appgate

DATA SHEET

SDP FOR AWS

With AWS, enterprises share responsibility for aspects of cloud security. Specifically, AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud and enterprises are responsible for what they put in the AWS cloud.

So organizations turn to AWS security groups in an attempt to secure access to their cloud-based workloads. Yet AWS native security groups are simple IP-based firewalls which do not provide the identity-centric access control needed by security teams to control user access to Amazon EC2 resources. Trying to control "who can access what" with static IP addresses and port mapping just doesn't scale.

TRADITIONAL SECURITY STRUGGLES WITH AWS USER ACCESS:

- It's located outside the company perimeter, and may be accessible without users present on the corporate network.
- Cloud environments are dynamic as servers are continuously created and terminated. Traditional security tools cannot keep pace, often granting users access to all services running on all instances within the cloud environment.

BENEFITS

Access based on user identity

Secure, encrypted connection between users and approved AWS instances

Makes entire AWS environment completely invisible

Perfect for DevOps – easy to deploy and adapts to added or removed instances in realtime

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

The AWS Shared Responsibility Model

CUSTOMER

RESPONSIBLE FOR SECURITY "IN" THE CLOUD

- Customer data
- Platform, applications, identity & access management
- Operating systems, network & firewall configuration
- Client-side data encryption & data integrity authentication
- Server-side encryption (file system and/or data)
- Network traffic protection (encryption/ integrity/identity)

AWS

RESPONSIBLE FOR SECURITY "OF" THE CLOUD

- AWS foundation services: Compute | Storage | Database | Networking
- AWS global infrustructure: Regions | Availability zones | Edge locations

APPGATE SDP: ADAPTIVE, IDENTITY-CENTRIC SECURITY

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

The Appgate SDP architecture is distributed, highly 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.

SOFTWARE-DEFINED PERIMETER

APPGATE SDP IS A SOFTWARE-DEFINED PERIMETER:

- 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 hyperscale, 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.

Appgate SDP delivers fine-grained access control adjusting access automatically based on changes in context while hiding all cloud resources—except those that the user is authorized to see. By making all other instances invisible, enterprises can simplify their security infrastructure, while granting access with confidence.

Appgate SDP policies make access decisions based on attributes from the person—user device, anti-virus, department, group membership, app permissions; the environment—location, time, security posture; and the infrastructure—network analytics, security groups, tags, hostnames. It's dynamic and scriptable, and encrypts one-to-one connections between the user and instance, and dynamically responds to the creation or termination of IaaS server resources. Every new instance is automatically traced and added or removed from the access filter.

Superior integrations with SIEM and IDS systems build bridges among security tools. The result is improved security and more efficient compliance reporting.

The Appgate SDP architecture is distributed, highly resilient and massively scalable.