SECURE ACCESS DATASHEET

Cyxtera™

AppGate SDP and Containers—a Perfect Match

Using a distributed, scalable, and highly available Software-Defined Perimeter (SDP) model, AppGate can easily and efficiently protect containerized applications and content from internal and external threats while significantly lowering costs.

In traditional computing environments, organizations use AppGate SDP to protect access to physical, virtual, and cloud-based resources. AppGate SDP policies will dynamically adapt to changes in the environment; granting access to server instances based on a combination of user attributes, server metadata, and overall system context. AppGate SDP can enforce the same type of dynamic access control to containerized applications.

Using a dynamic policy, AppGate SDP automatically applies access control to each newly launched container instance, without requiring manual intervention. Upon creation, access to a container will automatically be configured based on container attributes, naming, and user context. As long as the container has an addressable IP address, AppGate SDP can protect it.

AppGate SDP works with containers under the Docker platform, Kubernetes, Amazon, Red Hat and Microsoft.

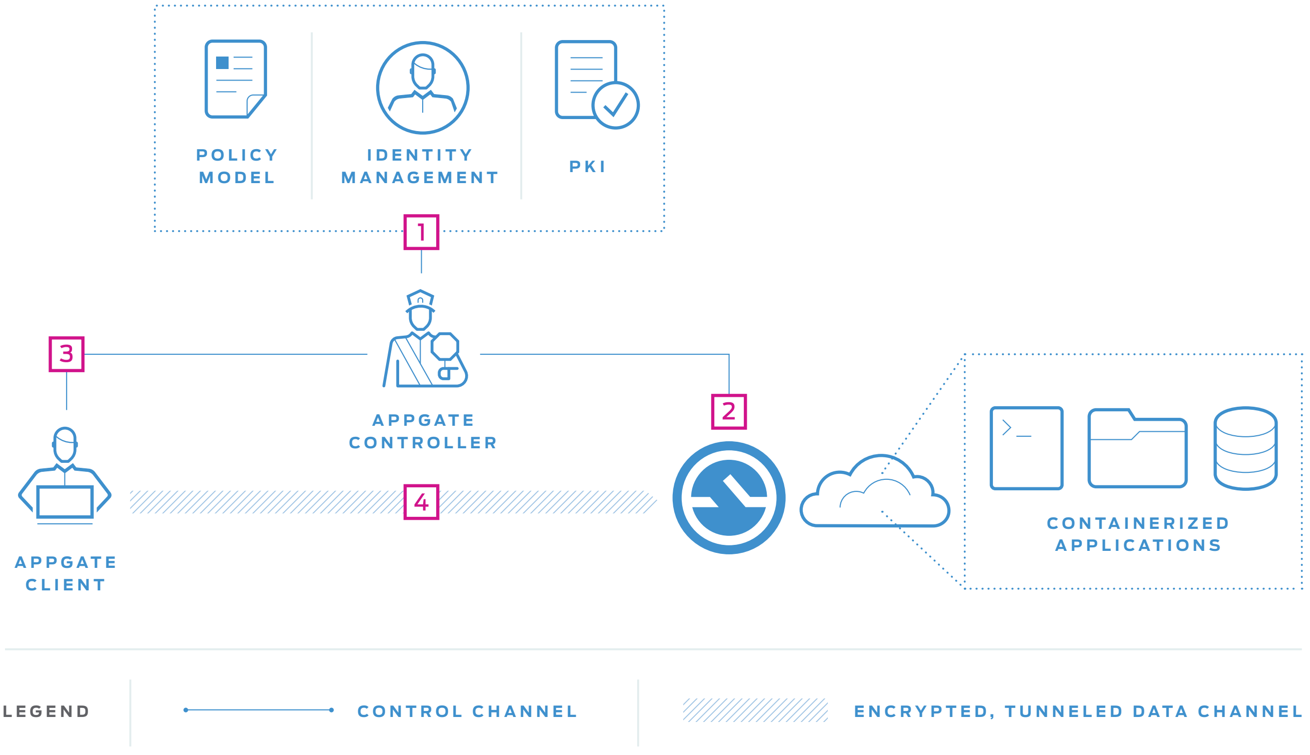
WHAT IS A CONTAINER?

A container is a fully, self-contained application instance, including all of its necessary dependencies, libraries and any other configuration files, in a single bundled package. A container runs independently on underlying infrastructure and operating system configurations, with much less overhead than traditional virtual machines.

Protecting Containers with AppGate SDP

1. Controller uses PKI and IAM to establish trust. Controller is an authentication point and policy store
2. Gateways protect cloud and network resources. Container-based application network traffic passes through Gateway
3. Clients securely onboarded, authenticate to Controller, then communicate with mutual TLS
4. Clients access container resources via Gateway
   - Mutual TLS tunnels for data
   - Real-time policy enforcement by Gateway
   - Security policies automatically applied to new container instances recognized by cloud resolver

Containers, which have grown in both scope and capability over the past few years, are now a core part of many organizations' development and deployment platforms, often forming the core of a DevSecOps initiative. At the same time, enterprises are increasingly adopting security solutions such as Cyxtera's AppGate SDP, to benefit from its identity-centric approach. Given these two trends, a natural question is how AppGate SDP can be used to secure access to containerized services.


POLICY MODEL
IDENTITY MANAGEMENT
PKI
1
3
APPGATE CONTROLLER
2
APPGATE CLIENT
4
>_
CONTAINERIZED APPLICATIONS
LEGEND
CONTROL CHANNEL
ENCRYPTED, TUNNELED DATA CHANNEL