FACT SHEET

IGEL ENDPOINT 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 workspaces that was created with this specific purpose in mind. Based on Linux and structured as a modular, read-only 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.
Auto log-off	By combining a session type with an auto logoff command, the user is logged out of the last session. The device executes “log off” command and logs the device off. Combined with Kerberos, the device is logged off and secure. 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 thin client • 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 (CONT)	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 at 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	HA includes two or several UMS servers within the network, for both redundancy and/or scaling, with an automatic failover mechanism. An integrated load balancer supports independent simultaneous booting process which is particularly useful for larger environments (500+ IGEL managed endpoints). It can also be used as a redundant system. Supported database clusters include Oracle DB (11g or higher) and Microsoft SQL Server (2012 or higher).
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. IGEL offers two options to control the use of USB devices to minimize the attack surface on IGEL UD endpoints. • Anti-theft, discrete USB port in the connectivity bar for IGEL UD3, UD6 and UD7 A guide on how to open the connectivity bar casing to insert a USB device in to the USB port is available on Knowledge Base • USB device deactivation In IGEL Setup you can configure rules to block access to undesired USB devices. A step-by-step guide is available on Knowledge Base (For more information visit www.igel.knowledgebase.com) 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.

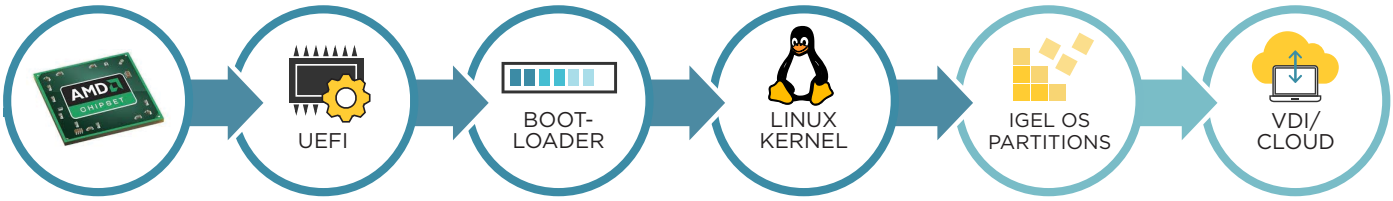
IGEL Chain of Trust

The Chain of Trust ensures that all components of your VDI/cloud workspace scenario are secure and trustworthy. Each component starting up 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.

With IGEL UD7 devices this begins already on the AMD hardware platform. A dedicated security processor checks the cryptographic signature of the UEFI (available from December 2019). On other IGEL 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 (from December 2019) on the hard disk are correct, IGEL OS is started and the partitions are mounted.

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.

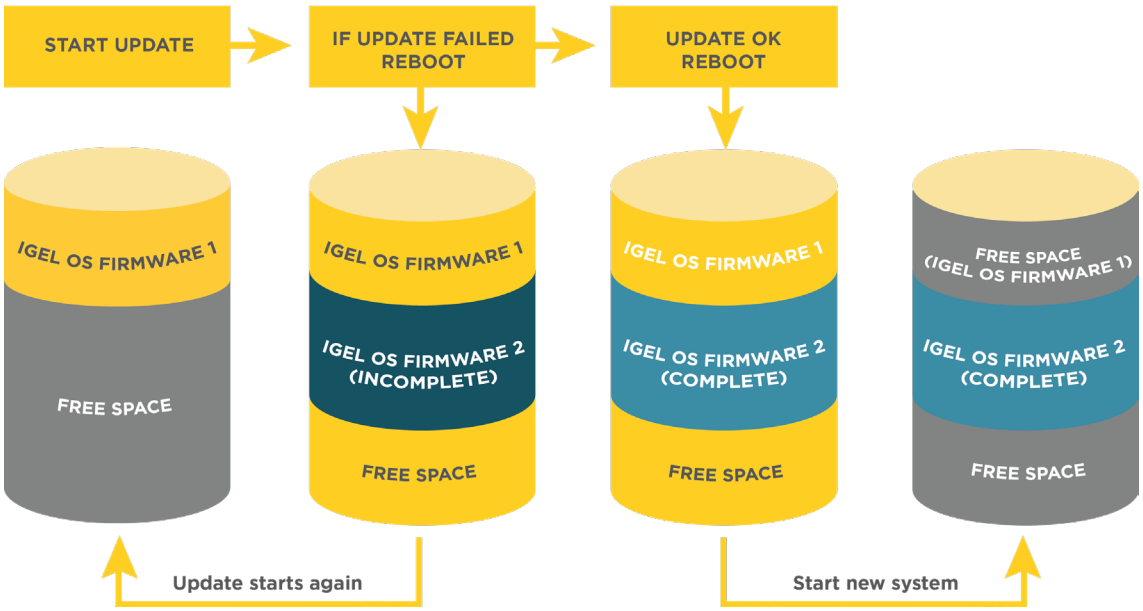
This chain makes sure that none of the components in your environment have been tampered with – a great foundation for secure end user computing.



SYSTEM INTEGRITY	CAPABILITY
Partitions confirmation checks	Hash value checks on both update and boot processes for both System and User partitions detect tampering. If positive, system will not boot. If any other partition is impacted, 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 tthat obfuscate data. Checksums of IGEL partitions avoid loading of modified code.
Protected configuration	Configuration is written to a dedicated and encrypted partition.
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 OS 10.04.100 and later. IGEL OS boots on systems with UEFI Secure Boot enabled – great for dual-booting on Windows 8 and 10 systems. • 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 • Currently on UD2, UD3, UD6, UD7 and future IGEL UD endpoints • On IGEL OS10, IGEL OS11, Windows 10 IoT • “Secure boot” mode is activated as the default value in the UEFI (BIOS) • For UD3 and UD6 endpoints only, a standard “Legacy Boot” mode can be set to boot previous IGEL OS versions • For those UD endpoints sold before this extension, a UEFI update is available on request only

SYSTEM INTEGRITY (CONT)	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 config files • Java is completely disabled • No downloads • Access Yubikey: two-factor authentication
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 (CONT)	CAPABILITY
Pre-installed SSO solutions	Smartcard support is individually adaptable using IGEL Partitions, supporting • IGEL Smartcard • **cryptas** • **SecMaker** NetID • **SafeNet** Aladdin eToken • **Elatec** TWN4 CCID • **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, supporting • PC/SC Lite • M.U.S.C.L.E. • HID OMNIKEY • REINER SCT cyberjack
Contextualizing	IGEL OS supports DeviceTrust to give control to meet governance requirements by granting access to apps and directory's depending on the access location.
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 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/support**

Revolutionary in its
Simplicity