Volterra

WHITE PAPER

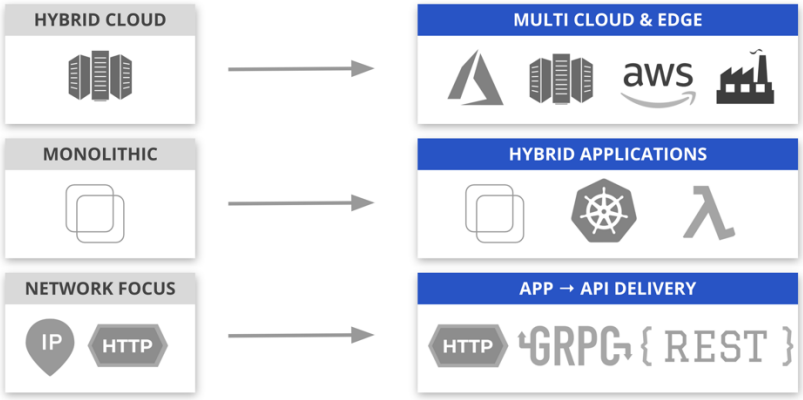
New Paradigm for Networking and Securing Modern Apps

Modern Apps: More Pieces, More Places

Globalization and consumerization of technology is requiring enterprises to become more agile so they can innovate and respond to change faster. Applications now need to be always on, scale rapidly to serve millions of users, have global availability, and respond in milliseconds. These market demands require modern applications that are different than what was common a few years ago. Modern app development techniques enable enterprises to innovate faster while reducing risk, time to market, and total cost of ownership.

While there are significant advantages of modern apps, they also increase the operational complexity and requirements for underlying infrastructure like networking, security and application services. This is due to new architectural components:

- **Microservices and serverless architecture** enable modular, independent and fine-grained development of components. These modular components enable faster development and rapid scaling of app.
- **Explosive use of APIs for communication across microservices.** Microservices access each other through application program interfaces (APIs). The proliferation of APIs per app has made existing security controls like network micro-segmentation ineffective, as inter-app communication is now occurring at the API layer with all traffic encrypted and multiplexed on the same network port.
- **Emerging deployment models — distributed app clusters and multi-cloud.** Modern apps and their microservices are also being deployed across multiple clusters and even across multiple cloud providers (to improve reliability and scale). However, these come with the problems of increased network latency that degrades user experience.



Modern Apps Create New Challenges in Networking and Security

A general claim that modern apps (built on microservices) are “simpler” when compared to traditional (i.e. monolithic) apps is inaccurate. While the complexity within an individual microservice may be reduced, the sophistication of orchestrating, operating, and troubleshooting a distributed system of microservices is significantly higher than with traditional applications. The microservices architecture shifts complexity from the space of app development into app operations (aka DevOps).

The following are networking and security challenges introduced by modern app architecture:

Operational complexity increases TCO and hampers collaboration

- **Proliferation of legacy siloed point-specific tools.** DevOps and NetOps use different point products and tools to support app infrastructure and operations, including load balancers/application delivery controllers (ADC), content delivery networks (CDN), API gateways and web app firewalls (WAF). Costs include not only around purchasing these services, but the extensive time required to effectively integrate and continuously operate them. Most of these tools were not designed for modern microservice- and container-based apps, so a full stack of them must be configured for every cluster. This complexity is compounded in multi-cloud deployment models.

- **No end-to-end visibility or policy enforcement.** Given the siloed deployment and operation of each cluster and the networking and security within it, it is nearly impossible to get end-to-end visibility of traffic and apply consistent policy to it.
- **Difficult to collaborate across DevOps, NetOps and developer teams.** Collaboration within app teams, as well as with infrastructure and operations (I&O) teams, is required now more than ever due to the added operational complexity of microservices, containers and distributed clusters and clouds. Lack of a properly integrated tool chain or workflow can negatively impact the KPIs (team velocity, mean time to recovery, mean time between failures, etc) for these teams and the business outcomes for their stakeholders.

Network security controls can't enforce zero-trust in modern applications

- **Lack of API-level security makes it extremely difficult to implement zero-trust.** All APIs (gRPC or REST) are encrypted and multiplexed over the same port, obliterating the value of network-level microsegmentation. Microsegmentation and routing at the API-level is critical to implement zero-trust security. Gartner notes that "By 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications."[1]

Multi-cloud deployment increases latency

- **Deployment across multiple cloud providers increases latency and reduces performance.** Latency is an important part of the quality of service that determines user experience and the degree of consumer satisfaction. End-to-end latency is one of the user-oriented characteristics employed for quality assessment of distributed software architecture. As modern apps are distributed across multiple clouds (for reliability, compliance, best-of-breed services), they have to go through multiple networking and security services in each location, as well as connect with unpredictable performance over Internet circuits, thus increasing latency and negatively impacting the quality of service and user experience.

New Paradigm Needed for Networking and Securing Modern Apps

Current point products -- designed for monolithic apps -- are ineffective in addressing the aforementioned challenges of properly networking and securing modern, distributed apps. A new paradigm should be built around the following design principles:

- **Integrated network and security tech stack.** Network and security services such as load balancer/ingress-egress gateway, WAF and API gateway should be delivered as integrated tech stack instead of as specific point solutions. This avoids the time-intensive work to properly integrate the layers and data paths of the multiple services required per cluster, as well as across clusters.
- **Cloud-native management in a distributed microservices environment.** Modern app networking and security must be designed to support a moderate to large number of microservices deployed on multiple clusters and even across cloud providers. For a cloud-native operational model, this requires the ability to be deployed in multiple locations yet managed as a logical cluster or zone.
- **Provide zero-trust API security throughout.** As modern apps are designed with containers and microservices, APIs are the primary service-to-service communications channel. Since any or all software components -- developed, inherited, or open sourced from libraries -- can contain multiple APIs, a modern app security solution must automatically identify all APIs throughout the app and control them with appropriate zero-trust policies like whitelisting and behavior analysis.
- **End-to-end visibility and policy.** As noted, modern apps are highly distributed in their microservices-based design and their multi-cluster deployment. This makes end-to-end visibility and policy enforcement both more difficult and critical than ever. Modern app networking and security must provide the ability to clearly see workflows and traffic from start-to-finish across microservices and clusters, as well as control them with appropriate policies.

Introducing Volterra

Volterra enables enterprises to securely deploy, secure and operate modern (and legacy) apps across multi-cloud and edge environments while addressing the new and increased challenges brought on by microservices, containers and the broad use of APIs. Unlike legacy infrastructure products that are focused on enabling monolithic web apps and centralized deployments (e.g. data center or single cloud provider), Volterra enables secure, fast and simplified operation of modern apps. Volterra offers a comprehensive set of capabilities through two core SaaS-based services:

- **VoltMesh** delivers high-performance networking and zero-trust security across multiple clusters, clouds and edge sites
- **VoltStack** automates the deployment and operation of distributed apps and app infrastructure across edge sites and public/private clouds
- **Volterra Global App Delivery Network (ADN)** is industry's first app-to-app network and security service with the ability to directly host workloads for maximum performance

Volterra's app-to-app networking and security platform addresses the operational complexity and improves the security of modern apps. Specific benefits include:

- **Simplifies + secures the deployment (Day 1) and operation (Day 2) of modern apps** by integrating a comprehensive set of app-to-app networking (load balancer/ingress-egress gateway, routing), security (WAF, API auto-discovery and control) and app services (API gateway) into a single SaaS-based service with centralized management across 100s of clusters in one or more cloud locations.
- **Eliminates many API-related security and operational challenges** by automatically discovering all APIs within an app (new development, existing or open sourced components) and employing zero-trust policy through whitelists and behavioral analysis
- Provides **end-to-end visibility and policy** by seeing all nodes and activity within and across the clusters and microservices of a modern app, and the ability to provide centralized reporting and policy enforcement across them

In summary, Volterra provides an end-to-end solution for modern, distributed app networking and security—all with the simplified operational model of a SaaS-based service.

[1]Gartner, "API Security: What You Need to Do to Protect Your APIs", Mark O'Neill, et al, 28 August 2019