Business Challenge: Securing Apps in a Diverse and Dynamic Environment

The combination of digital transformation and remote working mean enterprise apps need to be accessible anywhere and at any time for many different users. As they turn to public and private clouds to meet this demand, businesses are opening up major new attack surfaces. Many of an organization's apps (and the devices accessing them) are now located in a variety of tech stacks outside the enterprise's secure perimeter. With multiple environments, enterprises cannot easily maintain consistent and continuously update security policies at scale as systems are too siloed.

At the same time, monolithic apps are giving way to cloud-native apps, composed of microservices, which are continually exchanging data with each other. This complex architecture poses new security risks, particularly if app relationships and dependencies are unknown, and therefore, not inspected or protected. If multiple tech enclaves have different policies reflecting different business objectives and dynamics, poor segmentation can have a catastrophic impact. Moreover, many IT functions lack the tools

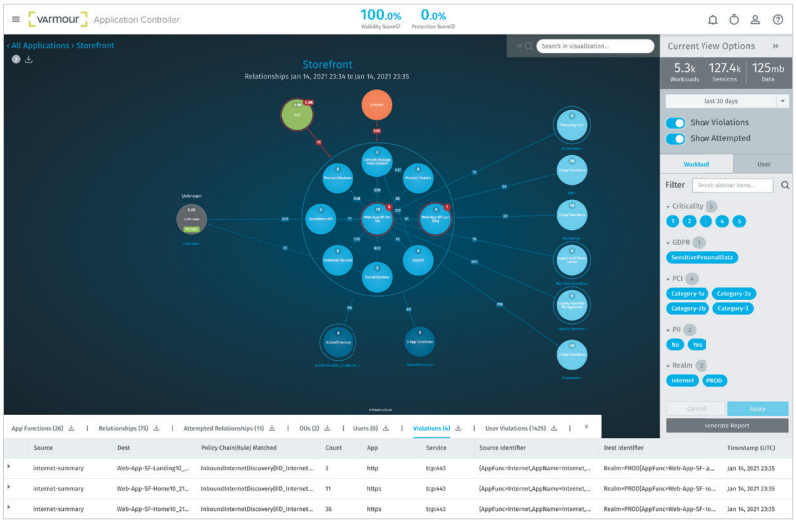

Figure 1. Visualize, create and deploy more effective and dynamic policies to control your most important apps faster.

Why vArmour?

Fast time-to-value and scalable

Unlike other segmentation platforms, vArmour's solution doesn't need new agents or appliances to collect telemetry data from applications or workloads. That makes it easy to deploy and scale quickly without disruption.

Complements existing platforms

The breadth of discovery and enforcement provided by vArmour's solution is unique, enabling organizations to build on their existing investments in technology platforms, such as Microsoft Azure, AWS, Tanium, VMware NSX, and other platforms.

Looking beyond location

Compared with network security vendors that use IP addresses or other transient network elements, vArmour provides far more granular segmentation of apps and workloads. It uses highly relevant, customizable, and distinct labels to enable very precise isolation policies.

Developer friendly

As well as creating and enforcing policies for existing apps, vArmour's solution can be employed by DevSecOps to build, model and deploy policies for new apps using CI/CD toolsets.

Product and Module

Application Controller
Application Policy & Protection Module

required to process large volumes of inbound telemetry data and enforce policies on distributed workloads or nodes. Against this backdrop, cyber attacks are becoming increasingly sophisticated, numerous, and large-scale, proliferating inside enterprise infrastructure.

As these dynamics make the concept of a security perimeter obsolete, many IT organizations are looking to adopt a Zero Trust approach – only connections that have been explicitly authorized can interact with enterprise apps. Rather than using location or an IP address to manage access to apps, a Zero Trust security policy focuses on "the who, the what and the why". Drawing on a granular and comprehensive view of inter-app and intra-app dependencies and relationships, orchestrated segmentation is an effective means to implement a Zero Trust policy, while ensuring apps aren't inadvertently broken.

vArmour's Orchestrated Segmentation Solution

As more agents and platforms are equipped with APIs, organizations have a greater choice of where and how to segment their apps. Employing an independent horizontal product to enable orchestrated segmentation across a heterogeneous environment has several advantages over other approaches, such as agent-, network-, hypervisor- or cloud-based segmentation. Rather than requiring the deployment of more technology, it leverages existing infrastructure investments, together with plug-in APIs, to deliver value quickly.

To successfully implement orchestrated segmentation and support a Zero Trust security policy, an organization needs near real-time visibility and control of app interactions across its enterprise IT estate. The vArmour Application Controller's modules can continually monitor and control app-to-app relationships across clouds and technology platforms, both within and between enclaves. To segment or isolate apps and workloads, the solution can automatically baseline actual behavior and then compute app access policies. It can also orchestrate and enforce policies with existing data platform systems, flagging anomalies that could represent security and compliance risks.

By enabling fine-grained isolation between apps, vArmour's solution greatly reduces the threats posed by malicious lateral network traffic and larger attack surfaces, bolstering the end-to-end security posture of Zero Trust implementations. Through machine learning, it can also automatically develop access policies for apps and simulate the impact of these policies before deployment. As a result, enterprise-wide rules can be generated in days, rather than months or longer. The solution can then be used to enforce these policies, while alerting the IT function to any variances and violations.

Key use cases

Protecting critical applications

Every enterprise has one or more applications that are critical to the business and will have exponential harm if compromised. Yet many organizations do not have effective security in place to protect these applications, failing to define specific access policies based on a full understanding of application relationships. The complexity of heterogeneous IT environments and toolsets makes effective auditing and monitoring of app communications access very difficult. As a result, many organizations are unaware of how actual events differ from their defined policies and where inappropriate access and lateral movements may drive significant risk.

vArmour's solution can quickly isolate and protect an organization's critical applications based on the actual behavior of the targeted apps, components, and app relationships, creating comprehensive and custom security policies in a few clicks, deploying into any environment the app is hosted, and then continuously monitoring to visualize and alert on real time data based on actual and attempted access or deviations from isolation policy. vArmour also enables organizations to easily respond to compliance requirements for attestation by generating custom reports for the critical applications.

Consistent app segmentation across the entire enterprise

Traditional network segmentation of apps simply won't work in today's hybrid cloud environments. Anchored in data centers, it is too manual and inflexible to enable Zero Trust security policies: agents required for heterogeneous workloads take too long to deploy, leave gaps that result in imprecise policies that don't work, and don't provide the scale that most organizations need for enterprise-wide.

This is a particular challenge in a multi-cloud environment with multiple independent "domain managers."

By contrast, vArmour's orchestrated segmentation solution can deliver the precision organizations need at scale. Drawing on its app-centric view of identity access, regardless of app type or hosting environment, vArmour can create and implement security policies that isolate and segment apps based on multiple trust attributes. By supporting identity-oriented segmentation across a hybrid–cloud environment, it enables an organization to implement effective and granular security and compliance enterprise-wide, in an infrastructure-independent manner. With real-time alerts and reports on any deviations from policy, the organization benefits from a far stronger security posture and less risk of malicious access.

Policy automation for DevSecOps (Policy-as-Code)

In many organizations, security policy and software development run in parallel and fail to keep pace with each other. With DevOps teams continuously deploying new and changed apps, security policies can quickly become outdated or are inconsistently applied, leading to vulnerabilities.

Designed for enterprise-wide policy management and to be integrated with existing CI/CD toolchains and workflows, vArmour can automatically create and deploy policies for both new and existing workloads. DevOps teams can visualize relationships between unobserved nodes, model and build policies for pre-staged nodes, and prior to deployment apply those policies automatically using CI/CD toolsets and workflows. By employing APIs, the solution can quickly ensure security policies continue to be effective for new apps being deployed rapidly by DevOps teams.

 | 650.564.5100 | info@varmour.com | 270 3rd Street, Los Altos, CA 94022