SOLUTION BRIEF

TURN USER ENDPOINT DEVICES INTO RANSOMWARE NON-TARGETS

Help Prevent Ransomware Attacks with IGEL OS

Hybrid working – the practice of working in the office, at home, elsewhere, or any combination, is here to stay. The flexibility it offers is a life buoy to many businesses and employees, especially during times of disruption. However, widespread remote work creates many challenges for IT security teams as the frequency and sophistication of ransomware attacks have reached an unprecendented scale. 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.

According to a recent analysis by international law firm RPC, the number of ransomware attacks reported to the UK's Information Commissioner's Office more than doubled between 2020 and 2021. The industry sectors that were most frequently impacted by attacks in 2021 were finance, insurance and credit, education and childcare, and those sectors privy to sensitive financial and personal data.

To mitigate the increased exposure to cyber risks, IT teams must act swiftly to safeguard the most vulnerable point in the network – the user device. Experts recommend a "defense in depth" strategy, or multi-layered approach of physical, technical, and administrative controls to safeguard a business from ransomware and malware threats. Throughout this brief we will take a closer look at various types of malware and learn how **IGEL OS and its ecosystem of integrated technologies** can help your people to have a protected and productive workday, every day, from anywhere.

END-USER EXPERIENCE IS THE KEY TO YOUR SECURITY LOCK!

The era of hybrid working is here and now. Providing a workspace that is easy to use, with instant and secure access to company apps and data, helps employees collaborate and work productively. Advanced capabilities are essential for IT teams to provide a productive workspace from any device or location. This will prevent employees getting frustrated, taking shortcuts, or seeking workarounds to access the content they need which can compromise security. IGEL OS is the managed endpoint operating system for secure access to any digital workspace. It is secure by design with a set of proactive security features, IGEL OS is helping to protect against ransomware attacks in business and organizations in healthcare, finance, retail, and government.

Malware is a contraction for "malicious software", and comes in many forms, each posing their own specific threats. Ransomware in particular has emerged as a uniquely insidious type given that it can bring a company to its knees operationally (think of a healthcare system) while extracting huge sums of money to simply return things back to normal. The most common types of malware that have infected the most organizations over the past decade include:

Phishing: a common method of cyber-attack that is successful since the emails sent, text messages and web links created look like they're from trusted sources. They're sent by criminals to fraudulently acquire personal and financial information.

Worms: are spread via software vulnerabilities or phishing attacks. Once a worm has installed itself into your computer's memory, it starts to infect the whole machine and in some cases... your whole network.

Viruses: Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus is able to replicate itself and spread through your systems.

Bots and Botnets: A bot is a computer that's been infected with malware so it can be controlled remotely by a hacker. That bot (or zombie computer), can then be used to launch more attacks or to become part of a collection of bots (aka a botnet). Botnets are popular with hacker show-offs (the more bots you collect, the mightier a hacker you are) and cyber criminals spreading ransomware. Botnets can include millions of devices as they spread undetected.

Trojan Horses: Just as it sounds, a Trojan Horse is a malicious program that disguises itself as a legitimate file. Because it looks trustworthy, users download it, and the enemy is unleashed. Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once you've got the Trojan on your device, hackers can use it to delete, modify, and capture data; harvest your device as part of a botnet; spy on your device; or gain access to your network.

Spyware: secretly records your online activity, harvesting your data and collecting personal information such as usernames, passwords, and surfing habits. It is usually distributed as freeware or shareware that has an appealing function on the front end with a covert mission running in the background that you might never notice. It's often used to carry out identity theft and credit card fraud. Once on your computer, spyware relays your data to advertisers or cyber criminals. Some spyware installs additional malware that make changes to your settings.

Ransomware: is a form of attack that denies or restricts access to your own files. It then demands payment (usually with crypto currencies) in return for letting you back in. The payments demanded are often in the multiple millions of dollars.

HOW IGEL OS HELPS TURN YOUR ENDPOINT DEVICE INTO A NON-TARGET

IGEL OS is built for VDI, DaaS, and digital workspaces, and helps protect your end-users' devices by making them both difficult and unappealing to target for hackers, through an array of integrated security capabilities within the IGEL OS operating system and management console. In essence, IGEL OS helps turn all your endpoints into "malware non-targets".

"IGEL OS has improved the stability of our endpoints, enabled secure access to cloud workspaces for our clinicians and staff members, and streamlined Windows patching and management, which we estimate will lead to $2 million in savings for our organization over the next three years."

- Kevin Conable, Director, IT Infrastructure at Kaleida Health

GAIN CONTROL - NO DATA STORED ON THE ENDPOINT DEVICE

No data is stored on the IGEL OS device – even if the user is working on their own PC or Notebook, all data is stored in the secure cloud or datacenter and not on the user's private hardware. Using VDI or desktop as a service (DaaS) to deliver applications, IT services, and even Windows desktops reduces the value to hackers of the already tiny attack surface on the device. IGEL works closely with Citrix, Microsoft Azure Virtual Desktop, VMware, and AWS to quickly integrate the latest clients and protocols (in some cases, on Day One) for virtual and cloud workspaces.

A RANSOMWARE NON-TARGET - IGEL OS HAS BUILT-IN AND PROACTIVE SECURITY

IGEL OS is read-only and tamper-proof

IGEL OS firmware files are encrypted and reside in a separate partition to ensure the OS cannot be tampered with or modified by malicious apps or extensions, making it inaccessible by ransomware.

IGEL OS is modular

This allows the IT Administrator to easily manage each endpoint device by removing unnecessary feature partitions. Only required features, apps and data can be visible by the user on a specific device.

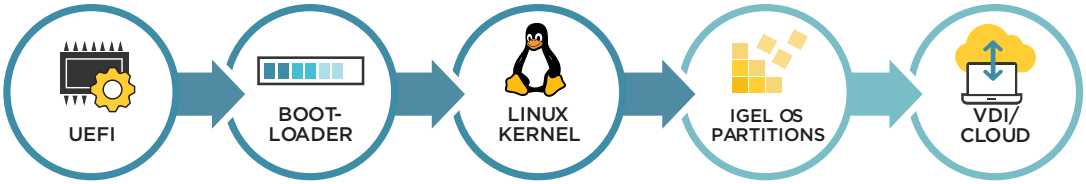
IGEL OS has a small attack surface

IGEL OS is designed and purpose-built for VDI, DaaS, and digital workspaces. It's tiny firmware "footprint" makes it very lightweight and efficient. In addition, any unnecessary features can be switched off, and no business data is stored on the device for hackers to target. Essentially, there is very little on an IGEL OS-powered device for hackers to target, with nothing of value on the device in return for their efforts.

A dedicated security team

Security is at the core of IGEL OS development, with a focus on security features and integrated capabilities. To offer a further layer of protection, pre-installed multi-factor authentication and single sign-on technology integrations support access control via integrated PKCS11 libraries that support the use of popular smart card readers and biometric solutions.

IGEL Chain of Trust and Secure Boot



IGEL OS features a **"chain of trust"** for end-to-end system integrity that is verified with each boot up process. A sequence of cryptographic signature verifications start with UEFI secure boot and extends all the way to the digital workspace VDI host or cloud. The chain of trust thus ensures that every time the IGEL OS-powered device boots, none of the firmware and software in the startup sequence have been tampered with. If indeed the chain of trust detects a failure condition at any step, the end-user is alerted, and IT can take appropriate action.

UNIFY AND CONTROL THE ENDPOINT DEVICES YOU ALREADY OWN

With IGEL, enabling secure and controlled access to essential apps, desktops and data from personal PCs and laptops is quick and easy to deploy, even remotely.

Take the endpoint device out of the security equation by standardizing the operating system with IGEL OS on the devices you already have. Any compatible x86-64 device - PCs, laptops, and thin clients from **HP, LG, Lenovo, Dynabook, OnLogic and other popular vendors** can be transformed in to a IGEL OS-powered endpoint.

DON'T MISS A BEAT - SIMPLIFY MANAGEMENT AND CONTROL OF ALL ENDPOINT DEVICES

Automated Updates at scale

With IGEL OS, security updates are deployed quickly and reliably via IGEL's management console. Even in areas of variable bandwidth, and up to 300,000 devices with advanced capabilities. Move Windows to the data center or cloud where it is much easier to secure, patch and protect. Automating this update process reduces the burden on IT staff and protects user endpoint devices from threats.

Granular Access and control Policies

IT can define user groups based on role, location, or any contextual policy. IT can also set user profiles with features and capabilities they need on their device, manage USB port permissions, and control access to applications. All of this can be linked to Active Directory and managed remotely via the IGEL management console.

Easy and secure remote management of devices

Manage and securely monitor remote devices, without VPNs, from a single console with the IGEL Universal Management Suite. Today's hybrid work environment demands powerful management of remote, "off-network" endpoints. The IGEL Cloud Gateway (ICG) feature extends the management console reach by creating a secure, encrypted connection to each remote user device.

Secure Shadowing for Helpdesk

The ICG enables IT and helpdesk teams to securely shadow a remote device for troubleshooting purposes. For example, a helpdesk engineer can take over the endpoint device's keyboard and mouse.

RAPID DISASTER RECOVERY WITH IGEL UD POCKET

The IGEL UD Pocket, a small USB device, is essentially "IGEL OS on a stick" that can temporarily turn any compatible x86-64 device into an IGEL OS-powered end-point – simply insert the UD Pocket into a USB port and boot IGEL OS. This makes it a great solution for disaster recovery scenarios where people need to quickly access their work environment from any available computer, like their home PC for example.

WATCH THE VIDEO OF HOW AN INTERNATIONAL INSURANCE COMPANY USED UD POCKET FOR BUSINESS CONTINUITY

REQUEST A SECURITY DEMO
IGEL.COM/SECURITY-AT-THE-EDGE