



In today's dynamic and interconnected digital landscape, organizations face ever-evolving cybersecurity challenges and heightened risks. The traditional approach to security is no longer sufficient to protect against sophisticated threats and ensure seamless connectivity across distributed networks. To meet these demands head-on, COSGrid Networks introduces COSGrid SASE, an innovative solution that combines the power of secure access service edge (SASE) with advanced security capabilities. With COSGrid SASE, organizations can securely connect their distributed workforce, defend against emerging threats, and simplify their security operations. By leveraging centralized security policies, streamlined management, and cost-effective deployment, SASE empowers organizations to stay ahead of the curve and strengthen their security posture in today's interconnected world.

Gaps in Effectiveness

- **Gaps in visibility and coverage:** SASE enables centralized security policies to be effectively managed and enforced in a decentralized network, reducing the risk of breaches or compliance violations
- **Volume and complexity of security tools:** SASE reduces the need for multiple point security solutions that are difficult to integrate and manage, simplifying the security operations and improving the threat detection and response
- **Limited budgets and security resources:** SASE lowers the cost and complexity of deploying and managing security solutions across multiple locations and devices, enabling IT teams to focus on more strategic tasks.
- **Lack of industry standards:** SASE provides a common framework and terminology for network and security functions, facilitating the communication and collaboration among service providers, vendors, and customers
- **Customer education and migration:** SASE helps customers understand the benefits and challenges of adopting a cloud-based security model, and provides guidance and support for migrating from legacy solutions to SASE

Highlights

- **Comprehensive Security:** COSGrid Z3 SASE offers a wide range of security functions including advanced threat protection, web security, DNS security, remote browser isolation, data loss prevention, and cloud access security broker. It ensures robust protection against known and unknown threats.
- **Simplified Deployment and Integration:** COSGrid Z3 SASE supports cloud, on-premise, and hybrid architectures, making it flexible and adaptable to different network environments. It integrates seamlessly with existing infrastructure and security tools, reducing complexity and simplifying deployment.
- **Enhanced Performance:** With SD-WAN capabilities, COSGrid Z3 SASE optimizes network performance by intelligently routing application traffic based on specific requirements. It ensures high-quality user experiences and efficient utilization of network resources.
- **Cloud-native Architecture:** Built as a cloud-native platform, COSGrid Z3 SASE leverages the scalability, agility, and elasticity of the cloud. It allows for seamless scalability and rapid deployment, ensuring that the solution can grow with the evolving needs of the organization.
- **Zero Trust Network Access (ZTNA):** COSGrid Z3 SASE incorporates ZTNA, providing granular access controls based on user identity, device posture, groups, location, and time. It enables secure access to applications and resources, reducing the risk of unauthorized access.
- **Improved Visibility and Reporting:** The solution offers comprehensive visibility and reporting capabilities, enabling organizations to monitor network traffic, detect anomalies, and generate actionable insights. It helps in enforcing acceptable use policies, defending against threats, and protecting sensitive data.

SASE is primarily delivered as a service and enables ZTNA based on the identity of the device, combined with real-time context and security policies. By 2024, 60% of enterprises will have adopted a SASE approach to security

How does COSGrid SASE helps?



A cloud-first architecture



Seamless security experience



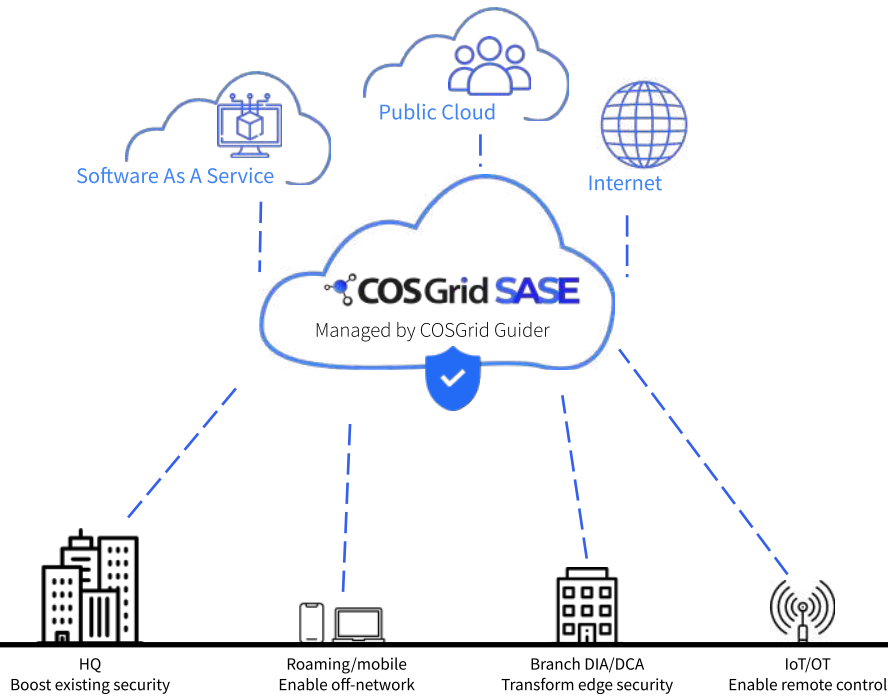
Zero Attack surface



Zero Trust Network Access

COSGrid SASE Overview

COSGrid SASE provides enhanced security, zero-trust connectivity, seamless deployment, and simplified management. With advanced threat protection, zero-touch provisioning, and a flexible architecture

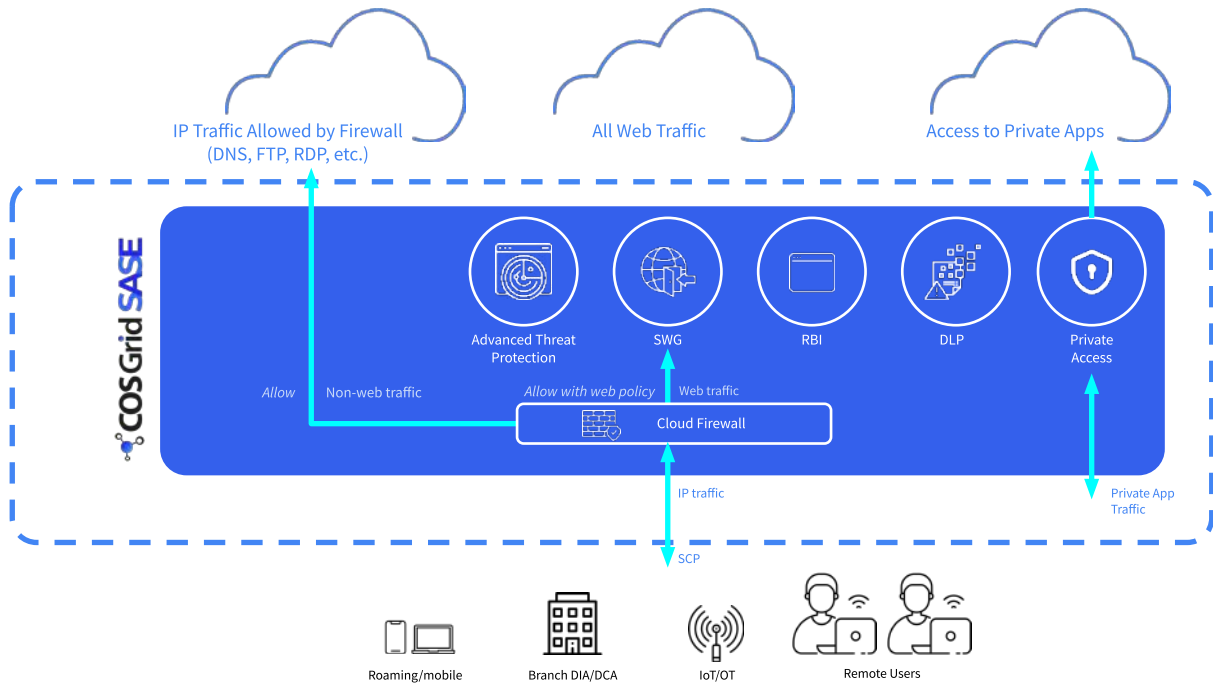


COSGrid SASE Architecture

COSGrid Z3 SASE ensures robust network performance, centralized security policies, and future readiness. It leverages 5G wireless and existing wired networks to create a secure and reliable connectivity experience, enabling organizations to protect their distributed sites and remote employees efficiently.



How it works



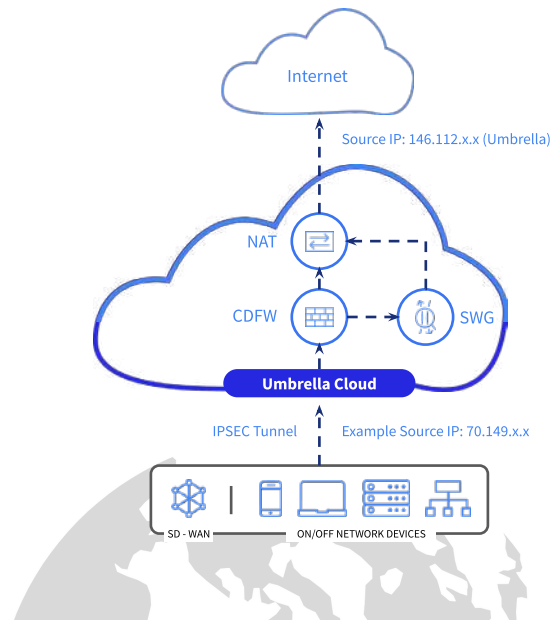
COSGrid SASE - Outcomes



COSGrid SecureGateway

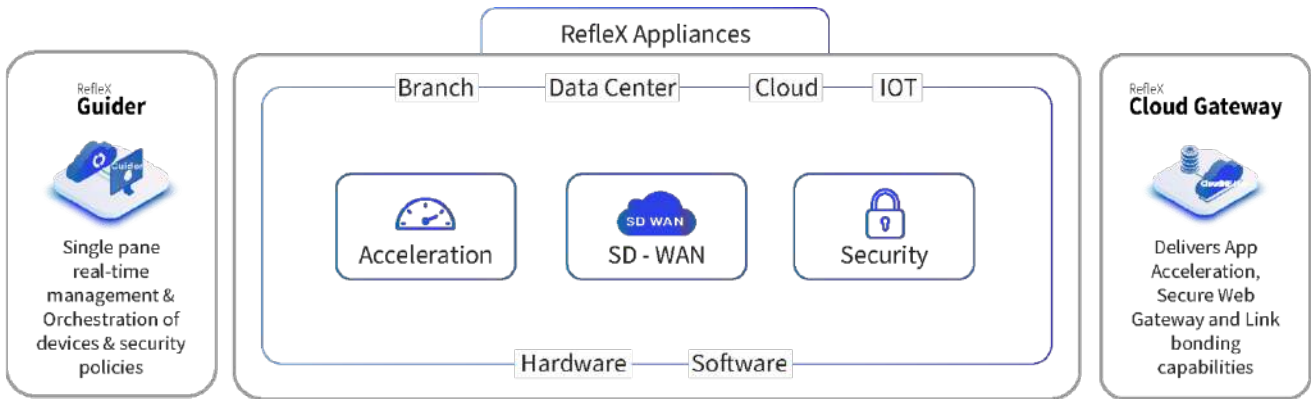
SecureGateway is a Secure Internet Gateway (SIG) solution that provides Firewall as a Service (FWaaS). It offers URL and content-based policies, granular app controls, and advanced visibility and reporting features.

- Selective bypass of Microsoft 365 traffic by better experience
- Full or selective SSL decryption
- App visibility and granular controls
- URLs Accessed reporting
- Granular App controls such as blocking uploads, e-mail attachments
- Automated User Provisioning via SAML and AD sync
- HTTPS Inspection with Decryption & w/o Decryption
- Selective Proxying & Selective Decryption
- URL Category and content based allow/deny policies



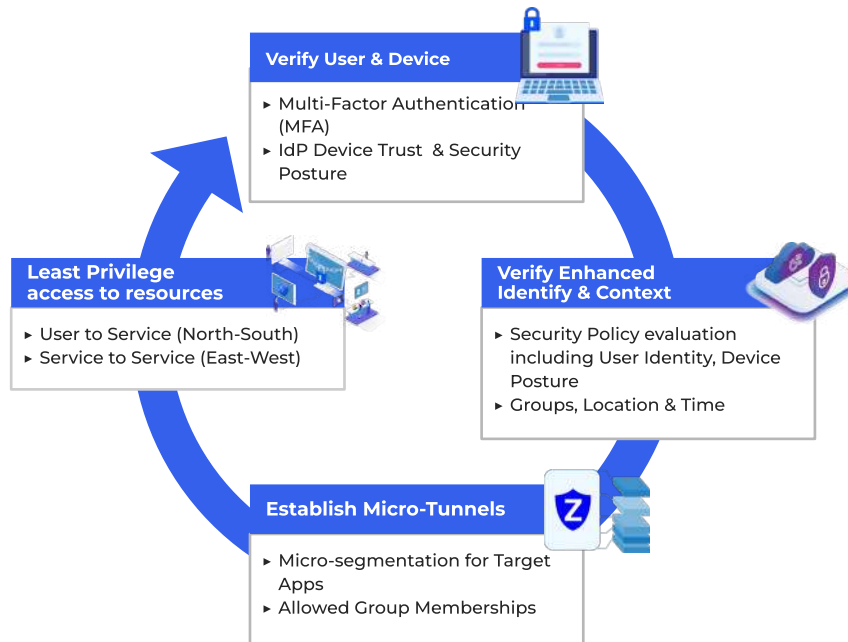
COSGrid ReFlex SD-WAN

COSGrid's ReFlex-WAN is a Cloud Managed Software Defined platform designed to transform WAN into a cloud-centric world. It is built to deliver the simplicity, flexibility and cost-effective WANs for any branch office locations and scale also seamlessly run and integrate with DC locations and Clouds deployed.



COSGrid MicroZAccess

Flexible multi-tenant and multi-use-cases Software-defined Micro-segmentation platform that mitigates risks, enhances productivity and simplifies management.



Peer to Peer Overlay model for improved privacy and performance



Flexible Deployment - Host/Workload Agent & Gateway approach



Integrated Device Trust and Superior Identity MFA based Access



Super Simple to Deploy and Manage










Platform approach for Comprehensive Security - Support in SD-WAN and SASE



Stateful device compliance checks before, and during, a connection Granular policy enforcement

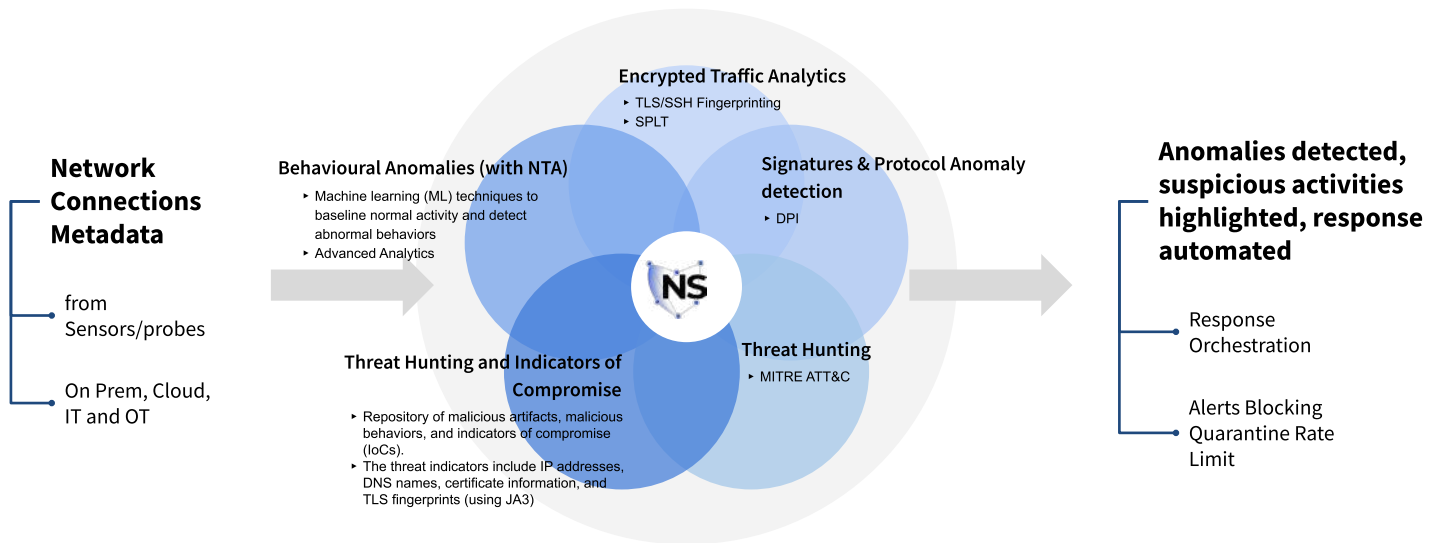
COSGrid Cloud Firewall

Multi-tenant yet virtual & dedicated Next Generation Firewall in Cloud

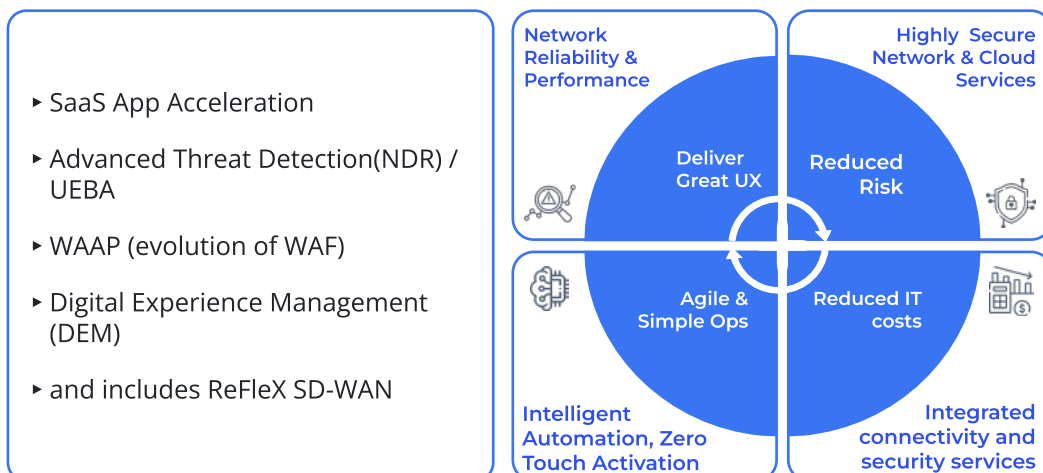
-  1st level of Protection for users & endpoint connecting to Internet from anywhere
-  Distributed Edge across geographies closer to the users & branch offices
-  Centrally manages IP, port, protocol and application rules (layer 3, 4 and 7)
-  Forwards web traffic (ports 80 & 443) to secure web gateway
-  Automated tunnels from SD-WAN or VPN/ZTNA in the end point
-  Deep Packet Inspection (DPI) on selective traffic/destination domains
-  Block high risk applications and protocols (layer 7 application visibility & control)

COSGrid Advanced Threat Protection

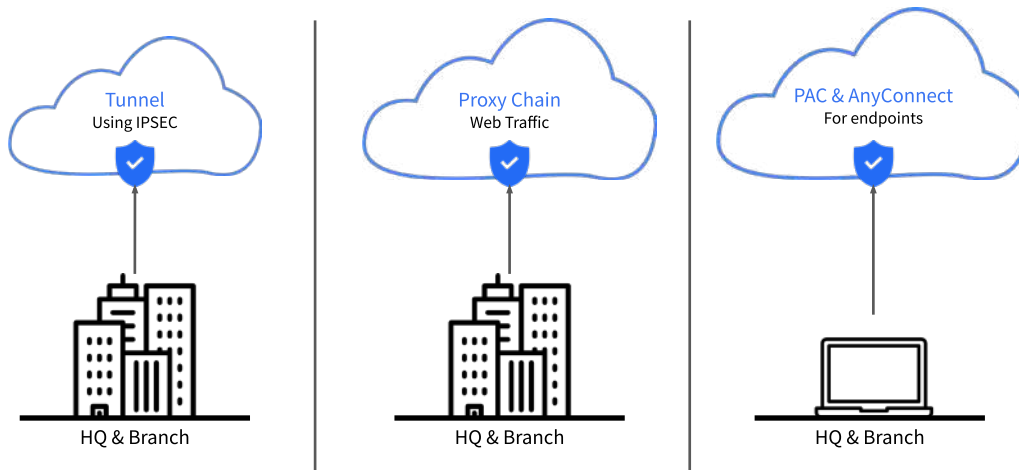
COSGrid NetShield NDR Empowers proactive threat hunting based on the MITRE ATT&CK framework to uncover hidden threats and respond swiftly to security incidents.



COSGrid SASE - Benefits



Deployment Options



Technical Specifications

Platform features	
Cloud-delivered deployment	100% cloud-native platform delivered as a SaaS service. For unique use cases, private and virtual service edges are available.
Data privacy and retention	When logging data, content is never written to the disk and there are granular controls to determine where exactly logging takes place. Use role-based access control (RBAC) to provide read-only access, username anonymization/obfuscation, and separate access rights by department or function, in accordance with key compliance regulations. Data is retained for a rolling period of six months or less, depending on the product. You can purchase additional storage that retains data for as long as desired.
Key compliance certifications	Certifications include: <ul style="list-style-type: none"> • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C See the full list of our compliance certifications here .
Granular API support	We maintain REST API integrations with numerous identity, networking, and security vendors. For example, you can share logs between Zscaler and your cloud-based or on-prem SIEM (e.g. Splunk). Learn more
Direct peering	Direct peering with major internet and SaaS providers and public cloud destinations ensures the fastest traffic path possible.
Service level agreements (SLAs)	
Availability	99.999%, measured by transactions lost
Proxy latency	< 100 ms, including when threat and DLP scanning is on
Virus capture	100% of known viruses and malware
Supported platforms & systems	
Client Connector	Support for: <ul style="list-style-type: none"> • iOS 9 or later • Android 5 or later • Windows 7 and later • Mac OS X 10.10 and later • CentOS 8 • Ubuntu 20.04
Branch Connector	Support for: <ul style="list-style-type: none"> • VMware vCenter or vSphere Hypervisor • Centos • Redhat

+91 90227 64534

[cosgrid-networks](#)

[@cosgridnetworks2141](#)

[@CosgridNetworks](#)

Ph: +91 90227 64534, +91 86101 44212 | E-mail: info@cosgrid.com

Address HQ: COSGrid Systems Private Limited - Velachery, Chennai - 600042

Address 2: COSGrid Networks Inc - New Castle, US, 19808



© 2023 COSGrid Networks All rights reserved.