SASE: network and cloud security across your distributed enterprise

Trends like hybrid working and the shift to multi-cloud are seeing enterprises become distributed in unprecedented ways. It means your once clearly-defined network perimeter has changed into a constantly-moving and disparate boundary, where the line between internal and external is blurred. How do you protect it? SASE has the answers.

Employees working from the office, home and on the road already existed before COVID-19, but the pandemic saw it increase rapidly. 95% of workers now say they want flexible work hours and 78%[1] say they want location flexibility and that means a change in how you keep users and data secure. It looks like hybrid working models are here to stay.

It also means you need to focus on optimizing office operational costs, embracing SD-WAN and SD-Branch technologies to enable greater agility and increased innovation without opening yourself up to greater risk. Multicloud gathered even more momentum in the last few years as business flexibility became a priority. Enterprises have sped up downsizing large data centres, and looked at ways to manage costs and meet sustainability targets through cloud consumption models, while also developing new ways to process data and provide unique user experiences.

It's also meant that enterprises have had to rethink traditional network infrastructure, where data centres could often be a barrier to scalability and a high cost centre. Many companies are now seeing the value in adopting a centralised cloud security approach hosted by a third-party partner – as epitomized by SASE.

orange™ Business

Challenges for the distributed enterprise

More geographically spread-out users mean more endpoints. In a more distributed enterprise, what was previously a tightly-defined security perimeter is now spread throughout offices, the cloud, homes, coworking locations, and more.

All these remote workers are accessing more and more data through the Internet, which exposes them to more malicious websites and potential data security breaches. Your office branches are also now exposed to Internet-based threats that they were previously protected from on traditional MPLS networks.

You need to make sure that no matter where end-users connect from, they are protected in a consistent way and can only access data and applications they're authorized to.

Zero Trust ensures that only approved people can access appropriate data and leverages deep visibility to build a full picture of potential threats. It tells you what is going on in your network and gives you centralized and consistent security management.

Your SASE checklist

Secure Access Service Edge (SASE) brings together the latest network and security solutions which includes multicloud and network security into a comprehensive and holistic security architecture designed to protect the distributed enterprise. It includes SD-WAN to provide end-to-end visibility with optimized traffic over internet or private networks to your cloud and data centre resources.

60%

of organizations will embrace Zero Trust as a starting point for security by 2025[2]

As users and data become increasingly distributed and the Internet becomes the new WAN, SASE can help you secure your distributed enterprise:

- Protect your traditional network connections: you still need to protect the data that travels between your offices and central data centres, and underpin that with resilient connectivity. SD-WAN and ZTNA (Zero Trust Network Access) are now the most effective network for protecting enterprise traffic and hybrid working.
- Protect your users in the cloud: Malicious websites, social engineering and traditional security attacks mean your connections to cloud must be protected. This protection must be consistent across the board, no matter where users are, and must be identity-based. Secure Internet gateways and RBI (remote browser isolation) can give you this functionality.
- Protect your data in the cloud: data in the cloud needs to be protected from internal and external threats. Data leak prevention (DLP) and cloud access security brokers (CASB) protect your data by ensuring it isn't downloaded and exfiltrated from PCs.
- Review your trust model: make sure people accessing your data are who they say they are.

Some tips for securing your distributed enterprise

With increased hybrid working and use of multi-cloud, you have apps, users, and data everywhere. This distributed landscape means traditional perimeter security is no longer enough: in a world of more sophisticated cyberthreats, you need a more sophisticated response.

1. **Adopt Zero Trust as your enterprise-wide strategy.** Step one is ensuring you have a zero-trust approach that is consistent across your entire organization. You will need a champion within your enterprise to drive this. Remember you are only as secure as your weakest point. Orange Cyberdefense can provide expert consultants to review your security posture.

2. **Define your zero-trust approach.** Take actions to improve your security posture. This could mean deploying identity-based security that restricts access to infrastructure and data. Network segmentation in the LAN/WAN and cloud along with application segmentation can help you keep the door locked tight. Ongoing and effective monitoring of threats and lifecycle maintenance across all your IT infrastructure are key.

3. **Begin with remote access.** Enterprises typically start with remote access as a key concern. Orange Business works with you to understand your remote access requirements and implement a solution that is tailored to your needs. Orange Business and Orange Cyberdefense can manage the solution for you and let you deploy it as a service, or we can give you a co-managed approach.

4. **Extend to SD-WAN.** As enterprises increase cloud usage and start to leverage the Internet for WAN connectivity, SD-WAN gives you the basis for secure networking. Increased visibility and automation ensure common security policies can be easily and consistently applied throughout your network, and SD-WAN also enables secure connectivity from sites to cloud. As an expert SD-WAN managed services provider, Orange Business can remove the risk and complexity of deploying and running an SD-WAN network and underlay through our global network and field services teams.

5. **Drive towards end-to-end SASE.** Bringing together the cloud security components such as CASB along with SD-WAN is what makes SASE real. Working with an expert SASE provider like Orange Business ensures you have access to the skills and resources needed to let you concentrate on running your business. Orange Business and Orange Cyberdefense can give you best-of-breed cloud-based security and SD-WAN capabilities to deliver an unparalleled end-user experience, while reducing complexity and security risk.

6. **Secure your users and data.** The Internet presents a whole new range of security threats, from attacks at network level through to malicious internet sites and more. Orange Cyberdefense can help you secure your data and users through cloud-based security so traffic crossing the Internet is as protected as your internal MPLS traffic was.

7. **Include your LAN from day one.** Ensure your LAN is up to date with all the latest security policies and versions using software-defined LAN (SD-LAN). Zero Trust starts from the user's device and office LAN and goes all the way up to the Cloud.

8. **Engage a partner to manage part of your security services.** Orange Business believes security should never be completely outsourced and it is the responsibility of everyone to make it work. Orange Cyberdefense can assist with major areas of security such as design and deployment, audits, or equipment maintenance.

Find out more about how Orange Business and Orange Cyberdefense can help you secure your distributed enterprise with SASE at www.orange-business.com/en/solutions/connectivity

orange™ Business

Orange Cyberdefense

1. https://futureforum.com/research/leveling-the-playing-field-in-the-hybrid-workplace/ 2. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio