vARMOUR DSS DECEPTION DATA SHEET

vARMOUR

Traditional security solutions are based on the idea of finding the needle in the haystack - to find the attacker within vast amounts of legitimate network and data center traffic. vArmour DSS Deception, at its core, is the natural corollary to traditional security solutions. It is designed to trick attackers to move outside the realm of legitimate traffic - outside the haystack - so that they can be easily identified and remediated.

vArmour DSS Deception distracts, stalls, and identifies attackers by creating the illusion of vulnerable workloads and services across the data center. Built on top of the vArmour DSS Distributed Security System, vArmour DSS Deception creates a broad synthetic attack surface with an extremely small resource footprint.

vArmour DSS Deception provides:

- Continuous monitoring for malicious actors scanning the data center or attempting to connect to synthetic workloads or services
- A range of containerized services for high-fidelity identification of attackers
- Ability to create the appearance of a large number of workloads and services using a single Deception Point
- Orchestrated and tightly secured Deception Points leveraging the vArmour Fabric
- Integration with vArmour Analytics for rapid investigation and incident response

BENEFITS

Earlier Compromise Discovery

By creating the appearance of vulnerable endpoints and services aross the data center and cloud, vArmour DSS Deception lures attackers into giving their presence away during the initial stages of an attack - as they are mapping their environment and beginning to spread laterally toward their objective. This early warning of an attacker in the environment gives network defenders the advanced notice required to investigate, respond, and remediate the attack before the attacker's objective has been achieved and the damage to the organization done.

Increased Detection Accuracy

vArmour DSS Deception identifies attackers where no legitimate traffic should ever occur - in empty IP ranges and disallowed protocols to protected workloads. As a result, determining whether an alert is the result of legitimate or suspicious/malicious traffic is vastly simplified. Additionally, as legitimate traffic does not touch these IP ranges or protocols, and thus doesn't generate alerts, the volume of alerts presented to security teams is dramatically reduced. The small number of alerts make the job of security analysts much easier and accelerate the organization's cyber response processes.

More Relevant and Actionable Intelligence

Full Layer 7 visibility and the ability to determine the full scope of a compromise delivers intelligence on adversaries far more reliable and actionable than aggregated external intelligence typically provided by commercial or public threat feeds. Armed with a detailed understanding of how adversaries attempted to navigate and exploit the environment, security teams can revise and reinforce existing controls to defend their networks.

Supported Services	HTTP/S, SMB, RDP, MySQL, Telnet, Ping, FTP, SSH
Sample Behaviors Identified	Connection Attempts, Port Scans, Failed/Successful Authentications, Brute Force Authentications, SMB File Access, File Uploads, SSH/Telnet Commands
Connection concurrency	Up to 100 connections per service, per Deception Point
Event throughput	Up to 1000 events per second, per Deception Point

ADVANTAGES OVER TRADITIONAL APPROACHES

vArmour DSS Deception enables organizations of all sizes to reap the benefits of a proactive security posture leveraging cyber deception techniques without the significant drawbacks of typical cyber deception solutions to date.

Broad deception coverage

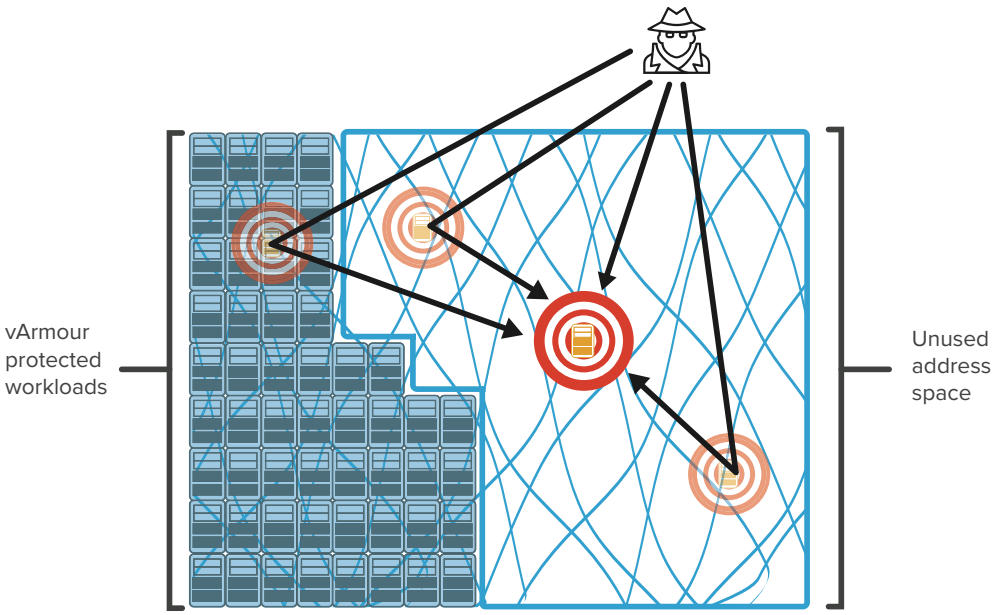
The ability to deceive an attacker is only possible if the deception is placed in the attacker's field of view. Most cyber deception solutions are extremely limited in their ability to confidently be seen by attackers navigating the network. vArmour DSS Deception delivers a vast deception surface by creating the appearance of thousands or even millions of exposed endpoints and services across unused IP ranges and protected workloads in the data center with no network changes required.

Extremely small resource footprint

The efficacy of a cyber deception solution generally scales linearly to the compute resources allocated. To achieve sufficient coverage, an equally large compute footprint is required - either via additional workloads or by consuming a portion of the resources across existing workloads. vArmour DSS Deception creates the appearance of endpoints and services with a single Deception Point. As new IP ranges and protected workloads are added, resource requirements remain static.

Secured Deception Points

As the intent of most cyber deception solutions is to entice adversaries to attack decoy systems, it must be expected that they will occasionally be successful in compromising both the decoy and the deception infrastructure itself. Having an adversary own the very system designed to stop them is, obviously, a very serious scenario. vArmour DSS Deception is protected by vArmour's patented micro-segmentation technology, ensuring only approved communications are allowed in, and preventing an attacker's ability to spread further in the event of a compromise. In addition, the vArmour DSS infrastructure provides full independent Layer 7 logging of all communications, so determining when an attack is taking place is clear and unambiguous.



Attackers are transparently routed to the vArmour Deception Point across protected workloads and unused address space.

Simple management and monitoring

Regardless of implementation, cyber deception solutions tend to be complex entities that require significant care and feeding to ensure the efficacy and integrity of the system. vArmour DSS Deception is integrated with the larger vArmour DSS so installation, configuration, management, and monitoring are painless and do not require multiple tools or interfaces.

Reduced care and feeding

The overall lack of quality security practitioners is an unfortunate reality facing all organizations. When addressing the various challenges with cyber deception solutions, not having qualified operators for such solutions amplifies the potential risks involved. By simplifying care and feeding, vastly improving security, and dramatically reducing the componentry and resources required, vArmour DSS Deception enables organizations to do more with less and make better use of the limited security expertise available.

WHY vARMOUR

vArmour DSS Deception is the industry's first simple, scalable, and secure cyber deception solution. Leveraging the broad coverage and inline power of vArmour's DSS Distributed Security System, vArmour DSS Deception enables organizations to incorporate a more proactive approach into their defense-in-depth strategies. By alleviating the many drawbacks of traditional cyber deception solutions vArmour DSS Deception delivers on the long-standing promise of deception technologies: rapid detection of attackers, more accurate alerts, and more specific adversary intelligence.

vArmour, the data center and cloud security company, delivers a distributed platform with integrated security services including software-based segmentation, micro-segmentation, application-aware monitoring, and cyber deception to help organizations protect critical applications and workloads. 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. Learn more at www.varmour.com

vArmour Inc. | 800 W El Camino Blvd., Mountain View, CA 650 564 5100 info@varmour.com