NETWORK AS A SERVICE

Mark Fishburn, July 2024

Contents

NETWORK AS A SERVICE

Enterprise-centric

Network as a Service (NaaS) is enterprise-centric rather than network or cloud-centric. This is the fundamental difference from other approaches such as SASE, or SSE, IP or Ethernet Services or MPLS. It's a layered approach that is

- Agnostic to the manner and number of providers that an enterprise uses to provide the service. Large and multinational organizations might use several concurrently.
- Transparent to the underlying architectures and the location of cloud, edge and data-center-based workloads. Sensitive to Critical Infrastructure OT direct links while using the internet for IP networking.
- Independent of the automation, identity, authentication and security policies and implementation such as SASE and SSE.
- Flexible to the on-demand business requirements as organizations constantly migrate independent of underlying technologies.

The Enterprise Aspiration

NaaS brings the opportunity for enterprises of all sizes to have a simple transparent interface with the network without having to get involved with its operation. They can depend on it enabling their applications, wherever they are located, to work with consistent performance and to work securely. The services are available on demand via subscription without being locked in to any provider or vendor.

Implications

As stated, NaaS differs from previous network and cloud-centric architectures and offerings such as SASE and SSE is that the focus is switched to the business, performance and application dynamics of today's organizations. This is, after all, what technology must serve. It begins and ends with the business priorities supported by the network suppliers, cloud providers and integrators – rather than business requirements that can be accommodated (or not) by the network and cloud service providers.

The Need for Network as a Service

The executive priorities of agility and responsiveness to business change have not been served by current/past network and cloud paradigms. What is missing for today's services is virtualization and on-demand service creation. The result has been long, complex, inflexible network implementation cycles.

Lack of support for low cost, simplified, connectivity has prevented, delayed or been unresponsive to rapidly changing business conditions such as frequent reorganization, new locations or M&A situations. Further, the complexity of network solutions of applications that span multiple cloud providers and multiple locations in multiple geographies make matters worse. In fact, being drawn into onerous

support of complex architectures does not serve organizations. Added to this, what amounts to a cyber war creates added business risk, impeding running a successful, profitable operation.

Collectively, these amount to a counter-productive constraint on business rather than an enabler. It goes against CIOs and IT managers goals of minimizing network complexity, costs, risk and simplifying management, provisioning, procuring and maintenance.

At a time of simple on-demand consumption, such a fixed approach to networking is an anachronism. The implementation choices reflecting the level of delegation to providers that works for the enterprise IT departments. Security is integral, with verification rather than trust being the watchword.

NaaS Attributes and Business Impact

Based on cost and business dynamics, the following is a deeper dive into why the attributes of NaaS impact the enterprises business goals. To be somewhat flippant, it comes down to what can only be summarized as a "wake me when it's over and leave me to run my business" attitude to networking.

NaaS Attribute	Positive Impact
A provider-delivered model with on-demand properties of cloud allowing use of network services **without owning**, building, **or maintaining** their own infrastructure.	Lower Cost, rapid response to changing business conditions.
NaaS allows users high performance with seamless access to any application anywhere from any location.	Performance and flexibility to operate and function from any existing or new location. Allows scalability for enterprise application workloads to meet business demand.
It provides dynamic user choice via on-demand, **consumption-based billing** (via portal- or API-based).	Ability to add, remove or upgrade services at will without commitment. Flexibility to align costs with consumption and location as application loads and business conditions vary.
NaaS brings **responsiveness to business dynamics**, irrespective of the underlying technology.	Maximizes user productivity and always available uptime even during peak times.
Naas brings choice allowing users to select from Platform or Infrastructure as a Service or Managed Services.	Allows users to match their network infrastructure to their expertise and desired technical involvement.
Aligned with Zero Trust Principles, it enables proper **verified delegation of all security functions** reducing the cost and expertise needed by the enterprise.	Network-Security-Application- Performance combination is critical with regulatory and corporate compliance. NaaS Security eliminates the need for scarce network security expertise.
Finally, NaaS brings much sought-after **simplification of operations** for enterprises with resulting cost reduction	NaaS – effectively "packages" network services to support the requirements of workloads rather than enterprises having to engineer the network services themselves.

Defining Network as a Service

NaaS provides a cloud-enabled, usage-based consumption model that allows users to acquire and orchestrate a network without owning, building, or maintaining their own infrastructure. The business requirements outlined above are driving the need for agile digital platforms for delivering the wide range of cloud, networking and security services utilized by large organizations. NaaS features a number of attributes that are aligned with critical business objectives.

NaaS Offers Choices to Match Enterprise Requirements

These choices vary driven by resources, expertise and preferred supplier relationships. It seems highly likely that NaaS solutions will require several business collaborations. The following are three examples of choices for NaaS but combinations from several suppliers may need to be accommodated in different geographies or enterprise divisions:

Managed Services

- A turnkey managed network to plug in client devices. Encompasses connectivity and security services as a package. Includes: customer premises equipment, third-party delivered and operated, provider delivered and operated, co-managed by customer and MSP and is dashboard/portal driven.
- Typical contracted outcomes include latency and application performance levels, availability, security and interoperability

Platform-as-a-Service (PaaS)

A cloud-enabled platform that allows creation of custom transport service via virtualized service objects without owning, building, or maintaining their own infrastructure.

- PaaS features: On-demand service enablement via Portal or APIs, outcome-based consumption, connectivity + network services, consumption-based billing and service agility.

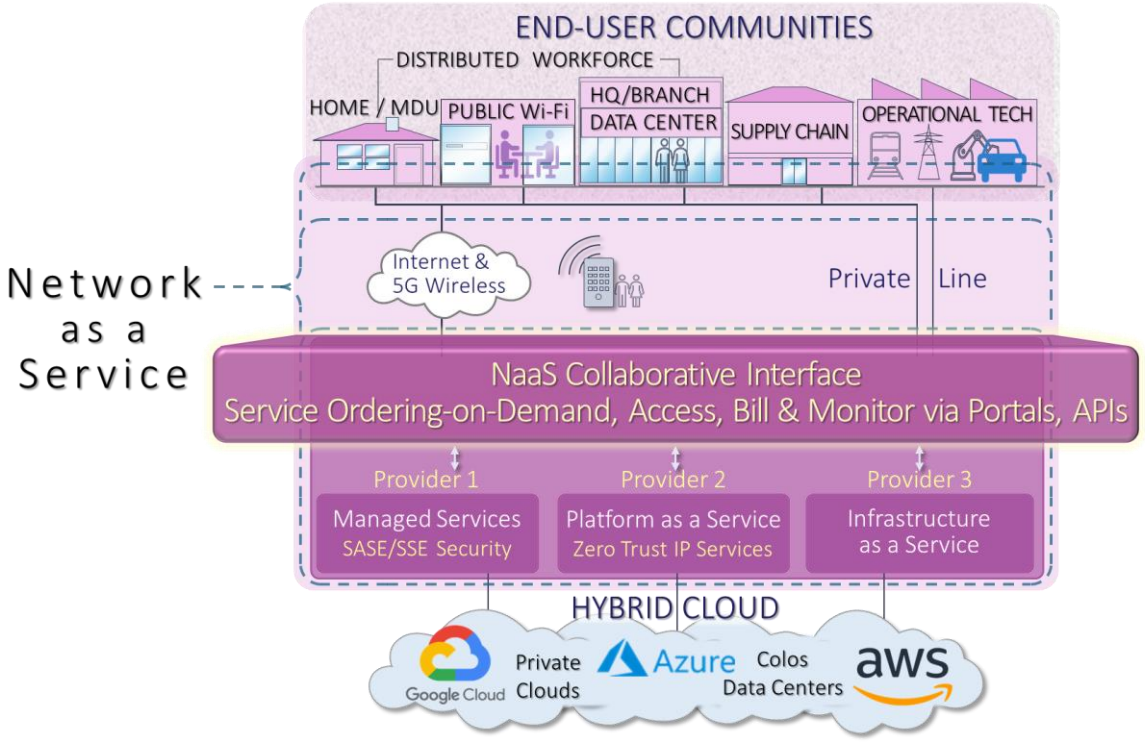
Infrastructure-as-a-Service (IaaS)

An automated platform that allows creation of customer defined “bare-metal” services on another provider’s premises and/or equipment. Provisioning may be traditional or API/portal orchestrated.

- IaaS features: Racks, power, servers and network devices managed by the provider, configured by customer/clients. Lifecycle management by provider and customer managed/owned devices. IaaS may just apply to areas of operations where applications or operational technology networks have demanding real time requirements, feature legacy IoT systems with separation or specialist security in a private data center.

SASE, SSE, Zero Trust and NaaS - Working Together

The diagram shows the true flexibility of a well-implemented NaaS system. It shows three providers operating in different geographies. One has implemented SASE/SSE and managed services via Internet access. The second implements the Zero Trust Principles with service attributes specified in the MEF 118 standard. The third services a critical infrastructure division operating over private lines to a service provider running an IaaS network. The Managed Service Provider provides common API services on-demand via a portal or via APIs. Finally, if NaaS is enterprise-oriented, shouldn't they be at the top of the diagram? It may look strange to network people but it does **turn the world of networking upside-down!**



The Heart of the Matter

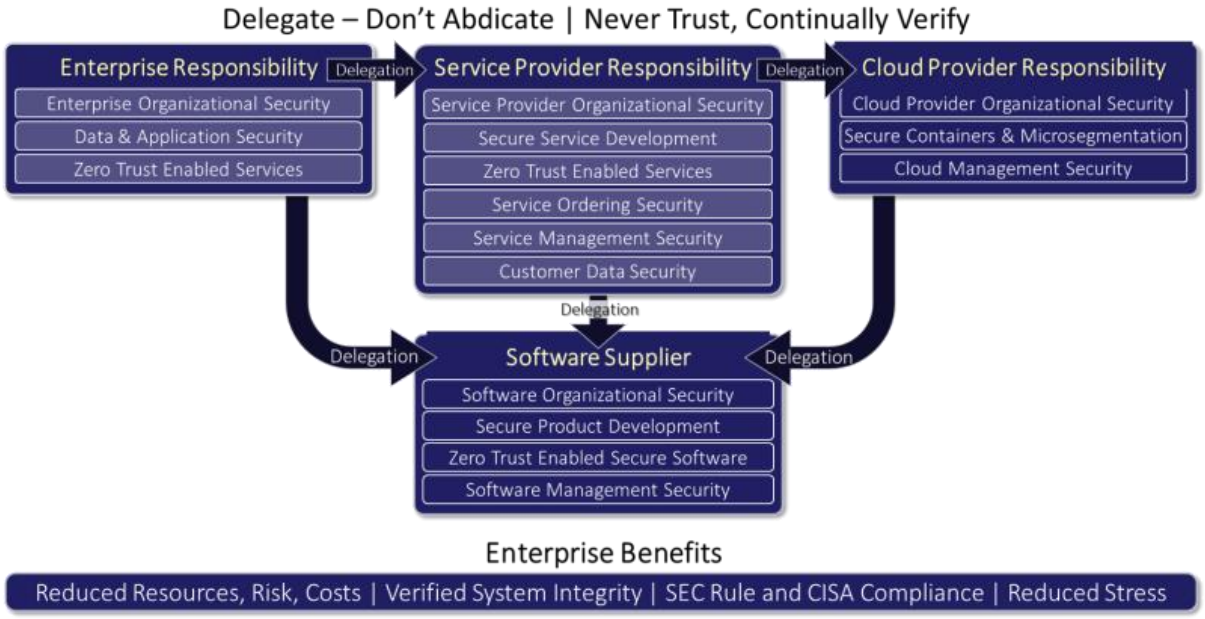
Shown above, is how NaaS fulfills the enterprise's requirements via a portal or secure APIs for on-demand ordering, consumption based billing, consistent performance and incident reporting.

NaaS can be offered in many forms as covered earlier: Infrastructure as a Service, Platform as a Service Managed Services and others. The scope of services can vary too as shown by the dashed lines above. It could be within the enterprise, at the network edge or where several providers are involved, service further into the network. It also shows that the fixed idea of "the Cloud" is being replaced by many different hybrid combinations of Cloud, colocation and private edge data centers. It's all NaaS!

NaaS - A Cybersecurity Breakthrough

Perhaps the most difficult aspect of cybersecurity are supply chains. Enterprises always retain responsibility but without direct control over suppliers, especially service/cloud providers, their software and hardware suppliers. NaaS brings the opportunity to apply Zero Trust's "Never Trust Always Verify" principle. I.e., to work with software and hardware providers with a common approach to self-verification and to strengthen every link in the defensive chain. For the first time security can be confidently delegated to the network providers.

The scope is shown below, with details on the cybyr.com/delegation page. For example, even the service ordering software should be developed with memory-safe languages, and its management should guard against denial of service attacks, etc.



It's the alignment of service ordering and billing that begin the process and the need to unify service offering without lock-in. Unified single pane monitoring and reporting means that those suppliers that also align their development and management will clearly become market leaders. The natural leaders will be the service providers who will also look to suppliers who can meet the requirements. These best practices naturally develop healthy security habits.

In turn, this will shift the burden from enterprises who typically have had to manage security themselves or risk abdication of responsibility. This frees up expert resources and avoid having to pay for high priced and hands on management of security operations.

NaaS Delegated Security Summary

The power of delegating, while not cannot be perfect, ensures that potential weak links are both identified and strengthened, is profound:

- Aligns with CISA self-attestation guidelines and Zero Trust principles
- Provides methodology for enterprises to delegate responsibility to supplies to enable proper accountability and governance.
- Reduces risks, costs and expert resources to oversee network, provider and cloud security and verifies system integrity
- Enables written security policy to meet SEC rules and reduce insurance costs
- Intercepts CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) 2024/2025

Operational Characteristics

- Organizational Security
  - Security Policy-driven, social engineering, insider threats, staff training, BYODs banned, MFA/Passkeys, malware detection & removal, etc.
- Data & Application Security
  - Asset curation, encryption, anti-phishing, least privilege, access, IdM, MFA
  - Cloud microsegmentation, secure containers, workloads, etc.
  - OT network separation
- Secure Service & Software Development
  - Per CISA best practices, coded in a memory-safe language
- Zero Trust Enabled Services and software
  - Authentication, policy management, enforcement, automated monitoring
  - Secure service and software management

Challenges to Widespread NaaS Adoption

- Network as a Service is definitely an ongoing journey that requires collaboration. One of the first steps is the availability of common ordering and billing portals or APIs. In order to meet the challenges of on-demand services ordered via a common portal, such a portal needs to exist.
- One approach would be to allow such a portal itself to be proprietary provided it supports commonly agreed secure APIs. Such a portal would be developed using DevSecOps best practices in alignment with the new CISA recommendations.
- This would also allow service provider collaboration since most large organizations span many countries. The same applies to cloud provider collaboration as almost all enterprises wish to connect to applications hosted by multiple cloud providers.
- Next, there is the question of network device ownership. Before the era of Cloud-centric and perimeter-less networking, Network as a Service was first mooted a decade ago. This was a sticking point. Today's implementation must address a related challenge that of ownership of equipment that is flexible enough to adapt to dynamic changes v. a subscription model that has a challenging price tag. As we said, this is a journey.

Acknowledgements, Source of the Work

- The evolution to Network as a Service is the next step in the journey of the Network driven by new technology, business models, centralized, decentralized, Cloud and hybrid ecosystems that have flowed back and forth for five decades. This NaaS work began with the Open Networking User Group Collaborative NaaS Project and was authored and posted on the ONUG Web site including reviews and contributions from Steve Wood, Cisco, Ken Patel, Verizon and members of the NaaS Project Team. It's been refined with new ideas since its publication and will continue to do so as the challenges listed are met.
- It has also grown from ideas in the MEF (MEF.net) as it explore NaaS, its security work on Zero Trust and SASE/SSE and from work in the Cloud Security Alliance. Before that work in the MEF on Carrier Ethernet and SD-WAN were a previous part of the journey.
- Both ONUG and the MEF are exploring the business requirements, leading use cases and underlying technologies critical for the adoption of Network-as-a-Service by large enterprises. The first iteration was presented at the ONUG Fall 2023 conference. It continues to evolve providing the context for use cases.

