Isolated Management Infrastructure

Executive Summary

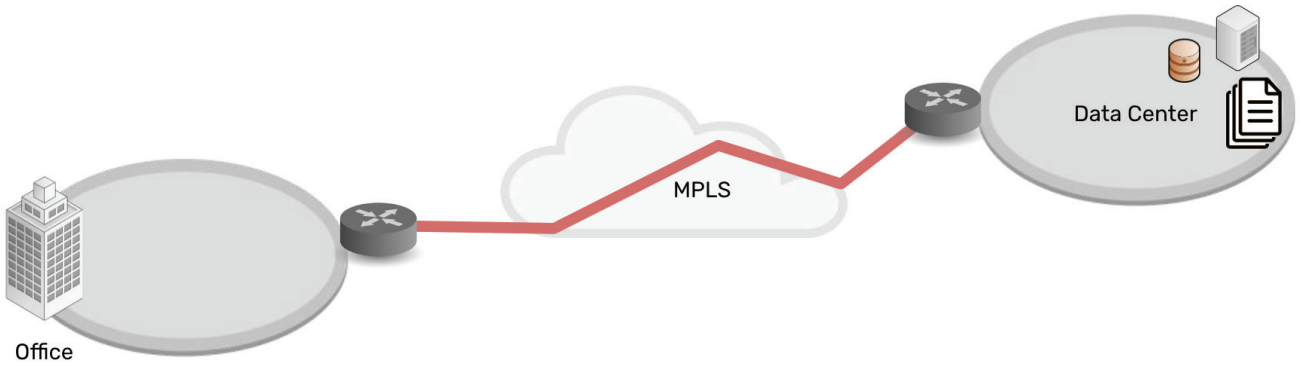
Business relies on network resilience. But network management now requires more than a 'break/fix' approach. Decentralized and growing architectures are spread across cloud, premises, and large IoT footprints. For shrinking IT teams, this presents resilience problems, as many are unaware of the best practice to help them care for their vast digital estate, maintain complex and delicate architecture, and recover quickly in case of attack. This gap means the network is a source of anxiety.

Big Tech solved these problems 10+ years ago, by doubling down on their management architectures. This best practice, which is now recommended by CISA, involves fully separating management networks from production networks into what's called Isolated Management Infrastructure. IMI goes far beyond serial console and out-of-band access, providing the management and service delivery capabilities teams need to reduce on-site upkeep, stabilize delicate architecture, and accelerate ransomware recovery.

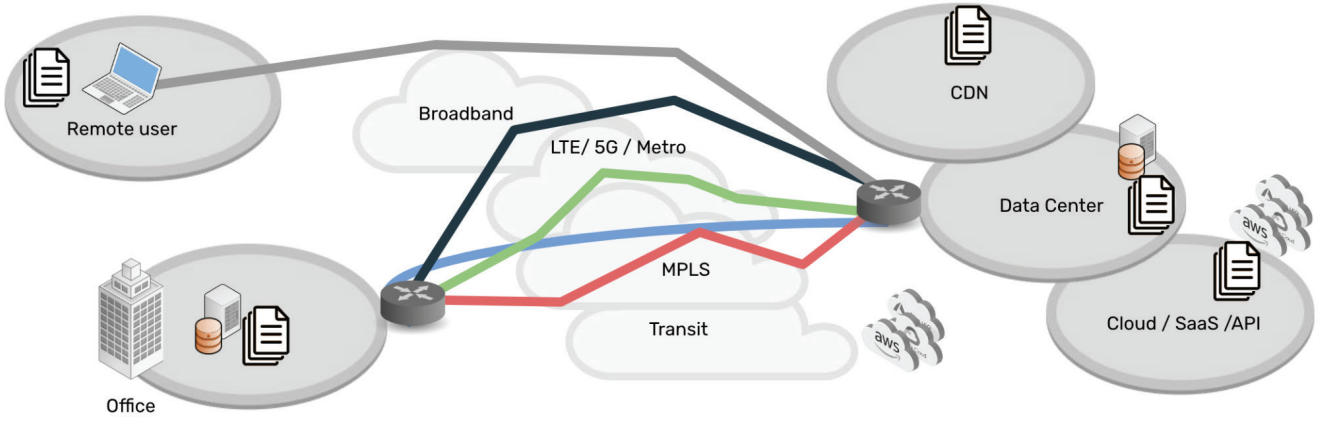
Big Tech's network resilience secret lies in ZPE Systems' Nodegrid hardware and software. Nodegrid is the only network resilience platform, delivering the Gen 3 capabilities that are required to build IMI. Now, organizations in every industry benefit from the best practices that have been trusted to run the public cloud for over a decade.

Problem : IT and OT are Widespread, Delicate, and Vulnerable

The network is at the center of how most organizations serve their customers. Twenty years ago, IT teams managed a centralized architecture. Achieving resilience was as simple as going on-site or remoting-in via serial console to fix issues at the data center.



Then in the mid-2000s, the advent of the cloud decentralized infrastructure, data, and computing. Architectures became geographically and virtually distributed, a complex mix of on-prem and cloud solutions. This allows companies to serve today's customers, who demand 24/7 reliability and on-demand services for work, school, and leisure.



But behind the scenes, this explosion of architecture created three resilience problems:

1. **Too Much Work**
   Infrastructure, data, and computing are widely distributed. Systems inevitably break and require work, but teams don't have the staff to keep up.
2. **Too Much Complexity**
   Pairing cloud and box-based stacks creates complex networks. Teams leave systems outdated, because they don't want to break this delicate architecture.
3. **Too Much Risk**
   Unpatched, outdated systems are prime targets for packaged attacks that move at machine speed. Defense requires recovery tools that teams don't have.

Here are a few real-world examples of teams battling these problems in 2023:

- Federal Aviation Administration: An overworked contractor unintentionally deleted files, which delayed flights nationwide for an entire day.
- Southwest Airlines: A firewall configuration change caused 16,000 flight cancellations and cost the company $1 billion.
- MGM Resorts: IT lacked recovery systems, which allowed an attack to persist for weeks and cause millions in losses per day.

Gap: IT Teams Lack Modern Best Practices

These problems exist because teams lack the best practices for modern network resilience. They must leverage technologies that extend their fleet management capabilities, automate infrastructure changes, and boost ransomware recovery efforts. But when it comes to actually implementing any of this, teams face a mind-boggling question: ***"How?"***

The answer lies in the best practices that Big Tech has trusted to run the public cloud for 10+ years. These best practices are called Isolated Management Infrastructure.

Solution: IMI and the Resilience Platform Approach

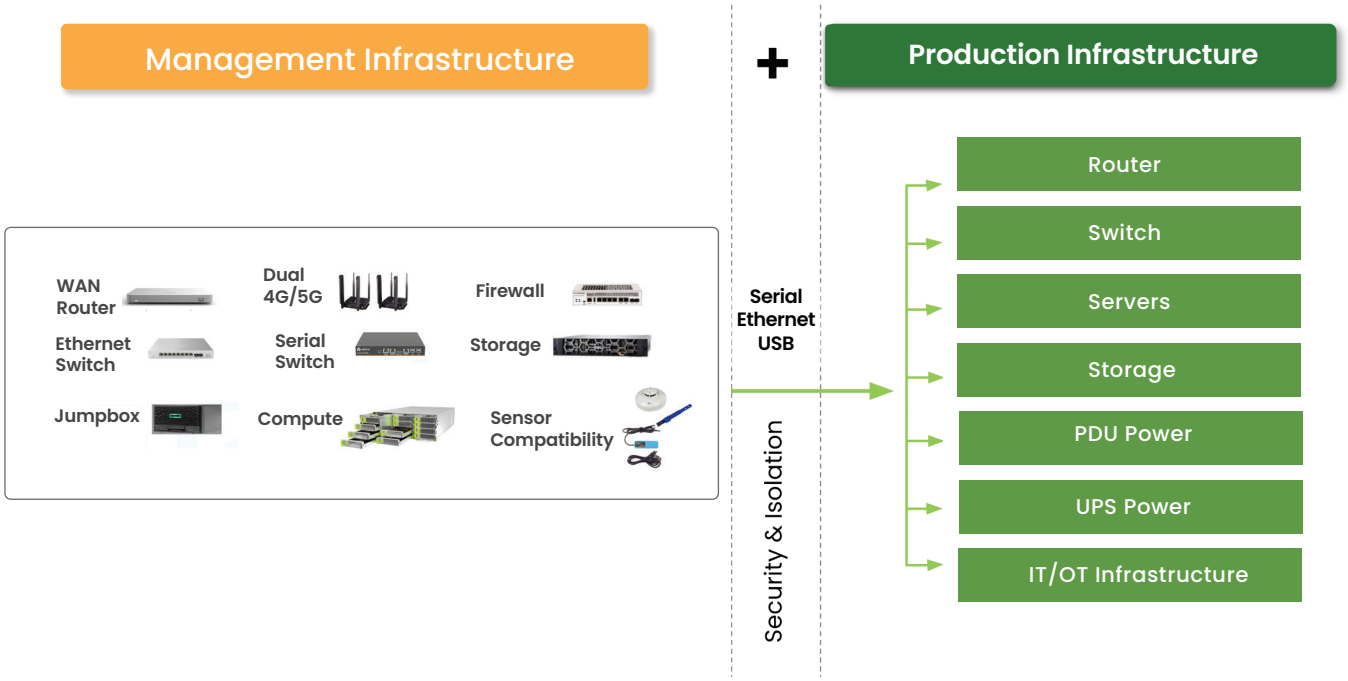
Traditional out-of-band serial consoles were designed to solve the problems of 20 years ago. These Gen 1 and Gen 2 devices offered simple remote troubleshooting and limited scripting. These were not enough for Big Tech, who had many global sites, automation-heavy environments, and threat vectors. Their teams still needed to answer practical questions, like:

- "How can we guarantee access to fix stuff that breaks, without rolling trucks?"
- "Can we automate change management, without fear of breaking the network?"
- "Attacks are inevitable — How do we stop hackers from cutting off our access?"

They understood that modern network resilience must account for system breakages, human error, and fast-moving attacks. This requires a platform approach to resilience. They addressed these concerns by creating the blueprint for IMI, which requires:

1. **Out-of-band management** that is fully isolated from production gear and connects to every type of management interface, to guarantee remote access
2. **Edge-native automation** for config and change management, allowing systems to continue operating in case of outages or change errors
3. **Isolated management interfaces** that use zero trust principles, are not open to the internet or production gear, and have full-stack routing with resilience features to ensure access and prevent attackers from reaching the management network

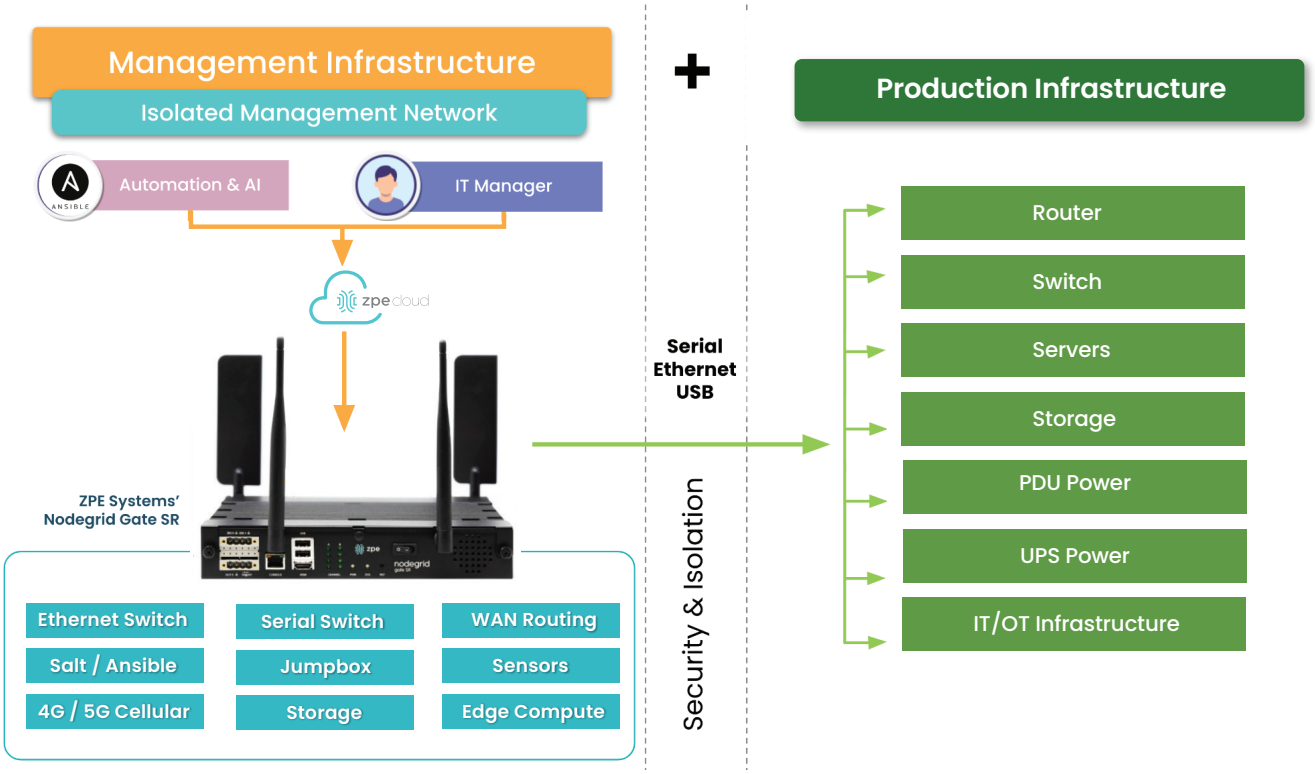
But creating this architecture would require nine or more management devices per site:



This is where ZPE Systems' Nodegrid resilience platform comes in.

ZPE Systems' Nodegrid is the Drop-In Resilience Platform

Big Tech was introduced to ZPE Systems during the initial stages of building IMI. Working together, they further developed the blueprint and the next generation of out-of-band management. Now, Big Tech and 400+ other organizations benefit from ZPE's Nodegrid resilience platform. ZPE's Gen 3 hardware and Linux-based Nodegrid OS combine all of the functions required for IMI.



Benefits of IMI using Nodegrid

Instantly fix breakages

Nodegrid's modular devices connect to serial, Ethernet, USB, and all types of management interfaces to provide a full virtual presence. This eliminates truck rolls and prolonged service calls. Teams gain instant remote access to any device in their fleet, where they can cycle power, re-image the OS, or fully rebuild production environments.

"We've quadrupled business, but this solution is actually shrinking our workload." —Blake Johnson, Network Architect, Living Spaces Furniture

Automate without anxiety

The open Nodegrid OS lets teams use any third-party or custom automation tools. Nodegrid devices have features of content delivery networks and can pull scripts, patches, firmware, and virtual appliances from ZPE Cloud and store them locally. This allows them to serve as the automation and deployment engine for every connected device — including unsupported legacy gear. Since it's all done out-of-band, teams can verify automation integrity before pushing to production, and if there's a mistake, press the 'undo' button to restore the last good configuration.

"Now, we deploy in an hour using one box instead of five, and it fits into our CI/CD pipeline so well that we can do proper lights-out management of all our sites." —Frank Basso, EVP Engineering, Vapor IO

Stop ransomware in its tracks

Nodegrid's IMI shields management interfaces from the Internet. If a production attack succeeds, IT teams retain management control. The Nodegrid resilience platform runs VMs, apps, and services of choice, so teams can deploy a Gartner-recommended Isolated Recovery Environment. Using the IRE, they can isolate infected gear, cleanse, and restore quickly without the risk of reinfection.

"ZPE has addressed all the aspects of maintaining our uptime to near 100%." —Aaron Lott, Network Engineer, DigiCert

---

For a step-by-step guide on building your Isolated Management Infrastructure, download our **Network Automation Blueprint.**

To learn more about ZPE's customers, IMI use cases, and Nodegrid resilience products, **download the corporate brochure.**