Multi-Cloud Service Interconnection Fabric

bayware

BUSINESS SITUATION

Accelerating digital transformation and rapidly changing customer requirements compel enterprises to continuously add and enhance applications. Enterprise are transforming how they develop and deploy applications; leveraging cloud-native principles and microservice architectures to enhance agility, improve time to market, and get lean. As they modernize, enterprises want to exploit the benefits of multi-cloud deployments, control communication flows wherever an application runs, and maintain private-cloud levels of security. Doing this is limited by today's complex networking solutions. Enterprises need an application-centric architecture that delivers programmability, observability and security; while underlying infrastructure remains general purpose.

BAYWARE SOLUTION

Bayware is a programmable network microservices architecture that gives every application its own secure, overlay network, all in software. This fit-for-purpose solution introduces the programmable service graph where each application microservice initiates and controls its own programmable communication flows; enabling the long-promised *intent-based networking*. Bayware radically simplifies the interface between an application and underlying networks. This accelerates continuous deployment of application services by eliminating constraints imposed by managing network configurations, and securely serves each application's data communications needs as they change and move across any cloud.

BAYWARE SERVICE INTERCONNECTION FABRIC

Bayware's network microservices uniquely enable direct programming of application data flows in software. This service interconnection fabric is the first secure, programmable network service graph. A service graph represents application microservices as nodes and network flows as edges. While the nodes are software by definition, Bayware extends that to the edges with network microservices. As secure, simple-to-program, lightweight communication *contracts*, these network microservices deploy with application workloads and provides an unprecedented level of control and agility in heterogeneous hybrid and multi-clouds. Bayware service interconnection fabric is a suite of distributed software components that run on standard x86 Linux machines and operate securely on top of any virtual or physical infrastructure.

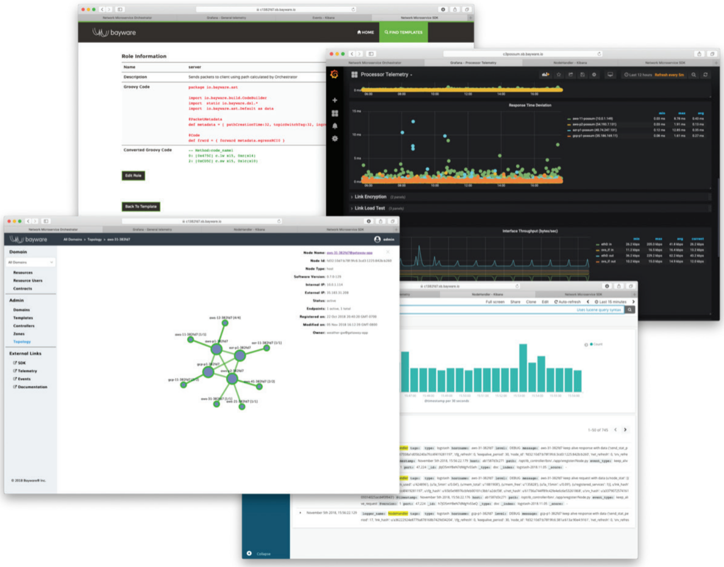

Figure 1: Bayware Service Interconnection Fabric, Observability and Telemetry, Network Microservice Programmability

BENEFITS

Application Intent Driven

- Map application service graph directly to Bayware service interconnection fabric – nothing lost in translation.
- Network microservices (communication contracts) are embedded in an application's own data stream to tell Bayware processors how to steer and deliver communication flows.
- Network microservices are made available to VMs and containers for virtually real-time update.

Pervasive security

- Application microservices initiate just the flows they need. All other flows are default deny.
- Micro-segmentation by default. Applications and flows are isolated by role-based access.
- Flows between workloads, in whatever clouds they are running, are automatically encrypted.

Multi-cloud native

- Network services become like applications - flexible, API-accessible microservices that they can develop, deploy, and modify quickly to serve to customers anywhere.

All Code – Brings Agility to Networking

- Enterprises get the same development and deployment agility and the same cloud-scaling benefits for their networking functions as they are getting from their cloud-native applications.

WHY BAYWARE

Bayware brings NetOps and SecOps into the DevOps model of continuous, application-centric deployment. It is all code: Enterprises get the same development and deployment agility and the same cloud-scaling benefits for networking functions as they are getting from cloud-native applications. Bayware has a unique solution for enabling application service to communicate across the diverse hybrid-cloud and multi-cloud infrastructures: (1) enables the network to respond to frequent additions, updates and changes in scale and location; (2) ensures that security and network policy meet compliance and corporate standards. Today's solutions do one, or the other well, but not both. Bayware's pervasive security automatically encrypts flows and is hyper-micro-segmented by default. This improves on security, observability and accountability for network usage rather than requiring compromises as the newest service mesh solutions do.

HOW BAYWARE WORKS

Bayware created and patented Network Microservices; micro-code communication contracts. Each is programmable; and can be designed and approved by networking and security professionals. Microcode is carried from the workloads in the packet headers, using standard IPv6 extension headers. The execution of the contract by software processors then creates the desired steering of packets through the overlay network. Creating service-to-service communication provisioning is easy:

1. Based on the service graph, program application intent and network policy as Network Microservices contracts; simply by adding application labels to the desired flow pattern from a library of contract types.
2. Deploy light weight Linux daemons (agents) on workload hosts that retrieve authorized Network Microservices to insert as highly compact microcode into IPv6 packet extension headers in response to applications.
3. Provision a fabric of processor software (on Linux x86 machines) in target VPCs to securely execute service-to-service communication only as authorized by received Network Microservice contracts.

BAYWARE DEPLOYMENT OPTIONS

Bayware breaks from Software Defined Networking (SDN) models that push complex reconfigurations into underlying networks, which were not built for continuous change. Bayware reduces acquisition and operation costs by running over the top of brownfield underlay networks, eliminating the need to install and configure any additional specialized networking appliances or controllers. Enterprises can run Bayware standalone using the underlying infrastructure of cloud providers' Virtual Private Cloud (VPCs). Bayware also runs in concert with application service orchestration systems and SDNs that provision lower layer data center and branch networking. Bayware provides an all-in-one solution for service-to-service communications.

BAYWARE DEPLOYMENT OPTIONS FOR HYBRID AND MULTICLOUD ENVIRONMENTS

Application Services	☐ Application services deployment and operation ☐ Services intrusion and anomaly detection ☐ End-to-end data encryption (mTLS) ☑ **Service network dependency management (service graph)** ☑ **Service discovery and instance selection** ☑ **Service-to service target selection**
Service to Service Communications	☑ **Role-based access control with network endpoint packet filtering** ☑ **Network interface for containers (CNI), VMs, and Linux servers** ☑ **Certificate-based network endpoint ID (crypto generated address)** ☑ **Hybrid and multi-cloud microsegmentation (default-deny)** ☑ **Policy-based (role/conditions) multi-cloud traffic steering / routing** ☑ **Automatic link encryption** ☑ **Node-to-node performance and security telemetry** ☐ Layer 3 IP connectivity
Packet Delivery	☐ Underlay provisioning ☐ Underlay configuration ☐ Underlay packet delivery performance monitoring and analysis

Figure 2: Bayware services in standalone or complementary deployments.

KEY FEATURES

One multi-cloud platform as a simple overlay solution - no complex stack

- Deploy as code as part of application deployment process – no changes to the application microservices, no forklift, no Linux kernel changes
- Service dependency management, i.e. management of service access graph (aka service graph)
- Service discovery and instance selection
- Node-to-node performance and security telemetry

Network services entirely abstracted from the underlay providers

- Network interface for containers (CNI), VMs, and Linux servers
- Certificate-based network endpoint ID (crypto generated address)

Micro-segmentation by default – pervasive security

- Role-based access control with network endpoint packet filtering
- Zero-touch workload attachment, with automatic link encryption

Policy-based (role/conditions) multi-cloud traffic steering / routing

- Encrypted site-to-cloud VPN to enable hybrid cloud
- Encrypted nulti-cloud peering to enable multi-cloud
- UI and SDK for programming flow level security and operations requirements
- Near real-time policy update and enforcement via active orchestration

ABOUT BAYWARE

Bayware, a San Francisco-based software company, brings NetOps and SecOps into the DevOps model of continuous, application-centric deployment by giving each hybrid-cloud application its own secure programmable overlay network, all in software. Bayware's unique network microservices architecture enables direct programming of application data flows; breaking from the SDN models which were not built for continuous change in a multi-cloud environment; and without the security and network observability compromises seen in the latest service mesh solutions.

LEARN MORE

- View Bayware introduction videos
- See a demo
- Test drive Bayware