Computacenter

SASE – ENABLING AND PROTECTING MODERN BUSINESS CONNECTIVITY

What is SASE? Why is it important? Where should you start? And what strategic decisions should you consider during the early phases of adoption?

WHAT IS SASE?

The acronym was first introduced by Gartner in 2019 and stands for 'Secure Access Services Edge'. With a combination of network and security components that are bound together as a single architecture, SASE can deliver the secure access requirements for modern enterprise.

The networking components of SASE encompass a number of areas, including; SD-WAN, content-delivery networks, network-as-a-service and bandwidth aggregation. To offer an easier to consume and more complete solution, selected networking equipment vendors have entered into partnerships with carriers to integrate their products and deliver off-the-shelf SASE offerings.

The security elements of the SASE architecture rely on network security functions including; VPN, firewall (as-a-service), Secure Web Gateway (SWG), Remote Browser Isolation (RBI), Cloud-Access Security Brokers (CASB) and DNS security. To enable secure access for users, devices and things, Zero Trust Network access (ZTNA) is an essential part of the SASE offering. To further enrich the SASE security stack, additional security functions including malware protection, Web-Application-Firewall/Web Application API Protection-as-a-service, DDOS prevention, Data Loss Prevention (DLP) and User-Entity-Behaviour-Analytics (UEBA) are also available dependant on the vendor portfolio.

SASE extends beyond a pure architecture to ensure that solutions aligned to the SASE design principles consider the following activities when facilitating and securing access:

- The identity of the entity connecting
- Context (e.g. type, health and behaviour of the device, sensitivity of the resources being accessed)
- Security and compliance policies
- An ongoing assessment of risk during each session.

All these capabilities should be offered together as a SASE service underpinned by a single architecture.

Architecture & Management
Cloud | On-Premise | Hybrid

NETWORK SECURITY	WEB SECURITY	(MOBILE) USER SECURITY ZERO TRUST NETWORK ACCESS	
			Malware Protection
			Web Application Firewall (WAF)
IDS/IPS service	Cloud Access Security Broker (CASB)		Web App. API Protection (WAAPaaS)
NW security Firewall cloud service (FWaaS)	Remote Browser Isolation (RBI)	ZTNA Continuous Inspection Zero Trust	DDoS Protection
NW security Firewall edge service	Secure Web Gateway (SWG) Functional capabilities	ZTNA MFA & Identity	Data Loss Prevention (DLP)
VPN service (Site-to-Site)	DNS Security	ZTNA/VPN Endpoint/Service Initiated	User Entity Behaviour Analytics (UEBA)

SECURITY FUNCTIONS

SD-WAN service Application-based path selection	SD-WAN service Performance/WAN optimisation	Rollout Automation Zero Touch provisioning
Carrier/CDN functions	Device connectivity WAN (ETH, Mobile 4G/5G)	Network as a service LAN/WLAN

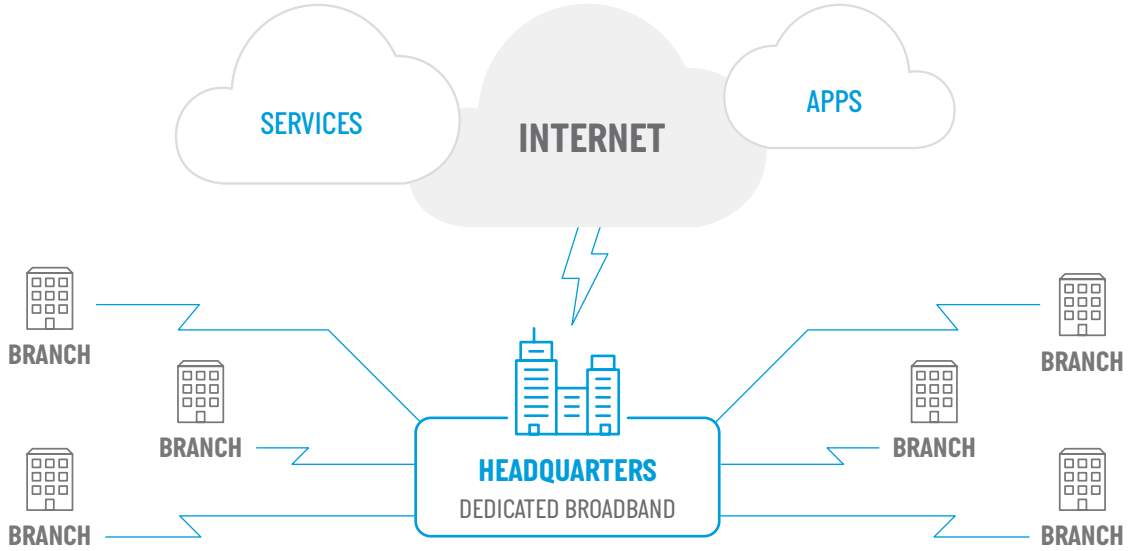
NETWORK FUNCTIONS

WHY IS IT IMPORTANT?

Secure Access Service Edge (SASE) describes the move to unified network and security controls operating in the cloud. It's a shift away from the traditional method of routing network traffic through the data center and managing security at the perimeter of an organisation's network.

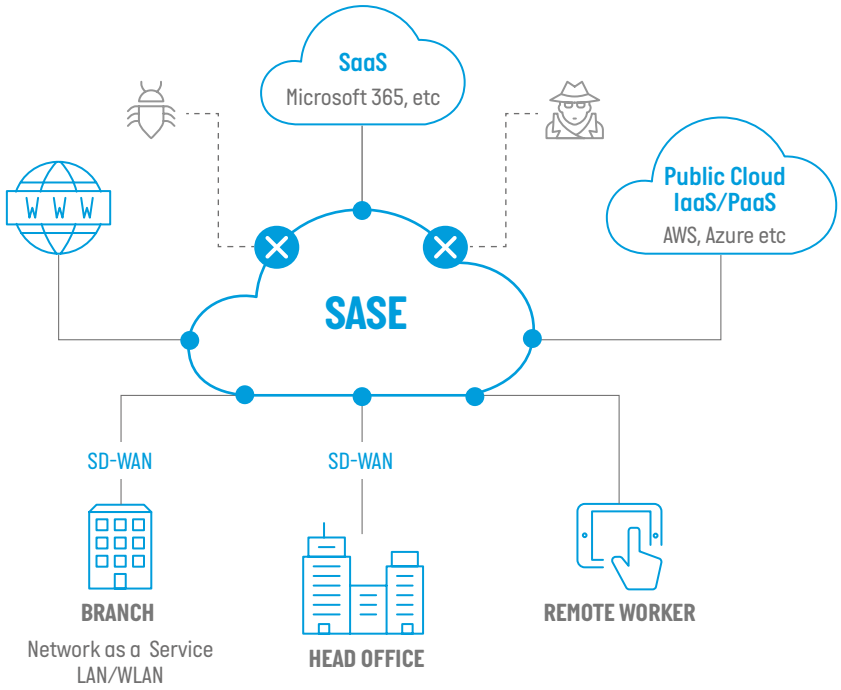
SASE differs by building on SD-WAN connectivity and concepts such as Zero-Trust networking. This delivers a single platform offering network security, web security and mobile user security alongside many other security control functions that are network-centric in nature. Driven by the growth of cloud adoption and increasing mobility of today's workforce, SASE is an answer to the problem of how to design, build and manage the network and security demands of decentralised traffic without routing it through a centralised data center.

With greater demand to access applications and data in the cloud from outside the traditional perimeter, traditional methods of routing network traffic have resulted in significant congestion and latency in the data center, bringing about a poor user experience and stifling instiutional agility. This has been highlighted by the fast transition towards hybrid working catalysed by the ongoing COVID-19 pandemic.



The key concept behind SASE is to distribute critical network and security functions from the cloud, closer to where the user and applications now are, connecting users via nearby Points of Presence (PoP) instead of routing them back to the centralised data center. In doing so, a SASE model will alleviate the burden of increasing data flowing through the data center, enable a more flexible network, speed up network response times and allow companies to apply Principles of Least Privilege (PoLP).

Taking this approach combines and unifies policy management which enables companies to quickly and efficiently secure traffic regardless of its origins or the location of corporate resources, making it an attractive option for many organisations.



TODAY'S VIEW OF THE SASE KEY STRATEGIC MARKET PLAYERS

As Gartner defined SASE in 2019, it is still a fresh concept and therefore is not easy to align with a single vendor or product set. Many providers claim to have significant component products of the overall SASE solution puzzle, but in our view, there is no single vendor with a definitive platform which can provide each SASE function today. We see three types of vendors that are developing SASE capability, and each has its own benefits and drawbacks.

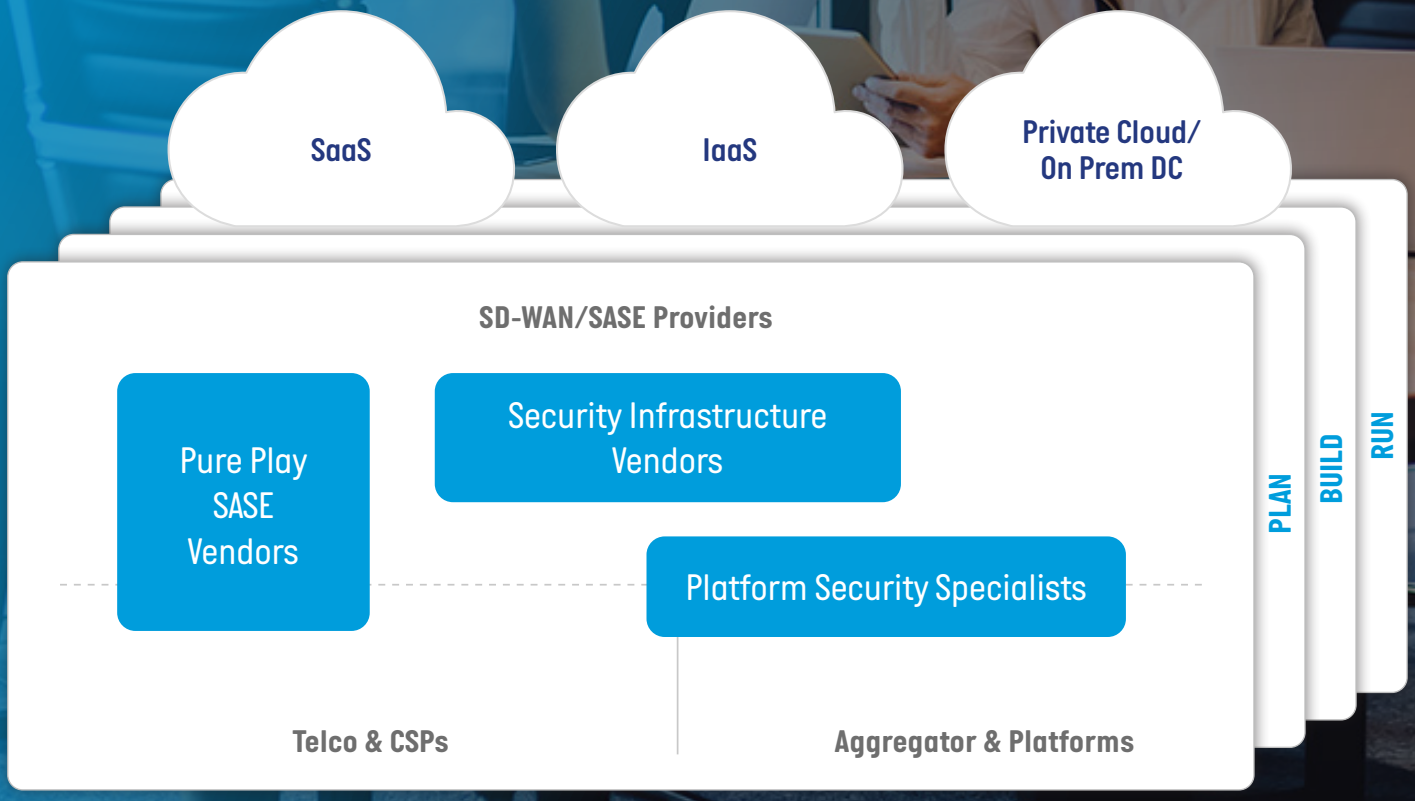
PURE PLAY SASE VENDORS
These vendors, with no historical infrastructure centric network or security legacy, arrived in the market as software only, born-in-the-cloud network and security vendors focused only on SASE style solutions. This makes it easier for them to add new features and functions in a cost-effective manner.

NETWORK AND SECURITY VENDORS
Vendors who have historically led the network and security infrastructure software and hardware market are evolving their legacy platforms by bundling current products, undertaking strategic acquisitions, or evolving hardware offerings to software ones and are taking the results to market as SASE solutions.

Whilst these vendors have a great depth of experience and impressive solution portfolios, there is still progress to be made to complete integrations as there are sometimes key capabilities still missing.

PLATFORM SECURITY SPECIALIST
Organisations that have been integrating network and/or security into their existing technology platforms are now adding additional SASE components as well. Whilst these vendors may evolve to become leading players in the future given the scale of their base, they still need to develop further capability to offer a complete solution. One platform vendor, for example, may have essential elements of the SASE framework that few of the others have, including identity and access management controls, but lacks the network infrastructure components such as SD-WAN.

Finally, it is also worth noting that the SASE marketplace is a fast evolving one, and in our view a number of security software vendors with 'point functions' are likely to become acquisition targets for use as the base platform to build and launch new SASE solutions.



How different vendors map to SASE requirements

SASE BENEFITS

The promised benefits of a SASE platform are extensive and support the move to cloud-based enterprise security combining network and security functions. Key benefits include:

- The ability to easily scale networking and security capabilities;
- Optimal security for applications that can live anywhere;
- Centralised, dynamic, role-based policies that streamline operations;
- The ability to consolidate previously stand-alone platforms;
- The potential to simplify complex multivendor security landscapes and achieve cost reduction via consolidation, and the removal of excess security software and infrastructure platforms;
- SASE environments are mostly cloud native by design which increases flexibility and reduces the operational cost of supporting large scale infrastructure centric security estates.

SASE CAUTIONS

SASE is still evolving as a concept and is not yet a go-to design for managing enterprise secure access across users, cloud and business requirements. As such there are several cautions worth highlighting:

- The scale of the change from a traditional network and security concept to a SASE model should not be underestimated. This is particularly important where organisations have entrenched network and security silos.
- Every SASE concept requires an underlay network (last and middle mile) which needs to be integrated or provided separately from the SASE solution.
- The speed of change to a SASE model will also need to be considered, given that any adoption will require numerous integrations and the deployment of a new overarching platform.
- Consideration also needs to be given to how security operations will be tooled. Processes will need to ingest new, and existing, data feeds from SASE solution components to build intelligence into SIEM platform correlation rules. This will ensure enterprise users will continue to be protected as organisations move toward the new target SASE model.
- Organisations will also need to invest in new skills to manage and troubleshoot a SASE environment. They will need to ensure that the SASE technologies they invest in have a suitable depth of troubleshooting capabilities.
- Conventional thinking suggests that SASE will reduce costs as it will remove expensive standalone security and networking appliances (reducing licencing and support costs). However, in our view, as there is no overarching platform today that can do everything, ROI will depend on understanding the cost (both Capex and Opex) of individual components, such as CASB for example. Organisations will be required to expend time and effort to undertake the required due diligence in order to integrate individual components into the final architected solution. As such, until this due diligence is undertaken, which typically involves multiple stakeholders, it may not be immediately clear where savings will occur or how soon they can be realised.
- There are an increasing number of vendors that are offering SASE solutions. Given that the market is still very new, the first wave of acquisitions has already taken place and it is clear some vendors will not survive. As such, backing the right vendor is especially important, and we would suggest organisations ensure they have access to the skills (either in-house or partners) that can provide clear insight into any differentiation and value across multiple vendor offerings.

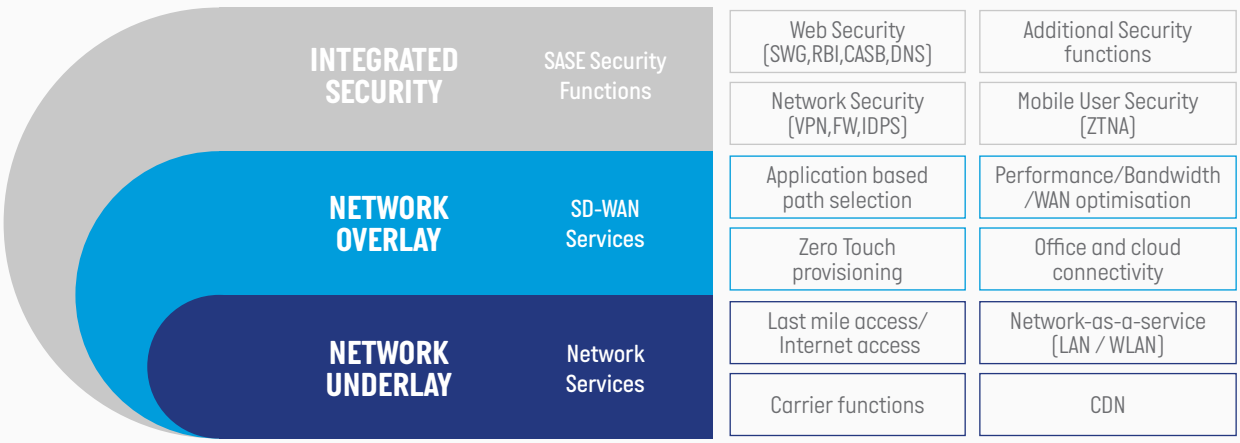
SUMMARY ANALYSIS OF THE SASE MARKET

The SASE market in 2021 is still in its infancy and whilst several vendors are already suggesting they could become dominant players we do not believe that there is a clear leader in terms of features and functions now. With so many vendors competing within this new market, selecting the right vendor to align to customer specific use cases is fundamental if business and operational benefits are to be fullyrealised.

MAKING THE RIGHT DECISIONS

It is important that customers choose vendors based on validated use cases and a clear understanding of both functional and non-functional requirements. This will ensure that value will be realised irrespective of the platform bought and that the operational and cost benefits from consolidation and optimisation when traditional platforms are removed can be realised, but with minimal business risk.

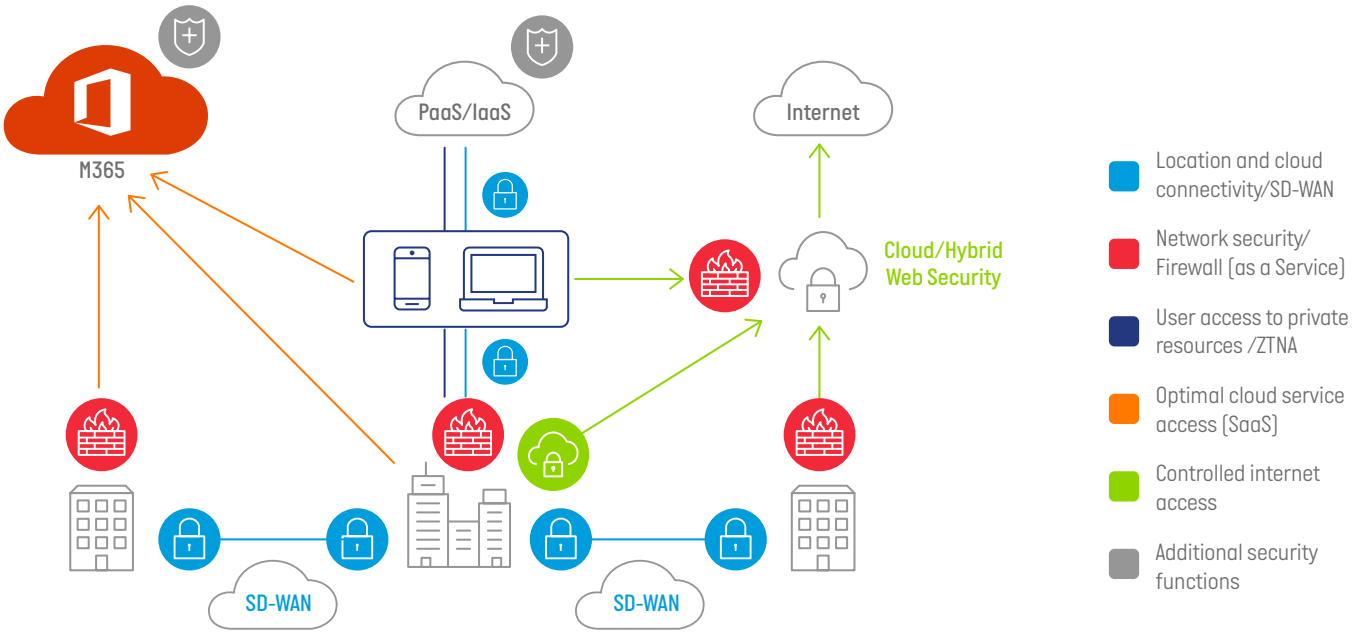
Network and security elements within the SASE stack



It is important not to lead product selection in a feature-centric manner. This approach has proved expensive to customers who inadvertently become locked into functionality that isn't required and receive sub-optimal functionality in the areas most needed. Finally choosing the right vendor can also help organisations realise a less complex solution that integrates better across all platforms.

SASE BUILDING BLOCKS

SASE solutions have several architectural options that reflect both different organisational requirements and the layers of protection required. It is our view that there are consistent, standard building blocks that should be incorporated into all SASE designs. These practical capabilities provide a firm foundation from which to build.



▲ SASE high level Reference Architecture

Location and cloud connectivity/SD-WAN

The secure SD-WAN overlay provides the secure connections between sites and cloud enterprise resources (IaaS/PaaS). Typically, a SD-WAN solution is the most flexible and effective way to meet these communication requirements and provides essential VPN encryption and base level security functionalities.

Network security/Firewall (as-a-Service)

Network security functions like firewalls provide communication control and are an important part of the architecture. They are inherently flexible and can be deployed in different ways. Deploying a Firewall as an edge service allows the architecture to follow SASE guidelines by moving the inspection engine to the sessions and not vice versa. This would be applicable to locations where direct internet access is the main connectivity pathway. Firewall-as a-service (FWaaS) brings this utility into the cloud, making it easier to consume than traditional firewalls. Instead of requiring hardware to get the benefits of a firewall, FWaaS extends the range of firewall capabilities to, and within, the cloud. This can be of significant value particularly to support mobile users. A centralised policy management and control capability is an important addition for both network security approaches.

User access to private resources/Zero Trust Network Access

User access to private resources requires secure connections for both users and mobile devices to on-premise and cloud enterprise resources. Zero trust network access is where access is authenticated once an identity has been validated, e.g. by an identity management solution, and has been assigned applicable privileges based on role and context. Implementing this concept of "Zero Trust", where there is no implicit trust applied to resource access, is a core component of SASE, and should provide continuous control during a session.

Optimal cloud service access (SaaS)

Optimal access to trusted cloud resources, e.g. M365. With M365, for example, the shortest, most direct route between the user and closest Office 365 endpoint will offer the best performance. However, it is also important to avoid security functions which intercept and decrypt network traffic in transit, because they often change, scrub, or block decrypted content. Applying these features to M365 user traffic, for example, causes changes to Office 365 protocols and data streams (outside standard and documented APIs). So an appropriate design which matches the needs of the SaaS application and provides adequate security is essential.

Controlled Internet Access

Controlled access to Internet and public cloud resources via cloud or hybrid web security requires features such as Secure Web Gateways, Remote Browser Isolation and DNS security.

Additional security functions

Overlaying additional security capability such as CASB, WAF (Web Application Firewall) and advanced malware protection provide added layers of protection for users of IaaS, PaaS and SaaS services.

OUR CONCLUSION

SASE will force the integration of network and security services into one architecture. We do not believe that SASE signals the end of on premise or traditional infrastructure security vendors, but the winners in this new market will be vendors with the most complete portfolios or those with the most effective integrations to third-party cloud resources or to the native providers themselves. More recently, two terms are gaining in prominence to describe the different types of SASE outcome:

Ingress SASE
Controls provide access from outside to internal applications within the extended enterprise.

Egress SASE
Capabilities that help your users gain access to services anywhere on the internet in a secure manner.

As these terms become common throughout the industry, it is worth considering if vendors can provide both outcomes or if their solutions are more focused on one specific area. This will help organisations to determine the right approach for a specific business outcome.

Computacenter considers SASE as a destination that is reached in stages. Starting with a clear defintion of requirements or security outcomes, understanding which vendors to consider, developing an understanding of the existing vendor landscape, identifying options for consolidation or integration, and developing a target design and architecture. These are just some of the activities we would recommend discussing from this paper.

LET'S TALK

If you are considering SASE and are not sure where to start, Computacenter can help. To access practical advice and guidance, understand your options and get support with defining your SASE strategy, architecture or vendor selection please contact your Computacenter Account Manager or email us at **SecurityEnquiries@computacenter.com.**

About Computacenter

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 16,000 people worldwide.

www.computacenter.com

Computacenter