Executive Guide to Agile NaaS

How to work with IT to develop a future-proof NaaS strategy

HPE aruba networking

Organizations now recognize that digital transformation is the key to new business models, expanded and enhanced customer engagement, and increased efficiencies. Pop-up retail stores, telemedicine, distance learning, and hybrid work are all examples of how IT can deliver innovative business outcomes.

More than ever, business goals and objectives are driving IT. This means IT must be agile enough to partner with the business—producing the outcomes required within the schedule and budget the business can afford.

Organizations are considering network as a service (NaaS) to accelerate their network modernization efforts to increase IT's responsiveness, agility, and efficiency.

Most people familiar with NaaS associate it with changing from a CapEx to an OpEx consumption model and enlisting a third party to manage day-to-day operations. That is NaaS in its simplest and most basic form.

This guide provides a more detailed and nuanced look at the implications of NaaS and, importantly, how a C-level executive or business manager can work with their IT teams to evaluate NaaS solutions. Selecting and implementing NaaS has both technical and business implications. As such, it should be a joint evaluation process between business and IT, where both work together to reach the right outcome.

Here are some things to consider in your evaluation.

One size does not fit all

Many NaaS vendors, especially those new to the market, force customers into a monthly payment model while they, the vendor, manage the network—often using untested and immature technology to shave costs. This approach overlooks several key decision criteria that help organizations determine the right NaaS solution, including:

- Risks that come with introducing cost-centric, new, and unproven solutions
- Level of security required
- Quality of the outsourced staff and their tools
- Ability of the underlying technology to match each organization's specific needs
- Type of financial model that best fits budget allocations

Let's look at each of these from a business perspective, with a set of recommendations for addressing each issue.

Understanding risks and costs

An attractive feature of NaaS is the ability to better manage network economics with monthly payments while 'flexing' up and down as needs change. But, unlike HPE Aruba Networking, many new NaaS vendors use suboptimal hardware to offer an attractive price and lack the portfolio to properly address key connectivity use cases (e.g., outdoor wireless). Design compromises, portfolio shortcomings, and lack of real-world exposure increase the risk that these solutions will not deliver the performance and reliability an organization needs—or that service level agreements (SLAs) promise. Ironically, a relatively small cost of a NaaS solution resides in the hardware and, as we'll explain below, that's where cost-focused vendors are at a decided disadvantage.

Recommendation: When considering NaaS options, carefully evaluate the quality, track record, and performance of the underlying hardware. Has the hardware been deployed in an environment that matches your organization's profile?

Fitting into your security strategy

The network is an integral part of a security strategy. Without a strong, built-in set of hardware and software security controls, the network can be an inviting target for attackers. Security, however, is often an afterthought, and NaaS vendors that prioritize cost and SLAs focused on simple activity measurements tend to rely on external, third-party appliances to provide security. This creates complexity and difficulty integrating with the broader security ecosystem, resulting in increased costs and a more vulnerable IT environment.

Recommendation: Carefully evaluate the security controls built into a NaaS solution and how they fit into the overall security architecture. Avoid adding unneeded third-party appliances and expand the SLA to cover security outcomes.

Network complexity continues to grow. Is the vendor up to the challenge?

Globally, organizations are struggling to staff their IT operations, including the networking team. Having a third party manage the network is appealing, but they will need the right tools to be successful. Whether the network is managed internally or by a third party, the answer is to increase the efficiency of network staff by using analytics (AI) and automation to handle mundane tasks and reduce the time to find and fix problems.

But the key to effective AI-powered solutions is the data lake used to train the AI models. Without a large volume and variety of relevant data, you cannot trust and act on the AI results. Despite many "self-driving" claims, network vendors with small customer bases are starved for data, and it will be many years before they have the AI needed to manage networks. Immature AI will only lead to poor network performance and unhappy users.

Recommendation: Insufficient and untrustworthy AI means that more people will be required to manage the network. Understand how the NaaS vendor will find (and afford) the people needed to manage the network. Adding additional people (if they can find them) to manage the network means that their cost structure won't be viable.

Managing Service Level Agreements (SLAs)

The idea of network services delivered and paid for like electricity is very attractive. However, networks need to successfully operate in a wide variety of physical environments, impacting the type of equipment required and how it is installed and tuned. A distributed retailer has different requirements than a six-story office building or college dormitory. Some NaaS vendors will try to cover up these differences with SLAs that oversimplify their guarantees. But without real-world experience across a wide variety of network sizes and operating environments, the SLAs and infrastructure they rely on will be best guesses based on generalized assumptions. Whether the SLA is right for the organization and will be met are big unknowns.

Recommendation: Understand how the NaaS vendor makes key performance decisions, such as where to place wireless access points and other networking equipment, and how they set, measure, and report on their SLAs. Importantly, define how information flows from the third party to the network team and how they will address issues such as poor performance, security breaches, and outages.

CAPEX or OPEX?

NaaS typically starts with the premise that payment is on a monthly (OpEx) basis. Many organizations will find that attractive, but there are instances where CapEx is the only practical acquisition route due to the funding process, lack of long-term visibility, and regulatory constraints. Even if an up-front CapEx acquisition model is the preferred strategy right now, there is no reason not to include NaaS as part of a longer-term strategy due to the flexibility and agility an OpEx-based funding approach provides.

Recommendation: Work with a NaaS vendor that offers a variety of acquisition models.

NaaS without compromise

The best NaaS strategy for an organization depends on a mix of factors. NaaS can be delivered in many different combinations of solutions, consumption, and management models, so don't get locked in or compromise on critical requirements. Each organization is unique and NaaS should satisfy each customer's needs and requirements—not stick to a rigid definition. Seek out a NaaS partner that has the agility to meet a wide range of requirements, both now and in the future.

The choice of a NaaS partner is not just an IT or a business decision. By establishing a robust evaluation process that starts with business requirements, a joint business/networking team can evaluate various options and arrive at the right NaaS solution for the organization.

Take the NaaS assessment to discover strategy recommendations tailored for your objectives.

Make the right purchase decision.
Contact our presales specialists.

Contact us

BP_AgileNaaS_RVK_070723 a00130188enw