FACT SHEET

SASE explained: A glossary for evolving network security

SSE, SASE, CASB, ZTNA: Even for seasoned professionals, modern security solutions can quickly turn into an alphabet soup of abbreviations, jargon and concepts that rapidly change while security needs shift.

As a trusted managed services partner, Spectrum Enterprise® is always ready to bring your team up to speed on the latest technologies to protect your organization.

Among them, secure access service edge (SASE) has emerged as one of the most powerful frameworks to protect users across locations, clouds and applications. SASE is the combination of a software-defined wide area network (SD-WAN) and secure service edge (SSE) — a cloud-based cybersecurity platform centered on the identity of users, devices and applications.

Since SASE is a combination of technologies, rather than a single off-the-shelf solution, it's helpful to become familiar with the networking and security concepts that make this framework so powerful.

SASE terminology defined

BYOD: Bring your own device	An IT policy that allows members of an organization to access network resources on their personal laptops or mobile devices.
CASB: Cloud access security broker	An on-premises or cloud-based policy enforcement point between users and cloud service providers. CASB offers visibility into cloud applications used across the network, user activity and volume to better manage cloud access and reduce risk.
Device trust	In addition to confirming the identities of users, security technology can ensure the devices they use are free from vulnerabilities and comply with an organization's security standards.
DLP: Data loss prevention	A combination of processes and technologies that helps prevent unauthorized access to sensitive data, such as information protected by the Health Insurance Portability and Accountability Act (HIPAA).
DNS: Domain name system	Security on the DNS layer — which directs traffic to IP addresses associated with domains — blocks malicious traffic, detects compromised systems and prevents threats from reaching end users through compromised ports or protocols.
FWaaS: Firewall as a service	A cloud-based service, often managed by a provider, replaces a premises-based firewall to protect a network from external threats and monitor network traffic.
IAM: Identity and access management	This combination of policies and security technologies is set by an organization to ensure users can access the network and cloud resources they need and that only authorized users can access sensitive data.

IPS: Intrusion prevention system	A solution that detects unauthorized attempts to access network resources and deploys measures to help prevent data breaches.
MFA: Multi-factor authentication	Beyond usernames and passwords, MFA adds additional validation and policy management to establish trust for remote users. This is often accomplished by establishing a user's identity through a secondary source, such as a text message, an email or an app on their mobile device.
NGFW: Next-generation firewall	A step up from a stateful firewall, an NGFW is a network security device that provides IT administrators with application-aware management of network resources, continuously updated threat intelligence and integrated intrusion and malware protection.
SSO: Single sign-on	An application that manages sign-on credentials and establishes trust across multiple services that require users to log in.
SWG: Secure web gateway	A cloud-based solution that enforces acceptable use policies, blocks malware and inspects web traffic to provide full visibility of accessed URLs and application controls.
UTM: Unified threat management	A solution that encompasses a firewall plus a combination of advanced security features like IPS, anti-malware protection and filtering of web content and URLs.
VPN: Virtual private network	A connection to a network for remote users or branch locations that relies on encrypted IPsec tunnels to prevent unauthorized access to data as it transits the internet.
WAF: Web application firewall	A security solution that protects application program interfaces (APIs) and web applications from malicious traffic and other threats.
ZTNA: Zero trust network access	A component of zero-trust architecture, ZTNA only grants access to network resources with continuous verification of information such as user ID, device identity and location — as opposed to previous security practices that assume a user is trustworthy after they're logged in.

Spectrum Enterprise simplifies the networking experience, no matter how complex the security landscape becomes. Our approach to SASE enables safer, more effective interaction between users, systems and content — wherever they are located. We can combine solutions from leading technology providers with flexible management and expert support to help your organization benefit from the latest approaches to cloud and network security.

Learn more about how Spectrum Enterprise can help secure your organization.

About Spectrum Enterprise®

Spectrum Enterprise®, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.