APP NOTE

RAPIDLY REGAIN CONTROL WHEN A CYBERATTACK STRIKES WITH THE IGEL UD POCKET

Approximately 37% of global organizations said they were the victim of some form of ransomware attack in 2021, according to IDC's 2021 Ransomware Study. In recent years the headlines of ransomware attacks wreaking havoc on critical infrastructure, governments, and business have unfortunately surged, with healthcare providers being a prime target. The frequency and sophistication of attack vectors like malware, phishing, and the scale of ransom amounts have been unprecedented, with no sign of abating. Cyberattacks can render essential services and processes at a standstill, resulting in financial loss, multi-million dollar ransoms, and potential loss of critical or sensitive data. A comprehensive disaster recovery plan is critical to ensure business continuity when your organization has been impacted.

The extent of attacks shows us even organizations with a comprehensive multi-layered security strategy can be affected, presenting the unnerving realization that every organization is at risk. Those organizations running Windows "fat clients" on their endpoints are especially vulnerable, as they require frequent and time-consuming patching and updates which only increase their risk. This and the global acceleration to hybrid work, have created the perfect storm for opportunistic cyber criminals to unleash a torrent of malware attacks. **Watch the IGEL OS Security video**

IN THE EYE OF A CYBER CYCLONE, A RAPID RESPONSE IS CRITICAL

IGEL OS is the managed operating system for secure access to any digital workspace

IGEL is helping IT administrators regain control of affected devices by providing employees with secure and managed access to company apps, data and desktops from ***any*** device, from anywhere, to restore productivity amidst a security episode - even from endpoints directly struck down by a cyber attack.

Devices infected with malware can boot IGEL OS from USB with IGEL UD Pocket . As IGEL OS is read-only and tamper-proof the firmware files are encrypted and reside in a separate partition, hence are inaccessible by exisitng malware. IGEL OS features a "chain of trust" sequence of cryptographic signature verifications starting with UEFI secure boot, extending all the way to the VDI host or cloud. This is verified with each boot up process to ensure the IGEL firmware and software in the startup sequence has not been tampered with.

REGAIN CONTROL WITH THE IGEL UD POCKET

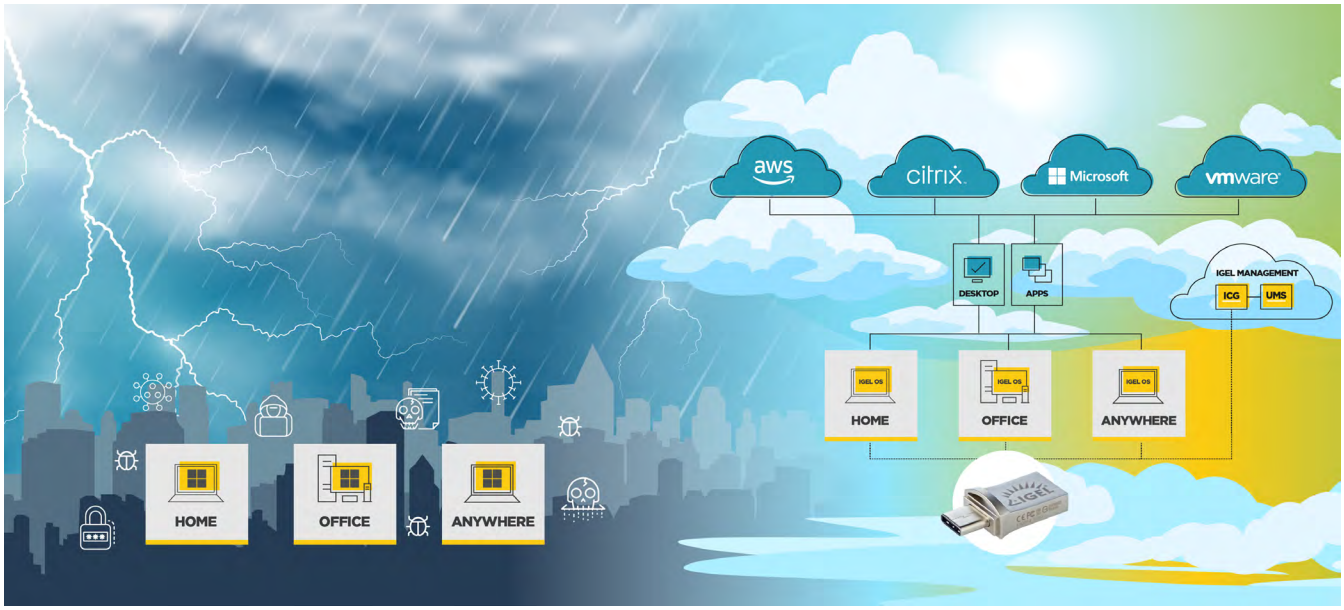
Transform any device into a secure company workspace

The IGEL UD Pocket, a small USB stick, enables an employee to temporarily turn their device of choice into a secure, managed workspace. Simply insert the IGEL UD Pocket into a USB-A or a USB-C port and boot from USB to IGEL OS to access your organization's Citrix, VMware, Microsoft AVD, or cloud environment. The UD Pocket can boot IGEL OS on any x86-64 device from any vendor, the most popular with IGEL customers being HP, LG, Lenovo, and Dell.

Learn how the IGEL UD Pocket helped a healthcare provider restore control amidst a malware attack

Regain control of remote devices and digital workspaces, even infected endpoints

In todays' world of hybrid work, disaster recovery plans demand powerful management of remote, "off-network" endpoints. The IT Administrator can deploy and control the IGEL OS devices from a single console with the IGEL Universal Management Suite (UMS). The IGEL Cloud Gateway (ICG) feature extends the management console reach by creating a secure, encrypted connection to each remote user device, without VPNs.



The calm after the storm

IGEL OS is a secure, read-only operating system, providing the employee an alternative to the infected OS they had been using. The UD Pocket runs the IGEL OS operating system directly from the USB device, so that the local, contaminated operating system, hard disk, and contents are not accessed or used. This complete separation of the local operating system and the IGEL OS makes the UD Pocket a powerful tool to restore productivity amidst a security episode. Once the episode has been resolved the UD Pocket can be unplugged, and the device reverts to the original operating system.

YOUR SAFE HARBOUR IN TURBULENT TIMES

Expert resources to accelerate deployment of your IGEL Disaster Recovery solution.

Premier Technical Relationship Manager (TRM)
An IT expert that understands your business and proactively helps you leverage IGEL UD Pocket, UMS and ICG in your environment to rapidly regain control of endpoint devices.

IGEL Academy offers focused, self-paced eLearning programs to equip IT admins with the know-how to leverage the full capabilities of IGEL OS and management console.

CONTACT IGEL DISASTER RECOVERY FOR MORE DETAILS

REQUEST A DEMO
IGEL.COM/DISASTER-RECOVERY/