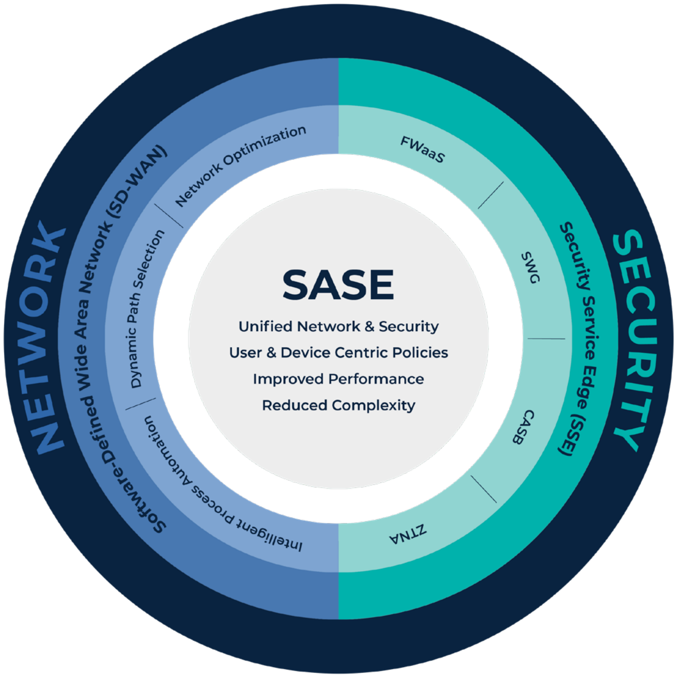
Guide to SASE

Cybercrime is projected to cost the global economy **$10.5 trillion in 2025**[1]. The FBI reports a 9% rise in ransomware attacks on U.S. infrastructure in 2024, with critical sectors like **manufacturing, healthcare, and finance most affected**[2]. To address these growing threats, organizations are turning to Secure Access Service Edge (SASE), a cloud-based service that combines networking and security in one platform. SASE delivers improved performance, reliability, and protection for networks.


SASE

Unified Network & Security

User & Device Centric Policies

Improved Performance

Reduced Complexity

NETWORK

Software-Defined Wide Area Network (SD-WAN)

Network Optimization

Dynamic Path Selection

Intelligent Process Automation

SECURITY

Security Service Edge (SSE)

FWaaS

SWG

CASB

ZTNA

How SASE Works

Gartner defines single-vendor SASE offerings as those that deliver multiple converged-network and security-as-a-service capabilities, such as software-defined wide-area network (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), network firewalling and zero trust network access (ZTNA). These offerings use a cloud-centric architecture and are delivered by one vendor. SASE securely connects users and devices with applications. It supports branch office, remote worker and on-premises general internet security, private application access and cloud service consumption use cases.[3]

IMPROVED CONNECTIVITY

- Combines MPLS, broadband, and 4G/LTE for optimized performance
- Reduces latency and packet loss for high-performance access
- Prioritizes critical applications to ensure consistent user experience

FAILOVER REDUNDANCY

- Enables dynamic path selection and automatic rerouting in the event of a connection failure
- Redundant nodes and services ensure business continuity during hardware or network failures
- Multiple pathways including MPLS, broadband, 4G/LTE, and satellite provide resilient connectivity options

NETWORK PROTECTION

- Next-Gen Firewall (NGFW) inspects traffic to detect and block cyber threats
- Secure Web Gateway (SWG) filters internet traffic to block harmful sites and enforce use policies
- Intrusion Prevention System (IPS) detects and blocks unauthorized access attempts

ACCESS CONTROL

- Enforce policies based upon user identity, role and device
- Multi-Factor Authentication adds an additional verification process
- Zero Trust Network Access (ZTNA) ensures users are continuously verified and only gain access to specific resources

[1] https://www.forbes.com/councils/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/
[2] https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/
[3] https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

MetTel

For more info, contact your MetTel agent or visit mettel.net.