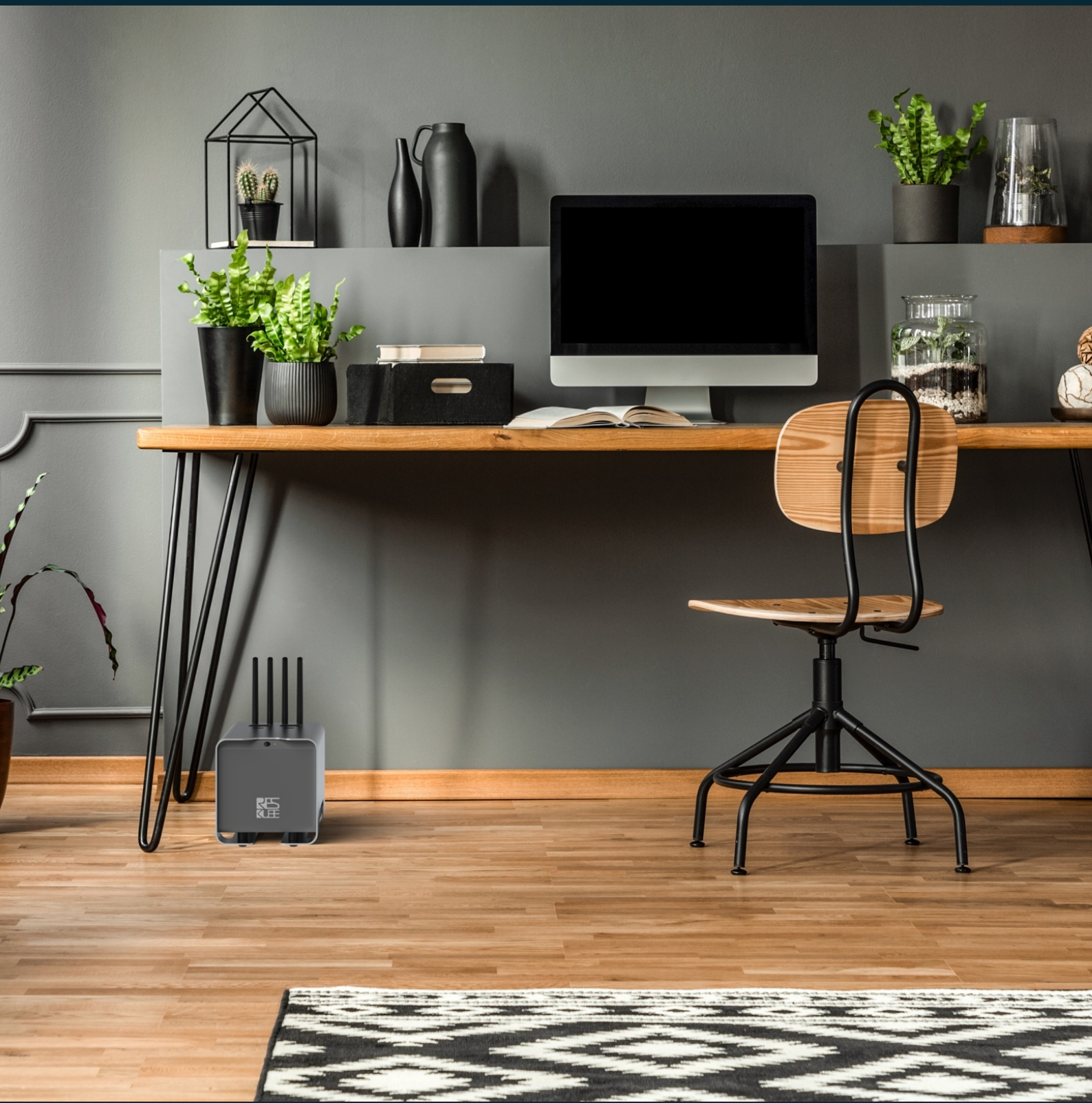
ResKube

Always on - everywhere.

Simple, cost effective security and resilience for the Critical Remote Worker



Tel: **020 3858 0099** *Email:* **info@fortressas.com** *Web:* **www.fortressas.com**

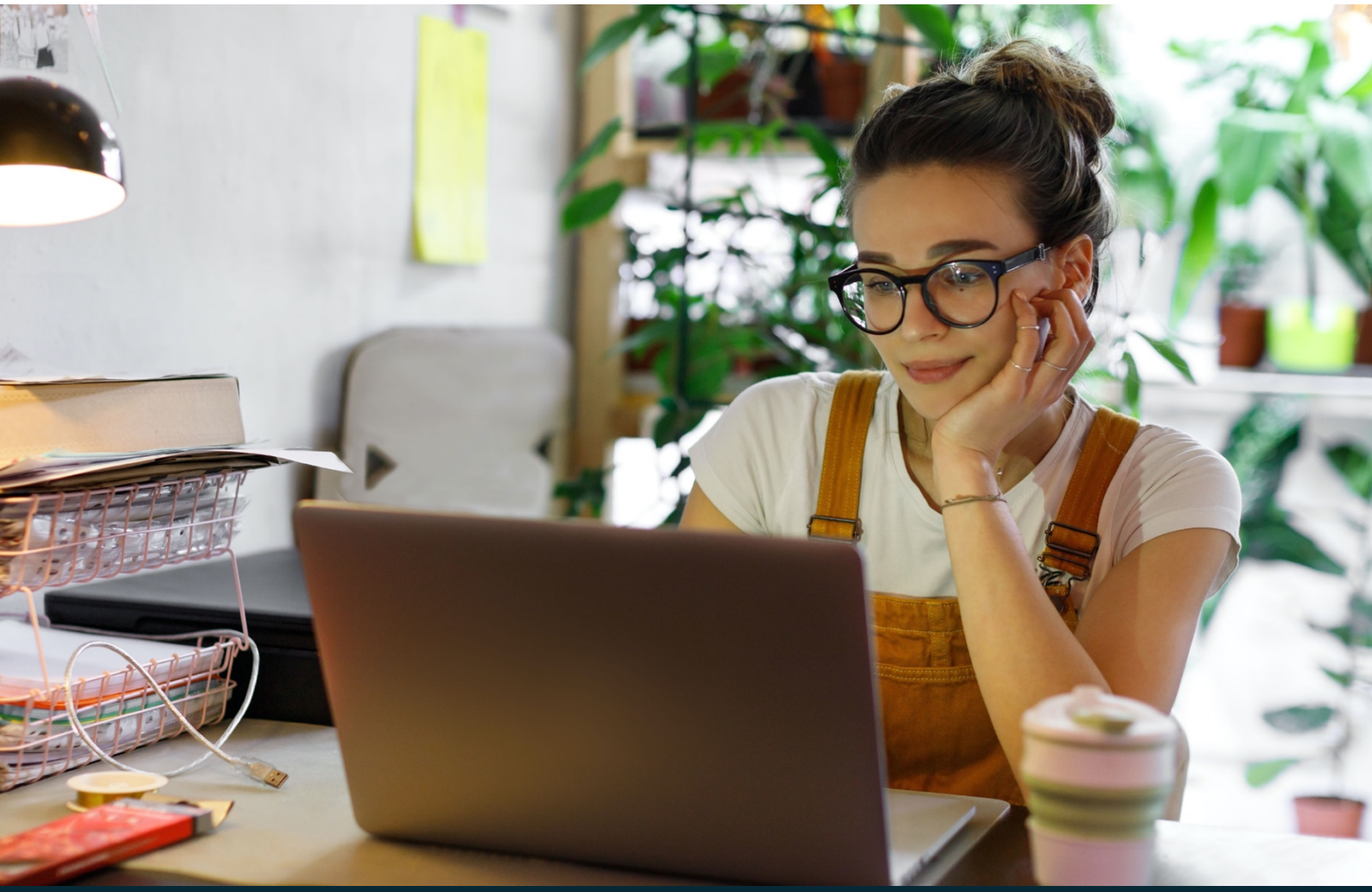
All change!

The world of work has changed forever as a result of the 2020 global COVID-19 pandemic. Homeworking and remote working have been proven to be as productive, if not more productive, than the corporate office.

As a result, we will never return to 5 working days in the office a week but move to hybrid working (Activity Based Working) with the corporate office used as a meeting and collaboration space, while the home office is use for “actual work”.

Many of these home workers still undertake time critical work (such as trading, live broadcast, leading commercial bids, building a legal case, editing, scheduling) that if interrupted will cause financial, operational or brand impact or harm to consumers, the company or other stakeholders.

Often, these staff will also deal with sensitive data that may be confidential to themselves, their customers or their companies and so need protection from hackers penetrating their often-insecure home networks.



Enterprise Resilience

Currently these critical individuals, and the companies that they work for, are reliant on the single points of failure in their home broadband internet and their home power supplies.

A surprising 4.7 million people in the UK suffered a “broadband outage” lasting more than 3 hours in the past year and this cost the economy some £1.5bn.

Events such as the August 2019 power cut, which cut power to 1.1 million households, hit the headlines but events affecting 1000s of homes happen every single day.

So, to prevent critical services from being interrupted by power and communications interruptions resilient systems must be put in place to support them.

It is estimated that 5-10% of staff run time critical work or are remunerated to a level where not being fully functional will cause significant financial impact.

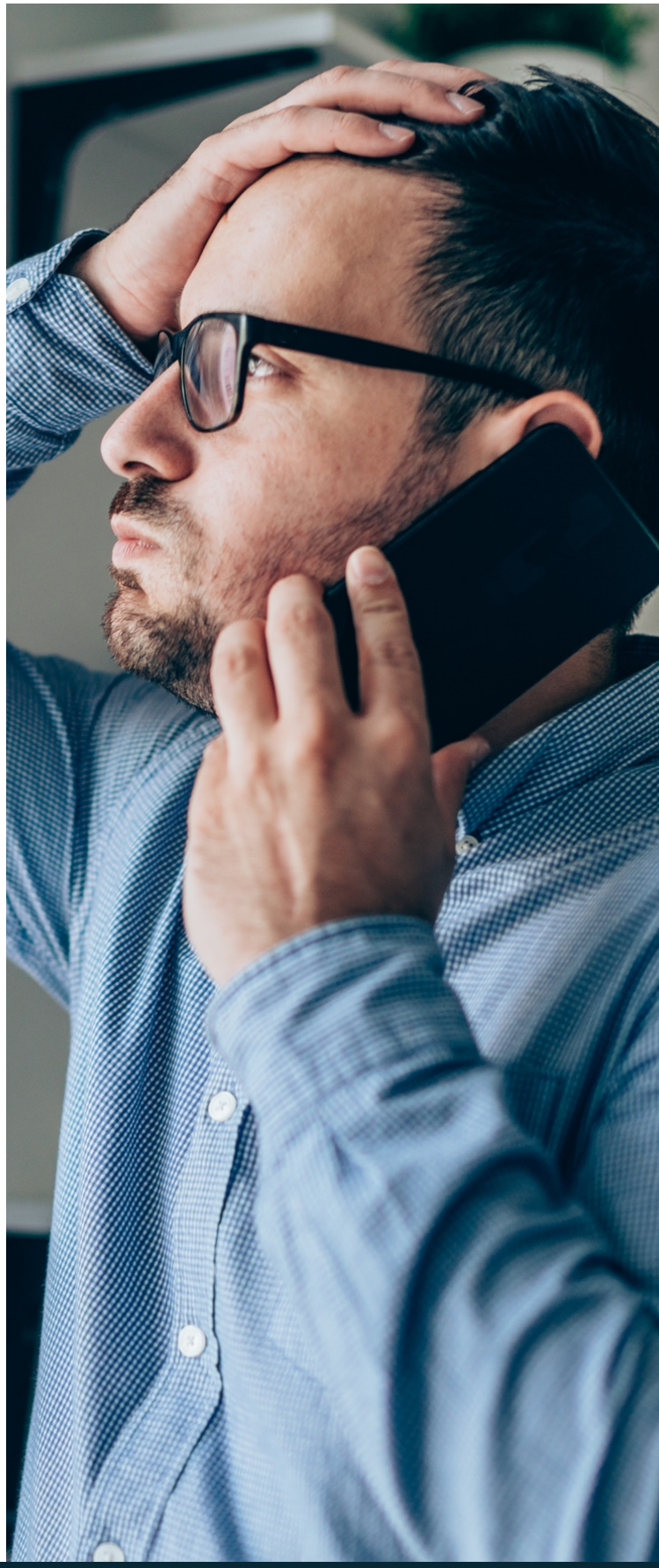
Cost Savings

Businesses are now reviewing the way their staff work, with many looking at a 40% reduction in office space in the coming years.

With a workstation in the City of London costing £13,000 per annum to support the savings of this process are huge.

The associated costs of resilience are also reducing as firms dispense with no longer needed Work Area Recovery facilities.

Some of these savings will need to be re-allocated to improving the resilience of those working at home.



The Challenge

Although these staff are highly skilled and critical, they often do not have a high level of IT knowledge.

Asking these staff to set up their own Uninterruptible Power Supply (UPS) and 4G failover router and network protection, and potentially a Next Generation Firewall or Unified Threat Management device is impractical and causing an IT Support nightmare. It also sends another two plastic devices and cables to your staff homes.

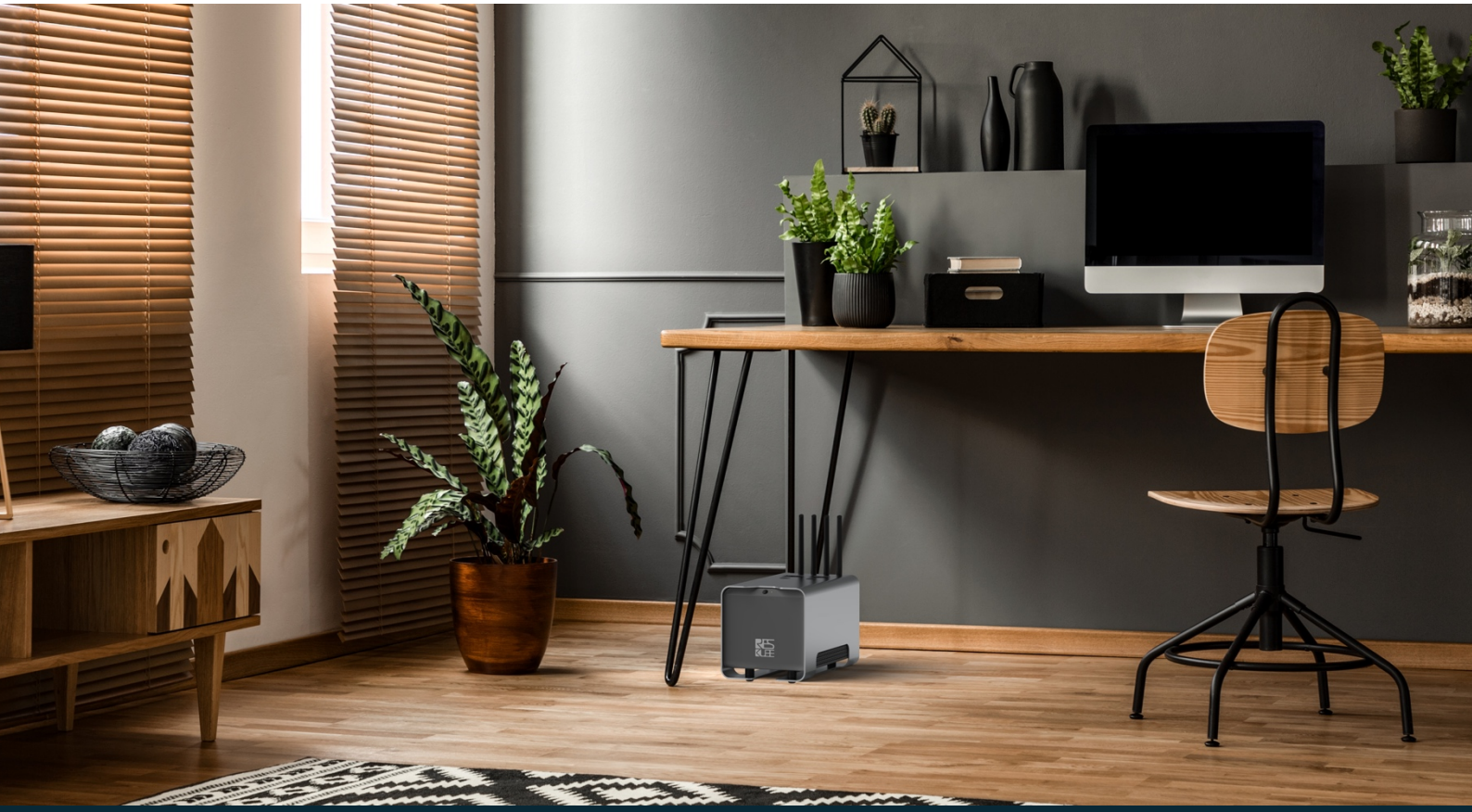
The alternative is your technical team travelling to the home of every critical or high value staff member or remote location to set the technology up, and in the years to come, support those devices. This is also, and certainly under pandemic social restrictions, impractical.

What is ResKube?

ResKube is an elegant solution to a surprisingly complex and messy problem, enabling even those doing time critical or high value work the flexibility to work from home. It does this while reducing the risk of interruptions to the delivery of critical business services or of cybersecurity breaches that would cause financial, operational or brand impact to the organisation.

ResKube has a sleek, minimalist design to fit comfortably in the home environment.

It provides a simple, cost effective, single device to provide high value or critical homeworkers with enterprise grade power and secure communications resilience. We call it a unified resilience solution (URS).



Tel: **020 3858 0099** *Email:* **info@fortressas.com** *Web:* **www.fortressas.com**

The ResKube Value

An incident stopping critical activities will not be excused by clients, regulators or financial stakeholders. When you or your team are let down by broadband or power providers, and all eyes turn to you, ResKube will ensure that you can continue delivering for your customers or stakeholders.

ResKube is designed to be “plug and play” out of the box, so that non-technical staff find it easy to set up. It also feeds into your existing network management tools and feed data into your existing network management systems so there is nothing new to learn or changes in process to make. It seamlessly provides the 5-10% of your staff, delivering higher impact or time critical services, the additional levels of resilience that they need while working remotely.

The value for enterprise customers lies in five main benefits:

1. **Simplicity** – it is one, enterprise approved and managed, device to send out to critical staff rather than cobbling together the UPS, failover router and VPN.
2. **Low Support Load** – A simple “4 Step Easy Start Guide” means non-technical staff will find it easy to implement. Home power and comms failures are no longer “an IT issue”.
3. **Management** – M2M SIM provides visibility, control and reporting via a Cisco Jasper dashboard, or via API into your existing network management tools.
4. **Flexibility** – Some staff are always critical, some are critical at specific times – ResKube can be dedicated to individuals or used as a pool device.
5. **Security** – VPNs work, and are relatively simple, but in a failover situation you will want to ensure that the staff actually turn it on. To force security during the immediacy of failover the APN is a much better solution, particularly if you want the added security of a Private APN which links the ResKubes directly to devices into your datacentres

Enterprise Grade Infrastructure

The ResKube is provisioned with a highly secure and ruggedised Machine to Machine (M2M) SIM delivering enterprise levels of security, visibility and control that are not available when using “retail” SIMs.

As an enterprise grade device, designed to be set in the home environment, ResKube can be made visible to your existing management platform, or be interrogated via the ResKube Management Portal.

ResKube Management Portal

The ResKube Management Portal is a Cisco Jasper Control Center based platform, providing all of the functionality one would expect from an enterprise management system. The data can be viewed through the portal or via API feeding into your existing network management platform.

It provides:

- Granular device visibility
- Alert me, deactivate it, cap it & avoid bill shock controls
- SIM lock to device
- Automation rules and triggers to control user connectivity behaviours
- API Integration
- Realtime fault diagnostics

Enterprise Grade Access Point Network

ResKubes connect to a specific enterprise grade Access Point Network (APN) which is more stable than the retail APN networks. This offers greater security, control and resilience.

ResKube can be provisioned with either an enterprise grade Public APNs or a Private APN dedicated to your business. Both types of APN use enterprise grade connectivity and use a dedicated M2M APN for reliability.

The Private APN option creates a mobile network specifically for your business, forcing the M2M SIMs to connect solely to your Private Network. This network is connected to specified termination equipment within your own datacentre via an IPSec tunnel.

Benefits of Enterprise Grade APN

The APNs provide a simple but highly effective method of extending your corporate network and the associated security to your staff working remotely. It is as if they are working within the security of the office.

The simplicity of connection for your staff is key to seeing positive returns from security investments, as staff will naturally gravitate to the simplest processes. With ResKube they simply connect to their home network provided by the ResKube.

If all traffic from all devices goes through the ResKube you can be assured of its security.

Sustainability

We all, enterprises and individuals alike, have a responsibility to do all we can to reduce our impact on the environment. Adding thousands of plastic devices to the homes of our workers goes strongly against this ethos.

Counter to popular belief plastic is not actually very recyclable. The recycling process requires huge amounts of energy and the resulting quality is inconsistent and only good enough to downcycle into plastic furniture, drain pipes or fleece clothing. These items are not recyclable. Often the quality is too poor to reuse and this plastic is burnt or dumped.

The design of ResKube has environmental sustainability as a key element. The casing is made of fully and infinitely recyclable aluminium. Specific efforts were also made to reduce the plastic in our components, their transportation and production. For example, the ResKubes distributed to the UK, EU and Nordics are made in the UK.

These efforts to reduce our environmental impact will continue and where possible plastics in future ResKubes will be compostable bioplastics.

One of the upsides of homeworking is the dramatic reduction in commuting and the associated reduction in environmental impact. Let's not offset this by filling our homes with extra plastic.

The ResKube Service

ResKube can be delivered as a Product or as a Service that includes the supporting services and support.

The **ResKube Service** provides the following:

- The ResKube device including:
  - Pre-configuration of the devices
  - Distribution to your staff
- 1Gb of 4G Data (other tariffs available)
- Ongoing support
- Repair/replace
- Battery replacement (after 3 years)

Optional Services Include:

- Private Access Point Network (APN)
- Secure Access Service Edge

Models and Use Cases

ResKube Home

ResKube Home provides resilience in the home work environment, providing sufficient time to continue to deliver critical activities and potentially hand over tasks to others outside the area of incident.

Its consumer-friendly design fits naturally in the home, so that staff are comfortable with a ResKube under their desk. This is a plug and play solution to those remotely running time critical activities.

The following are some examples:

Role	Time Critical Work
Remote Trading	Trades must be executed at specific times, whatever the circumstances. Clients or the firm will not accept excuses for missed opportunities.
Crisis Management	A crisis cannot wait and so those in the Crisis Management or IT Cyber Response teams cannot take a few hours out to wait for power and communications.
Senior Executives	Executives continually run critical activities and being out of action during preparation for negotiations, board report, company report, critical audit is not possible.
Bid Preparation	Bid deadlines are absolute and missing the deadline as a result of a failure in your organisation's business continuity will be unacceptable.
Live broadcast	Whether it is remote sports broadcast or you are a regular pundit or news teams – live means live!
Legal case preparation	Preparation for cases always runs to the last minute. Taking out a few critical hours in the run up to court time and being unprepared for a case is unacceptable and will damage brand.

NB: ResKubes may either be allocated to specific individuals or kept as a pool of devices to be sent to support staff for the period of a specifically critical projects, such as those outlined above.

ResKube Satellite

ResKube Satellite provides not just resilience but also access. It is a ruggedised device, designed to work in more challenging environments and to be moved more frequently.

In many instances, work happens where there is no fixed broadband line, such as construction sites, or temporary retail or sales offices. Securing data in these environments is often just as important as within the office.

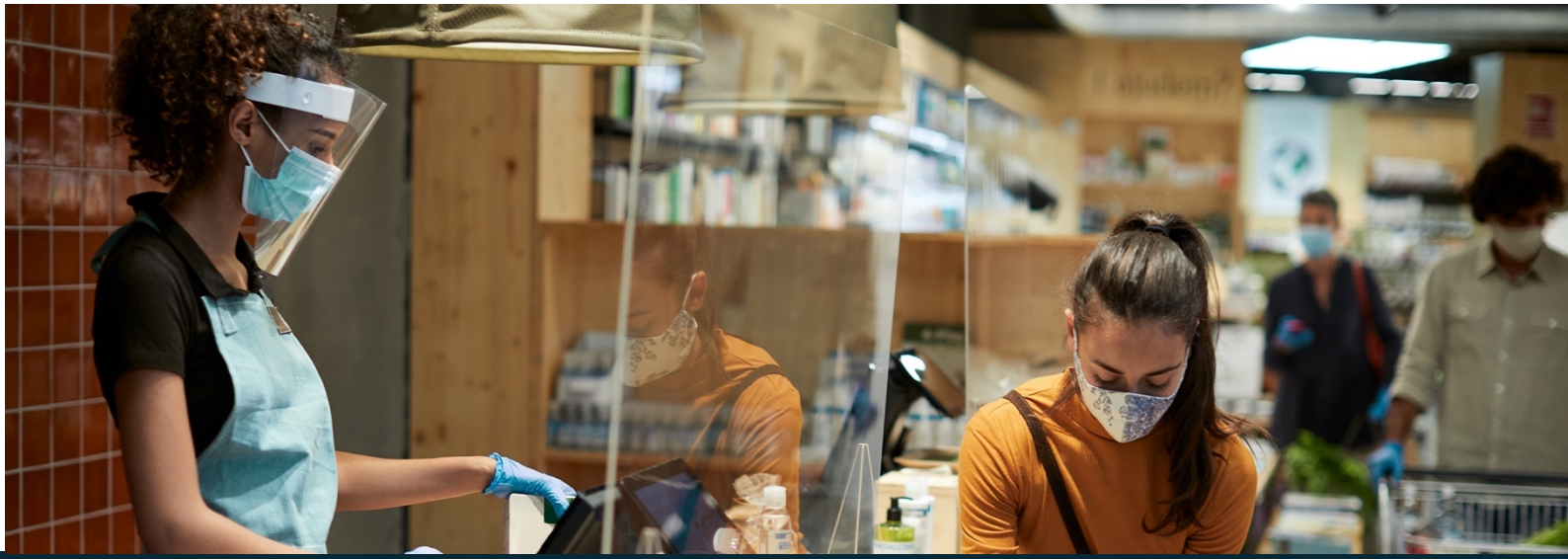
ResKube Satellite provides highly secure internet access in these circumstances and has dual 4G M2M ruggedised SIMs. Both 4G lines are always on and load balanced. So, should the primary fail, access is immediately switched to the secondary SIM, on another network.

It is also modular so the time running of the UPS can be increased.

ResKube provides internet access and power in rural or remote environments where communications lines are not available and power are intermittent, such as those outlined below.

Role	Time Critical Work
Rural Vaccination or Medical Centre	These pop-up sites will be required long into the future.
Construction Sites	Often in remote areas but with more and more internet connected devices and computing.
Temporary Sales Office or Retail	Providing real-time database or POS access.
Entertainment Venue/Pub	Screens showing Live Sports

NB: ResKubes may either be allocated to specific individuals or kept as a pool of devices to be sent to support staff for the period of a specifically critical projects, such as those outlined above.



Conclusion

ResKube gives you and your staff the flexibility, resilience and security to do more at lower risk in the new normal.

The range of innovative, patent-pending, products and services simply and cost effectively reduce the risk of power or communications interruptions or cybersecurity breaches causing financial, operational or brand impact to the delivery of critical business services delivered by remote workers.

When you or your team are let down by broadband or power providers, and all eyes turn to you, ResKube will ensure that you can continue delivering for your customers or stakeholders.

We call it a unified resilience solution (URS).

To recap, the value for enterprise customers lies in five main benefits:

1. **Simplicity** – it is one, enterprise approved and managed, device to send out to critical staff rather than cobbling together the UPS, failover router and VPN.
2. **Low Support Load** – A simple "4 Step Easy Start Guide" means non-technical staff will find it easy to implement. Home power and comms failures are no longer "an IT issue".
3. **Management** – M2M SIM provides visibility, control and reporting via a Cisco Jasper dashboard, or via API into your existing network management tools.
4. **Flexibility** – Some staff are always critical, some are critical at specific times – ResKube can be dedicated to individuals or used as a pool device.
5. **Security** – VPNs work, and are relatively simple, but in a failover situation you will want to ensure that the staff actually turn it on. To force security during the immediacy of failover the APN is a much better solution, particularly if you want the added security of a Private APN which links the ResKubes directly to devices into your datacentres