kyndryl

Kyndryl Secure Access Service Edge Services

Digital transformation enables businesses to unlock and hone their competitive edge using cost-efficient, shared, and scalable IT services from cloud service providers, accessible from virtually anywhere through a low-cost network: the Internet.

The Internet can play a pivotal role in digital transformation. The traditional approach of a hub-and-spoke network leads to challenges in providing cost-effective, low-latency, secure connections for a good user experience in a highly distributed IT environment. The Internet needs to become a vital part of the corporate network fabric, requiring a new, holistic management and monitoring approach that controls all edges and visibility and orchestration capabilities to manage and operate this new network fabric.

At the same time, rapidly increasing security vulnerabilities are amplified by unmanaged end-user devices and moving applications to cloud, requiring a new mindset for approaching security.

What is secure access service edge?

Secure access service edge (SASE) solutions are a new category of network security that integrates networking and security into a cloud-delivered service. At its core, SASE converges zero-trust networking capabilities from software-defined wide-area networks (SD-WANs) and remote user access with security features like firewalls, cloud access security brokers (CASB), secure web gateway (SWG), and other services into a single identity-centric solution.

Why SASE and why now?

Today's workers are using all kinds of devices accessing corporate data from anywhere, at any time, from multiple geographical locations. The rise of cloud computing and mobility have uprooted many fundamental assumptions about legacy technology infrastructure. The days of guarding a fortified perimeter like the corporate data center have given way to environments without perimeters, spreading applications across a variety of cloud, data center, and on-premises environments. And with data flowing everywhere, businesses often have to contend with general lack of control across user and network activity.

This combination of identity, networking, and security into a single, cloud-centric delivery model can greatly simplify the architecture of IT infrastructure and create a continuously updated security posture that can evolve to meet ever-changing threats and business needs.

By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020.1

Zero-trust security service edge

Traditionally, the security perimeter was synonymous with the physical perimeter of an organization. Any asset within this perimeter was shielded from the public and only visible to privileged, known identities like employees, business partners, or customers. Data flow to and from the Internet was easily controlled, allowing for a standardized, centralized security management approach.

Moving assets outside this protected enclave results in less control over some parts of the IT infrastructure. The new security services edge (SSE) architecture model addresses security requirements of a distributed IT architecture by moving security controls to all edges with unified monitoring and management capabilities. Additionally, applying zero-trust methodology supports a manageable security architecture that is highly resilient against common threats like zero-day attacks and ransomware.

Our approach

The Kyndryl™ Secure Access Service Edge solution provides zero-trust access to enterprise IT resources hosted on the cloud and in the data center, with a vendor-neutral approach to WAN, security solutions and services, and consistent application, policy, and user experience. Our SASE solution is designed to deliver end-to-end cloud security capabilities to minimize threat exposure, maximize user experience, and help eliminate traditional, high-cost on-premises solution components like firewall, proxy, and VPN gateway. With deep experience at the convergence of cloud-managed SD-WAN and cloud-delivered security, Kyndryl can work with you to advise, build, and manage your WAN solutions.

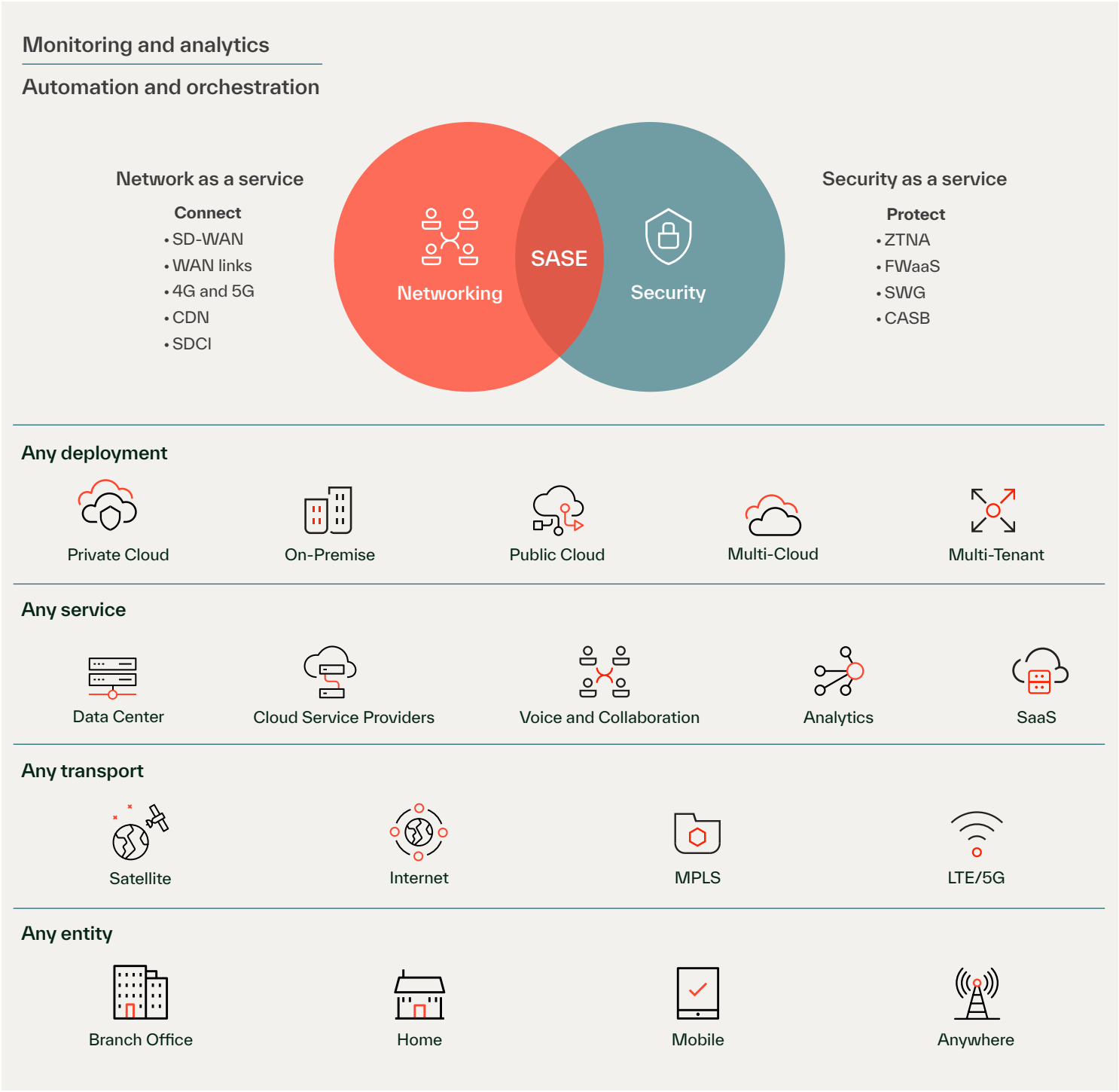

Figure 1: Kyndryl Secure Access Service Edge

Core Components

Secure web gateway (SWG)	URL filtering | Policy ontrol enforcement | Application control | Remote browser isolation
Cloud access security broker (CASB)	Sensitive data protection | Threat protection | Greater visibility
Zero-trust network access (ZTNA)	Identity-based access | Micro-segmantation | Risk-based posture validation
Firewall as a service (FWaaS)	Data packet inspection | Intrusion prevention | Application-level security
Advanced threat protection	Real-time visibility | Context awareness | Data awareness
Granular policy management	Location- or device-specific access control policies | Cloud-based management

Figure 2: Kyndryl SASE features and capabilities

SD-WAN

SD-WAN takes a software-defined approach to managing WANs, providing link redundancy and load balancing, and using intelligence to route traffic based on defined performance and business priorities. Typically, SD-WAN is deployed at the branch or remote office level using a router or next-generation firewall (NGFW) device to optimize on-net users' access to the Internet. You can also implement SD-WAN from within the cloud-delivered service and offered as-a-service—analogous to private networks from WAN service providers that use multiprotocol label switching to deliver optimized connectivity to other cloud services or as-a-service applications.

Secure web gateway

Secure web gateway is a web gateway or proxy solution where a user's web-based traffic is forwarded or proxied to a web gateway or proxy server that applies web filtering, DNS security, antivirus, anti-malware, anti-botnet, SSL inspection, and data loss prevention functions to the traffic before sending it to the Internet.

Zero-trust network access

Zero-trust network access (ZTNA) is a solution that protects applications by only allowing access to trusted entities. As a result, ZTNA is a viable alternative to VPN for accessing protected resources on your organization's network.

Cloud access security broker

Cloud access security broker (CASB) is a software or hardware solution located between users and a cloud service to enforce security policies around cloud-based resources.

Firewall as a service

Firewall as a service (FWaaS) is a firewall solution delivered as a cloud-based service that can scale and have new services provisioned to meet changing and expanding needs. FWaaS creates a location-independent perimeter firewall for security-rich access to enterprise resources, with next-generation firewall (NGFW) capabilities like web filtering, advanced threat protection, intrusion prevention system, and domain name system (DNS) security.

Figure 3: Transformative value of Kyndryl SASE

Why Kyndryl?

Kyndryl has deep expertise in designing, running, and managing the most modern, efficient, and reliable network and security infrastructure the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side by side with our customers to unlock potential.

Next steps

Discover how Kyndryl SASE can help you unlock new value from your digital transformation journey. Schedule a free consultation today. Talk to an expert.

kyndryl

1 *Checking in on SASE*, Gartner, March 2021