Solution Overview

Cisco ACI and vArmour Security Architecture

vArmour Distributed Security System (DSS) augments the Cisco® Application Centric Infrastructure (Cisco ACI™) platform by enforcing security for segmentation of virtual workloads. This capability allows Cisco ACI customers to more effectively build security into their application policies for policy and regulatory compliance.

Challenges

- Application visibility: Understand application behaviors and patterns between individual workloads in virtual and cloud environments.
- Application-aware policy control: Apply application-layer policies to workload behaviors.
- Threat detection: Identify and quarantine compromised workloads rapidly and scalably.

Solutions

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

Benefits

- Detect threats faster with application-layer visibility for every workload.
- Simplify compliance and security operations by including security in the network infrastructure.
- Reduce costs in the data center by eliminating traditional hardware-based perimeter solutions and moving to automated, software-based security controls.
Overview

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

The vArmour DSS and Cisco ACI platforms enable organizations to rapidly secure and automate their cloud infrastructure. Application-aware microsegmentation delivers insight and control across the data center. Using the vArmour and Cisco ACI platforms, applications are deployed safely and securely while reducing costs.

Cisco and vArmour Solution

vArmour DSS delivers application visibility, policy control, and threat detection across multicloud environments. This software-only security system operates across private and public cloud environments, giving organizations insight into and control over their entire cloud infrastructure.

Cisco ACI reduces total cost of ownership (TCO), automates IT tasks, and accelerates data center application deployments. It achieves these benefits using a business-relevant software-defined networking (SDN) policy model across networks, servers, storage, security, and services.

Together, the Cisco ACI and vArmour DSS platforms deliver application-aware visibility, microsegmentation, threat detection, and quarantine capabilities for every workload in your data center. The vArmour fabric sits on top of Cisco ACI infrastructure and integrates with the Cisco Application Policy Infrastructure Controller (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 Cisco ACI fabric. After applications are mapped and analyzed, DSS can apply application-layer security policies, and program policy changes into the Cisco ACI fabric.

This shared data allows vArmour to provide application-aware microsegmentation of workloads synchronized with Cisco ACI policies.

Figure 1 provides an overview of the Cisco and vArmour solution.

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 environments that support the Cisco ACI platform. Using these tools, organizations can take inventory of their existing applications and their interdependencies, 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 what was 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. Through linkage to vArmour and Cisco ACI policies, rogue workloads can be quarantined, and policies can be dynamically updated to secure the application.
Application-Aware Microsegmentation

Segmenting the data center and enforcing security policies between those segments is critical to reduce the risk of APTs and lateral spread of threats. With Cisco ACI and vArmour DSS, organizations can segment workloads based on logical application groupings instead of 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 microsegmentation of individual workloads.

Microsegmented 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, and compliance in-scope assets can be segmented from out-of-scope assets. Individual workloads that have been compromised can be dynamically quarantined, and ultimately blocked from the network.

Consistent Application-Object Model

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

Conclusion

vArmour DSS in combination with the Cisco ACI platform 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.

For More Information

www.cisco.com/go/aci