graphiant

Secure SASE Without Decryption

Enterprises require secure connectivity for remote and hybrid workers, but many SASE platforms introduce privacy and security concerns by decrypting customer traffic. Graphiant's SASE solution removes this risk by delivering unified connectivity, security, and compliance without decryption-based inspection, preserving true end-to-end encryption while enabling modern secure access for a distributed workforce.

Key Benefits

Securely Support Remote and Hybrid Work

Enable secure access for a distributed workforce without relying on legacy VPNs, improving your security posture while maintaining user productivity.

Reduce Attack Surface

Enforce zero-trust, identity-based access, limiting users and devices to only the applications they are authorized to access and significantly reducing lateral movement.

Improve Threat Prevention and Detection

Inspect traffic closer to the user, enable faster identification and mitigation of threats, reduce dwell time and breach impact.

Unify Visibility Across Your Environment

Leverage a single platform to provide end-to-end visibility into remote users, on-premises locations, public clouds, and neo-cloud environments, enabling comprehensive monitoring and faster security decision-making.

Comprehensively Protect Your Data

Enable protection for every layer in your data stack, from user and application to cloud and AI data, through centralized, policy-driven security controls.

Preserve End-to-End Encryption

Maintain true end-to-end encryption by never decrypting customer traffic outside your environment, protecting data privacy and integrity at all times.

Eliminate Centralized Decryption Risks

Unlike traditional SASE solutions, Graphiant avoids centralized decryption points that create single points of vulnerability. Threat assessment and policy enforcement are performed directly on the user device, without relying on in-line proxies.

Key Features

1. Zero Trust Network Access

Graphiant's SASE solution delivers zero-trust network access by replacing implicit network trust with identity and context-based access controls. Users and devices are granted access only to the specific applications they are authorized to use, rather than broad network access. This approach significantly reduces enterprise attack surface, prevents lateral movement, and enables secure access for remote users, on-premises locations, cloud environments, and AI workloads, all enforced consistently across the enterprise.

2. Threat Detection and Content Filtering

Our SASE solution provides advanced threat detection and content filtering to protect users and applications from malicious activity. Using security policies, enterprises can block known and unknown threats, malicious websites, and risky content before they can impact the environment. Continuous monitoring of traffic patterns and behavior helps detect threats early, reduce dwell time, and enforce acceptable use policies.

3. Data Loss Prevention

DLP capabilities help safeguard sensitive enterprise data across users, applications, cloud and AI environments. Our policy-driven controls monitor and prevent unauthorized data movement, reducing the risk of data leakage and accidental exposure. By enforcing consistent data protection policies across the entire environment, our solution enables enterprises to protect critical information, support compliance requirements, and maintain visibility into how data is accessed and used.

How it works

01

Select your remote users

Choose the specific users that require remote access and assign them to the appropriate access policies.

02

Configure your application and security policy

Define which applications these users can access and apply security controls.

03

Install the Graphiant agent and connect

Install the lightweight Graphiant agent on the user's device to securely connect it to the Graphiant secure fabric.

Real World Use Cases

Secure Your Remote and Hybrid Workforce

Give your remote and hybrid employees fast, secure access to the applications they need. Graphiant enforces zero-trust access so users connect only to approved applications from any location, helping you reduce risk while maintaining productivity and visibility.

Protect Sensitive Data and Maintain Compliance

Safeguard your most sensitive data and meet regulatory requirements for dealing with PII and HIPAA data. Graphiant actively monitors and prevents unauthorized data movement using DLP techniques while preserving end-to-end encryption and providing clear visibility into how data is accessed and used.

Reduce TCO with a Simplified Network and Security Stack

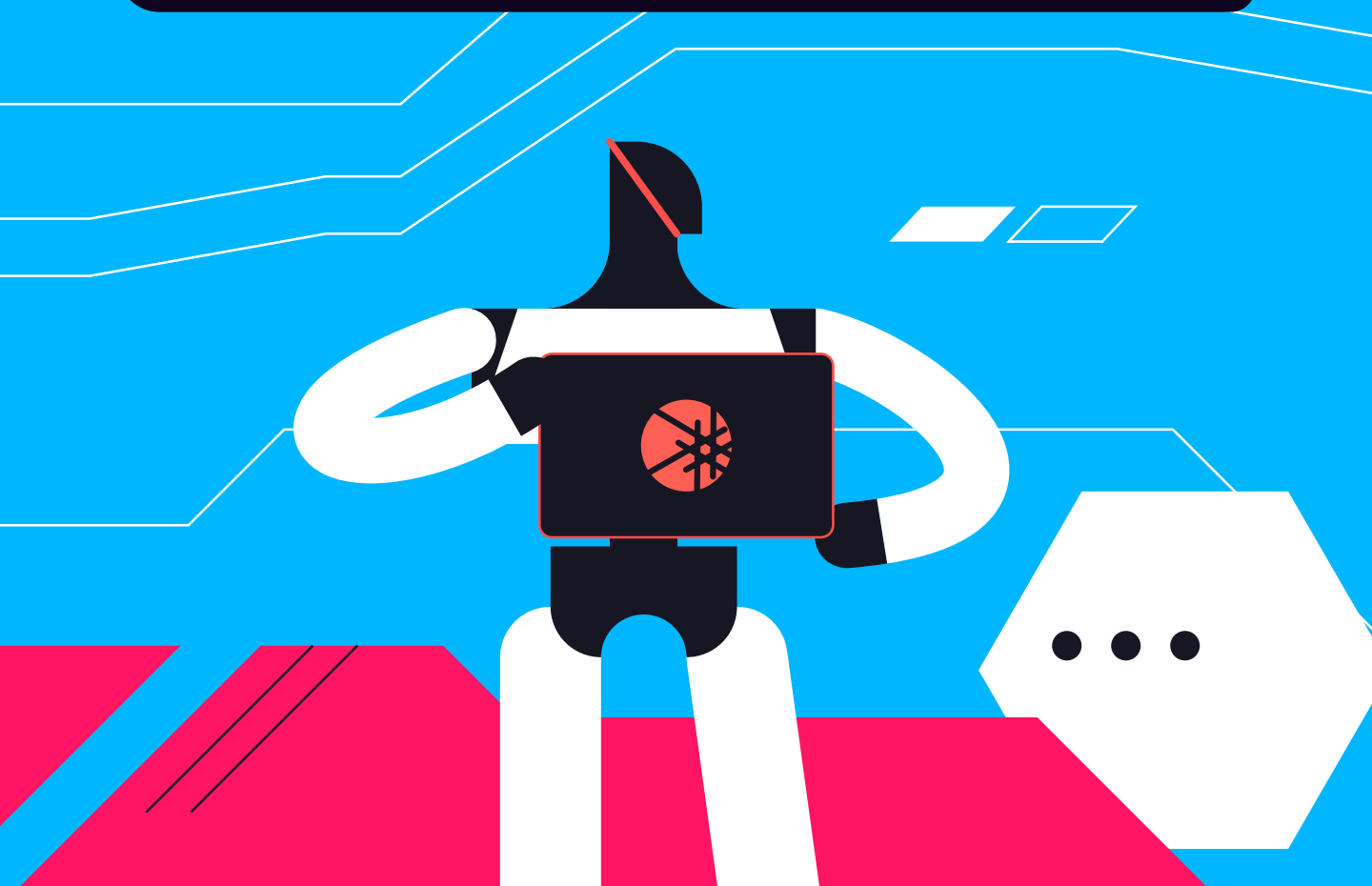
Replace disconnected networking and security tools with a single, cloud-delivered SASE platform. Graphiant helps you reduce operational complexity, eliminate configuration gaps, and strengthen your security posture while lowering infrastructure costs.

Enforce Data Sovereignty with Geo-Fenced Access

Control where your data can be accessed and enforce national or regional boundaries with geo-fenced policies. Graphiant prevents unauthorized access to sensitive or sovereign data, reducing regulatory risk when operating across global environments.

Graphiant SASE - Secure your enterprise, without compromise

Graphiant's SASE solution enables your enterprise to securely connect remote and hybrid users to the applications they need, without adding complexity or compromising security. By delivering consistent zero-trust access controls, strong data protection, and compliance-ready policies, without decryption-based inspection, we empower your organization to support a dynamic, productive workforce from anywhere while maintaining the security and compliance standards your business requires.



graphiant

Assured, Agile, Awesome.

Follow us on: