Who Done IT
RANSOMWARE CHALLENGE

INFO SHEET

SECURING THE EDGE WITH IGEL.

Enterprise Edge Security Challenges and How IGEL Addresses Them

IGEL OS, the next-gen edge OS for cloud workspaces, has earned a strong reputation for its simple, smart, and secure approach to end user computing and cloud workspaces. While security must be aggressively addressed throughout an enterprise's IT architecture from the innermost hardware and software in the data center or cloud out to each end-user's fingertips, replacing Windows or any other operating system on user endpoint devices with IGEL OS can vastly simplify and streamline the task of securing any organization's endpoints.

Today, companies are facing more security-related challenges at the edge – the most vulnerable point in the network – as multiple forces combine to create a "perfect storm" of potential endpoint threats that need to be addressed. Some of these are classic challenges that have existed literally for decades, and others are relatively new. In no particular order, these challenges include:

- **Work from home**
- **Advanced malware including ransomware**
- **Endpoint device OS and application software patching**
- **Increasing user experience expectations**

WORK FROM HOME

The COVID-19 pandemic has become an unfortunate fact of life around the world, sparing no country, business, or person in how they conduct their everyday routines, operations, and behaviours. For businesses, the pandemic ignited the need starting in March of 2020 to quickly move employees from their office or primary workplace to their homes. The work-from-home (WFH) movement had started long before the arrival of the pandemic and was gradually increasing, but COVID-19 turned WFH into an immediate need in order to preserve business continuity. Now that the "emergency" phase of WFH has come and gone, many organizations have decided to let many if not most of their people continue to work from home – either completely or partially – indefinitely, regardless of when it's deemed safe for people to return to the office.

While WFH is proving to offer newfound end-user freedom while saving money and helping reduce carbon emissions, it creates a new strain on company security. Managing and controlling company policies and permissions across a widely dispersed workforce can be difficult, and people working from home oftentimes prefer to use their endpoint device of choice, which may or may not be a company-issued device. Since most user devices may now be "off network" (no longer configured on the company LAN), it can be difficult to maintain the same level of insight and maintenance/support on those endpoints without nailing up an expensive VPN connection to each user's home. So, from the perspectives of end-user device management, control, support, troubleshooting and cost, the surging WFH phenomenon is creating some new headaches for IT organizations.

ADVANCED MALWARE INCLUDING RANSOMWARE

Malware has been a constant challenge for organizations for decades and it shows no signs of slowing down. The constant game of cat-and-mouse between malicious hackers and anti-malware software developers is an epic battle that never ceases. As anti-malware software gets more sophisticated (e.g., behaviour tracking and pattern matching in addition to anti-virus signature detection, etc.), so too does the malware itself. A particular recurring menace for organizations is ransomware, where malicious software invades an organization's IT infrastructure or storage and compromises data that can only be made accessible to the organization again upon payment of a ransom, oftentimes in the millions of dollars. Given that user endpoint devices are the most common entry point for malicious software including ransomware, organizations with hundreds, thousands, or many thousands of user endpoint devices face the possibility of a "headline grabbing" attack literally every day.

ENDPOINT DEVICE OS AND APPLICATION SOFTWARE PATCHING

By now most of us who are using Windows on our endpoint device understand that software patches and updates are common. Let's face it – any software at some point needs to be updated, but updating and patching the operating system on a user device, especially Windows 10, is disruptive for both the end-user and the IT team who needs to schedule those updates. Since almost every OS update includes multiple security-related fixes, the need for timely, recurring updates is critical.

But these end-user device updates and patches come at a cost. End-user frustration can build quickly while the update and patching process takes place, oftentimes with at least one or more system restarts. For many of us, this signifies the time to grab a coffee or maybe run an errand. And if for some reason the update or patch does not complete successfully, the end result is a more vulnerable device and then yet another update process. The IT organization needs to not only schedule these patches (traditionally on "patch Tuesday"), but it needs to make sure the right software gets updated on the right endpoint devices based on company policies and permissions per end-user role within the company. For organizations with hundreds or many thousands of endpoints, updating and patching is a tedious, time consuming, and error-prone (unfortunate) fact of life that involves multiple potential security exposures.

INCREASING USER EXPERIENCE EXPECTATIONS

Work-from-home and end-user mobility have changed how people work, but their expectation of an immersive, high-fidelity user experience on their endpoint has not changed. In fact, it has only elevated as people spend more time than ever in computing and collaborating via multimedia experiences. Whether it's viewing a training, technical, or sales video, attending a virtual event, or meeting remotely with teammates via a unified communications tool like Microsoft Teams, Zoom, WebEx, or GoToMeeting, people are expecting a high-quality experience devoid of audio "hiccups", video jitter, or any other form of poor quality that hinders the experience.

It's clear that the freedom end-users enjoy from the new work-from-anywhere model comes with greater expectations that place even more of a burden on IT teams who may have to deal with company-issued or personal endpoint devices that may lack needed processing power or memory, or off-network challenges like sub-optimal bandwidth or "last mile" limitations to the users' homes. Keeping end-users happy while making sure their endpoint devices are secure and fully controlled by the enterprise creates an IT dilemma: how to attain and maintain one of these crucial goals without negatively impacting the other.

THE ENDPOINT DEVICE SOLUTION: START WITH THE OS

Step 1 in helping address the primary challenges mentioned above is to move Windows to the secure data center or cloud and use an endpoint operating system designed specifically for easy and secure access to cloud workspaces – IGEL OS. Linux-based and featuring a small "footprint" with a modular design for minimal attack surface, and read-only to prevent tampering with the firmware, IGEL OS can dramatically decrease the time and effort needed to protect your network edge.

IGEL OS itself is extremely difficult for attackers to target, and it features a "chain of trust", a sequence of cryptographic signature verifications that starts on the device system-on-chip (SoC) on select IGEL endpoint models or the UEFI for other devices and extends all the way to the cloud workspace VDI host or cloud. The chain of trust thus ensures that every time the IGEL OS-powered device boots, none of the key process firmware and software in the startup sequence has been altered. If indeed the chain of trust detects a failure condition at any step, the end-user is alerted, and IT can take appropriate action.

IGEL OS can run on any compatible x86-64 device with a 1GHz processor and at least 2GB of RAM. Since it is platform-independent software, it serves as a great way to unify endpoint devices like PCs, laptops, and thin clients from Dell, HP, Lenovo, and other device vendors, including IGEL endpoints, onto a single endpoint OS platform.

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

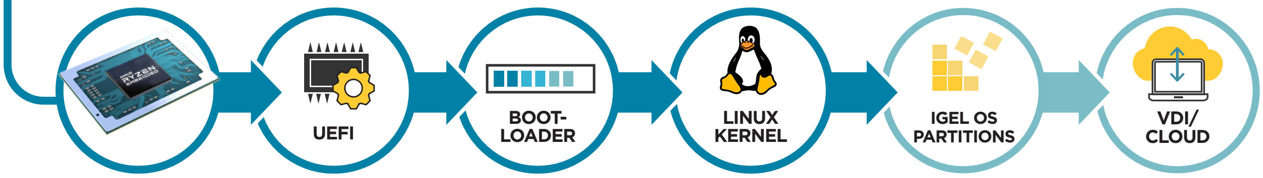
2 UEFI checks the bootloader for a UEFI Secure Boot signature

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)



IGEL OS can also be accessed via a thumbnail-size USB pluggable device called the UD Pocket, which is essentially "IGEL OS on a USB stick". The beauty of the UD Pocket from an ease-of-use and security standpoint is that it can be plugged into any compatible device, including a user's personal (non-work) PC or laptop, and once booted from the UD Pocket USB port, that device becomes the user's IGEL OS-powered work device with their familiar work cloud workspace and apps. IGEL OS is stood up in a fully secure, separate environment to provide the user's work environment and nothing else, with all data stored in the secure cloud. It's the perfect solution for at-home/remote user freedom (including device of choice) while the company retains full management and control of that user's endpoint while IGEL OS is running.

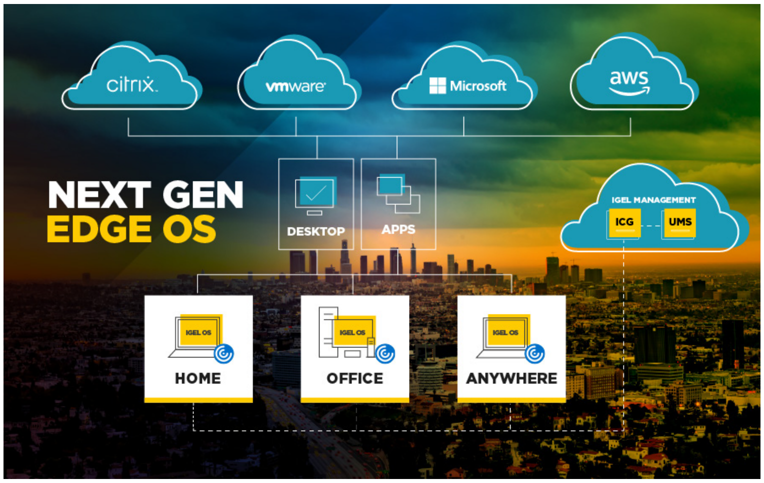
When the UD Pocket is unplugged, the user's personal device goes back to its standard operating system and configuration.

ENDPOINT MANAGEMENT AND CONTROL THAT IS SECURE BY DESIGN

Given the inherent security and minimal attack surface of IGEL OS and its chain of trust, IT teams can be confident that their widely dispersed work-from-home workforce is using an endpoint OS they can trust. But it goes beyond just the OS. It is how IGEL OS-powered endpoints are managed and controlled by the IGEL Universal Management Suite (UMS) software. UMS profiles can be linked to Active Directory, and end-user policies and permissions can be easily set up on the UMS console. Either way, whether there are hundreds or tens of thousands of endpoint devices, it is easy for a UMS console administrator to ensure that every IGEL OS-powered user endpoint device is configured with the correct IGEL OS image for each end-user. Since IGEL OS is modular, this means that some users will have "less IGEL OS" running on their endpoint than others which ensures a minimal OS footprint and attack target on each device.

It is from the UMS where IGEL OS-powered endpoints get updated with the latest IGEL OS version. IGEL OS firmware updates and patches are miniscule in terms of size and frequency compared with Windows 10 updates and patches, and are distributed by a network-friendly "buddy update" technique to accelerate the process and minimize bandwidth consumption. IGEL OS updates between the UMS and the updated endpoints are secure, as they are cryptographically signed and validated by IGEL OS before getting loaded onto the target endpoint(s). With IGEL OS and the UMS, IT teams can finally say good-bye to the tedium, scheduling, and cost burden of updating endpoint devices. Since IGEL reduces the frequency of patching, centralizes patch distribution, and makes the patch process almost invisible to the end-user, Missy couldn't have "missed" patch Tuesday and left her device vulnerable.

But what about the hundreds or thousands of end-users who may be located outside the company LAN, "off network" so to speak, working from home for example? For management and control of those dispersed, remote endpoints, the IGEL Cloud Gateway (ICG) feature works in unison with the UMS to create a secure, encrypted connection to each remote user device to enable full management and control from the UMS console, just as if that device was located back on campus or in the office. The ICG does not require any VPN service or connection, and it even enables IT and helpdesk personnel to securely shadow a remote or WFH endpoint.



FINALLY, TAKE YOUR ENDPOINTS OUT OF YOUR SECURITY EQUATION!

CSOs, CIOs, and IT directors are currently facing a "perfect storm" of simultaneous challenges when it comes to addressing enterprise-wide security threats. Work-from-home, malware and ransomware, software updates and patches, and ever-increasing end-user experience demands all pose their own unique set of challenges. And the network edge remains the most vulnerable and most popular point of attack for cyber criminals. Fortunately, IGEL can offer immediate help across all your endpoint devices, whether hundreds or tens of thousands, with IGEL OS via download or the UD Pocket, the IGEL UMS, and the IGEL Cloud Gateway.

Imagine not having to worry about the security profile or vulnerability of your end-users' endpoint devices across your enterprise, no matter how many devices there may be (up to 300,000) or where they may be located. Imagine eliminating the costly, time-consuming Windows updating and patching process from all of those endpoints. Think of how effective you can be thwarting potential malware attacks when you can focus on one place – the data center or cloud – instead of many hundreds or thousands of device locations. And finally, imagine all of your users, enjoying productive, fulfilling work experiences on their devices of choice without you – or them – being impacted by application and anti-virus software "overkill". It's all possible. With the next-gen edge OS for cloud workspaces.

IGEL | Who Done IT
RANSOMWARE CHALLENGE

DON'T LET THE CASE GO COLD! MISSY IS NO LONGER A SUSPECT - GET BACK IN THE GAME TO WIN A FREE APPLE AIRTAG: www.IGELWhoDoneIT.com