SOLUTION BRIEF

Communications Service Providers
Network Security

vArmour* Boosts Network Security with Microsegmentation

vArmour has developed vArmour DSS Distributed Security System to help protect enterprise data and applications with microsegmentation whether in the data center or in the cloud.

Introduction

The pace and scale of security threats are increasingly potent, which, when combined with users' pervasive reliance on being connected, means security breaches have an escalating impact. Compounding this threat is the fact that protecting a security perimeter is increasingly harder thanks to cloud computing and other changes in how networks are built and used. These security gaps can be easily exploited by hackers who have few restrictions for lateral movement once they've found a way past the firewall.

vArmour's* security product offerings, based on its application-centric architecture and featuring policy planning and microsegmentation, are designed to utilize the advanced features and performance of servers powered by Intel® Xeon® Scalable processors and Intel Xeon processors E5. This hardware-software combination delivers application visibility and dependency mapping and ongoing application and data security features needed to help protect today's distributed and multi-faceted data centers.

The Challenge

Many enterprises utilize firewalls to build a security perimeter at the borders of their networks. While this is still a sound strategy, the security-enabled perimeter approach has limitations with today's complex and varied network makeups. This model is challenged by the extension of networks into distributed computing models and by corporate computing assets being hosted on cloud services. Both of these require extending the firewall to these non-enterprise locations. In addition, the emergence of the Internet of Things (IoT) will see enterprise networks add potentially thousands of wirelessly connected sensors on both sides of the firewall, adding new challenges to the security-enabled perimeter.

The classic defense of a firewall, a gatekeeper that determines who gets in and who gets out, does not effectively protect a network's assets in a distributed environment. Furthermore, once the firewall is breached, the attacker has unfettered access to wreak havoc with everything within the perimeter. And fragmented security solutions to manage policies across heterogeneous systems create inefficiencies and security gaps.

vArmour's alternative is an approach that helps protect each asset within the network by microsegmenting workloads to build a firewall around every application. Instead of looking for unknown bad, vArmour locks down each workload with known good and rejects all other communications.

The Solution

vArmour augments the security-enabled perimeter by moving the same security controls that were traditionally at the perimeter next to each asset. The vArmour DSS Distributed Security System is a software-based system that provides protection features for legacy physical systems, virtual machines (VMs), and cloud-based systems in a cohesive system that helps detect and protect against attacks.

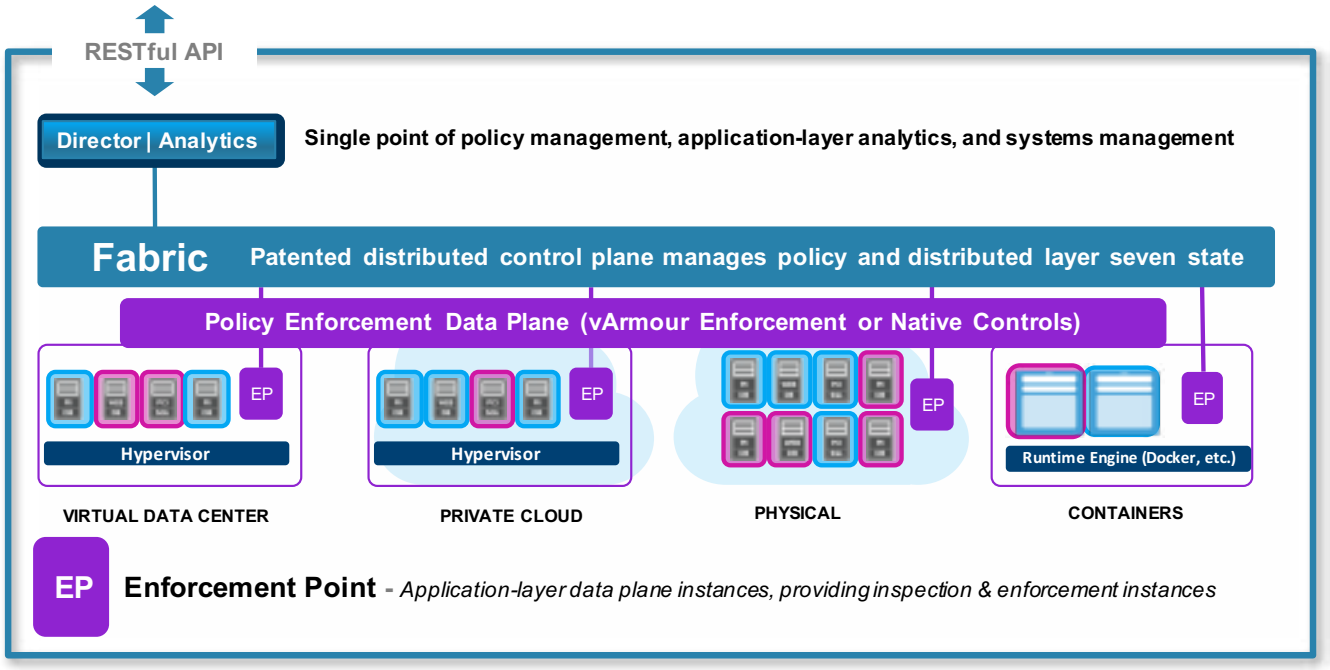

Figure 1. vArmour system architecture[1]

As shown in Figure 1, the vArmour Fabric comprises a network of distributed sensors called enforcement points (EPs) that act like a cohesive, logical entity and provide enforcement of security policies close to the compute asset. This sensor fabric watches the communications of every application and asset, including east-west communications between hypervisors and other instances, and north-south traffic to the network.

vArmour's Policy Planning offering (Policy Architect) auto-discovers and auto-labels workloads with full application and flow knowledge. This enables customers to visualize all their applications, interdependencies, and communications between app components. This greatly enhances an organization's ability to devise appropriate policies, taking into account the desired security posture, regulatory requirements, and threat intelligence, to name a few enterprise concerns. These application-aware network-agnostic policies are intent driven (no IP addresses and port numbers) and can be enforced by the vArmour fabric using EPs available for virtual machines, containers as well as physical servers, wherever they reside, on premises or cloud.

To add protection to physical servers, vArmour has packaged its enforcement point as an ISO image that can be run on servers based on Intel® architecture and become part of the fabric. vArmour uses and recommends servers powered by Intel Xeon Scalable processors and Intel Xeon processors E5 and utilizes technologies like the Data Plane Development Kit (DPDK) to provide the throughput needed for application layer visibility via deep packet inspection and application metadata at data center network speeds.

Using the vArmour Fabric, data center security teams can see a top-down view of the network by auto-discovering how applications are being used, by whom, how they interact, and their dependencies. Full deep packet inspection (DPI) of network traffic gives visibility into application context and interactions. With integration into user directories and metadata repositories, data center security teams can visualize relationships of users and applications for inter-hypervisor and workload-to-workload traffic.

Reduces the Attack Surface

vArmour DSS reduces the number of entry points to critical assets and the attack surfaces by restricting communication between authorized systems with application and stateful controls that limit the opportunity for lateral data spread. Each asset has dynamic and independent protection features, either in the premises or in the cloud, whether physical or virtual. Whether it is customer data, workloads, intellectual property, shared services, active directories, or external system connections, each asset can have a colocated security sensor tracking data flows for security problems, regardless of where it resides.

Dynamic Policies for Protection

vArmour DSS helps protect applications and data assets by dynamically setting policies that determine how applications are used, who is using them, dependencies, and how they interact. Understanding application dependencies improves

situational awareness and the overall understanding of application behaviors to improve security policies and better defend networks against attackers. vArmour DSS accelerates policy creation with intuitive visualizations and intent-based policy templates to streamline policy creation and maintenance processes. Out-of-band validation of candidate policies using observed network communications ensures smooth policy deployments.

Holistic Network EP Distribution for Additional Protection: Physical, Virtual and Cloud

Figure 2 shows the how the three elements of vArmour DSS comprise a single distributed security fabric that stretches across the entire network of physical, virtual, and cloud-based systems. Application-based segmented protection features and consistent policy enforcement deliver modern-day security techniques to legacy physical systems along with virtual and cloud-based systems.

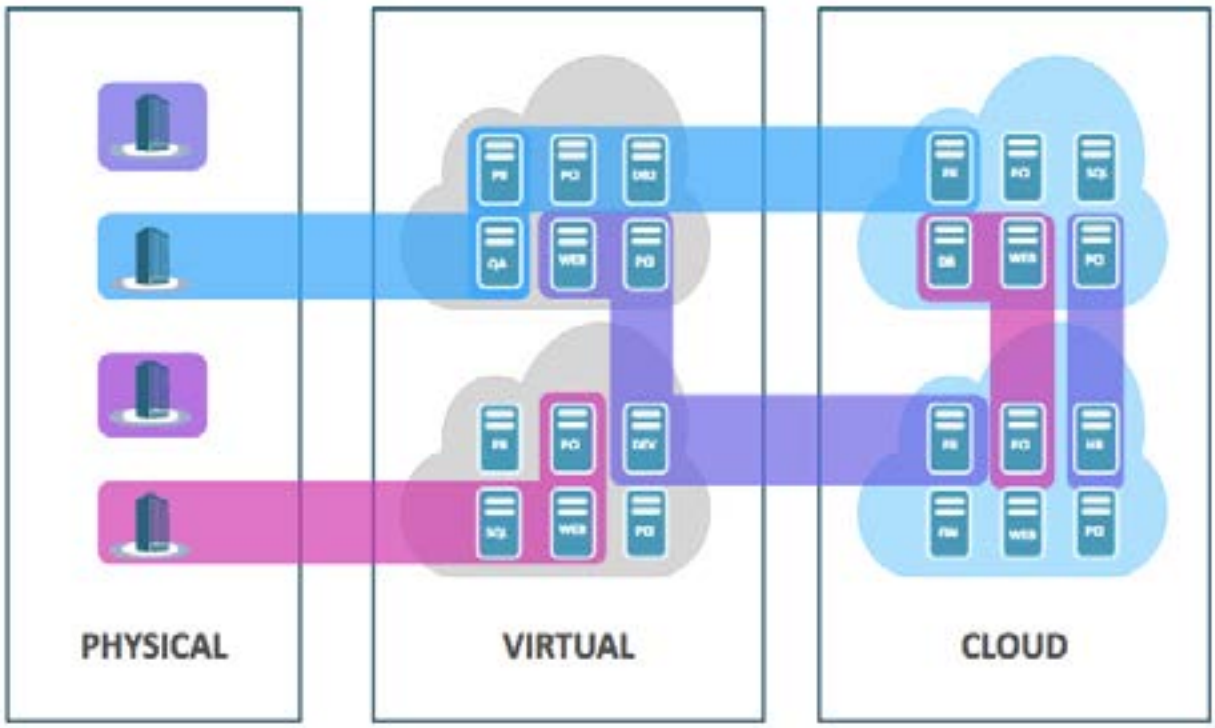

Figure 2. The vArmour system can span physical, virtual, and cloud networks.

Intel and vArmour

vArmour specifies its software to be instantiated on Intel Xeon processor-based servers with DPDK implemented to handle the intense processing requirements of DPI that makes microsegmentation so effective. Other critical processor technologies include Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) for accelerated encryption processing and open source Hyperscan multiple regex matching library to boost DPI performance.

The Intel Xeon processor Scalable family is the successor to the Intel Xeon processor E5 and E7 product lines and has been developed with high scalability for virtualized workloads. The Intel Xeon processor Scalable family features new technology for compute, network, and storage workloads.

Network performance is important for the solution as it must support 40 GbE data flows. Intel networking technologies that are used in the vArmour DSS include the Intel® Ethernet Converged Network Adapter XL710.

Conclusion

For complex, heterogeneous distributed networks of today, modern security systems are needed to help protect an increasingly porous security perimeter. vArmour, running on servers powered by Intel Xeon processors, does this by creating perimeters for each of the digital assets—applications, virtual network functions, and more—where they are located in the network. Thus, additional protection is comprehensive regardless of whether that application is in the data center, the remote office, or the cloud.

About vArmour

vArmour, the data center and cloud security company, delivers agentless integrated security services to auto-discover application communications, optimize policy modeling, and protect critical applications and workloads across multi-clouds. Based in Mountain View, CA, the company was founded in 2011 and is backed by top investors including Highland Capital Partners, Menlo Ventures, Columbus Nova Technology Partners, Work-Bench Ventures, Allegis Capital, Redline Capital, and Telstra.* The vArmour

DSS Distributed Security System is deployed across the world's largest banks, telecom service providers, government agencies, healthcare providers, and retailers. Partnering with companies including AWS, Cisco, HPE, and VMware,* vArmour builds security into modern infrastructures with a simple and scalable approach that drives unparalleled agility and operational efficiency.

About Intel® Network Builders

Intel® Network Builders is an ecosystem of independent software vendors (ISVs), operating system vendors (OSVs), original equipment manufacturers (OEMs), telecom equipment manufacturers (TEMs), system integrators (SIs), enterprises, and service providers coming together to accelerate the adoption of network functions virtualization (NFV)-based and software-defined networking (SDN)-based solutions in telecom networks and in public, private, and hybrid clouds. The Intel Network Builders program connects service providers and enterprises with the infrastructure, software, and technology vendors that are driving new solutions to the market. Learn more at http://networkbuilders.intel.com.

[1] Figures courtesy of vArmour.

0118/DO/H09/PDF ♻Please Recycle 336978-001US