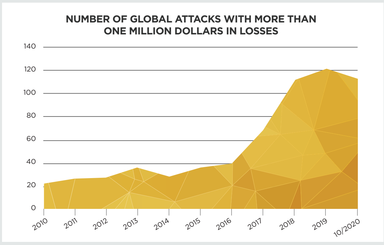
TRANSFORM AND SECURE GOVERNMENT ENDPOINT DEVICES WITH IGEL

Providing complete security while under constant budgetary pressure is the biggest challenge for publicly funded IT teams.

Risks Increase and Losses Grow

Crippling cyber-attacks on government agencies, defense, and high-tech companies are on the rise.



https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Major Challenges in Government IT

- Adhere to special, stringent security requirements
- Budget pressure
- Aging hardware
- E-government projects
- Disaster recovery

- Identity & access management
- Optimal workspace performance and flawless user experience
- Unstable/inconsistent data access
- Increasing security threats, including cyber attacks

Extend the Life of Existing Hardware

IGEL helps government agencies to extend the life of existing PCs, minimizing capital and operational expenses to free up budget for critical/highly visible projects.

- Convert and optimize most x86-64 devices to IGEL OS quickly and easily
- Boot legacy and unmanaged devices to a secure, managed workspace with UD Pocket

This helps government agencies move quickly and save money by deferring large hardware investments until they are truly necessary.

IGEL helps simplify and secure endpoints within government environments

1. BENEFIT FROM A SECURE, TRUSTED OS
A read-only, modular OS keeps endpoints as lean as possible and minimizes the attack surface of the device.

2. SHIFT WINDOWS FROM ENDPOINTS TO THE DATA CENTER OR CLOUD
Moving Windows from endpoints to the data center or cloud simplifies management and keeps data centralized for better security.

3. MANAGE AND MONITOR ALL ENDPOINTS WITH A SMALL TEAM
The IGEL Universal Management Suite (UMS) offers support for up to 300,000 endpoint devices from a single console.

4. EXECUTE ENDPOINT UPDATES FASTER AND MORE RELIABLY
The UMS and IGEL Cloud Gateway (ICG) make updates secure, fast and ultra-reliable, including a unique "buddy update" feature that speeds updates and conserves bandwidth from office, branch, or home.

5. DELIVER SIMPLE AND EFFICIENT REMOTE SUPPORT
Secure shadowing enables technical support teams to assist users no matter where they are — on the government/agency LAN, off-network, or anywhere else.

6. USE AN IP-BASED CRYPTOSYSTEM
IGEL OS supports 3rd party technology that is approved for processing classified information up to and including SECRET, NATO SECRET, and SECRET UE/EU SECRET.

Advance Security and Compliance Efforts

Moving Windows workspaces and storage to the data center or cloud delivers immediate security and compliance benefits for the government. IGEL extends this added assurance to endpoints by creating a complete "chain of trust" from device boot to cloud workspace execution.

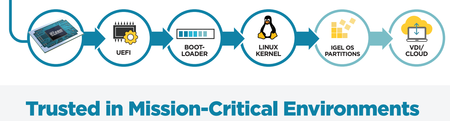
THE IGEL CHAIN OF TRUST

- 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. Any UEFI supported devices* with IGEL OS: 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 the certificate of the connected server

*with UEFI Secure Boot deactivated the process starts at bootloader (3)



Trusted in Mission-Critical Environments

IGEL is deployed in some of the most demanding government IT environments in the U.S.

IGEL IS THE SIMPLE, SMART, AND SECURE WAY FOR ALL GOVERNMENT INSTITUTIONS TO PROTECT, MANAGE, AND CONTROL ENDPOINTS.

TO LEARN MORE OR REQUEST A FREE TRIAL, VISIT IGEL.COM

IGEL
next-gen EDGE OS
for cloud workspaces