Whitepaper

# SASE:

## The Imperative for IT/ITeS Companies in a Hybrid Work Environment

# TABLE OF CONTENT

# Introduction

> According to a Stanford University study, as of March 2023, about 30% of the workforce continues to work remotely, while the majority has returned to the office. This shift towards a hybrid work model presents unique challenges for the IT/ITES sector, particularly in terms of network management, security, and performance. SASE emerges as a crucial technology that can help navigate these complexities, providing robust, secure, and efficient network infrastructure for the hybrid workforce

In the rapidly evolving digital landscape, the IT/ITES sector stands at the forefront, driving innovation and enabling businesses to adapt and thrive. As this sector continues to grow and transform, it faces a unique set of challenges and opportunities. One of the most significant shifts in recent years has been the transition to a hybrid work environment, where remote and office work coexist. This shift, while offering numerous benefits such as increased flexibility and access to a wider talent pool, also introduces new complexities in terms of network management, security, and performance.

The IT/ITES sector, with its reliance on high-speed, secure, and efficient data transmission, is particularly affected by these changes. The need to access corporate applications securely from various locations, the increased demand for high-quality audio and video communication, and the heightened cybersecurity threats are just a few of the challenges that this sector needs to address. Moreover, the legacy systems that many IT/ITES companies still rely on can create blind spots, leading to security vulnerabilities and performance issues.

In this context, Secure Access Service Edge (SASE) emerges as a crucial technology. SASE is a new approach to network security that combines network and security functions with WAN capabilities to support the dynamic, secure access needs of organizations. By adopting SASE, IT/ITES companies can optimize their network performance, enhance security, and navigate the complexities of a hybrid work environment more effectively.

This whitepaper explores the role of SASE in the IT/ITES sector, discussing the challenges of a hybrid work environment and how SASE can help address these challenges. It delves into the key expectations from a SASE solution and how it can help IT/ITES companies modernize their network infrastructure and improve the security and efficiency of their networks.

# The Hybrid Workforce in IT/ITES

The IT/ITES sector, a critical driver of the global economy, has experienced a significant shift towards a hybrid work model. According to a Stanford University study, as of March 2023, about 30% of the workforce continues to operate remotely. This transformation has been largely facilitated by advancements in technology, such as high-speed internet and cloud computing, which have made it possible for employees to work efficiently from virtually anywhere.

However, the transition to a hybrid work model is not without its challenges. One of the primary issues is ensuring reliable and secure connectivity for remote workers. With employees accessing sensitive corporate data from various locations, often on personal devices, the risk of cyber threats increases significantly. This necessitates robust security measures to protect both the company's and clients' data.

Collaboration is another challenge in a hybrid work environment. Teams are now distributed, with some members working from the office and others remotely. This requires effective communication tools and strategies to ensure seamless collaboration and maintain productivity levels.

Moreover, managing the performance of IT infrastructure becomes more complex in a hybrid work model. With increased demand on network resources due to remote work, IT/ITES companies need to ensure their systems can handle this load while still providing a smooth user experience.

In this evolving landscape, the IT/ITES sector needs to continually adapt and innovate to effectively manage these challenges. The adoption of technologies like Secure Access Service Edge (SASE) can play a crucial role in this regard, offering solutions to optimize network performance and enhance security in a hybrid work environment.

# SASE in IT/ITES

## 1. Providing Secure and Lag-free Access to Corporate Applications

Providing secure and lag-free access to corporate applications is a key challenge in a hybrid work environment. IT/ITES companies often use high bandwidth applications for tasks like data analysis and software development, which require optimized network performance. SASE can help by providing secure remote access, optimizing network performance, and improving application delivery.

### The Challenges

- **Security:** When employees access corporate applications from outside the office, they are at a greater risk of being attacked by hackers. This is because they are not protected by the same security measures as when they are in the office.
- **Performance:** When employees access corporate applications from a remote location, they may experience lag time. This is because the applications may be located in a different data center, which can add latency to the connection.
- **Cost:** Providing access to corporate applications to remote employees can be expensive. This is because organizations need to invest in the infrastructure and software to support remote access.

### Solution

**Despite these challenges, there are a number of steps that organizations can take to provide secure and lag-free access to corporate applications to remote workers. These steps include:**

- **Using a secure remote access solution:** A secure remote access solution can help to protect corporate applications from unauthorized access. These solutions typically use encryption and other security measures to protect data in transit and at rest.
- **Optimizing the network:** Organizations can optimize their networks to improve performance for remote workers. This can be done by investing in high-speed internet and by using a content delivery network (CDN) to cache frequently accessed content closer to remote users.
- **Using a cloud-based application delivery controller (ADC):** A cloud-based ADC can help to improve performance and security for remote workers. ADCs can optimize application traffic and provide security features such as SSL offloading and intrusion detection.

By taking these steps, organizations can provide secure and lag-free access to corporate applications to remote workers. This will help to improve productivity and employee satisfaction.

## 2. Addressing Enterprise Blind Spots

Legacy infrastructure can create blind spots, leading to security vulnerabilities and performance issues. IT/ITES companies need to modernize their infrastructure to support a secure, performant, and user-friendly hybrid work environment. This can be achieved by migrating to the cloud, upgrading to newer systems, and implementing security measures such as SASE.

**Some of the most common blind spots include:**

**Security vulnerabilities:** Legacy infrastructure is often more vulnerable to security attacks than newer, more secure systems. This is because legacy systems are often not patched or updated as frequently as newer systems. As a result, they can be more susceptible to malware and other attacks.

**Performance issues:** Legacy infrastructure can also lead to performance issues for remote workers. This is because legacy systems are often not designed to handle the increased traffic that comes with a hybrid workforce. As a result, remote workers may experience slow loading times, dropped connections, and other performance problems.

**User experience:** Legacy infrastructure can also lead to a poor user experience for remote workers. This is because legacy systems are often not designed to be used in a remote environment. As a result, remote workers may find it difficult to use legacy systems, which can lead to frustration and decreased productivity.

> **"The IT/ITES sector faces unique security challenges in a hybrid environment. SASE can mitigate these risks by providing a unified security architecture that protects users, devices, and applications from a variety of threats."**

## Plugging the Blind Spots

The desired future state for enterprises with legacy infrastructure is to have a hybrid work environment that is secure, performant, and user-friendly. To achieve this, enterprises need to invest in modernizing their infrastructure. This can be done by migrating to the cloud, upgrading to newer systems, and implementing security measures.

By modernizing their infrastructure, enterprises can create a hybrid work environment that is secure, performant, and user-friendly. This will allow them to attract and retain top talent, improve productivity, and reduce costs.

Here are some specific steps that enterprises can take to modernize their infrastructure and create a secure, performant, and user-friendly hybrid work environment:

**Migrate to the cloud:** The cloud offers a number of benefits for enterprises, including scalability, security, and cost-effectiveness. By migrating to the cloud, enterprises can improve their security posture, reduce their IT costs, and increase their agility.

**Upgrade to newer systems:** Older systems are often more vulnerable to security attacks and can lead to performance issues. By upgrading to newer systems, enterprises can improve their security posture and ensure that their systems are up to date.

**Implement security measures:** Security measures such as firewalls, intrusion detection systems, and data encryption can help to protect enterprises from security attacks. By implementing security measures, enterprises can reduce their risk of a data breach or other security incident.

By taking these steps, enterprises can modernize their infrastructure and create a secure, performant, and user-friendly hybrid work environment. This will allow them to attract and retain top talent, improve productivity, and reduce costs.

## 3. Optimizing Audio/Video Communication

With the rise of video conferencing and other applications, there is a growing demand for high-quality audio and video. Networks need to be optimized for audio/video access, which can be achieved by investing in high-speed fiber optic networks, content delivery networks (CDNs), and edge computing. SASE can further optimize network performance for these applications.

**There are a number of ways to optimize a network for audio/video access. Some of the most important factors include:**

**Bandwidth:** Audio and video require a lot of bandwidth, so it is important to have a network that can support the required speeds.

**Latency:** Latency is the time it takes for data to travel from one point to another. Audio and video are very sensitive to latency, so it is important to have a network with low latency.

**Jitter:** Jitter is the variation in latency. Audio and video are also sensitive to jitter, so it is important to have a network with low jitter.

**QoS:** QoS stands for Quality of Service. It is a set of techniques that can be used to ensure that audio and video traffic gets priority on the network.

**In order to enable efficient data flow across the cloud and through to the network edge, it is important to invest in the following communication infrastructure:**

**High-speed fiber optic networks:** Fiber optic networks are the best way to deliver high-quality audio and video. They are capable of carrying large amounts of data at very high speeds.

**Content delivery networks (CDNs):** CDNs are a network of servers that are distributed around the world. They are used to deliver content, such as audio and video, to users with the lowest possible latency.

**Edge computing:** Edge computing is a distributed computing paradigm that brings computing resources closer to the end user. This can help to improve latency and reduce the load on the network.

By investing in the right communication infrastructure, organizations can ensure that they have a network that is optimized for audio/video access. This will help to improve the quality of experience for users and enable them to enjoy the best possible audio and video.

## 4. Mitigating Security Challenges

The IT/ITES sector faces unique security challenges in a hybrid environment. Employees may use weak passwords, connect to unsecured Wi-Fi networks, or fall victim to phishing attacks. SASE can mitigate these risks by providing a unified security architecture that protects users, devices, and applications from a variety of threats.

**Weak passwords and security practices.** Employees are often more lax about security when they are working from home, which can lead to weak passwords, insecure devices, and other vulnerabilities.

**Unsecured Wi-Fi networks.** Employees may connect to unsecured Wi-Fi networks when they are working from coffee shops, libraries, or other public places. This can expose sensitive data to attack.
Phishing and social engineering attacks. Employees are more likely to fall for phishing and social engineering attacks when they are working from home. These attacks can lead to the compromise of employee credentials and sensitive data.

**Data breaches.** Data breaches can occur at any time, but they are more likely to occur in a hybrid environment. This is because there are more endpoints and more opportunities for attackers to gain access to sensitive data.

**To mitigate these risks, organizations should implement a comprehensive security program that includes:**

**Employee security awareness training.** Employees should be trained on security best practices, such as strong passwords, secure devices, and how to spot phishing attacks.

**Use of security tools.** Organizations should use security tools to protect their networks and data, such as firewalls, intrusion detection systems, and data loss prevention solutions.

**Implementing a zero-trust security model.** A zero-trust security model assumes that no one is trusted by default, even if they are inside the network. This model helps to protect organizations from attacks, even if they are successful in breaching the perimeter.

By taking these steps, organizations can help to protect their data and employees from security threats in a hybrid environment.

> Legacy infrastructure can create blind spots, leading to security vulnerabilities and performance issues. IT/ITES companies need to modernize their infrastructure to support a secure, performant, and user-friendly hybrid work environment.

## 5. Leveraging SASE for Network Optimization

SASE offers a scalable, flexible, and unified security architecture that can improve network performance and security. It can reduce latency, improve bandwidth utilization, and consolidate multiple security solutions into a single platform. This makes SASE an invaluable tool for IT/ITES companies looking to improve the security and efficiency of their networks.

Overall, SASE can be a valuable tool for organizations that are looking to improve the security and efficiency of their networks. If you are considering implementing a SASE solution, we recommend that you do your research and select a solution that meets your specific needs.

**Here are some of the benefits of using SASE solutions:**

**Improved security:** SASE solutions can help to improve security by providing a unified security architecture that can protect users, devices, and applications from a variety of threats.

**Increased flexibility:** SASE solutions are cloud-based, which makes them more scalable and flexible than traditional on-premises solutions. This can be beneficial for organizations that need to support a distributed workforce or that need to quickly scale their network security capabilities.

**Reduced costs:** SASE solutions can help to reduce costs by consolidating multiple security solutions into a single platform. This can also help to reduce the need for dedicated IT staff to manage and maintain multiple security solutions.

If you are looking for a way to improve the security and efficiency of your network, we recommend that you consider implementing a SASE solution.

# Expectations from a SASE Solution

IT/ITES companies expect a SASE solution to provide improved security, increased flexibility, and reduced costs. The solution should be easy to use, scalable, and secure. A SASE solution that meets these expectations can help IT/ITES companies modernize their network infrastructure and improve the security and efficiency of their networks.

SASE, with its cloud-native architecture, offers a unified approach to network security and connectivity, making it an ideal fit for the dynamic needs of the IT/ITES sector. It provides a scalable, flexible, and secure solution that can adapt to the changing demands of a hybrid workforce. With its ability to consolidate multiple security solutions into a single platform, SASE not only simplifies network management but also significantly reduces costs.

Moreover, SASE's zero-trust security model offers robust protection against the unique cybersecurity threats faced by the IT/ITES sector. Whether it's defending against ransomware attacks, preventing data breaches, or mitigating insider threats, SASE provides a comprehensive security solution that protects users, devices, and applications from a variety of threats.

In a sector where data security and network performance are paramount, the adoption of SASE can be a game-changer. By modernizing their network infrastructure with SASE, IT/ITES companies can not only navigate the complexities of a hybrid work environment more effectively but also enhance their operational efficiency, reduce costs, and ultimately drive business growth.

In conclusion, as the IT/ITES sector continues to evolve and adapt to new ways of working, the adoption of SASE is not just an option, but a necessity. It's a strategic investment that can empower companies to secure their networks, optimize performance, and thrive in the era of hybrid work.


CISCO