DATA SHEET

vARMOUR DSS DISTRIBUTED SECURITY SYSTEM

<V/A> vARMOUR

DEEP INSIGHT AND CONTROL FOR MULTI-CLOUDS

Security Implications in Multi-Clouds

Organizations around the globe are being transformed by software and digital systems, radically changing the way businesses interact, operate and compete in the market. These changes are affecting all areas of IT, especially the data center. Critical data is more accessible to all than ever before with the advent of virtualization, cloud and the emergence of multi-clouds—a mix of many best-of-breed public and private cloud services. With the adoption of multi-clouds, increases in consumer devices, and greater collaboration between business partners, the traditional perimeter has become porous, making the notion of a well-defined perimeter gone and the traditional security controls that were designed to protect it, simply out of date. Organizations lack visibility of their users, applications, and traffic within and across clouds that cannot be monitored with their existing tools; they lack fine-grained and pervasive security controls that dynamically travel with the workload with simplicity; and they lack the ability to quickly and easily provision security to new workloads and applications without slowing down the business.

The vArmour Solution

vArmour addresses these data center security challenges by delivering the industry's first distributed security system that provides application-aware micro-segmentation with advanced security analytics. Built in software, vArmour DSS Distributed Security System is architected to scale security across multi-clouds with deep insight and control of individual workloads. With its patented application-aware micro-segmentation capabilities, vArmour DSS moves security controls that were traditionally at the perimeter down next to each asset, wrapping fine-grained protection around every workload, regardless of where it resides. Workload-level visibility and control of inbound, outbound, and lateral traffic patterns from vArmour DSS helps organizations detect and prevent application misuse, policy violations, and advanced persistent threats across complex multi-cloud environments from a single system.

vARMOUR DSS IN ACTION

Network Visibility

Gain fine-grained Layer 7 visibility of all workload communications, even within the same hypervisor, that traditional perimeter security solutions cannot see.

APT Prevention

Continuously monitor all data center traffic patterns to identify suspicious or anomalous behaviors as well as the capability to divide the extensive data center environment into smaller, more protected zones or segments to reduce attack surfaces—all from one single system.

Broad Security Across Multi-Clouds

Secure workloads across multi-clouds (both private and public) by enabling organizations to extend and apply their own consistent, global policies and auditing across cloud vendors.

Environmental Separation

Segment workload and application communications based on environmental conditions even on the same shared infrastructure—whether isolating assets based on production versus non-production or by application tiers (web, application, database).

Compliance Assurance

Segregate regulated and non-regulated data on the same shared infrastructure to adhere to compliance mandates in any industry.

Rapid Breach Detection and Forensic Investigations

Garner context-aware security intelligence to detect anomalous or malicious activity by quickly determining what machines, systems, and resources are involved in an attack, reducing forensic investigation time from days to minutes, and then systematically quarantining those workloads.

AT A GLANCE

Visualize and analyze your network, application, and user traffic across clouds.

Find high-risk applications and suspicious behaviors that you didn't know were there and shouldn't be.

Secure your cloud with application-aware micro-segmentation to prevent and stop malicious threats.

Operationalize security management with global policies that auto-scale with new applications and workloads, making it easier to manage complex environments.

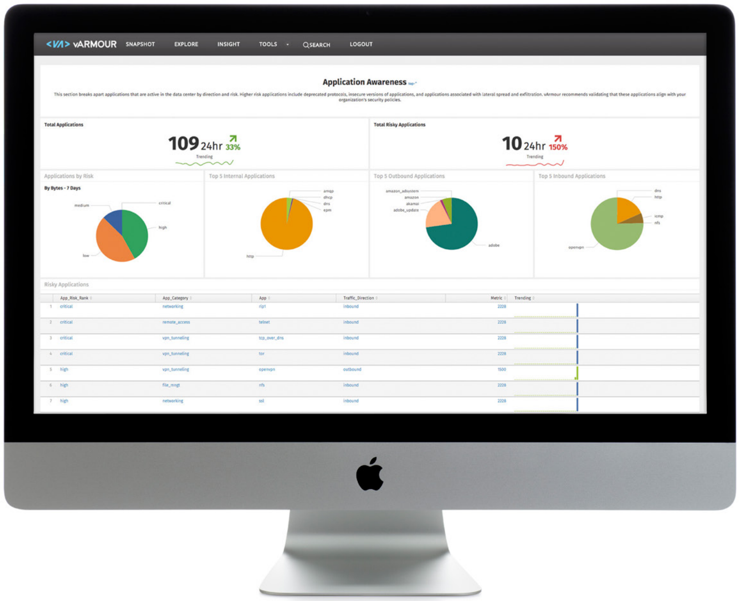
KEY FEATURES

Highly Scalable Distributed Architecture

vArmour DSS is a software-only solution, built specifically for virtualized and multi-cloud environments, that implements a single logical system comprised of multiple, autonomous sensors. These sensors are connected through the vArmour Fabric, which then shares information and context across the system, unlike agents or network overlays, which cannot. Security processing is dynamically distributed across the vArmour Fabric for greater system performance and without reliance on load balancers.

Continuous Monitoring and Unparalleled Visibility

Full deep packet inspection is conducted on all traffic, no packet sampling, up to Layer 7 with deep understanding of application context and interactions. With integration into user directories and metadata repositories, organizations can visualize relationships of users and applications for inter-hypervisor and workload-to-workload traffic across clouds.



Application Awareness

This section breaks apart applications that are active in the data center by direction and risk. Higher risk applications include deprecated protocols, insecure versions of applications, and applications associated with lateral spread and exfiltration. vArmour recommends validating that these applications align with your organization's security policies.

Risky Applications

	App_Risk_Rank	App_Category	App	Traffic_Direction	Metric	Trending
1	critical	networking	rip1	inbound	2228	
2	critical	remote_access	telnet	inbound	2228	
3	critical	vpn_tunneling	tcp_over_dns	inbound	2228	
4	critical	vpn_tunneling	tor	inbound	2228	
5	high	vpn_tunneling	openvpn	outbound	1500	
6	high	file_mngt	nfs	inbound	2228	
7	high	networking	ssl	inbound	2228	

Fine-grained Micro-segmentation Made Simple

vArmour's application-aware micro-segmentation can be deployed in three simple steps and in less than 30 minutes without requiring complex network overlays, service-chaining, or deploying of resource-intensive components. Controls are placed next to each workload and are independent of the workload itself. vArmour DSS offers the flexibility of providing both zone-based and workload-level segmentation on any underlying infrastructure, so organizations have the freedom to segment workloads in any heterogeneous cloud environment.

Precise Threat Detection and Rapid Investigation

With application-layer visibility, vArmour DSS correlates contextual information in real-time from the vArmour Fabric to better detect patterns of abuse and misuse, without dependencies on signatures. With sophisticated threat analytics, organizations can detect a compromised workload and the lateral spread of the attack—whether it's an APT, malware or an insider threat—and can easily find the entry point and full spread of the breach.

See and Stop Malicious Behaviors in One System

Visibility and detection solutions are typically not enough to swiftly stop modern attacks. vArmour DSS is an integrated system that not only provides the ability to spot threats and analyze the attack steps as part of the kill chain, but it can also stop the current threat and prevent new attacks or reinfections of compromised systems. With vArmour DSS, organizations can readily update policies based on malicious behaviors identified in the environment, which are then enforced across the vArmour Fabric.

> *"We used to have limited visibility of traffic flowing between virtual machines on the same hypervisor. With vArmour, not only can we see and inspect this traffic in real time, but we have the ability to bring policy enforcement down to every asset in our environment."*
>
> –HEAD OF IT SECURITY,
> LEADING GLOBAL INVESTMENT FIRM

Broad Infrastructure Support

Since security is decoupled and independent from the underlying infrastructure, vArmour DSS offers a software-based, extensible architecture that can auto-scale with workloads and applications everywhere and anywhere they reside—on-premises using VMware, Nutanix, or OpenStack KVM, or off-premises in Amazon Web Services. With native support for live migration using VMware vMotion and OpenStack KVM, security policy automatically travels with the workload and application without disruption.

Simplified Operations Across Clouds

Unlike traditional perimeter solutions, vArmour DSS provides a single point of policy management and control that scales within clouds and infrastructure providers, eliminating security silos while lowering the cost and complexity of security management. Additionally, security controls are automatically provisioned to new applications and workloads, removing the need to manually write new policies as new workloads are provisioned. Full featured JSON/REST APIs makes vArmour DSS integrate seamlessly with third party orchestration and automation systems.

WHY vARMOUR

Broad

Extensible architecture provides scalable security across private and public cloud infrastructures.

Deep

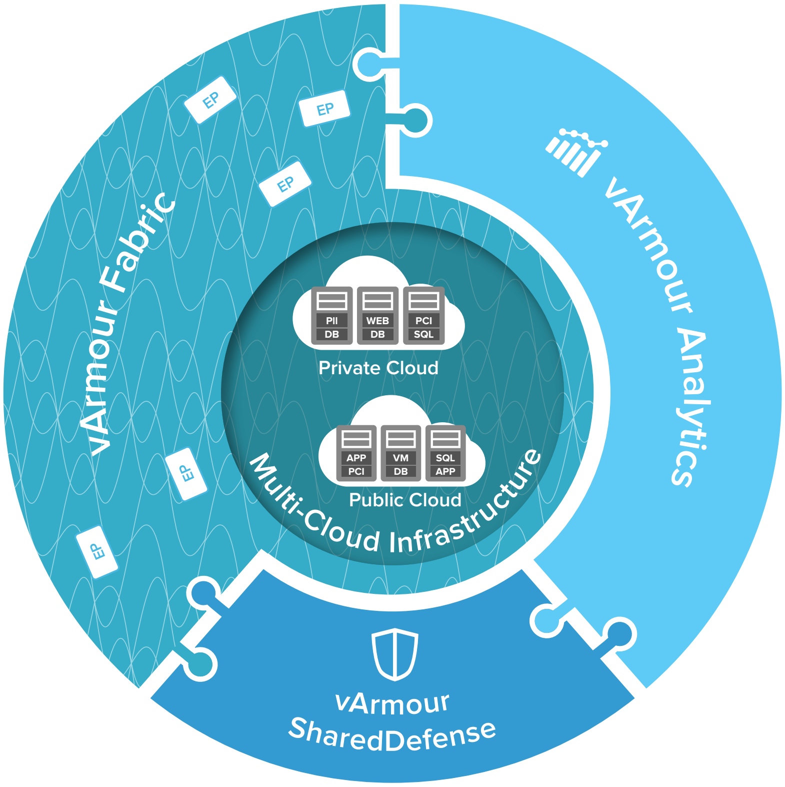
Contextual visibility into relationships of user, workload and application traffic from Layer 2 to Layer 7.

Control

Micro-segment every workload to prevent and stop unwanted behaviors with inline policy enforcement with 3 clicks in 30 minutes.

ARCHITECTURE

vArmour DSS Distributed Security System is comprised of distributed sensors that are connected by an intelligent fabric and managed as a single, logical entity—no individual agents or single-instance policies to manage. vArmour DSS consists of three primary components: vArmour Fabric, vArmour Analytics, and vArmour SharedDefense.



vARMOUR DSS DISTRIBUTED SECURITY SYSTEM

vArmour Fabric

is connected together as one logical system that deploys inline distributed sensors to perform deep packet inspection of all workload traffic, baseline normal workload communication patterns across sensors, and enforce security policies. With fine-grained protection next to each asset, vArmour isolates every workload and its communication within and between hypervisors, instances, and everything else on the network. As traffic passes through the Fabric, it provides:

- Deep packet inspection that generates detailed Layer 7 metadata that feed vArmour Analytics as well as other third party visibility tools, such as SIEM, for contextual insight into all workload communications.
- A single point of policy management that controls every intra- application interaction—no siloed tools to correlate.
- Distributed security processing that easily scales to meet application demand, minimizing the consumption of infrastructure resources.
- Inline enforcement of policies through micro-segmentation to take swift action when malicious behaviors are detected in vArmour Analytics.

vArmour Analytics

provides visualizations into all workload traffic collected by the Fabric. These traffic patterns are analyzed to detect and alert on suspicious and potential threats. Analytics provide users with insights to deploy policy changes based on unexpected application or workload behaviors. These policies are implemented and enforced throughout the multi-cloud environment via the Fabric. Analytics provides:

- Continuous monitoring across networks, applications, workloads, and users for end-to-end visibility.
- Out-of-the-box and custom trend visualizations to determine overall security posture.
- Drill-downs into specific behaviors of workloads or users for further investigation.
- Highly detailed historical views of all network traffic activity for a given period of time.
- Customizable dashboards that can be tailored to each Analytics user's preferred view from graphs to tables to correlate a wide range of data (including source and destination IPs, application/workload details, and geo trends).
- Custom alerting for rapid investigation and response to compromised workloads.

vArmour SharedDefense

is an opt-in hosted service that continually updates vArmour DSS with a global view of security events, behavioral anomalies, threat characteristics, and laterally-moving threats across customer environments. With SharedDefense, vArmour threat analysts associate intelligence from vArmour research and customers to recommend areas of risk that should be addressed. SharedDefense provides:

- Analysis and detection of current threats to keep vArmour DSS customers protected.
- Smarter insights to update policy to prevent advanced attacks.
- Federated threat detection across vArmour customers in similar regions and more.

GET STARTED WITH vARMOUR

Take the first step to greater security inside your data center with vArmour DSS-V. Request your free download of vArmour DSS-V for application-layer visibility and threat detection at www.varmour.com/dssv.

Request Free Download

TECHNICAL CERTIFICATIONS

vmware READY APPLICATION SOFTWARE

NUTANIX PARTNER NETWORK NUTANIX READY NETWORKING & SECURITY

amazon web services Partner Network TECHNOLOGY PARTNER

nuagenetworks

splunk>

ABOUT vARMOUR

Based in Mountain View, CA, vArmour is the data center security company that is the leader in application-aware micro-segmentation with advanced security analytics. The company was founded in 2011 and is backed by top investors including Highland Capital Partners, Menlo Ventures, Columbus Nova Technology Partners, Citi Ventures, Work-Bench Ventures, and Allegis Capital. The vArmour Distributed Security System is deployed in a significant number of the world's largest banks, telecom service providers, government agencies, healthcare providers, and retailers, and is leading the industry with a new patented, distributed approach to data security that allows organizations to deliver IT at the speed of business. Along with partners like Amazon and VMware, vArmour secures many of the largest data center and cloud environments in the world.