua GenuCard support includes full management through the IGEL UMS with connection buildup through the IGEL managed client and support for ADSL, LAN, EDGE, 3G and 4G connections. VS-NfD, NATO RESTRICTED and RESTREINT UE are authorized and certified.
Keyboard encryption	Keyboard encryption via the Cherry Secure Board guarantees immediate encryption of keystrokes.
IP-based cryptosystem	IGEL OS supports SINA workstations from secunet that are approved for processing classified information up to and including SECRET, NATO SECRET and SECRET UE/EU SECRET.

INTEGRATED TECHNOLOGIES	CAPABILITY
Pre-installed SSO solutions	Smartcard support is individually adaptable using IGEL Partitions. The following are tested with IGEL OS. • IGEL Smartcard • **SecMaker** NetID • **SafeNet** Aladdin eToken • **Gemalto SafeNet** middleware for Gemalto/SafeNet eToken, IDPrime smart cards and token • **cryptovision sc/interface** middleware for cryptovision smart cards • **Gemalto IDPrime** smart cards • **Athena IDProtect** middleware for Athena IDProtect smart cards • **A.E.T. SafeSign** middleware for SafeSign smart cards • **Secmaker Net iD** middleware for Net iD smart cards • **Coolkey** middleware Coolkey • **OpenSC** middleware OpenSC • **90meter** middleware Smartcard reader support is individually adaptable via IGEL Partitions. The following are compatible with IGEL OS. • Elatec TWN4 CCID • PC/SC Lite • M.U.S.C.L.E. • HID OMNIKEY • REINER SCT cyberjack Authorization software integrated in IGEL OS • **Imprivata** OneSign ProveID Embedded • **Evidian** AuthMgr
Contextualizing	IGEL OS supports DeviceTrust which takes into account various contextual information (IP, geolocation, network etc.) when controlling access to data and applications. This makes it easy to implement fine-grained, compliant access control.
Pre-installed biometric solutions	IGEL OS supports biometric peripherals like • Crossmatch fingerprint readers • Fujitsu palm vein scanner

IGEL's focus is on providing the ultimate endpoint OS for cloud and digital workspaces, and security and data protection is at the forefront of our IGEL OS design and development efforts. The above information represents an ever-growing set of integrated capabilities designed to provide the strongest possible endpoint protection and reduce the attack surface at the network edge.

Visit igel.com to learn about the very latest developments and features from IGEL to help further fortify your endpoints and ensure that your transition to the cloud is as easy, and ***secure***, as possible.

Visit us online at **igel.com/security-at-the-edge/**

IGEL
next-gen EDGE OS
for cloud workspaces