Cisco Application Centric Infrastructure and vArmour Joint Security Architecture Solution Overview

Gain insight and control of advanced security threats in the data center. vArmour DSS Distributed Security System delivers application aware micro-segmentation with advanced security analytics on top of Cisco Application Centric Infrastructure (ACI).

Executive Summary

Private cloud architectures enable organizations to develop and deploy applications at higher speed and scale than ever before. Cloud architectures can also offer a dramatic improvement in security by building security into the fabric of the data center. However, legacy perimeter-based approaches to security are ineffective in cloud environments—a new class of security system is needed.

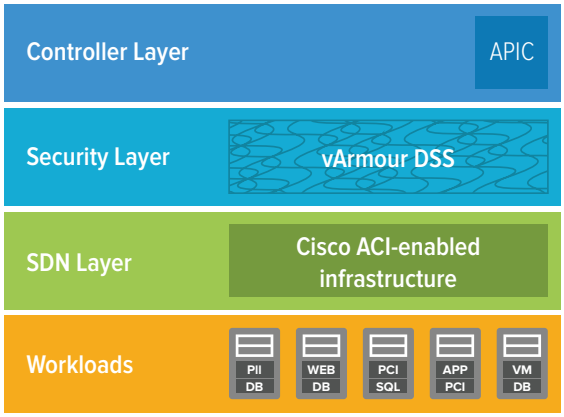
vArmour DSS and Cisco Application Centric Infrastructure (ACI) enable organizations to rapidly secure and automate their cloud infrastructure. Application-aware micro-segmentation delivers insight and control across the data center. With vArmour and Cisco ACI, applications are deployed safely and securely, while reducing costs.

Solution Overview

The vArmour DSS delivers application visibility, policy control, and threat detection across multi-cloud environments. This all-software security system operates across private and public cloud environments, giving organizations insight and control of their entire cloud infrastructure.

Cisco Application Centric Infrastructure (ACI) reduces TCO, automates IT tasks, and accelerates data center application deployments. It accomplishes this using a business-relevant software defined networking (SDN) policy model across networks, servers, storage, security, and services.

Together, Cisco ACI and vArmour DSS deliver application-aware visibility, micro-segmentation, threat detection, and quarantine capabilities for every workload in your datacenter. The vArmour Fabric sits on top of ACI-enabled infrastructure, and integrates with APIC to share information about workloads and policies.



Cisco ACI provides a robust SDN framework that overlays both physical and virtual networking environments. The Cisco ACI Controller (APIC) dynamically shares information about network assets with vArmour DSS. vArmour can then visualize and analyze all application traffic passing through the ACI fabric. Once application flows are mapped and analyzed, vArmour DSS can apply application layer security policies, and program policy changes back into the ACI fabric. This shared data allows vArmour to provide application-aware micro-segmentation of workloads in sync with ACI policies.

Challenges

- Application Visibility: Understanding application behaviors and patterns between individual workloads in virtual and cloud environments.
- Application-aware Policy Control: Applying application layer policies around workload behaviors.
- Threat Detection: Identifying and quarantining compromised workloads rapidly and scalably.

Solutions

- Get application layer visibility into every workload by monitoring communications of individual workloads (layers 4-7 using stateful packet inspection).
- Control application behaviors with application-aware microsegmentation.
- Detect APTs and laterally-spreading attacks rapidly using advanced analytics.
- Quarantine and remediate compromised hosts in real-time.

Benefits

- Detect threats faster with application layer visibility for every workload.
- Simplify compliance and security operations by baking security into your infrastructure.
- Reduce costs to secure your data center by eliminating costly, hardware-based perimeter solutions and moving to automated, software-based security controls.

Application Visibility and Threat Analytics

Building and securing a dynamic data center begins with visibility. vArmour DSS provides application visibility down to the individual workload, spanning both traditional environments and ACI-enabled environments. Using these tools, organizations can take inventory of their existing applications, their inter-dependencies, as well as monitor changing application behaviors and relationships.

When coupled with vArmour Analytics, that application visibility becomes a powerful tool for detecting suspicious behaviors and potential security threats. It presents correlated views of all application communications to detect risky and suspicious behaviors - making the previously hidden, visible. vArmour enables precise tracing and rapid investigation of compromised workloads and, in a breach, the entry point and spread of an attack. By linking back to vArmour and ACI policies, rogue workloads can be quarantined, and policies can be dynamically updated to secure the application.

Application-Aware Micro-Segmentation

Segmenting the data center and enforcing security policies between those segments is critical to reduce the risk of APTs and lateral spread. With Cisco ACI and vArmour DSS, organizations can segment workloads based on logical application groupings, not based on traditional network zones. Using Cisco ACI, organizations can create layer 3 and 4 policies based on EndPoint Groups (EPGs). vArmour builds on that capability, enabling application-aware micro-segmentation of individual workloads.

Micro-segmented policies can be based on a variety of static and dynamic attributes. Web servers can be segmented from database servers (even when individual workloads are spun up or spun down). Staging servers can be segmented from production servers; compliance in-scope assets segmented from out of scope assets. Individual workloads that have been compromised can be dynamically quarantined, and ultimately shut off from the network.

Consistent Application Object Model

To ensure consistency in policies and management, vArmour can integrate with Cisco APIC to dynamically exchange policy object information. When policy objects are created or modified in one system, they can be dynamically updated in the other. This ensures consistency in policies, and simplifies troubleshooting and operations.

Summary

The vArmour DSS combined with Cisco ACI delivers application visibility, policy control, and threat detection for dynamic infrastructure. This joint solution enables organizations to rapidly and securely deploy applications, while radically reducing costs.

About vArmour

vArmour delivers the first distributed security system that transforms how organizations protect their virtualized and cloud assets in a world without perimeters. vArmour micro-segments every application in the data center by wrapping protection around every workload, delivering fine-grained visibility and control in dynamic cloud environments. The vArmour DSS is a single logical system composed of multiple autonomous, distributed sensors and enforcement points that are connected by an intelligent fabric.

Learn more at www.varmour.com.