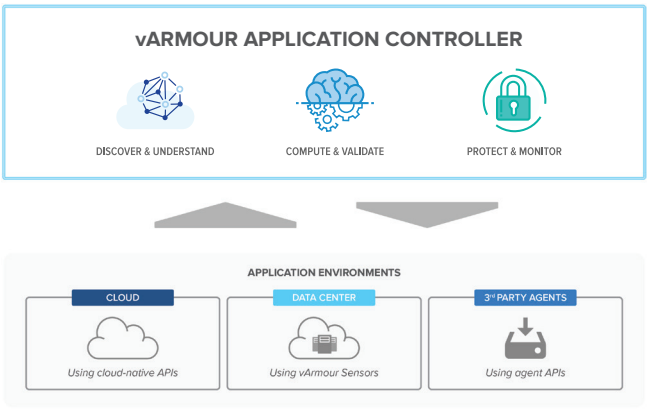
PROVEN SECURITY FOR HYBRID CLOUD APPLICATIONS

Application security management has always been a challenging endeavor, exacerbated by the rapid expansion to public cloud. Lack of understanding of application communication behaviors, errors resulting from manually developed policies, and risks associated with deploying policies all impact organizations' ability to reduce the attack surface on their applications and to keep pace with the ever-increasing velocity of change.

vArmour Application Controller helps CISOs and security teams better understand their rapidly changing environments, and effectively manage application security policies. It is the only security system that auto-discovers applications, provides complete application relationship maps, computes intent-based security policies, and protects applications running on various computing platforms (physical, virtual, container) across public and private clouds--all without having to install agents on endpoint workloads.



HIGHLIGHTS

- Discover and visualize applications and their relationships across environments
- Accelerate policy development by using intent-based policy templates
- Simulate impact of candidate policies with observed communications before deployment to production
- Deploy policies across various compute platforms and environments
- Get best practice and compliance reports of critical applications
- Leverage rich sets of APIs to seamlessly integrate with external orchestration and CMDB systems

LICENSING FLEXIBILITY

vArmour Licensing Portability help customers maximize their ROI in hybrid cloud security by allowing licenses to be migrated as application infrastructure changes over time. From physical, to virtual, to public cloud and to containers, vArmour Licensing Portability will provides an infrastructure agnostic solution.

KEY BENEFITS

1. Discover and Understand

Understanding real application behaviors is critical for developing policies to reduce exposed attack surfaces while not impacting the operation of the application. By capturing real world application communication patterns across multiple environments and infrastructures, vArmour Application Controller discovers workload types, application clusters, and dependencies so that security administrators can easily visualize application relationships, and create granular intent-based policies to keep applications secure.

Furthermore, Application Controller's application relationship maps enable administrators to further classify their applications, and/or enrich their sources of truth such as CMDBs. The collected data also accelerates reporting and investigative tasks for compliance monitoring, network troubleshooting, and incident response.

2. Compute and Validate

Typically, the more large and complex an application is, the more difficult it is to secure. vArmour Application Controller alleviates this challenge by automatically discovering and labeling workloads, enabling visualization of applicatio behaviors, and offering intent-driven policy templates. Securing applications--large or small; simple or complex--is now a far more straightforward exercise that requires dramatically less time to accomplish. Creating policies can be as simple as selecting an application and applying an intent-based policy template. For example, a security administrator could select sets of PCI-DSS servers and apply the PCI-DSS Compliance template to generate candidate policies. Manual policy editing is supported for those cases where non-standard policies are required.

Deploying candidate rules to production without accidentally impacting other services or applications can be a nerve-wracking exercise. vArmour Application Controller eliminates potential unintended consequences by validating candidate policies against the real observed communications. For example, security administrators can observe which traffic flows would be blocked by the candidate policies, how permissive or strict their policies are with regard to historical traffic, etc.

3. Protect and Monitor

Distributing policies to protect applications and monitoring the efficacy of those policies are requisite parts of the application security lifecycle. Firms today face twin challenges: not only do they need to ensure that their elastic and dynamic workloads are always protected by up-to-date and accurate policies but they also need to provide proof, on a regular basis in regulated industries, that their critical applications and systems are protected by

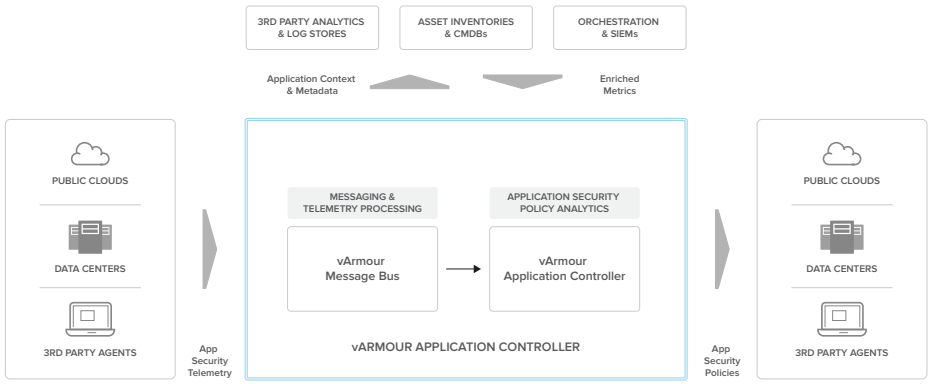
precise policies that can be traced to business justifications.

vArmour Application Controller makes it easy to implement consistent policies across environments. In private clouds, it works directly with vArmour Sensors to enforce policies on all application-level flows in and out of workloads (physical, virtual or container). In addition, it can program third party agents. In public clouds, it can program cloud native controls such as Network Security Groups in Azure and Security Groups in Amazon Web Services.

Moreover, vArmour Application Controller provides tooling to monitor the status and efficacy of the deployed policies. Users can measure the amount of attack surface on a set of workloads. They can observe how effective deployed policies are: e.g., identify unused policies in the last 90 days, see policies producing deny hits over a threshold, etc. They can monitor if any deployed policies have been changed by some other source other than the Application Controller itself, and compare the running policies with the policies of record on vArmour Application Controller.

vARMOUR APPLICATION CONTROLLER ARCHITECTURE

The vArmour Application Controller is designed to work in and across public and private cloud environments, and to be highly scalable. Its architecture consists of the following components:



vArmour Message Bus

vArmour Message Bus is vArmour Application Controller's distributed log processing engine based on Apache Kafka. The engine takes in application and network flow logs from telemetry producers such as

vArmour Sensors, public cloud flow log sources and third party agents. Message Bus can forward those logs to third party log processors such as SIEMs. But its main function is to turn the logs into deduplicated, summarized, enriched sets of flows (consisting of sources, destinations, services, applications, and other metadata), and continuously send those processed flows to the Application Controller. A Message Bus instance can process over 30 million application-level session logs per hour, and can scale horizontally by adding more instances. Message Bus also stores processed flows in its data store for a configurable period (a year by default).

vArmour Application Controller

Application Controller is vArmour's application security analytics engine that provides application visibility and policy computation functions across environments. The capabilities are enabled by its highly enriched graph of assets (applications, workloads), the connectivity relationships among them, and various attributes and metadata associated with those assets and relationships. The graph is continuously updated with processed telemetry from the Message Bus, and is further enriched by workload and traffic classification information from external sources of truth such as CMDBs and orchestration systems.

The rich dataset makes it possible to view not only complete relationships among applications but also examine the efficacy of security policies associated with those applications. Application Controller's built-in policy templates make it easy to dial up and down the policy granularity on an application or group of applications. Its policy simulation capabilities show the potential impact of candidate policies as well as any potential conflicts among the policies--all prior to actual deployment. Lastly, its label-based policy language naturally supports policy automation necessary for dynamic, elastic workloads of cloud applications and workloads.

Application Controller can be deployed on premises, in cloud or as a vArmour-hosted software as a service (SaaS). An Application Controller instance can handle 20,000 workloads and 2 million application relationships.

USE CASES

Auto-discovery of applications and relationships

- What applications are running in my public and private clouds?
- What application functions are they performing? E.g., Web tier? App tier? DB tier?
- What are the communication patterns of my workloads? How do I make sense of the relationships?

Reporting of critical applications

- What communications are legitimate, unexpected, or in violation of policy?
- Are critical applications protected according to best practices or policies?

Creating intent-based policies

- How do I develop safe, accurate policies inline with my security objectives across environments?
- How do I create segmentation policies for applications I don't understand?

Evaluate policies

- How do I quantify the efficacy of my segmentation policies?

Ensure accuracy of policies

- How do I ensure my security intentions and business objectives are translated accurately into policies?