

IGEL in Federal Government:

Modernize Government IT with a Simple, Smart, and Secure End User Computing Approach

Technology plays a central role in the missions of many U.S. government agencies, and the challenges that federal government IT teams face in delivering secure and cost-effective desktop computing infrastructure have never been greater.

Federal agencies face constant budgetary pressure to do more with less. Meanwhile, the challenges of balancing legacy technologies with new computing requirements are always growing. Adding to this challenge is the fact that security must be a central consideration at every level of the federal government IT stack.

Virtual Desktop Infrastructure and Desktop-as-a-Service in Government

Virtual desktops and applications are widely used within the government sector. Federal agencies were among the first organizations to recognize the operational efficiency and security advantages of executing desktops delivered from highly controlled data center environments using technology from vendors like Citrix, VMware, Amazon, and Microsoft.

Centralized desktop execution gives federal personnel access to the IT resources they need while avoiding storage of sensitive data on endpoint devices that are much more challenging to secure. However, virtual desktop infrastructure (VDI) requires a substantial investment in on-premises data center equipment that must also be maintained and upgraded over time. This is leading many federal IT teams to explore new cloud-based desktop-as-a-service (DaaS) approaches like Amazon WorkSpaces, which can be run in the Amazon Web Services (AWS) GovCloud infrastructure that is operated and secured to U.S. government standards.



VDI and DaaS Benefits and Challenges

In addition to limiting the distribution and storage of sensitive information, adopting VDI or DaaS can also significantly reduce federal agencies' endpoint device management complexity, cost, and risk.

Replacing Microsoft Windows on the endpoint with a lightweight and secure edge operating system can greatly reduce operational costs and security risk. It can also vastly reduce endpoint hardware costs by delaying endpoint device "refresh" cycles.

However, many efforts to deploy non-Windows endpoints encounter obstacles in demanding federal IT environments, including:

- Insufficient security controls
- Incompatibility with specialized government peripherals
- Lack of support for required authentication workflows
- Incompatibility with AWS GovCloud
- Non-compliance with U.S. trade requirements

Simplify and Secure VDI and DaaS with IGEL

IGEL combines a lightweight, software-defined endpoint operating system called IGEL OS with powerful, centralized management to enable secure, high-performance VDI or DaaS. IGEL helps federal agencies using VDI and/or DaaS to fully realize the promise of simpler and more secure access to cloud workspaces with software-defined endpoints that are:

- Simple to manage and highly scalable
- Enabled with a wide range of remote desktop protocols, including Citrix, VMware, Microsoft RDP and WVD, and Amazon WorkSpaces (PCoIP)
- Secured to U.S. government standards
- Capable of supporting a vast range of peripherals, including specialized federal peripherals and authentication workflows (SIPR Tokens/CAC/PIV/RSA)
- Developed and supported entirely in U.S. trade compliance countries (100% TAA Compliant)
- Compatible with a broad range of PC, laptop, and thin client hardware

Efficient and Reliable Management

IGEL OS was purpose-built for remote management and has a much smaller footprint than a traditional operating system. Any required firmware updates are delivered in a fast and ultra-reliable manner using an efficient "buddy update" approach that reduces the impact of bandwidth bottlenecks. This includes devices in controlled government environments, as well as remotely deployed devices, which are seamlessly provisioned and updated through the IGEL Cloud Gateway (ICG). In fact, even off-network remote endpoint devices can be securely shadowed for support and help desk purposes using the ICG technology.

IGEL Universal Management Suite (UMS) makes it simple and efficient for IT to manage up to tens of thousands of endpoints from a single console. UMS works in concert with IGEL OS to give federal IT teams precise, centralized control over how endpoints are configured and which features and customizations are available to government personnel, by policy.

Extensive VDI and DaaS Vendor Interoperability

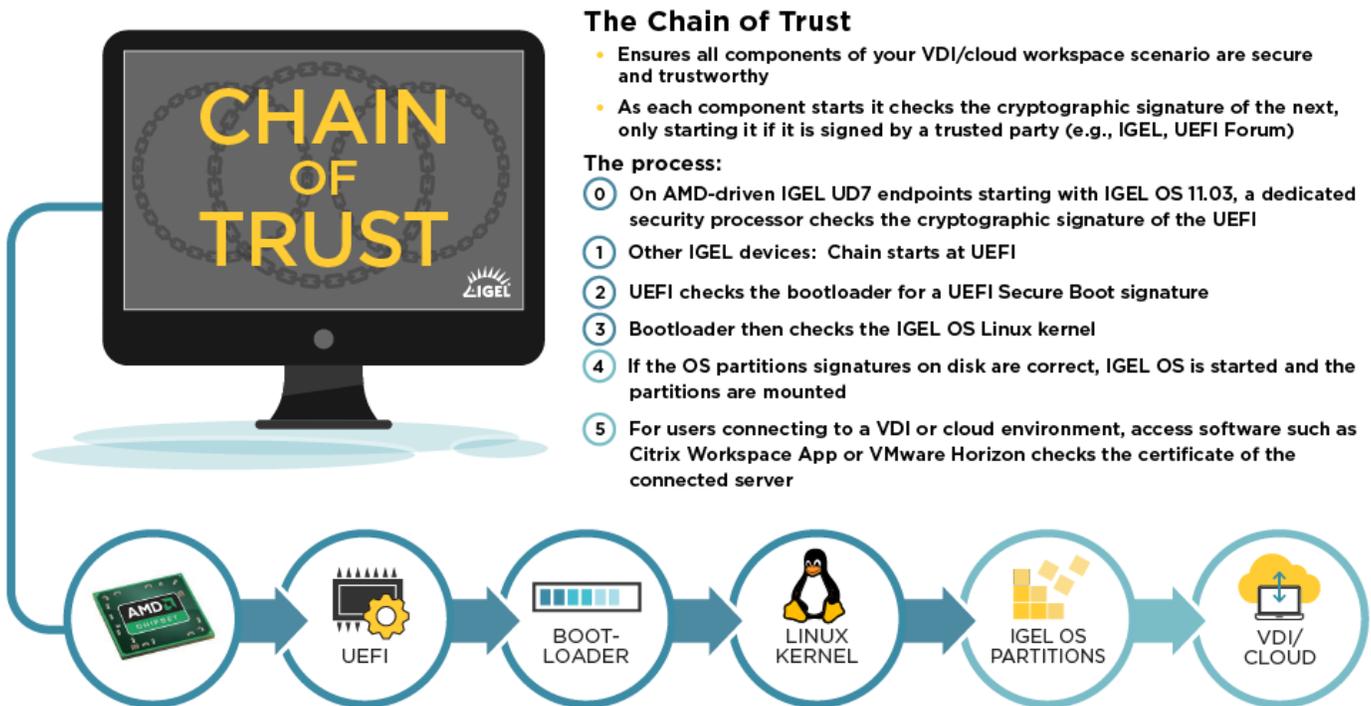
IGEL OS features over 80 integrations with desktop computing technology partners. This includes support for all major remote desktop clients, including Citrix, VMware, and Microsoft RDP/RemoteFX. IGEL OS also supports traffic offloading to the endpoint for unified communication tools like Skype for Business and Cisco Jabber (JVDI).

IGEL also partners with leading desktop performance and user experience testing and optimization technology providers, including Lakeside Software, Liquidware*, and LoginVSI*.

Secured to U.S. Government Standards

Security is central to IGEL's software design and development. This gives federal IT teams the flexibility to enable required functionality while keeping the device attack surface as small as possible.

IGEL is also unique among end user computing hardware and software providers by offering a "complete chain of trust" from the endpoint processor or UEFI process to the destination server/cloud. The complete chain of trust involves each process in sequence to check the validity of the ensuing process before it allows that next process in the chain to proceed. Consider the following diagram:



IGEL OS features integrated encryption to ensure that any information that must remain persistent across device reboots is protected. IGEL also uses the Center for Internet Security (CIS) Workbench framework to benchmark and grade IGEL OS's security.

Compatible with Specialized Peripherals and Workflows

IGEL OS supports many specialized peripherals and end-user workflows required by federal agencies. This includes Common Access Cards (CAC) with Personal Identity Verification, SIPR tokens, as well as tokens from a wide range of commercial vendors. Smart card support can be delivered through direct integration with licensed HID ActivClient middleware or using open source alternatives like OpenSC.

In addition to standard authentication, IGEL supports more advanced workflows that include multiple smart cards for access to a range of environments or segmentation of administrative privileges.

IGEL OS also includes support for specialized, security-focused peripherals such as Cherry keyboard encryption, wherein the Cherry keyboard can authenticate itself with a certificate and the key transmission is encrypted. This renders hardware key loggers useless and because the standard keyboard channel is locked, BadUSB attacks cannot be carried out on it.

*Available beginning December, 2019

Designed to Minimize Procurement Costs

IGEL's endpoint management approach is designed to help federal IT teams adopt new desktop technologies while extending the life of existing hardware. IGEL's Workspace Edition software and UD Pocket USB boot option make it easy to convert devices to IGEL OS and run IGEL OS on legacy hardware, deferring costly hardware upgrades.

IGEL's Workspace Edition software license is perpetual and hence portable, providing the flexibility to leverage past license investments on new hardware by simply reassigning them through an easy-to-use web-based portal.

Trusted in Mission Critical Environments

IGEL is deployed in some of world's most demanding government IT environments, including:



IGEL's flexible and secure approach supports specialized use cases that span both classified and unclassified networks and include a broad range of specialized hardware, peripherals, and security requirements. Custom partitions enable new specialized government interfaces and protocols to be rapidly supported by IGEL OS without necessarily waiting for the next release of the software.

U.S. Federal government installations must adhere to a variety of stringent, targeted security and data protection requirements, while still giving government workers the freedom and flexibility to work where and as they wish. This classic "push-pull" of end user freedom vs. IT control creates a dilemma for many Federal installations. As a software defined, platform-independent endpoint OS, IGEL OS has emerged as the endpoint OS of choice, given its extremely small attack surface and the ease at which it can be deployed, scaled, managed, and maintained.

For Federal government installations, the next-gen edge OS for cloud workspaces from IGEL is the best way to quickly and adaptively satisfy the needs of end users and IT staff.

Download IGEL Workspace Edition to Get Started Today

Are you looking to transform end user computing at your federal agency? [Download IGEL Workspace Edition for free](#) to experience the simplest, most cost effective, and most secure way to deliver VDI and DaaS desktops to your users.

Your IGEL Workspace Edition download will include 3 IGEL OS licenses and complete access to IGEL UMS for management, all of which are free to use for up to 90 days.

Visit us online at igel.com

Revolutionary in its
Simplicity