

Fast, Simple, Secure Cloud Migration with vArmour

Background

To improve business agility, many enterprises are migrating their applications to the cloud to take advantage of what cloud deployments can offer. These include reducing the capital expense associated with private data centers; and leveraging a cloud-native and DevOps approach. By shifting CapEx to OpEx, resources can be freed up for more urgent business needs. And when applications can be developed, maintained and managed on the cloud quickly and securely, enterprises can create a better customer experience.

Challenges with existing cloud migrations

Yet, despite the promise of these benefits, many enterprises face significant challenges when they embark on their cloud migration journey. The challenges, detailed in a recent study by McKinsey & Company, can result in costly consequences for the enterprise.¹ Delays can lead to unanticipated service outages, which can lead to dissatisfied customers, lower employee productivity, lower revenue, increased risk of security breaches, and penalties incurred due to service level agreements (SLAs).

And they are becoming more costly. According to Uptime Institute's Global Data Center Survey 2021, the percentage of companies that have experienced outages that cost \$100,000 or more has increased by 24% from 2019 to 2021.²

Achieving fast, simple and secure cloud migration

For successful cloud migration, organizations must ensure that applications do not suffer service outages due to unknown or undocumented dependencies or security gaps. This challenge is exacerbated with the adoption of modern microservices architectures that rely heavily on interconnected functions that communicate constantly. In addition, hidden vulnerabilities can emerge post-migration due to inconsistent application security policies between data centers and cloud environments.

But absent a clear visibility of the relationships of all the applications, enterprises can struggle to identify and mitigate potential issues before the migration.

Today enterprises typically rely on manual processes to provide dependency mapping for the relevant applications, which can cost millions of dollars per year and return incomplete or inaccurate data. What is clear is that the current solutions do not work.

¹ "Cloud-migration opportunity: Business value grows, but missteps abound", 2021, McKinsey & Company

² "2021 Data Center Industry Survey Results", 2021, Uptime Institute

vArmour: The foundation to successful cloud migration

vArmour simplifies and accelerates application migration to the cloud securely by automatically mapping the relationships and dependencies between applications and workloads across all enterprise environments. With these insights, organizations can be sure the application behavior—including the security policies—are accounted for in new cloud deployments to avoid service outages, security gaps and cost overruns.

Speed & accuracy with automatic mapping, no new agents

vArmour's automatic mapping capabilities quickly improves the accuracy of application relationship visibility. The solution generates an intuitive and easy-to-use visualization, providing an end-to-end overview of all applications including unknown dependencies and assets that need to be migrated together. Customizable filters get the application information quickly via a unique Relationship Search function using intuitive natural language searches.

vArmour is easy and fast to deploy with no new agents or changes to existing IT architecture required. Most comparable solutions require the deployment of new agents for every workload to be mapped, which takes time and resources to plan for and deploy. Once applications are in the public cloud, agents can also lose track of migrated workloads, resulting in visibility gaps.

Reduced security risk with policy creation and enforcement

With vArmour, enterprise security teams can automatically create security policies based on application behavior across IT environments and orchestrate these policies into the cloud for enforcement post-migration. They can model and simulate the impact of new security policies prior to cloud deployment, reducing the likelihood of service outages or compromised applications. Enforcing consistent security policies across multi-clouds enables enterprises to strengthen their security operations and minimize gaps, vulnerabilities, and breaches.

Improved application resiliency with dynamic visualization

vArmour baselines and visualizes enterprise application traffic patterns over time to ensure these patterns are replicated consistently in the cloud. It provides dynamic and continuous view of the dependencies, and compares to pre-migration metrics to ensure applications are working as they should after migrating to the cloud.

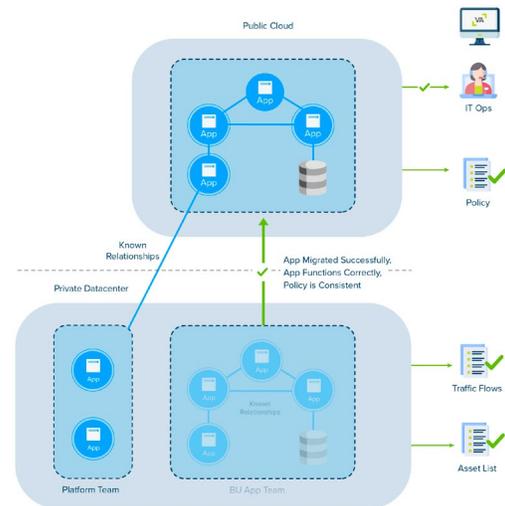


Figure 1.

Application visibility with vArmour ensures simple, secure cloud migration.

See What You've Been Missing

With vArmour, enterprises achieve faster application migrations to the cloud. Operations teams can prioritize migrations and reduce the risks of migration failure or service disruptions. Security teams can strengthen security posture by understanding application dependencies that may expose new vulnerabilities in cloud environments that can be exploited. Regulatory compliance for a hybrid environment can be achieved and proven easily.

Modern applications today are dynamic, interconnected and interdependent. The solution to operate and secure them must be just as modern—a new requirement in present and future IT environments.

To learn more about how vArmour can expedite and secure your cloud migration journey, please visit varmour.com.

Find out more about vArmour