appgate

DATA SHEET

SDP FOR GCP

Adaptive, Identity-Centric Security for Public Clouds

Security in the cloud is a shared responsibility and that’s true with Google Cloud Platform (GCP). Cloud providers protect the underlying infrastructure and customers protect their data. This model presents unique challenges that don’t align with Zero Trust principles.

Zero Trust is a security framework that is founded on the principle of least-priviledged access to network resources. To achieve Zero Trust, it’s essential to employ an identity-centric access model. Yet with GCP, security teams have to rely on Security Groups, which are simple IP-based firewalls. They don’t provide the identity-centric information security teams need to control user access to Google’s Compute Engine or Cloud Storage resources. It’s nearly impossible for security teams to control and scale secure access using static IP addresses and port mapping.

GCP SECURITY CHALLENGES

- Cloud environments are dynamic because servers are continuously created and terminated.
- Access is available to users not on the corporate network.
- Users are granted broad entitlements to services running on all instances within the cloud environment instead of least-privileged access.

BENEFITS

Aligns with Zero Trust principles of identify-centric access

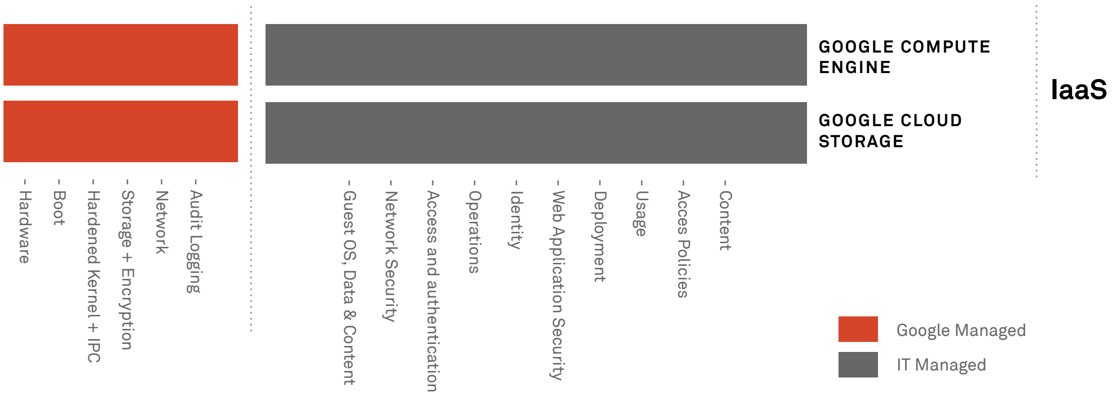
Provides secure, encrypted connection between users and approved GCP resources

Makes the entire GCP environment completely invisible

Supports DevOps because it’s easy to deploy and adapts to added or removed instances in real-time

Built like the cloud for the cloud – massively scalable, distributed and resilient

SHARED SECURITY MODEL:
Where Google ends and IT controls begin



APPGATE SDP: ADAPTIVE, IDENTITY-CENTRIC SECURITY

Appgate SDP for GCP delivers least privilege, secure network access. It dynamically creates a secure, encrypted network segment of one that's tailored for each user session. It simplifies the cloud user access problem and eliminates over-entitled network access.

APPGATE SDP FOR GCP:

- Integrates with AD to provide initial user authentication and assignment of conditional access rights. At the time of actual access, claims are checked again to ensure the user still complies with the security policy.
- Provides identity-centric remote access with simultaneous connections directly from user's device to any number of sites. Each SDP Gateway is stateless and built to accept many thousands of secure client (mTLS) connections simultaneously. It can be clustered for high availability and linear scale.
- Allocates policies to users based on rules that include any number of claims dynamically evaluated in real-time. Appgate SDP sets access rights based on available GCP metadata and current context.

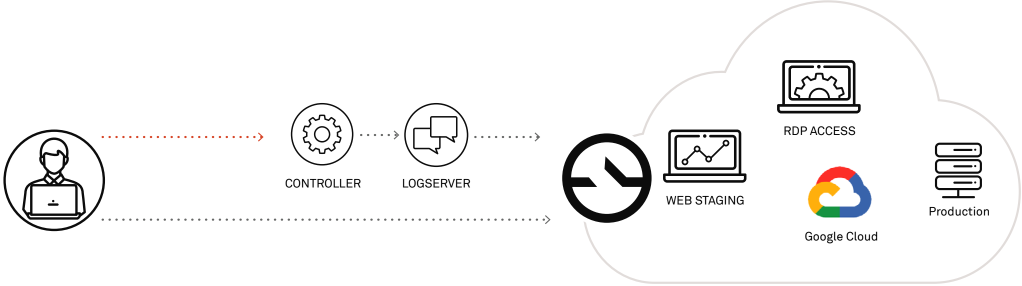
Appgate SDP for GCP architecture is distributed, resilient, and massively scalable. It allows enterprises to implement a global, highly available secure access system in any hybrid environment with greater control and improved economics.

WHAT IS APPGATE SDP?

Appgate SDP for GCP is a Software-Defined Perimeter—a network security model that dynamically creates one-to-one network connections between the user and the instances and services they access. Appgate SDP for GCP is:

- Designed around the individual: authentication is based on the person, environment, and infrastructure. It's context aware, dynamically adapting policy based on environmental, infrastructure, or organizational changes.
- Built for the cloud: it's distributed and stateless, built for hyper-scale, microservices architecture, with API-driven entitlements.
- Based on the Zero Trust model: It takes an "authenticate first, connect second" approach, ensuring that only authorized users can connect over an encrypted connection to cloud instances and resources. This reduces the attack surface and significantly improves security.
- Able to deliver fine-grained access control adjusting access automatically based on changes in context.
- Engineered to cloak all cloud resources—except those that the user is authorized to access. By making all other instances invisible, enterprises can simplify their security infrastructure, while granting access with confidence.

Appgate SDP delivers fine-grained access control adjusting access automatically based on changes in metadata while hiding all GCP resources


CONTROLLER
LOGSERVER
RDP ACCESS
WEB STAGING
Google Cloud
Production