

**R-Com  
Intellegence  
Briefing**



The **IGEL** Dossier

# Inside the Operating System Trusted by the Military

*Restricted Access*



**r-com**  
consulting

# INSIDE THE SECRET OS

---

As an IGEL partner, we've worked alongside their technology for years - but after a recent briefing, where we sat down with their team we realised we didn't. What we heard felt more like a classified briefing. Some of it we can't repeat. What we can is here. This dossier was created to share what we learned, and what we're allowed to tell you.

You probably haven't heard of IGEL OS. That isn't a coincidence. The organisations using it don't talk about it, and for good reason. It's embedded in some of the most sensitive systems on earth - government networks, defence operations, hospitals, and major financial institutions. The places that simply can't afford to fail.

When the CrowdStrike update took down hospitals and grounded flights across the world, the systems running IGEL didn't even flinch. They stayed up, carried on, and quietly proved a point most people missed.

Now, some of the largest casino groups on the planet - organisations that run on 24-hour uptime and attract constant cyber attention are moving to IGEL too. They've seen what happens when you rely on luck, and they know this is the only system that holds.

***The people using IGEL aren't chasing innovation. They're trying to survive it.***





# IT AND OT ARE CONVERGING

For decades, IT and operational technology (OT) lived in separate worlds - and for good reason.

OT often runs air-gapped, isolated systems that control the things that can't ever go down: hospital scanners, factory floors, water treatment, power distribution and of course IT looks after everything else.

***But with IGEL those boundaries are dissolving. Perhaps completely.***

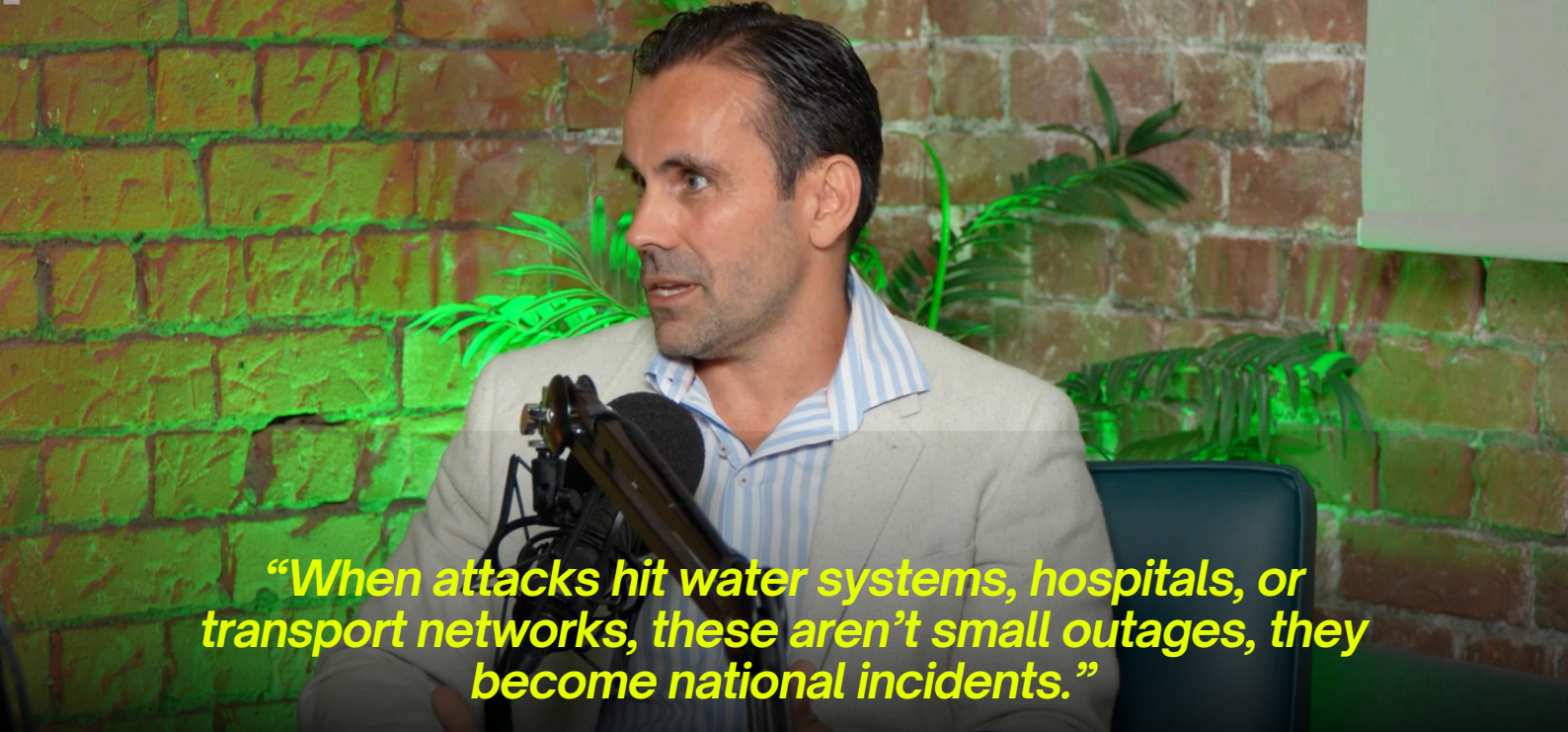
Digital transformation, remote monitoring, compliance pressures all are forcing OT to connect to corporate networks for the first time. And that's where the risk begins.

When you bring decades-old machinery online, you expose systems that were never built to be patched, updated, or secured.

When you bring decades-old machinery online, you expose systems that were never built to be patched, updated, or secured.

***You can't replace them.  
You can't shut them down.  
But you can't afford to leave them open either.***



A man with short dark hair, wearing a light blue striped shirt and a grey blazer, is seated and speaking into a professional microphone. He is positioned in front of a rustic brick wall. To his right, there is a green fern plant. The scene is lit with a warm, slightly greenish light.

***“When attacks hit water systems, hospitals, or transport networks, these aren’t small outages, they become national incidents.”***

***-Justin Thorogood, IGEL***

That’s why IGEL developed its **Managed Hypervisor**, in collaboration with Audi to create a secure layer between IT and OT.

It allows legacy, air-gapped devices to operate within modern infrastructures without ever being directly exposed to the network.

This is what’s keeping factories, power stations, and hospitals connected - without making them vulnerable.





# IGEL MANAGED HYPERVISOR

*Containing the Past to Protect the Future*



***Built with German precision. Secured by design.***

The IGEL Managed Hypervisor was developed in collaboration with a leading German automotive manufacturer that needed to keep legacy workloads alive without compromising security. The challenge was clear: production systems, diagnostic tools and control software that were too critical to retire but too old to defend.

The result was a new class of endpoint virtualisation. The IGEL Managed Hypervisor runs directly on the device, creating a secure and centrally managed environment where legacy applications continue to operate safely on modern hardware. It is a lightweight Type 1 hypervisor that removes dependency on the original operating system while maintaining full performance and offline capability.

This is not cloud or VDI. There is no migration, no hidden dependency on network uptime and no loss of control. The workload stays local, contained and managed through IGEL's Universal Management Suite alongside every other endpoint.



# IGEL MANAGED HYPERVISOR

*Containing the Past to Protect the Future*



***Legacy app, secured inside IMH***

In healthcare that can mean a radiology system running securely in isolation. In manufacturing, a control interface that remains live but protected from corporate risk. In finance, trading software that stays compliant without costly rebuilds.



Developed out of necessity, the IGEL Managed Hypervisor has become the quiet future of legacy system protection. It is a solution built for the real world, where replacement is not always possible but security must still be absolute.





# THE BACKUP PLAN THEY DON'T TELL YOU ABOUT

---



Every few months, it's the same headlines, hospitals shut down, airlines grounded, entire companies frozen by a single update gone wrong.

**And every time, it's treated like there was no way around it.**

**That's a lie.**

Most organisations won't move away from Microsoft. They don't have to. But they also don't have to keep gambling on it being secure...

That's why IGEL built **Business Continuity** not to replace Windows, but to protect it. The **Dual Boot system** creates a clean, secure IGEL partition that sits beside your Windows environment. When the worst happens - ransomware, bad patch, failed update, you reboot into IGEL OS and carry on working while IT repairs Windows in the background.

And when the damage runs deeper, or if you need a baby step in the right direction? there's UD Pocket (insiders call it IGEL CANDY) a secure USB loaded with IGEL OS. Plug it in and boot from it, and your machine becomes a fully managed, compliant endpoint in seconds.

***These global meltdowns don't have to happen.  
There's already a way out, most people just  
don't know it yet.***



# BUSINESS CONTINUITY

## *Dual Boot and UD Pocket, Resilience in Motion*



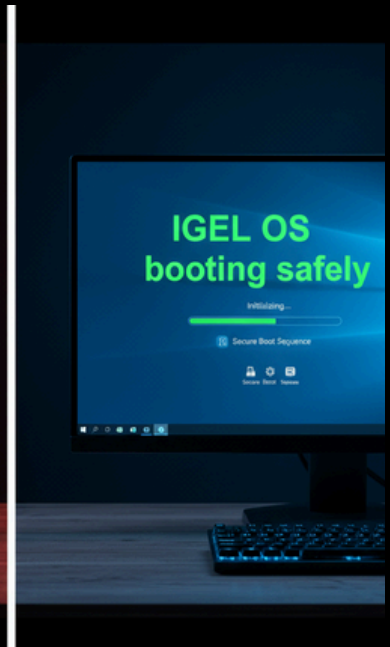
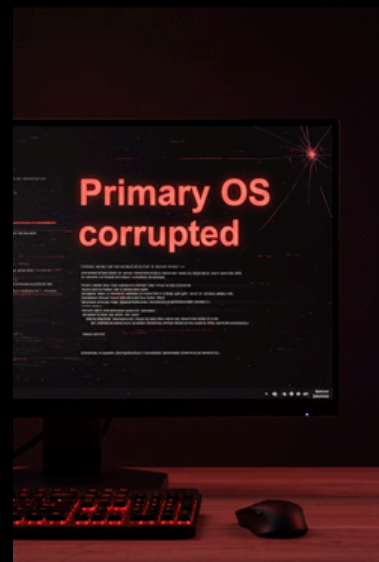
***When others go dark, this stays on.***



When disaster strikes, most organisations realise too late that resilience was never built into their endpoints. IGEL's Business Continuity solutions Dual Boot and UD Pocket were created to make recovery immediate, portable and predictable.

### ***Dual Boot: Two systems, one failsafe.***

The IGEL Dual Boot configuration installs a secondary secure IGEL OS alongside the existing operating system. If the primary OS fails due to ransomware, corruption or an update meltdown, devices can switch instantly into IGEL mode and restore full access to virtual desktops, SaaS apps or cloud workspaces within minutes.





# BUSINESS CONTINUITY

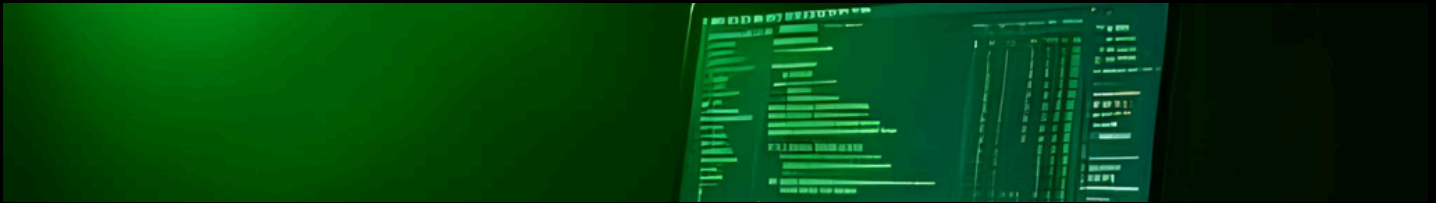
---

## *Dual Boot and UD Pocket, Resilience in Motion*

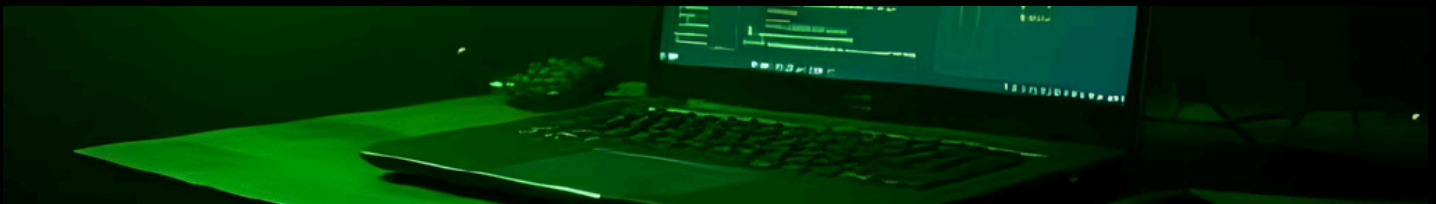


### **UD Pocket: The OS on your keyring.**

The UD Pocket is a bootable USB device that turns any compatible machine into a secure IGEL endpoint. In a crisis flood, fire, ransomware or hardware failure — staff can plug in the UD Pocket and continue working from home or a temporary site on any available device.



### **Your endpoint, anywhere.**



For highly regulated sectors such as healthcare, government and finance, this level of portability means continuity without data compromise. Each UD Pocket session runs from read only IGEL OS, leaving no trace when removed.

Together, Dual Boot and UD Pocket redefine resilience. They turn recovery from a crisis into a simple reboot. No hardware replacement, no rebuilds, no panic. Just continuity, by design.

# THE NUMBERS DON'T LIE

Most cost-saving stories rely on projections. IGEL doesn't.

***Every deployment begins with a TCO (total cost of ownership) analysis based on real client data rebuilds, licences, support calls, even power draw.***

That number becomes the benchmark. Every project is tracked against it and the result is consistent: the savings materialise, and the system pays for itself.

That's why CIOs who started with IGEL for security stay for the economics.





# IGEL OS IS THE ENGINE; R-COM IS THE DRIVER.

Our team specialises in regulated, complex, never-offline environments - finance, healthcare, manufacturing, government. the engine; R-COM is the driver.

We design, deploy, and manage IGEL infrastructures that have to work first time, every time.

***Our mission is simple: keep your organisation operational, compliant, and resilient no matter what breaks elsewhere.***



**Contact the UK team for a  
confidential technical  
briefing:**

Your Partner for Today and Tomorrow.

We're confident in our technical expertise and measure our success by yours. We believe in what you can achieve with the right technology and partner.

Let's create a digital workspace that supports your team now and in the future.

#### GET IN TOUCH

Email: [salesupport@r-comconsulting.com](mailto:salesupport@r-comconsulting.com)

Phone: 0161 343 3833

Web: [r-comconsulting.com](http://r-comconsulting.com)



# STATE OF SYSTEMS PODCAST: IGEL

---



## **“The Biggest Secret in Cybersecurity”** *- featuring Justin Thorogood, IGEL*

In this episode of State of Systems, we pull back the curtain on the uncomfortable truth behind the UK’s digital backbone - from NHS hospitals to the critical national systems still running on decades-old software.

Our guest, Justin Thorogood, Global Channel Chief at IGEL, joins us to expose why endpoint security has become the true front line in today’s cyber war.

As hackers move faster than governments can patch, Justin reveals how IGEL’s read-only operating system is quietly protecting the systems you depend on every day - keeping defence, healthcare, and finance online when everything else fails.

***“We’re talking about warships, hospitals, and critical networks — the places that simply can’t go down.”***

*-Justin Thorogood, IGEL*

---

Click here to listen:





# ACCESS GRANTED

---

*You now know the system they didn't want  
you to know about.*