Is it time to redefine your IT Service Expectations?

To be one step ahead of cybercriminals, you need the best network security possible. With IT solutions like secure access service edge (SASE), you'll benefit from cutting-edge protection against attacks from bad actors.

While SASE is not new, ransomware attacks, the increase in remote work, and the demand for efficiency have contributed to the growth of this new framework of security. Net-Tech provides the IT support Seattle organizations need, including SASE.

What Is Secure Access Service Edge (SASE)?

Secure access service edge, or SASE (pronounced "sassy"), was first described in Gartner's August 2019 report ,***The Future of Network Security in the Cloud,*** and expanded upon in their 2021 Strategic Roadmap for SASE Convergence (footnote).

SASE is not a single product. It's an overarching framework built on the idea that network security should efficiently support employees while ensuring comprehensive security. It takes a different approach from traditional network security in that the emphasis is on protecting entity (user) access and not on creating perimeters around networks.

How Security Trends Have Created the Need for SASE

In recent years, SASE has become more defined as demand has grown. More employees are working remotely, at the "edge" of traditional networks. Traditional solutions no longer work because they rely on fixed approaches to security that are not flexible enough for today's employees.

In the past, organizations offered specific remote access products (such as VPNs) that worked for their small number of remote employees. Now, the increasingly large number of remote employees has changed the requirements for network security.

The demand for both top-quality security and easier access for remote workers has created a dilemma which SASE aims to solve.

Remote workers need solutions that support them outside of a centralized office. They need less hassle when accessing organizational tools and resources. SASE provides more protection with less friction.

The Core Components of SASE

Cybersecurity threats are worse now than ever. The overarching framework of SASE is to provide users with local security and the most efficient service.

Experts have identified 5 key tenets of the SASE framework:

Cloud-based service architecture

Dynamic & local enforcement of policy

Central visibility and logging

Network security for mobile and IoT

Minimized latency

Adopting these core components ensures that an organization is following SASE best practices.

Why IT Support Teams Like Net-Tech Recommend SASE

More IT leaders are looking to adopt SASE because of the 3 key benefits it offers: lower costs, better user experience, and stronger network security.

Decreases IT Costs and Increases IT Solutions

To fight the growing threat of cybercrime and to support remote employees' needs, many organizations have spent significant amounts of money, time, and manpower establishing new systems. This was especially true during the rush to remote work that took place at the beginning of the COVID-19 pandemic.

However, according to Zscaler, "Even with this increase in cost and complexity, the network security model still can't scale, isn't agile, and is simply not effective in a digital world."

The existing legacy network security model, which is focused on creating perimeters around applications, isn't sufficient for today's workforce. This model relies on multiple products, resulting in high costs. Integrating multiple products also complicates processes. SASE provides alternative solutions that simplify these issues.

Users Come First

To help all users work efficiently, SASE takes the approach of supporting entities (users) first and pushing security as close to them as possible. The SASE framework focuses on providing optimal bandwidth and the lowest latency. In the SASE framework, the security stack should be placed as close to the user as possible in internet exchanges.

Reduces Risk

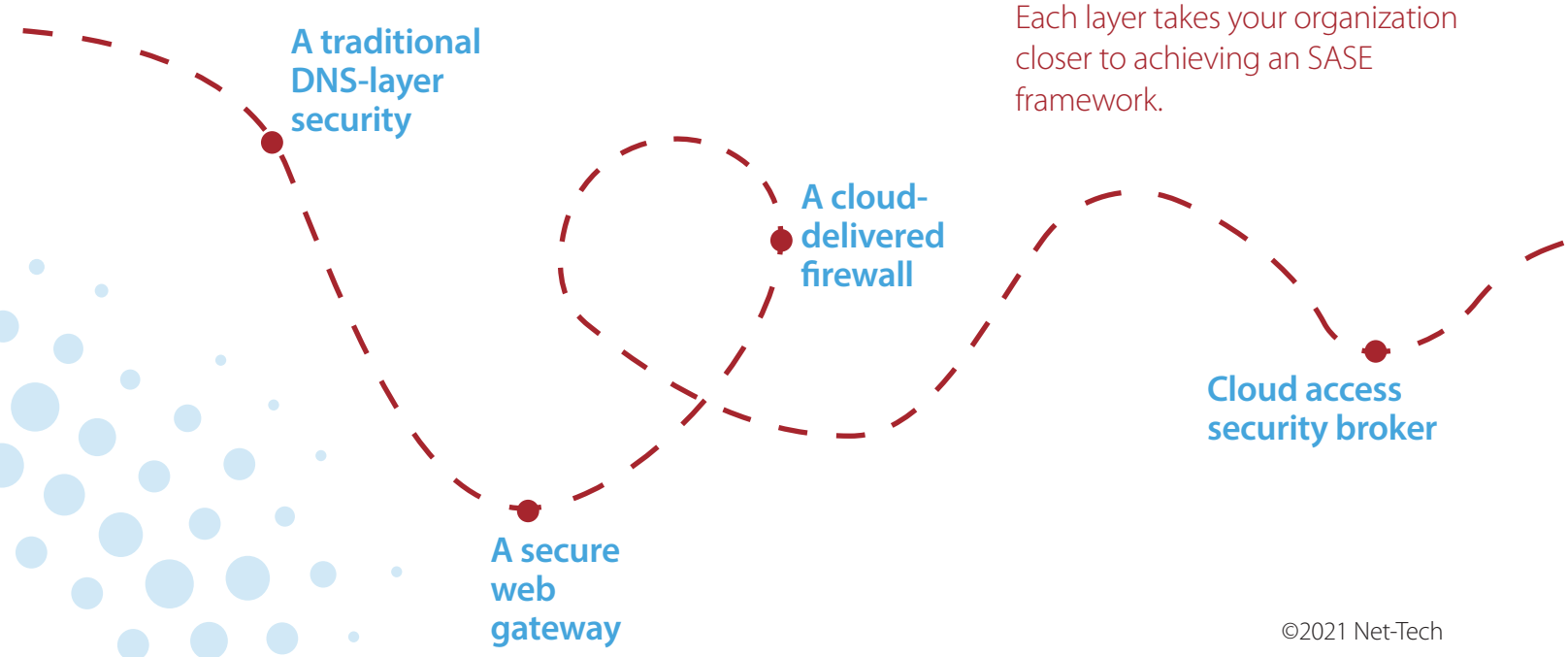
Remote work has created security nightmares for some organizations. The need for users to access data from a variety of locations creates more opportunities for vulnerabilities to be exploited. However, remote work isn't going away, and neither are these security issues.

SASE aims to solve this remote-work problem by prioritizing the adoption of a Zero-Trust Network Access (ZTNA) protocol. This means that users are granted access to the files they need on a file-by-file basis, rather than having access to all organizational data. A ZTNA approach greatly reduces the risks to network security.

Cloud Integration and SASE

If you consolidate services into a single platform, you simplify your operations. You can streamline almost every aspect of your networking and security processes. Companies like Cisco offer umbrella coverage that allows you to consolidate services into one platform that extends across users, devices, clouds, campuses, and branches.

Cisco explains how, with SASE, you can combine and integrate multiple security services. One potential SASE model contains 4 layers:



Each layer takes your organization closer to achieving an SASE framework.

Planning for Network Security Through SASE

Before you begin planning to adopt the SASE framework, it's important to remember that this is a long-term process and not a quick switch. Just as it has taken years to change from on-premise to cloud-based models, it will take time to achieve an SASE framework.

If your organization will be transitioning to a remote environment, it is especially important to plan to establish an SASE security model.

You should plan for:

1. **Cloud-based service architecture**
2. **Dynamic & local enforcement of policy**
3. **Central visibility and logging**

No single tech company can provide a complete SASE framework. Multiple different vendors will need to be brought on to meet SASE requirements. Net-Tech offers the IT support Seattle organizations can depend on to begin building an SASE framework.

How Net-Tech Supports SASE

Net-Tech is a future-ready professional technology organization providing next generation managed IT services. We prioritize adopting the best tools and setting up our clients with the right frameworks. Organizations can adopt an SASE framework through our IT subscription program.

Net-Tech will build the SASE framework for your organization. When it comes to the architecture of the model, you don't need to make any decisions. We take care of it all: tools, monitoring, and updates are all handled with complete transparency.

Are you interested in learning more about SASE or changing your IT approach? Reach out for a complimentary IT analysis today.

Want to discover more ways to keep your systems safe?

Contact us for a complimentary IT analysis with one of our top cybersecurity experts today.

Call (425) 452-8324 or visit net-tech.com

net-tech