Hewlett Packard Enterprise

Extending security and compliance to the hybrid cloud

Enterprises are embracing public and private cloud infrastructure to improve the speed and agility of their businesses and to lower costs. Organizations would like to replicate security and compliances practices built for on-premise environments to hybrid cloud environments. To do this, interoperability and new tools designed specifically for hybrid environments are required to supplement existing controls.

Traditional perimeter-based security is not designed for the cloud

Private and public clouds and even data centers have become major blind spots for many organizations overly dependent on perimeter security. This is because activities taking place within the data center and between virtual machine (VMs) on host servers are not visible. New approaches that are designed for today's multi-cloud world are needed to bridge the gap between traditional network security approaches, which focus on perimeter activity and new solutions with visibility into activity taking place in cloud environments regardless of location.

HPE Security ArcSight ESM and vArmour Distributed Security System (DSS)

In today's hybrid IT environments, workloads can be deployed, managed, and then disappear before they can be seen or picked up by traditional security tools, making the workload the new perimeter and the new point of enforcement. vArmour provides a layer of visibility, control, and protection to every workload deployed in virtual, private cloud, and public cloud environments. Incidents of concern from those environments are manifested and correlated with additional security information in HPE Security ArcSight ESM for further investigation and response. Suspect workloads can be quarantined instantly and remediated by security analysts who execute a command from within the HPE Security ArcSight ESM console to vArmour.

Leveraging existing workflow, operations, and tools, vArmour DSS and HPE Security ArcSight ESM protect your investment in security operations center (SOC) tools while extending to cloud in an easy-to-use, efficient-to-deploy, and economical combination.

Key benefits

- Move confidently to the cloud knowing that each application is secured and connected regardless of location.
- Extend existing security infrastructure and compliance framework seamlessly to the cloud.
- Establish "built-in" security into each workload ensuring complete visibility and control across data center, virtual, and cloud environments.
- Unify all security tools into a common console that simplifies process.

Use cases

Monitoring of application traffic
Together, HPE Security ArcSight ESM and vArmour Distributed Security System provide application visibility, deep analytics, and behavioral monitoring to secure your data center, virtual, and cloud environments.

- Combine application traffic inside data centers with cloud environments and on-premise environments
- Identify risky application behaviors (such as unknown applications, user behavior anomalies, and forbidden communication between apps) and trigger notification alerts

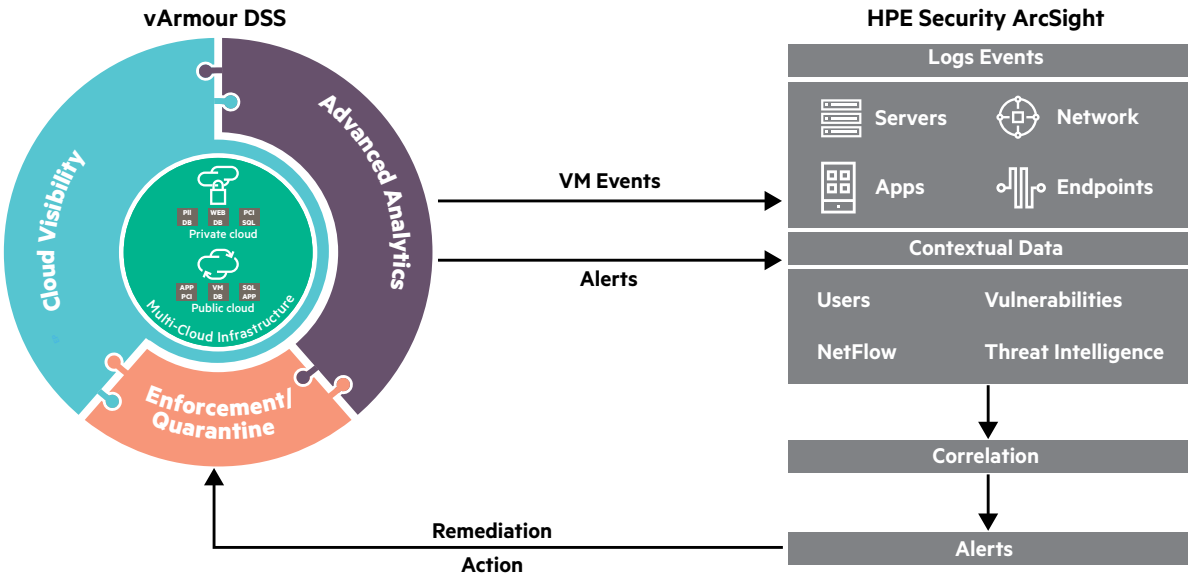

Figure 1. Extending Security Visibility and Control Across Multi-Cloud Environments

- Create rules to trigger alerts in real time when risky behavior or anomalies are detected

Detect, investigate, and mitigate threats

With the joint solution, HPE Security ArcSight ESM can correlate events in the cloud with on-premise activity and contextual information, detect threats in real time, and deliver automated responses via vArmour.

- Increase detection fidelity by triggering alerts when combining application-layer telemetry for networks, applications, and users
- Correlate data from multiple security solutions such as endpoint, firewall, proxies, user behavior, and DNS malware analytics to enrich and accelerate analysis of potential threats
- Investigate and respond in real time to isolate risky assets; quarantine instances; or enable deeper forensics by pivoting between HPE Security ArcSight ESM and vArmour

Control security policies across the data center and cloud with micro-segmentation

HPE Security ArcSight ESM can trigger application-based security policies to vArmour to be deployed around individual VMs in minutes while maintaining a single point of global policy creation and enforcement across cloud and infrastructure providers. With HPE Security ArcSight ESM, security policies can be monitored for compliance or violation.

- Deliver fine-grained, application-specific policies around individual workloads, enabling applications regulated and non-regulated assets to comingle on the same infrastructure
- Apply security policies to new workloads as they are provisioned, decreasing time to market of new applications and improving overall business agility
- Monitor micro-segmentation policies for compliance or violation using HPE Security ArcSight ESM

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at

hpe.com/software/hpesm

varmour.com/product/overview

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-5017ENW, April 2016