***When*** *organisations* ***experience*** *disruptions or cyberattacks on their critical IT infrastructure,* ***they want to*** *quickly and effectively restore operations with minimal downtime and financial loss,* ***so they can*** *ensure continuity of essential services, protect their reputation, avoid legal liabilities, and minimise economic impact.*

***When*** *organisations* ***adopt*** *cloud solutions for computing and storage,* ***they want*** *total control over maintenance and costs* ***so they can*** *maximise their return on investment (ROI) and minimise waste in power, computing, and storage, thereby ensuring optimal efficiency and profitability.*

**The Scope of Resiliency Challenges in Non-Cloud IT Infrastructure**

Non-cloud IT infrastructure, by its very nature, is typically deployed and maintained within the physical premises of an organisation. This setup might include servers, networking equipment, storage devices, and the associated software running on this hardware. Unlike cloud environments, where redundancy, failover mechanisms, and continuous updates are often managed by cloud service providers, non-cloud infrastructures require manual configuration and maintenance to achieve similar levels of resilience.

The lack of built-in resilience in non-cloud IT infrastructure means that any failure, whether due to hardware malfunctions, software bugs, or external attacks, can have a catastrophic impact. For instance, a single point of failure in a non-cloud system can bring down entire networks or critical applications, leading to downtime, data loss, and potentially severe financial losses. This issue is not confined to a particular operating system or type of computer; rather, it is a universal problem across all types of IT infrastructure that do not leverage cloud technologies.

**Manual Remediation: A Significant Drawback**

One of the most critical drawbacks of non-cloud IT infrastructure is the need for manual remediation in the event of a failure or attack. Manual remediation typically requires human intervention to diagnose the problem, restore backups, apply patches, and bring systems back online. This process is time-consuming, prone to human error, and often requires specialised knowledge that may not always be readily available.

For example, if a critical server in a non-cloud environment fails, IT personnel must manually assess the damage, which could involve replacing hardware components, reinstalling software, or even restoring entire systems from backups. This process can take hours or even days, depending on the complexity of the infrastructure and the nature of the failure. By contrast, cloud environments often have automated failover mechanisms that can switch to backup systems almost instantaneously, minimising downtime and reducing the need for manual intervention.

**The Universal Nature of the Problem**

The problem of insufficient resilience in non-cloud IT infrastructure is not limited to a specific operating system or type of computer. Whether it is a Windows-based server, a Linux machine, or a macOS workstation, all are susceptible to the same fundamental issues. The lack of built-in redundancy, reliance on manual remediation, and potential for catastrophic failures are common across all non-cloud environments.

For instance, in a Windows environment, a failure in the Active Directory service can disrupt the entire network, affecting authentication, authorisation, and access control across all connected systems. Similarly, in a Linux-based environment, a failure in a key service like DNS or DHCP can bring down the network, making it impossible for devices to communicate with each other or the outside world. In both cases, the recovery process requires manual intervention, which can be slow and cumbersome.

**The Emergence of New Exploits: CVE-2024-6768**

The vulnerabilities of non-cloud IT infrastructure are further exacerbated by the emergence of new exploits, such as CVE-2024-6768. This particular exploit is a recent example of how attackers can target non-cloud environments to cause significant disruption. CVE-2024-6768 is a vulnerability that allows malicious actors to ‘brick’ Windows systems, rendering them inoperable. Once a system is bricked, it becomes effectively useless, as it cannot boot or function normally. This type of attack is particularly dangerous because it can bypass traditional security measures and directly affect the integrity of the operating system.

One of the most alarming aspects of CVE-2024-6768 is that once a system is bricked, applying updates or patches becomes impossible. This creates a catch-22 situation where the system is vulnerable to further attacks, but there is no way to mitigate the risk because the system is already in a compromised state. This vulnerability highlights the critical need for resilient IT infrastructure, as systems without built-in redundancy or failover mechanisms are at significant risk of total failure in the face of such exploits.

**The Inadequacy of Traditional Security Measures: Need for last line of defence**

Traditional security measures, such as firewalls, antivirus software, and intrusion detection systems, are often insufficient to protect against attacks that exploit vulnerabilities like CVE-2024-6768. These measures are typically designed to prevent unauthorised access, detect malicious activity, and block known threats. However, they do not address the fundamental lack of resilience in non-cloud IT infrastructure. Once an attack successfully compromises a system, traditional security measures offer little in the way of remediation, especially if the system is rendered inoperable.

For example, a firewall might prevent unauthorised access to a network, but it cannot stop an attacker from exploiting a vulnerability in the operating system itself. Similarly, antivirus software might detect and remove malware, but it cannot reverse the damage caused by an exploit that has already bricked a system. This lack of built-in resilience in non-cloud IT infrastructure underscores its criticality; once an attack succeeds, recovery options are limited and often require extensive manual intervention.

Clearly, there is a gap in the integration of disparate cybersecurity solutions. What is needed is a last line of defence that protects against both known and unknown vulnerabilities and does not produce cascading failures if one solution fails.

**The Scale and Impact of the CrowdStrike Incident**

The CrowdStrike incident was a sophisticated and widespread cyberattack targeting critical infrastructure and high-profile corporations, including several Fortune 500 companies. The attack was particularly devastating in Australia, causing significant disruptions across various sectors, including healthcare, finance, energy, and utilities. The impact of the incident was both financial and operational, with widespread consequences for businesses and the general public alike.

**Financial Damage: A Global and Australian Perspective**

Globally, the financial damage from the CrowdStrike incident was estimated to be at least USD 5.4 billion. This figure reflects the direct costs of the attack, such as ransom payments, lost revenue due to operational downtime, and expenses associated with remediation and recovery efforts. It also includes indirect costs, such as reputational damage, legal fees, and the long-term impact on customer trust and market share.

In Australia, the estimated financial damage was around AUD 1 billion. While this figure represents a fraction of the global total, it is still significant, particularly when considering the size of the Australian economy relative to other major global markets. The financial impact in Australia was compounded by the critical role that many of the affected companies play in the national economy, particularly in sectors such as healthcare, energy, and finance.

**Mean Time to Recovery (MTTR): A Critical Metric**

One of the key metrics used to assess the severity of a cyber incident is the Mean Time to Recovery (MTTR). This metric measures the average time it takes for an organisation to fully recover from a cyberattack, from the initial detection of the breach to the complete restoration of services and systems. In the case of the CrowdStrike incident, the MTTR was approximately 72 hours, or three days.

While 72 hours may not seem like a long time, in the context of a cyberattack, it can feel like an eternity. During this period, the affected organisations were unable to operate normally, leading to significant operational disruptions and financial losses. For sectors that provide critical services, such as healthcare and utilities, even a short disruption can have serious consequences for public safety and wellbeing.

**Disruption to Critical Infrastructure and Services**

One of the most alarming aspects of the CrowdStrike incident was its impact on critical infrastructure and services in Australia. The attack disrupted operations in several key sectors, including healthcare, finance, energy, and utilities. These disruptions had far-reaching consequences, affecting not only the organisations directly targeted by the attack but also the broader public who rely on these services.

**Healthcare: Hospitals Unable to Access Patient Records**

The healthcare sector was among the hardest hit by the CrowdStrike incident. Several hospitals and healthcare providers in Australia were affected, leading to a complete shutdown of their IT systems. As a result, healthcare professionals were unable to access electronic patient records, which are essential for diagnosing and treating patients. The inability to access these records forced many hospitals to revert to manual processes, which are slower and more prone to error.

The disruption to patient records had serious implications for patient care. In some cases, critical treatments and surgeries had to be postponed, leading to delays in care and potentially worsening outcomes for patients. The incident also put a significant strain on healthcare workers, who were already stretched thin due to the ongoing pressures of the healthcare system.

**Finance: Delays in Financial Transactions**

The financial sector also experienced significant disruptions due to the CrowdStrike incident. Several major financial institutions in Australia were affected, leading to delays in processing financial transactions. These delays impacted a wide range of services, from everyday banking transactions to large-scale corporate payments.

The disruption to financial transactions had a cascading effect on the broader economy. Businesses that rely on timely payments to manage their cash flow were particularly hard hit, as delays in receiving payments disrupted their operations. The incident also resulted in a loss of confidence among consumers, who were concerned about the security of their financial information and the reliability of their financial institutions.

**Energy: Disruptions to Power Grids and Supply Systems**

The CrowdStrike incident also had a significant impact on Australia’s energy sector, particularly on the power grids and energy supply systems. The attack targeted critical infrastructure responsible for the distribution of electricity across the country, leading to widespread power outages and disruptions to energy supply systems.

The disruption to power grids had immediate and serious consequences for both businesses and households. In some areas, power outages lasted for several hours, affecting everything from manufacturing operations to household heating and cooling systems. The energy supply disruptions also had a knock-on effect on other sectors, particularly those that rely heavily on a stable and continuous supply of electricity, such as healthcare facilities and data centres.

**Utilities: Disruptions to Water Supply Systems**

In addition to the energy sector, the CrowdStrike incident also affected Australia’s water supply systems. The attack disrupted the IT systems that control water treatment plants and distribution networks, leading to interruptions in the supply of clean water to households and businesses.

The disruption to water supply systems raised serious public health concerns, particularly in areas where the water supply was temporarily interrupted or contaminated. In some cases, residents were advised to boil their water before use, while in other areas, water had to be trucked in to ensure a continuous supply. The incident also highlighted the vulnerability of Australia’s critical infrastructure to cyberattacks and the need for greater investment in cybersecurity measures to protect these essential services.

**Remote KVM**

**Introduction**

In today’s digitally connected world, the reliance on technology for critical infrastructure operations has reached unprecedented levels. Across various sectors, from healthcare and finance to energy and government services, the backbone of modern society is increasingly dependent on sophisticated IT systems. However, with this dependence comes a significant vulnerability—one that has become more apparent and pressing as cyber threats grow in complexity and frequency. The event of 19 July 2024, where a widespread cyber incident crippled 8.5 million Windows devices, serves as a stark reminder of this looming threat. The aftermath of such an attack was catastrophic, causing billions in damages and highlighting the glaring inadequacies in the resilience of non-cloud IT infrastructures.

**The Growing Dependency on Digital Infrastructure**

Digital transformation has been a key driver of economic growth and innovation across all sectors. The adoption of advanced technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT) has enabled organisations to enhance efficiency, reduce costs, and create new business models. However, this transformation has also led to a growing dependency on digital infrastructure, making it a critical component of daily operations for many organisations.

In sectors such as healthcare, financial services, energy, and transportation, the smooth operation of digital infrastructure is not just beneficial—it is essential. Hospitals rely on electronic health records (EHR) and connected medical devices to provide patient care. Financial institutions depend on complex IT systems to process transactions and manage risk. The energy sector requires sophisticated control systems to manage the distribution of electricity, oil, and gas. These examples illustrate the critical role that digital infrastructure plays in ensuring the continuity of essential services.

However, the increasing reliance on digital infrastructure also exposes organisations to significant risks. Cyberattacks, system failures, and other disruptions can have severe consequences, ranging from financial losses to threats to public safety. The July 2024 incident, where 8.5 million Windows devices were rendered inoperable, serves as a grim reminder of the potential impact of such disruptions. The event not only caused significant financial damage but also highlighted the vulnerability of critical infrastructure to cyber threats.

**The Problem: Lack of Resilience in Non-Cloud IT Infrastructure**

The core issue at hand is the lack of resilience in non-cloud IT infrastructure. Unlike cloud-based systems, which are designed with redundancy and failover capabilities, non-cloud infrastructure often lacks these essential features. This makes it more susceptible to disruptions caused by cyberattacks, hardware failures, and other unforeseen events.

The July 2024 incident is a prime example of this vulnerability. The attack targeted a specific flaw in Windows devices, rendering them inoperable and causing widespread disruption. The lack of built-in resilience in these devices meant that once they were compromised, there was no easy way to restore them to operational status. The result was a prolonged period of downtime, with organisations scrambling to deploy manual remediation steps—a process that was both time-consuming and costly.

This lack of resilience is not limited to Windows devices. It is a broader issue that affects all types of non-cloud IT infrastructure, from servers and networking equipment to industrial control systems. The problem is further compounded by the fact that many organisations do not prioritise resilience in their IT strategies. Instead, they focus on minimising costs and maximising efficiency, often at the expense of security and reliability.

The consequences of this approach can be disastrous. In the case of the July 2024 incident, the downtime caused by the attack resulted in an estimated $5.4 billion in damages to Fortune 500 companies in the United States alone. In Australia, the impact was also significant, with damages estimated at $1 billion. The hardest-hit areas were regional towns and small to medium-sized enterprises (SMEs), which often lack the resources and expertise to quickly recover from such incidents.

**The Problem: Cloud Costs Are Too High And Inefficient.**

As more and more businesses move their critical services into the cloud, they are discovering that the costs to migrate and operate cloud environments are too high. This has sparked a renaissance of solutions aimed at keeping costs down, including rigorous cost monitoring solutions, visualisation tools, multi-cloud strategies to spread expenses, real-time analytics tools, reporting tools, and cost-optimisation tools. All these initiatives stem from the reality that the cost of running a cloud environment is excessive.

Additionally, when a cloud provider experiences downtime, their priority is to recover the larger businesses first, leaving smaller businesses to recover at a slower pace.

The solution is for organisations to take their cloud environment into their own hands by gaining complete control of their private cloud infrastructure.

**The Human Cost: Disruption to Critical Services**

The financial impact of the July 2024 incident is only part of the story. The disruption to critical services had far-reaching consequences for society as a whole. Hospitals were unable to access patient records, financial transactions were delayed, and power grids were disrupted. These are not just inconveniences—they are events that can have life-threatening consequences.

For example, in the healthcare sector, the inability to access electronic health records can delay critical treatments, leading to potentially fatal outcomes. In the energy sector, disruptions to control systems can cause power outages, which can have a cascading effect on other critical services, such as water supply and transportation. In the financial sector, delays in processing transactions can undermine confidence in the banking system, leading to broader economic instability.

The July 2024 incident highlighted the fragility of our digital infrastructure and the potential for widespread disruption in the event of a cyberattack or other incidents. It also underscored the importance of resilience in ensuring the continuity of critical services. Without adequate resilience measures in place, organisations are vulnerable to a wide range of threats, from cyberattacks and natural disasters to human error and equipment failures.

**The Evolving Threat Landscape**

The threat landscape is constantly evolving, with new vulnerabilities and attack vectors emerging regularly. Cybercriminals are becoming increasingly sophisticated, using advanced techniques such as artificial intelligence and machine learning to identify and exploit weaknesses in IT systems. The July 2024 incident involved a new exploit (CVE-2024-6768) that was specifically designed to "brick" Windows devices, rendering them permanently inoperable.

This type of attack is particularly concerning because it targets the very foundation of digital infrastructure. By rendering devices inoperable, attackers can cause widespread disruption and force organisations to invest significant time and resources in recovery efforts. In the case of the July 2024 incident, it was estimated that it took an average of 1.5 hours to deploy a service technician to each affected device, resulting in a total of 12.75 million hours of lost productivity. The total cost of this downtime was estimated at $700 million, with an additional $500 million in potential losses due to extended recovery times.

The evolving nature of the threat landscape means that organisations must be constantly vigilant and proactive in their approach to resilience. Traditional methods of managing IT infrastructure, which rely on periodic updates and manual intervention, are no longer sufficient. Instead, organisations need to adopt a more holistic approach that considers the entire lifecycle of IT systems, from initial deployment to ongoing maintenance and eventual decommissioning.

**Challenges in Building Resilient Infrastructure**

Building resilient IT infrastructure is not a straightforward task. It requires a deep understanding of the criticality of business processes, the capabilities of underlying technologies, and the potential impact of disruptions. Moreover, the process of identifying and analysing critical infrastructure assets is time-consuming and often physically challenging, particularly in complex environments such as industrial facilities and data centres.

One of the main challenges is the lack of visibility into the entire IT ecosystem. In many organisations, IT infrastructure is fragmented, with different departments and business units using their own systems and tools. This can create silos that make it difficult to identify and address vulnerabilities. Additionally, many organisations lack the expertise and resources to conduct thorough assessments of their IT infrastructure, particularly when it comes to non-cloud assets.

Another challenge is the need to balance resilience with other business priorities. Organisations are under constant pressure to reduce costs and improve efficiency, which can lead to trade-offs in areas such as security and reliability. For example, organisations may choose to delay or forgo critical updates to minimise downtime, even if this increases the risk of a cyberattack.

Finally, there is the challenge of staying ahead of the evolving threat landscape. As new vulnerabilities and attack vectors emerge, organisations must continually update their resilience strategies and implement new measures to protect their IT infrastructure. This requires a proactive approach to threat intelligence and a willingness to invest in new technologies and processes.

**The Economic Impact of Inadequate Resilience**

The economic impact of inadequate IT resilience is significant. The July 2024 incident, for example, resulted in billions of dollars in direct damages, not to mention the broader economic impact of the disruption to critical services. However, these costs are just the tip of the iceberg. The long-term consequences of inadequate resilience can be even more damaging, leading to lost revenue, reputational damage, and reduced competitiveness.

In the case of the July 2024 incident, the damage to the affected organisations' reputations was severe. Many customers and clients lost confidence in their ability to provide reliable services, leading to a loss of business and a decline in market share. This is particularly true for SMEs and regional businesses, which often operate on thin margins and cannot afford to lose customers.

In addition to the direct financial impact, inadequate resilience can also lead to regulatory penalties and legal liabilities. In the aftermath of the July 2024 incident, several organisations faced lawsuits from customers and business partners who suffered losses as a result of the disruption. These lawsuits not only resulted in significant legal costs but also further damaged the organisations' reputations.

Furthermore, inadequate resilience can have a broader impact on the economy as a whole. When critical infrastructure is disrupted, it can create a ripple effect that impacts other sectors and industries. For example, a power outage can disrupt transportation networks, leading to delays in the delivery of goods and services. Similarly, a cyberattack on a financial institution can undermine confidence in the banking system, leading to a broader economic downturn.

**Target Market**

ResQ Cloud’s primary target market is the critical infrastructure sector. This includes:

* **Energy Sector:** Nuclear reactors, electrical grids, oil and natural gas facilities, pipelines, and fuel storage.
* **Chemical Sector:** Petrochemical manufacturing, agricultural chemical production, and chemical distribution.
* **Transportation Sector:** Airports, seaports, railways, highways, bridges, and public transit systems.
* **Water and Wastewater Systems:** Water treatment plants, reservoirs, dams, pumping stations, and sewer systems.
* **Communications Sector:** Telecommunication networks, internet service providers, and satellite systems.
* **Financial Services Sector:** Banks, stock exchanges, payment systems, and clearinghouses.
* **Healthcare:** Hospitals, clinics, and medical supply chains.
* **Emergency Services:** Police, fire departments, and emergency management systems.
* **Food and Agriculture:** Farms, food processing facilities, distribution networks, and food safety systems.
* **Government:** Defence industrial base, federal government facilities, and national security systems.

These sectors are characterised by their reliance on IT infrastructure that is often outdated, non-resilient, and vulnerable to cyber threats. The potential impact of downtime in these sectors is immense, ranging from financial losses to threats to public safety. Therefore, the demand for a solution like ResQ Cloud, which offers fast and effective recovery from cyber incidents, is high.

**Competitive Analysis**

The market for IT resiliency solutions is competitive, with several established players like ServiceNow and Battleground offering crisis management and business continuity management systems. However, ResQ Cloud differentiates itself by providing a solution that is both hardware-agnostic and capable of reducing mean time to recovery (MTTR) from 72 hours to just 30 seconds. This significant reduction in recovery time is a key selling point that gives ResQ Cloud a competitive edge.

### **Key Competitors**

While there are no direct competitors, there are several players in the ecosystem. We will integrate all these solutions into a seamless experience to provide 100% resiliency.

**BCMS**

* **ServiceNow:** A leading provider of IT service management (ITSM) solutions that includes features for crisis management and business continuity. However, ServiceNow's offerings are primarily software-based and may not be as effective in environments where non-cloud IT infrastructure is prevalent.
* **Battleground:** Offers comprehensive business continuity and disaster recovery solutions. While Battleground has a strong presence in the market, its solutions may not provide the same level of agility and speed in recovery that ResQ Cloud offers.

**IP-KVM** All existing IP-KVM solutions have a limitation of relying on the existing network.

* **Sipeed NanoKVM:** Lichee NanoKVM is an IP-KVM product based on LicheeRV Nano, inheriting the extreme size and powerful features of LicheeRV Nano. The Lichee NanoKVM is available in two versions: NanoKVM Lite, which is a basic configuration suitable for individual users with certain DIY capabilities and enterprise users with bulk requirements; and NanoKVM Full, which is a full version with a sophisticated case and complete accessories, as well as a built-in system mirror card that is ready to use at boot, recommended for individual users.
* **PiKVM:** PiKVM is a feature-rich, production-grade, open-source, Raspberry Pi-based KVM over IP device. It allows you to manage servers or workstations remotely, regardless of the operating system state or whether one is installed. PiKVM lets you turn on/off or restart your computer, configure the UEFI/BIOS, reinstall the OS using the virtual CD-ROM or flash drive, and much more! Everything works as if you were working directly on a remote system. It's true hardware-level access with no dependency on any remote ports, protocols, or services!
* **TinyPilot:** TinyPilot is a device that plugs directly into your bare-metal server, providing a virtual console during BIOS and boot. It allows you to debug boot failures, install a new OS, and adjust your BIOS settings, all without ever connecting a keyboard, monitor, or mouse. You can also upload disk images and mount them on your remote server. TinyPilot is an inexpensive, open-source device for controlling computers remotely.

**Secure Communication:**

* **Tailscale:** Tailscale is a VPN service that makes the devices and applications you own accessible anywhere in the world, securely and effortlessly. It enables encrypted point-to-point connections using the open-source WireGuard protocol, meaning only devices on your private network can communicate with each other.
* **Twingate:** Provides secure access through zero-trust principles, replacing traditional VPNs for remote work, enabling centralised management, user connectivity, and application-level privilege without infrastructure changes.
* **Headscale:** An open-source, self-hosted implementation of the Tailscale control server. HeadScale-ui is a complementary project that provides a web UI for this.
* **NetBird:** Connect your devices into a single secure private WireGuard®-based mesh network with SSO/MFA and manage access with just a few clicks.

**Product Positioning**

ResQ Cloud will position itself as the ultimate solution for IT resiliency in critical infrastructure. The key value propositions are:

* **Rapid Recovery**: The ability to reduce mean time to recovery (MTTR) from 72 hours to just 30 seconds is unparalleled in the market.
* **Hardware-Agnostic**: ResQ Cloud can operate on any single-board computer (SBC), making it highly versatile and scalable.
* **Comprehensive Coverage**: The solution is designed to work across various sectors, from energy to healthcare, ensuring that critical infrastructure remains operational even in the face of severe cyber threats.
* **Ease of Mass Control**: The solution’s capability to reboot and apply manual remediation steps with a single click to multiple nodes in parallel simplifies the recovery process, making it accessible even to organisations with limited IT resources.
* **Out-of-Band Control**: Even if the company network is down, it can manage the target nodes. Bringing down the network is one of the key strategies to prevent lateral movement while the remediation is being carried out.
* **Detection, Alert, and Protection Against Cyberattacks in Sidecar Mode**: If a cyberattack completely cripples the target node, recovery is only possible with physical access. By running in sidecar mode, ResQ Cloud can assume complete control even if the target node is compromised.