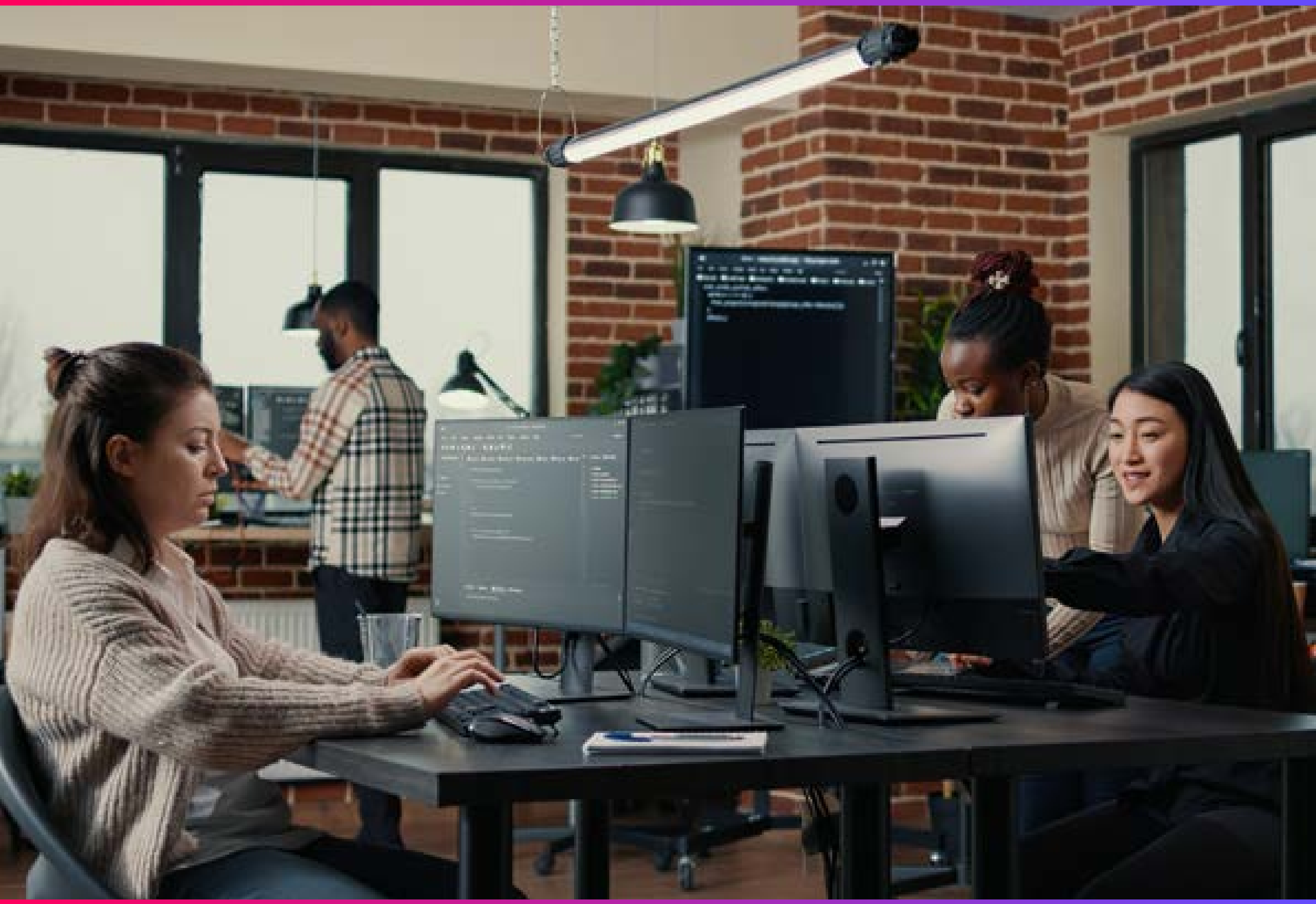
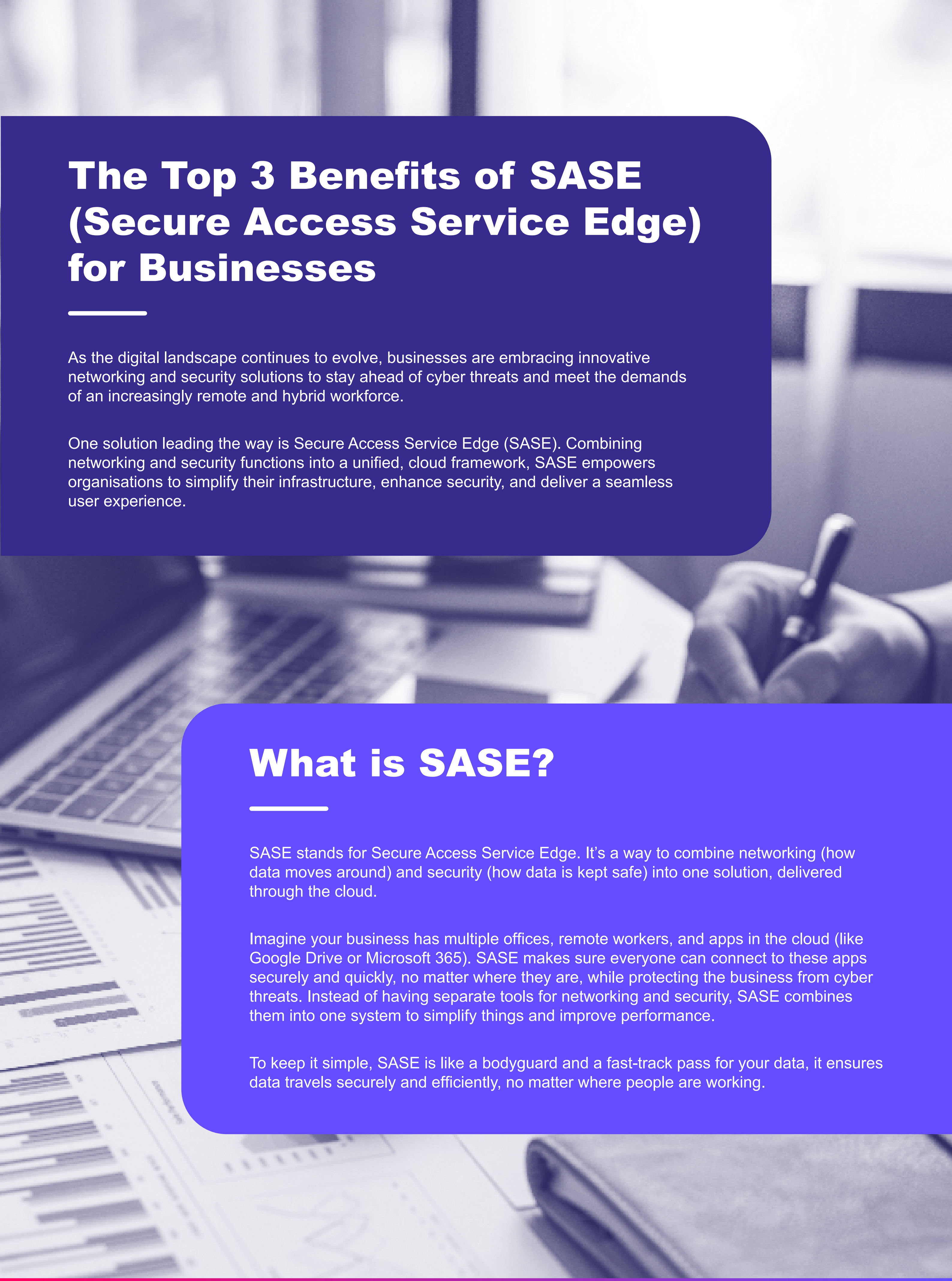
onecom

3 Benefits of SASE

(Secure Access Service Edge) for Businesses





The Top 3 Benefits of SASE (Secure Access Service Edge) for Businesses

As the digital landscape continues to evolve, businesses are embracing innovative networking and security solutions to stay ahead of cyber threats and meet the demands of an increasingly remote and hybrid workforce.

One solution leading the way is Secure Access Service Edge (SASE). Combining networking and security functions into a unified, cloud framework, SASE empowers organisations to simplify their infrastructure, enhance security, and deliver a seamless user experience.

What is SASE?

SASE stands for Secure Access Service Edge. It's a way to combine networking (how data moves around) and security (how data is kept safe) into one solution, delivered through the cloud.

Imagine your business has multiple offices, remote workers, and apps in the cloud (like Google Drive or Microsoft 365). SASE makes sure everyone can connect to these apps securely and quickly, no matter where they are, while protecting the business from cyber threats. Instead of having separate tools for networking and security, SASE combines them into one system to simplify things and improve performance.

To keep it simple, SASE is like a bodyguard and a fast-track pass for your data, it ensures data travels securely and efficiently, no matter where people are working.

Let’s explore the top three benefits of adopting SASE and how it can revolutionise business operations

1. Enhanced Security with Zero Trust Principles

Cybersecurity has become a top priority as businesses face an ever-increasing number of threats, from ransomware to data breaches. Traditional security approaches, often tied to on-premises infrastructure, struggle to keep pace with the complexities of modern, cloud-based operations. SASE addresses this gap by embedding security into the network itself, offering robust, integrated protection that travels with users and devices wherever they are.

Zero Trust Architecture: SASE operates on the principle of “never trust, always verify,” ensuring that every user, device, and connection is authenticated and authorised before gaining access. This reduces the attack surface and prevents unauthorised access to sensitive data.

Comprehensive Threat Detection: By integrating advanced security features such as secure web gateways (SWG), cloud access security brokers (CASB), and data loss prevention (DLP), SASE identifies and mitigates threats in real time.

Protection for Remote and Hybrid Workforces: With employees accessing corporate networks from various locations and devices, SASE provides consistent security policies across the board, ensuring that your business remains secure no matter where work happens.

For businesses, this enhanced security framework means reduced risk, fewer breaches, and greater confidence in protecting sensitive data.

Do’s and Don’t

Do:

- Implement a “never trust, always verify” approach to all users, devices, and applications.
- Continuously monitor and assess access permissions based on user behaviour and risk.
- Use multi-factor authentication (MFA) and encryption to secure access points.
- Segment your network to limit the lateral movement of threats.
- Regularly update and patch software to address vulnerabilities.

Don’t:

- Assume that any device or user within your network is inherently safe.
- Ignore insider threats or potential vulnerabilities in trusted users.
- Overcomplicate authentication processes, leading to user frustration.
- Delay implementing Zero Trust due to perceived complexity, as it’s easier to scale when done early.
- Forget to educate employees on the importance of Zero Trust principles.

2. Simplified IT Infrastructure and Cost Savings

Traditional networking and security solutions are often complex, requiring multiple appliances, platforms, and tools to function effectively. This complexity can lead to higher costs, administrative burdens, and inefficiencies. SASE streamlines this by consolidating networking and security into a single, cloud-native solution.

Consolidation of Tools: With SASE, organisations no longer need to deploy separate VPNs, firewalls, and other security appliances. Instead, these functions are unified, reducing management overhead and improving operational efficiency.

Centralised Management: SASE's cloud-based architecture allows IT teams to manage and enforce policies from a single platform, eliminating the need for multiple systems and interfaces. This centralisation saves time, reduces errors, and provides greater visibility into network and security performance.

Lower Total Cost of Ownership (TCO): By replacing legacy hardware with a cloud solution, businesses can reduce hardware and maintenance costs while benefiting from the scalability of a subscription-based model.

For businesses, this simplification translates to reduced complexity, lower operational costs, and more time for IT teams to focus on strategic initiatives.

Do's and Don't

Do:

- Consolidate tools and platforms to streamline operations and reduce redundancy.
- Leverage cloud-based solutions to reduce physical hardware costs.
- Invest in automation to minimise manual tasks and improve efficiency.
- Regularly audit your infrastructure to identify and eliminate unused or outdated systems.
- Choose scalable solutions that grow with your business needs.

Don't:

- Stick with legacy systems that are costly to maintain and prone to downtime.
- Assume that simplification means compromising on functionality or security.
- Neglect user training, as efficient systems are only effective when used correctly.
- Focus solely on cost savings at the expense of long-term scalability and performance.

3. Improved Network Performance and User Experience

In today's fast paced business environment, slow networks and poor user experiences can hinder productivity and frustrate employees. SASE enhances network performance and user satisfaction by leveraging cloud-based capabilities and intelligent traffic routing.

Optimised Connectivity with SD-WAN: SASE integrates Software-Defined Wide Area Networking (SD-WAN) to intelligently route traffic across the most efficient paths, ensuring faster and more reliable connections. This is especially beneficial for businesses with multiple locations or global operations.

Low Latency for Cloud Applications: As more organisations adopt cloud-based tools like Microsoft 365 and Zoom, SASE ensures that these applications perform smoothly, even during peak usage times. By bringing networking and security closer to the edge, SASE minimises latency and improves response times.

Seamless Remote Access: With a growing remote workforce, SASE delivers secure and consistent access to resources, no matter where employees are located. This ensures an experience free of frustrations, enabling employees to stay connected and productive.

By improving network performance and user experience, SASE enables businesses to maintain high levels of productivity and deliver exceptional service to their customers.

Do's and Don't

Do:

- Prioritise solutions like SD-WAN and SASE to optimise network performance and reliability.
- Regularly monitor network performance and conduct proactive maintenance.
- Implement Quality of Service (QoS) policies to prioritise critical applications.
- Ensure consistent connectivity and low latency for users, even in remote locations.
- Gather user feedback to address bottlenecks and improve experience.

Don't:

- Assume all users have the same network requirements; HPE Aruba Networking tailors solutions to specific needs.
- Overload the network with unnecessary traffic or applications.
- Ignore performance issues in remote locations or branch offices.
- Let outdated hardware slow down your network performance.
- Sacrifice user experience for cost savings, as both are essential for productivity.

onecom

Need guidance on where to begin?

Connect with a Onecom expert to explore tailored solutions for your contact centre.

www.onecom.co.uk