

# The Future of Edge Networking

Discover four ways to transform your edge capabilities

# Your Future Depends on Edge Networking

As business becomes increasingly distributed, your global network needs to be more capable outside of the data center. Meeting your changing requirements means having a robust edge – one that can handle more than simply funneling data back to the core. This will be critical to supporting everything from remote IoT devices & sensors, to entire branch networks and even faraway locations, all without slowing down your business.

“By 2022, more than 50% of enterprise-generated data will be created and processed outside the data center or cloud.”  
–Gartner

In this ebook, we’ll show you four key areas that can help you improve your edge networking capabilities. You’ll be able to deliver a better user experience with benefits like:

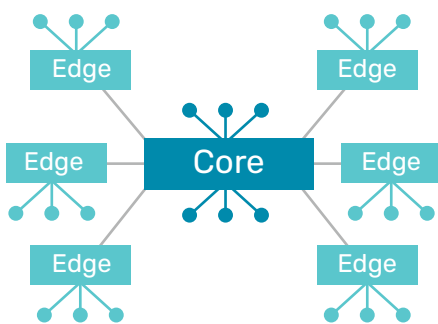
- Lower latency for real-time responsiveness
- Optimized bandwidth for fast speeds & less waiting
- Reliable access to boost internal & external customer satisfaction

But first, you might be wondering – What is edge networking?

## What is Edge Networking?

This relatively new concept might leave you with a couple questions like:

- What is edge networking?
- How is it different from edge computing?



Edge networking and edge computing are technically very different. Here’s a brief breakdown to clear up any confusion.

**Edge networking** consists of the means through which edge systems connect back to the data center or to your distributed cloud services applications.

**Edge computing** involves taking parts of the data center or core and moving them closer to the edge. This can include things like computing workloads, data storage, and application services.

Because this eBook aims to help you on a high level, we’ll take a step back and use **Edge networking** to combine both terms.

# Why Do You Need Better Edge Networking?

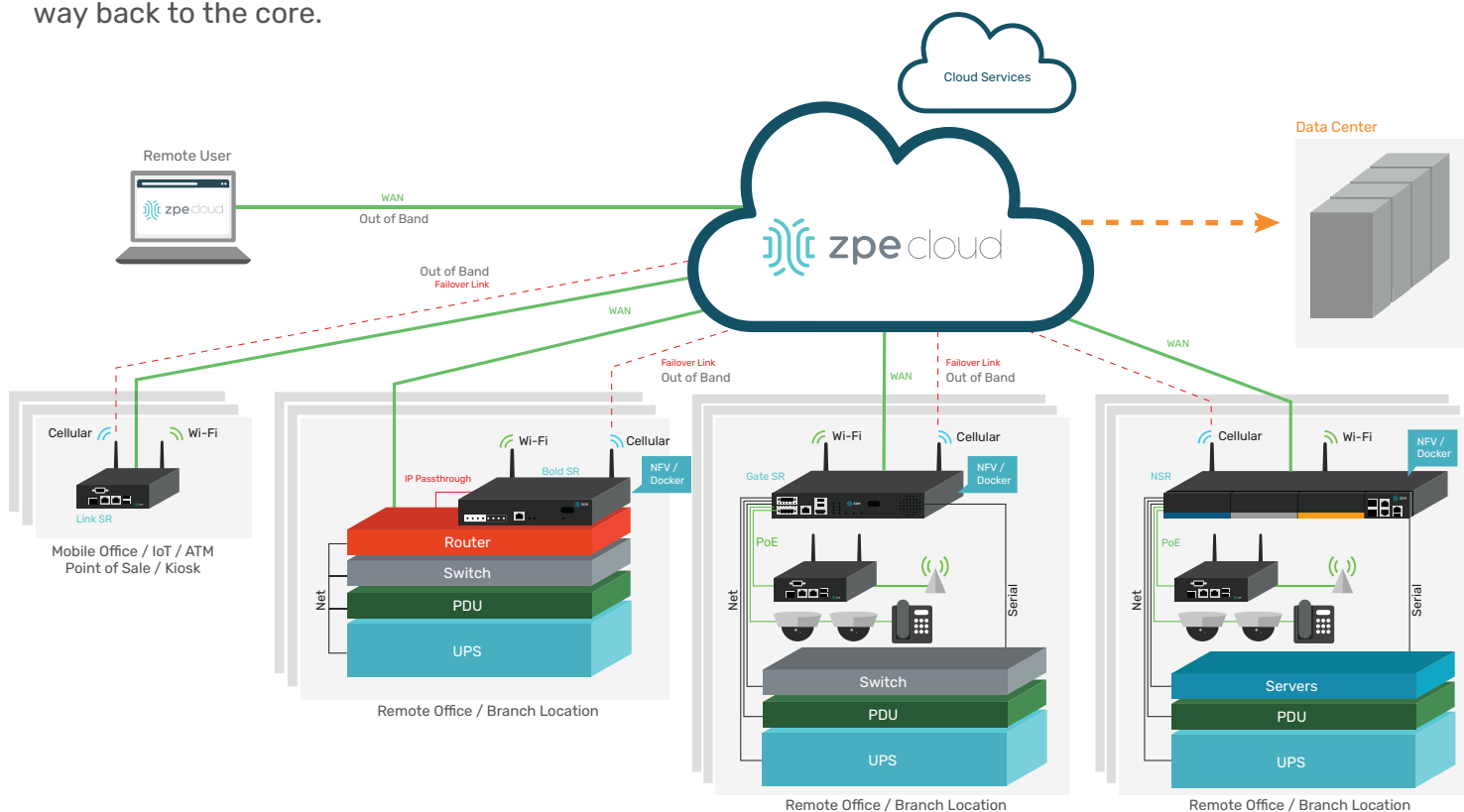
Traditional networking consists of the data center, which is at the core of the enterprise, and branch locations, which are at the edge. The networks at these branch locations funnel data back to the data center for processing. The data center is responsible for the heavy lifting, such as computing strings of information, analyzing trends, storing critical data, and more.

However, edge locations are growing in number and complexity, which means the data center is becoming increasingly overwhelmed. Also, not all the communication from the branch offices is related to services in the data center, but instead, to services hosted in the cloud.

Edge locations go beyond traditional branch offices, and their requirements for IoT, industrial data, communications, and even remote work put enormous stress on the data center. This leads to bottlenecks, latency, poor application performance, and ultimately business that can't move as quickly as its users demand. This is why networking and computing are now required at the edge.

**“With a stronger, more capable edge, you can relieve your stressed data center and optimize your global networks”.**

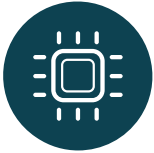
By distributing your workload, you can achieve responsive and balanced networking from the edge all the way back to the core.



## Key Areas for Better Edge Networking

Edge networking is a young landscape that will mature in coming years. This can make it difficult to pinpoint specific technologies or competencies for improving your networks. It's important to remember that your edge networking strategy should include a living plan that can adapt as your needs change (and they most certainly will change).

To help you evolve into the future with better edge networking, here are four key areas you can focus on:



### Distributed Processing and Control

To optimize networks and get granular management.



### Deep and Comprehensive Security

To protect from an increase in attack opportunities.



### Wide Ranging Extensibility

To ensure you can readily adapt to changing standards and requirements.



### Valuable and Controllable Data

To provide the right data to the right systems & users.

# Distributed Processing & Control

Merge the core with the edge and stay in control

With the future of networking, the data center as you know it will never be the same. One requirement involves moving core processes close to the edge. This helps you offload some of the work from your data center, while also allowing you to optimize the user experience at every corner of your enterprise.

But how do you lay the right foundation for all this? It starts by implementing the appropriate hardware, software, and management capabilities.

## Hardware

One key component of better edge networking is the appliances you choose. 'Edgified' is a term that, when referring to hardware, indicates appliances built with features and specs designed for edge implementations. Edgified hardware is necessary because it delivers simplicity, horsepower, and hardened security.

Future edge deployments will require convenient, plug 'n play setup. Edgified hardware makes it effortless using zero touch provisioning over WAN. You don't need to send trained staff to install & configure devices. Instead, any local employee can simply connect and boot your edgified appliances, and automation performs all your configuration tasks.

Edgified hardware is also capable of performing multiple functions in a single box. These include not only networking tasks like routing, switching, and failover, but also increasingly critical jobs like computing and storing data. As edge and core functions continue to merge closer together, your enterprise will need powerful, all-in-one devices.

Finally, edgified hardware is built with security in mind. This means the box's internal components come from trusted vendors like Intel® that ensure secure integrations with other hardware & software providers. Beyond components, edgified appliances give you cloud connectivity so you can manage devices and maintain security no matter where you are.



## Software

The software you deploy is essential groundwork for your future edge capabilities. To keep up with the evolving landscape, your software platform must be powerful. You can no longer settle for purpose-built appliances that come with simple operating systems. You need multi-function devices with a robust software layer that supports virtualization and automation.

Virtualized network functions (VNFs) help you meet edge requirements and move away from one major limitation of traditional networking – the rigid, cumbersome stack. With a strong operating system and hypervisor, you can deploy virtualized environments for SD-WAN, firewalls, cybersecurity, IoT monitoring, and more – all on a small, streamlined stack.

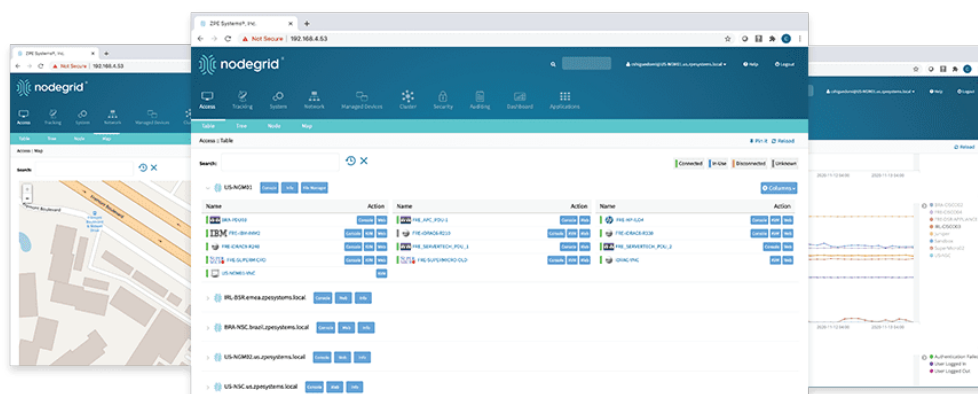
Edge software also lets you unlock the full power of automation so you can optimize your networks. This includes everything from initial deployment via zero touch provisioning, to self healing, automated routing, troubleshooting, and more. Automation is key to providing a smooth experience for internal and external network users.

## Management

The future of edge networking is bringing more distributed locations. It's not practical – or economical – to continue spending money on on-site support and management. You need a platform that gives you centralized control of everything, so you can save on support costs and maximize your ROI. This includes management capabilities for not just your distributed networks, but also for your underlying infrastructure components.

The future of edge networking lets you access your global WANs and LANs with the press of a button, using remote out-of-band that gives you omnipresent control. It shows your networking topology on a unified interface, and puts you in charge of your SD-WAN & firewall solutions, Guest OS & virtualization layer, and cloud integrations.

With your network more distributed than ever, your edge out-of-band solution needs to empower optimization. This includes everything from being able to remedy issues with third-party VNFs, to updating device firmware, to recovering from failures at the network, system, or platform level.



# Deep & Comprehensive Security

Trust less, protect more

Growing your enterprise's global footprint helps you meet demand and invest more in your business. But this also comes with increased security risks. With your networks cast far and wide, you become a larger target for hackers, attackers, and other malicious groups. This is why deep, comprehensive security is critical to your future edge networking capabilities.

Start your efforts by choosing a trusted hardware platform, and build a zero trust security posture to protect every network connection.

## Hardware

Setting up a secure edge isn't possible without protected hardware. When you launch a new network location, you need to make sure your data stays safe before, during, and after deployment. In order to achieve total peace of mind starting at the moment you ship your boxes, choose edge hardware that includes at least these features:

- **GPS Tracking** – See the exact location of your devices as they move to their destination. If they get lost or stolen, GPS tracking makes them easy to find.
- **No Pre-configuration Required** – Deploy hardware that can remain completely unconfigured until it's time to provision. This makes it impossible for your data to fall into the wrong hands.
- **Geofencing** – Set up geographic markers that allow your devices to boot only when they're safely at their destination
- **Secure Platform** – Make sure your hardware platform's integrity stays intact, with features like secure boot, signed OS, self-encrypted disk, and trusted platform module (TPM).

## Zero Trust Security Framework

When it comes to protecting interactions with your network, a zero trust approach helps you achieve thorough edge security into the future. Though your enterprise will continue to add more points of access, zero trust security allows you to protect them all by segmenting traffic and employing appropriate safeguards.

Edge networking is already becoming increasingly identity based, and taking a zero trust approach will help you address the security requirements of both the data center and cloud.

So what does the future edge network look like with zero trust security?

- **Segmented** – Implement a software-defined perimeter (SD-P) that lets users access only the resources they need. This helps you secure and optimize for end users, network admins, and everyone in between.
- **Authenticated** – Deploy multi-factor authentication and password protection to safeguard every interaction, whether it's a salesperson trying to connect on the go, or an engineer accessing a remote branch device.
- **Monitored** – Ensure edge interactions remain under watchful eyes with trail logs, alerts, and notifications. Your future network monitors data and alerts you to suspicious activity.

## Wide-ranging Extensibility

Be free to customize and adapt to change

Even the most experienced industry leaders struggle to keep up with the evolving networking landscape. Standardizing on a single vendor's solution may have satisfied requirements from 10 - 15 years ago, but this can lead to catastrophic consequences in the near future and beyond. As edge technology leaders have yet to emerge and the market faces inevitable volatility, it's critical to choose a platform that can readily adapt to shifting requirements.

### Why Extensibility?

Wide-ranging extensibility is a must for successful edge networking into the future. It helps you:

- Customize your solutions to fit your exact needs.
- Remain free to choose & adapt as the market evolves.
- Grow into the future without being held back by vendor lock-in.

### How Do I Choose a Platform?

Many platforms offer improved distributed processing and complete security, but few provide the extensibility to keep you future-proof. Fewer still offer solutions that are truly vendor-neutral and give you complete freedom when it comes to third-party and custom integrations.

When considering your future edge networking capabilities, look for an extensible platform that helps you:

- Integrate the right solutions for your exact needs, regardless of vendor.
- Deploy third-party and custom applications so you can evolve alongside the market.
- Avoid vendor lock-in using a truly vendor-neutral software layer.

## Need Extensibility? Look no Further than Nodegrid

Nodegrid OS gives you complete vendor-neutral extensibility to accommodate all your third-party and custom solutions. The Nodegrid Services Router also gives you hardware flexibility, with modular add-ons that let you tailor your virtualization, compute, networking, and serial capabilities.





---

## Valuable and Controllable Data

Give the right data to the right systems

Using traditional core-to-edge networking means data is processed at the core. But the future will bring enormous amounts of data from the edge and only exacerbate the issues of conventional infrastructures. With more distributed data, how do you make sure that information gets processed correctly?

At the edge, it's important to deploy analytics and monitoring solutions that can detect which data is valuable to local systems and users. This is especially true for edge implementations that require real-time responsiveness. Your network will be able to serve end users appropriately while sending low-value information back to the data center for further processing.

This also aids in information lifecycle management, and machine learning & artificial intelligence (ML/AI) efforts. In the future edge, valuable data will be stored close to where it is used, whether it means being accessible to a banking customer, a cloud-connected device, or a kiosk featuring artificial intelligence systems.

An extensible platform only empowers your data management capabilities so you can optimize and maintain your distributed networks. You can leverage third-party and custom data solutions that provide valuable insights, while giving you in-depth control to address your changing requirements.

---

## Want to see your future in edge networking?

Visit [www.zpesystems.com](http://www.zpesystems.com) to set up a free Nodegrid demo, and see the future of edge networking – today.

Edge networking will see many changes in coming years. But you can lay a strong, flexible foundation that covers all four of these critical requirements. Nodegrid is the only solution that gives you total freedom of choice, on an Intel-based platform featuring the powerful Nodegrid OS.