

Faster, More Secure Cloud Migrations with vArmour

Background

Increasingly, many enterprises are now migrating their applications to cloud environments—public, private, or hybrid. Their reasons include the desire to reduce the costs associated with operating private data centers; and/or use innovative cloud native services focusing application development teams on delivering new business value faster. With fewer privately hosted applications, enterprises will spend fewer resources on supporting the underlying infrastructure and more on running the business.

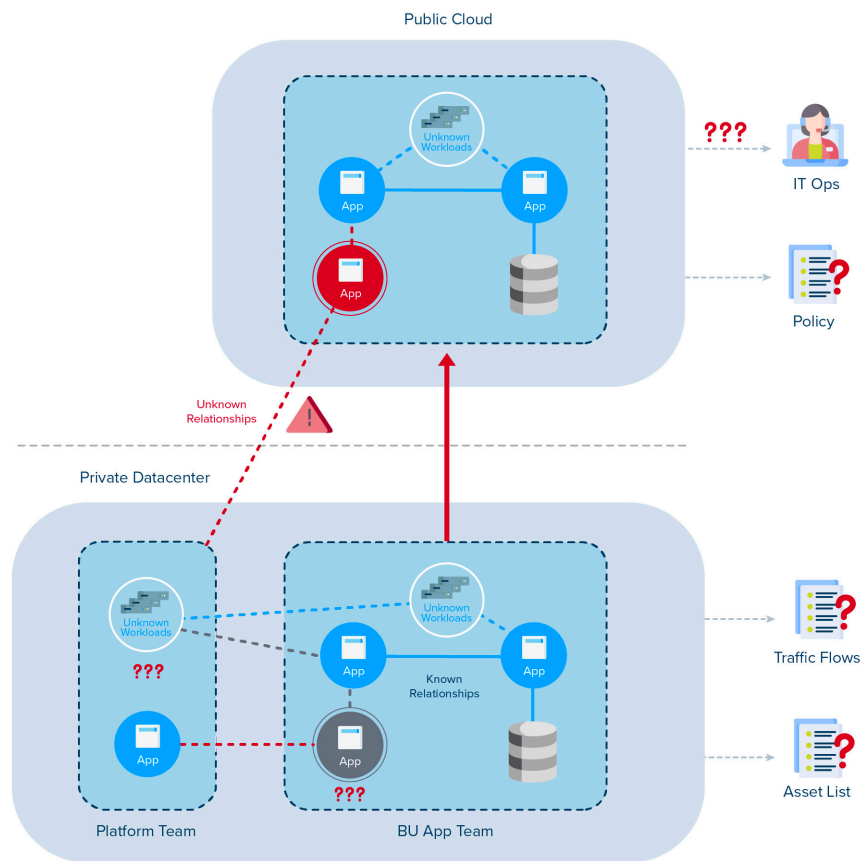
Challenges with Existing Cloud Migrations

Despite high priority strategic mandates or contractual cloud spend commitments, many enterprises still face significant challenges with cloud migration. Many report that the process has moved slower than anticipated; rather than migrating hundreds of applications or more, they can only move a handful at a time. While refactoring or rewriting applications for the public cloud is both complex and expensive, other factors are contributing to this challenge.

Organizations must ensure that applications do not suffer service outages or break other applications during cloud migrations, often due to unknown or undocumented dependencies. Degraded application availability can have significant detrimental consequences for the business including lost services revenue, lower customer satisfaction, and service level agreement (SLA) penalties. But absent a clear understanding of dynamic application relationships, cloud operations teams can struggle to identify and mitigate potential migration issues before they occur. This challenge is exacerbated with the adoption of modern microservices application architectures that rely heavily on interconnected functions that communicate constantly. In addition, once the migration is complete, hidden vulnerabilities can emerge and become more easily exploited due to inconsistent application security policies between private data centers and newer cloud environments.

Instead, organizations can invest in methodologies and techniques to prevent these kinds of issues. Ensuring no service outages or security breaches during or after a cloud migration can be costly and time-consuming because cloud teams typically must rely on manual processes to provide dependency mapping for the affected applications. Due diligence easily can soar into the millions of dollars per year. Even then, organizations still grapple with incomplete or inaccurate data that impact services or worse, result in regulatory compliance issues. In many cases, dependencies are unknown because the applications were originally deployed years ago and internal subject matter expertise has been lost over time. What is clear is that the current methodology and processes that many organizations use today is unsustainable.

Figure 1. Enterprises struggle with costly delays in application migrations to public clouds without visibility.

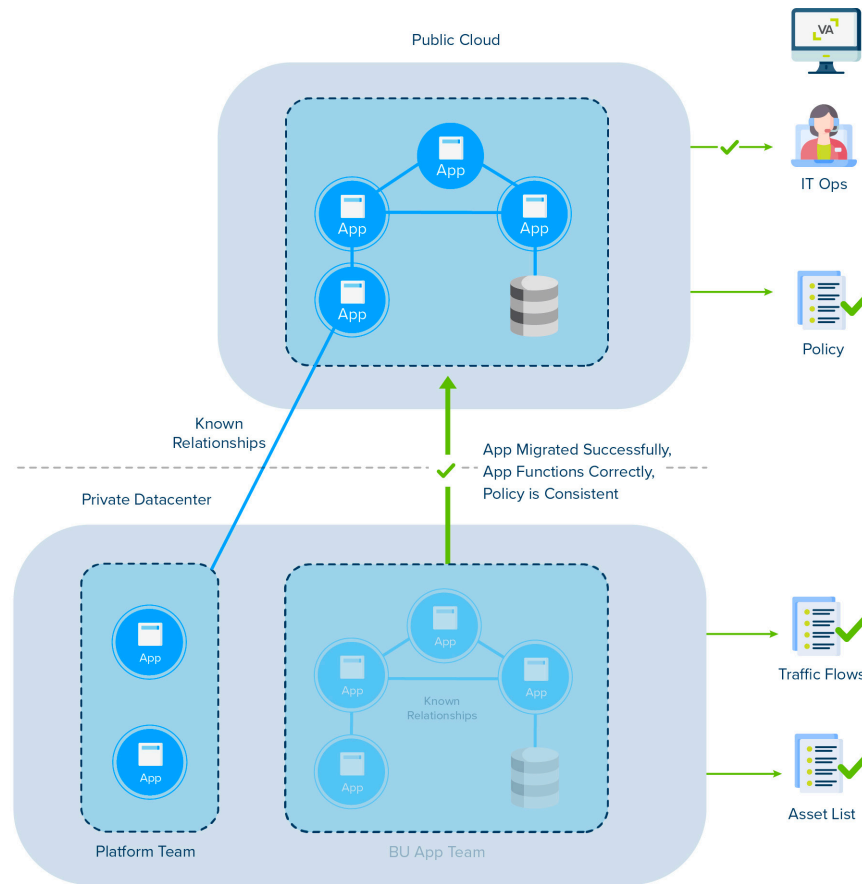


vArmour Accelerates Cloud Migrations

vArmour solutions simplify and accelerate application migration to the public cloud by *enabling (and automating) the visibility and understanding of application relationships and dependencies* across all enterprise environments. With this information, organizations can more effectively plan their migrations to ensure that application behavior—and the existing dependencies—are accounted for in new cloud deployments. This helps enterprises to avoid the typical problems of service outages and security vulnerabilities that they currently experience.

With vArmour's application relationship and dependency mapping solution, enterprises can discover unknown applications and assets that connect to and support the applications being migrated. vArmour generates an intuitive and easy to use visualization of the application infrastructure, so organizations can look at an end-to-end high-level view of all applications, as well as drill down into specific applications for granular detail. Enterprises can also baseline and visualize application traffic patterns over time to understand behavior better and thus ensure these patterns can be replicated in a consistent manner in the cloud. Operations teams can manipulate the application dependency maps with customizable filters to get the information they need faster, leveraging a unique Relationship Search function using intuitive natural language searches to pinpoint and reduce issues and uncertainties.

Figure 2. With vArmour, enterprises accelerate migrations and ensure consistent multi-cloud security.



Relationships Matter

Understanding application relationships enables enterprises to not only achieve higher application availability but also more effective and consistent application security. With vArmour, organizations are able to create security policies based on behavior across the enterprise and orchestrate these policies automatically into private cloud and cloud native environments for enforcement. In addition, organizations can model and simulate the impact of new security policies prior to deployment in cloud environments, reducing the likelihood of service outages or compromised applications. Enforcing *consistent security policies* across multi-cloud environments enables enterprises to simplify their security operations and minimize gaps, vulnerabilities, and breaches.

Most comparable solutions require the deployment of new agents for every workload to gain the visibility that enterprises need for cloud migrations. This prerequisite introduces significant challenges because organizations must first plan for and deploy these agents, which takes time, consumes resources, and disrupts services. Once applications are in the public cloud, agents can also lose track of dynamic workloads and result in policy conflicts. *vArmour never requires new agents or appliances.* Organizations can have confidence in their ability to achieve full visibility across environments, migrate faster, and fully support any applications hosted in the cloud.

Enterprises can eliminate the manual auditing of application dependencies, improve the accuracy of their application and asset inventory, and generate reports easily for application teams. With vArmour, you achieve faster application migrations to the cloud, lower the risk of service outages, and ensure a stronger security posture across all cloud environments. Compliance across multi-cloud can be achieved and proven much easier as well.

Why It Matters

Leadership teams care about modernizing their applications as fast as possible to become more agile, deliver greater value to customers, and create competitive advantage. Cloud operations teams need a better understanding of relationships among applications and system components to help prioritize migrations and reduce the risks of project delivery failure or service disruptions. And security teams need to understand application dependencies that may expose new vulnerabilities in cloud environments that can be exploited to move laterally back to private data centers.

See What You've Been Missing

Enterprises have struggled with cloud migrations for their applications due in part to a lack of understanding of application dependencies. Existing manual processes are too slow and inefficient for today's business environment. vArmour can automate this process and improve accuracy so cloud migrations are smoother and result in fewer service outages. Modern applications today are dynamic, interconnected and interdependent. Operating and securing them must be just as modern—a new requirement in today's environment and that of tomorrow.

[Find out more about vArmour](#)