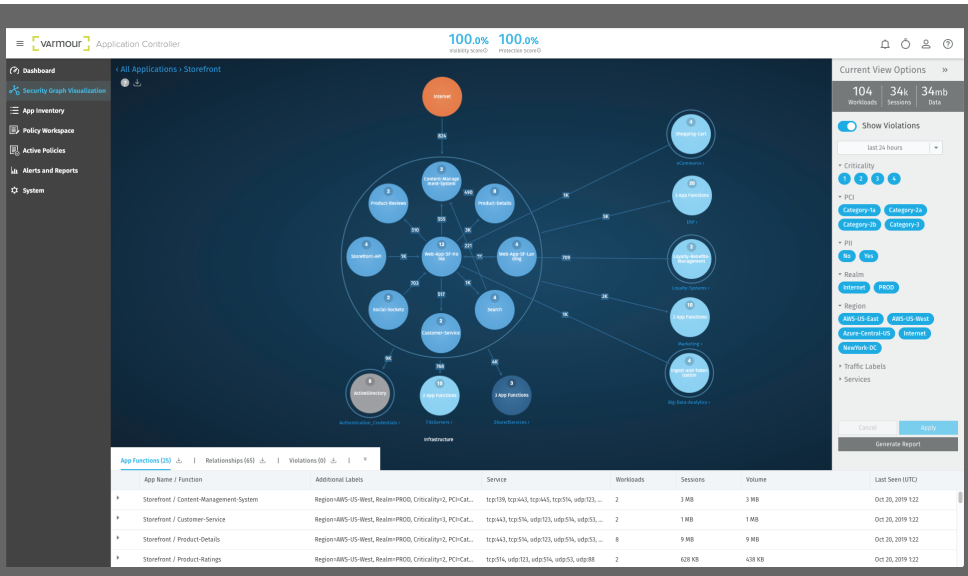
# vArmour & Tanium Joint Solution Brief

## VARMOUR AND TANIUM ENABLE CONTINUOUS APPLICATION RELATIONSHIP MANAGEMENT FOR ENHANCED APPLICATION VISIBILITY TO SECURE ENDPOINTS

**The Challenge: Complex application relationships extend across cloud and the connected workforce.** To holistically secure any applications, considering the globally distributed workforce, third-party web services or source code, and the increasing movement of platforms to public cloud infrastructures, Operations and Information Security teams must be able to detect and quickly respond to performance or security events. And without a thorough understanding of how an application behaves - and more importantly, how its relationships to other services and systems impact behavior - responses to any event may not effectively address the situation. Without full visibility and control, Information Security teams leave themselves open to cyberattacks and other forms of disruption, and an overreliance on point products only adds to the problem. Furthermore, without an application relationship management platform, the efficiency - for example, the cost of poor response - can thoroughly exhaust human resources and negatively impact customer experience.

**The Solution: Continuous Application Relationship Management across endpoints on-prem and cloud.** Tanium offers a single, unified endpoint management and security platform to manage and secure endpoints, on-premises or in the cloud.. vArmour Application Controller complements the Tanium platform, providing enhanced visibility to understand application relationships within and across the environment, and enables automated security policy computation and management for risk, regulatory, or compliance requirements.

As the leader in Continuous Application Relationship Management, vArmour provides enterprise-wide visibility and control of application relationships, simplifying the historically complex process of modeling and managing enterprise applications. Enterprises commonly have hundreds or thousands of applications (with thousands of internal and external relationships) strewn across classic data centers, private clouds, and public clouds. vArmour Application Controller models applications with the vArmour Security Graph to baseline application communications, scope security boundaries, and orchestrate security policy enforcement. The vArmour partnership with Tanium brings rich new telemetry and insights into the vArmour Security Graph, enriching the context and extending the reach of application visibility and control across the enterprise.



vArmour Security Graph Maps Application Relationships

Together, Tanium and vArmour is an industry-leading solution for unprecedented visibility and control across Tanium infrastructure, critical to the security of diverse enterprise IT and security environments. The Tanium and vArmour integrated approach accelerates detection rates, lowers response costs, and minimizes the impact to customers and/or services consumers.

## HIGHLIGHTS and BENEFITS:

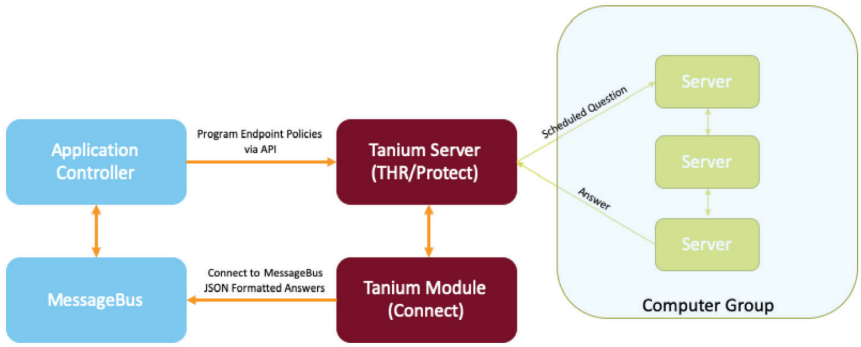
- Centralized interface that visualizes application relationships across endpoint systems in cloud or on-premise to understand overall attack surface.
- Centralized configuration and control of data flow either at the endpoint, the application cloud environment, or both.
- Clear visibility into application relationships and dataflow behavior between endpoints and within cloud connected environments.
- Multi-level telemetry processing to build a holistic picture of application risk exposure and compliance scope.
- Bi-directional information to gain context of the wider environment, including endpoint metadata and application relationships ensure consistency of security policy even when ‘off network’.
- Visibility into intra-application communications between systems and networks allows IT Operations teams to ensure high QoS levels while maintaining compliance with all regulatory or certification requirements.

## vArmour AT A GLANCE

**Offices:** North America, Asia-Pacific, Europe, Australia

**Leading Verticals:** Finance, Telecom, Energy and Utilities, Healthcare, Retail

**Technology Partners & Supported Platforms:** Tanium, Tufin, Gigamon, Amazon Web Services (AWS), Microsoft Azure, VMware NSX, Kubernetes, Cisco ACI, Digital Shadows




### The Tanium and vArmour Joint Solution

The joint vArmour and Tanium enables consistent validation of asset inventory accounting for all application connections and dependencies. This increases the efficiency and effectiveness of vulnerability and risk assessments, compliance audits and remediation, and the overall performance of critical business applications and services.

Tanium Threat Response and Tanium Protect, coupled with vArmour Application Controller, enables Cloud Operations and Information Security teams to detect and visualize critical relationship events for any given application. With the means to depict user and systems communications along with data flow behavior, the combined Tanium and vArmour solution can deploy preventive controls to protect applications.

From an operational context, Tanium Asset and Patch augmented with vArmour Application Controller Security Graph, enables consistent mapping and management of regulatory or certification bound environments. The Tanium and vArmour platform allows for targeted and prioritized enforcement of systems patching - whether for performance tuning or compliance.

Leveraging Tanium Discover and Deploy along with vArmour Application Controller ensures that newly added or rogue systems attached to a protected application scope are either quickly removed or brought into compliance.

Both vArmour and Tanium support frictionless enablement and automation ability to reduce operational and integration risks tied to human error. Both platforms have exposed APIs that ensure consistent policy enablement and/or enforcement across multiple environments and endpoints.

## USE CASES

**Application-aware visibility across the estate:** Clear visibility into application relationships and endpoint behaviors on Tanium endpoints and any other IT and security infrastructure.

**Automated Security Policy Computation and Management:** Create, monitor, and enforce endpoint communications policies with application context for risk, regulatory, or compliance requirements.

**Application Intelligence:** Monitor and manage data flow and connectivity to accelerate the detection of shadow IT activities and rogue systems throughout the global workforce.

**Accelerated Detection and Response:** Pinpoint detection of lateral movement, malware propagation, command-and-control communications, and/or suspicious shadow IT activity for a faster time to respond.

**Consistently and Continuously Adhere to Compliance Standards:** Map application and endpoint scope within regulated or certified operating environments. Enforce access control, security and performance monitoring, and security controls down to the endpoint.

**Ease of Deployment and Easy Scalability:** vArmour provides coverage and scalability for even the most disparate cloud connected networks, collecting environmental data and enforcing environmental policies down to the endpoint leveraging the capabilities of the Tanium platform.