vArmour Distributed Security System: Protecting Assets in the World without Perimeters

Re-thinking Security in the Digital World

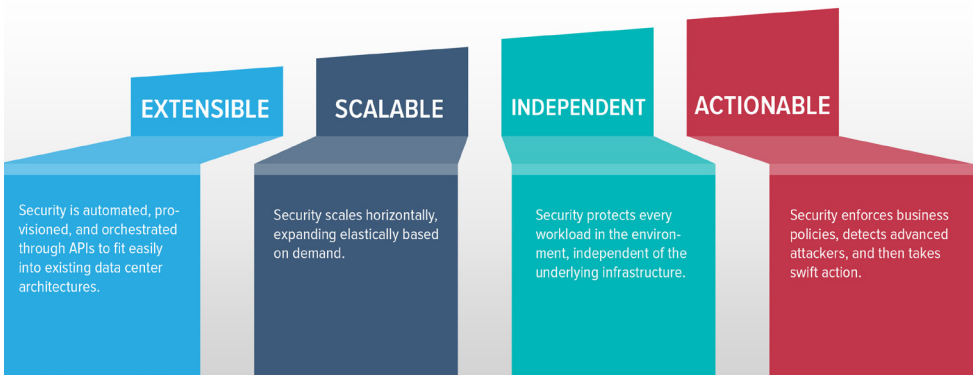
Digital transformation is powering companies to re-think, re-design and re-invent their business. New technology advancements in analytics, big data, mobility, social and cloud computing are radically changing the way businesses interact, operate and compete. For organizations to grow, they must transform their business and its underlying technology infrastructure to move faster, innovate, and stay connected with their customers, suppliers and partners – all while maintaining the necessary security standards.

At the center of this change is the new data center; transforming to be highly distributed and software-defined, and scaling at the speed of the business – to be more agile and efficient. In this dynamic world, can your organization fully secure new processes, applications, and infrastructure? Can your organization harness the advantages of cloud infrastructures faster without the risk?

Unfortunately, relying on traditional security won't get you there. The traditional, well-defined perimeter is long gone. Assets and data are scattered everywhere, both inside and outside the enterprise with over 50 percent* of workloads now virtual, and assets are highly mobile. And with 83 percent* of traffic now traveling "east to west" within the data center, the value of perimeter-based approaches continues to shrink. It's not enough to build a better and better perimeter – security must be done differently in the new world.

A New Approach to Data Center Security

In a world without perimeters, security has to fundamentally change. Security has to be built from the ground-up with key principles for the new data center: extensible, scalable, independent and actionable.



Key Principles for Distributed Security

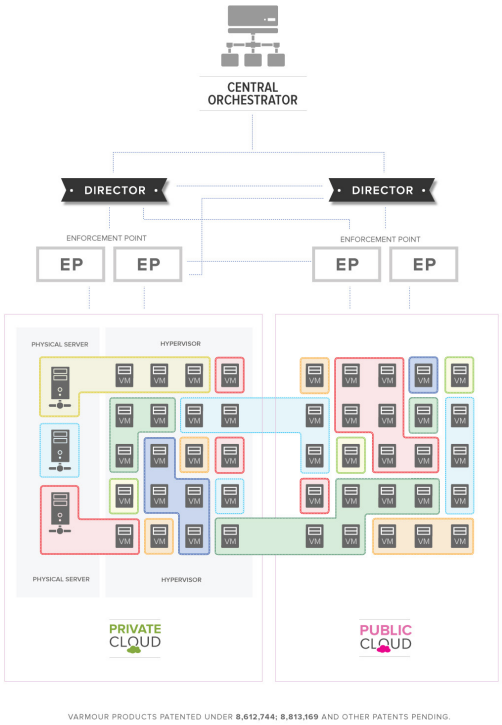
*Source: Gartner

vArmour Distributed Security System: Protecting Assets in the World without Perimeters

vArmour Distributed Security System

With its Founders' heritage in network security, vArmour designed the first distributed security system that transforms how organizations protect their virtualized and cloud assets in a world without perimeters. The vArmour Distributed Security System is a single logical system composed of multiple autonomous, distributed sensors and enforcement points that are connected by an intelligent fabric.

By placing the controls directly next to the assets being protected, vArmour allows organizations to micro-segment each workload, even from other workloads on the same hypervisor. Micro-segmentation enables organizations to securely hyper-consolidate their infrastructure, by separating the infrastructure topology from the security topology, allowing workloads at different security levels to share common infrastructure. This approach not only significantly improves infrastructure utilization, but also dramatically reduces potential attack surfaces for greater security.



vArmour micro-segments workloads to share capacity while maintaining security controls.

vArmour Case Study: Fortune 100 Company

Situation

- Fortune 100 Company
- Three global data centers

Key Challenges

- Lack of visibility into east/west traffic
- PCI DSS 3.0 compliance
- No response capability against lateral spread

Results

- Saw value within two hours: unknown threats and compliance violations
- Within 24 hours saw 157 points of unique behavior
- Enterprise-wide roll-out to enable detection and response per-host
- Enable PCI 3.0 compliance

"vArmour was enabled in our production environment and within two hours identified some interesting behavior. So interesting, we're meeting with executives from the company to discuss expanding the scope of our efforts since we've found incredible value with the product within the first 24 hours of deployment."

—VICE PRESIDENT, INFRASTRUCTURE
FORTUNE 100 COMPANY

To schedule a demo, download technical white papers, or learn more about vArmour, visit www.vArmour.com.