DATA SHEET

Tanium Cloud Workloads

Unified protection and management for containerized workloads with unparalleled visibility and control

Risks of unprotected and unmanaged containers and clusters

DATA BREACHES

Containers with vulnerabilities or non-compliance can lead to significant data breaches.

OPERATIONAL DISRUPTIONS

Anomalies, whether from rogue containers or policy violations, can disrupt business processes.

LOSS OF TRUST

Security lapses can erode customer trust and loyalty.

Tanium Cloud Workloads provides visibility and protection for containerized environments, including image vulnerability scanning, container run-time inventory, rogue container identification, and Kubernetes policy enforcement.

Business impact of unprotected containers and container image repositories

As businesses increasingly transition to containerized applications and cloud-native architectures, they face significant challenges in maintaining security, compliance, and control. Traditional security approaches often fall short in addressing the unique characteristics of containerized environments, leaving organizations vulnerable to various risks.

Visibility gaps: Limited insight into container images and running containers can lead to undetected vulnerabilities and security breaches.

Compliance challenges: Maintaining regulatory compliance across dynamic, rapidly changing containerized environments is complex and resource intensive.

Security vulnerabilities: Unprotected containers and associated orchestrators can become entry points for cyberattacks, potentially leading to data breaches and system disruptions.

Operational inefficiencies: Lack of unified management tools for cloud-native environments can result in disjointed processes and increased operational overhead.

These challenges can have severe consequences, including financial losses, operational disruptions, and damage to an organization's reputation and customer trust. In today's competitive landscape, ensuring the security and efficient management of cloud-native environments is not just a technical necessity — it's fundamental to maintaining business viability and customer confidence.

How Tanium Cloud Workloads addresses cloud-native risk and compliance

Tanium Cloud Workloads provides a comprehensive solution for securing and managing cloud-native containerized environments, offering unparalleled visibility, control, and compliance capabilities.

Tanium Cloud Workloads delivers:

REAL-TIME CONTAINER MONITORING

Container visibility

Get a comprehensive view of all running containers across popular hosts and orchestrators.

History and content details

With the ability to view container image history, enterprises can ensure they are running the most secure and up-to-date versions.

Rogue container detection

Not all have been authorized. Identify rogue and unauthorized containers that may introduce vulnerabilities or non-compliance into your environment.

VULNERABILITY MANAGEMENT FOR IMAGES

Continuous scanning

Perform ongoing registry scans of container images and their third-party components for vulnerabilities.

Vulnerability assessment

Conduct thorough vulnerability scans on container images to identify and address security threats proactively.

CONTAINER ORCHESTRATOR POLICY ENFORCEMENT

Runtime policy management & enforcement:

Control is paramount in a digital environment. Enforce and audit cluster runtime policies to ensure clusters and cluster resources adhere to operational and security norms.

Action on policy violations

The ability to identify and act on containers images that violate established policies before they spin-up provides an additional layer of security and operational efficiency.

Tanium Cloud Workloads offers a unified, agent-based approach to securing and managing cloud-native environments. By providing comprehensive vulnerability management, real-time container monitoring, and Kubernetes policy enforcement, it empowers organizations to confidently embrace containerization and cloud-native architectures. This solution bridges the gap between traditional security approaches and the unique challenges of modern, dynamic IT environments, enabling businesses to maintain robust security, ensure compliance, and optimize operational efficiency in their cloud-native journey.

Tanium Cloud Workloads expands the portfolio of endpoints we protect and is a key component of the Tanium platform.

The Tanium platform offers comprehensive IT operations and security management from a single agent. It delivers complete, accurate, and real-time endpoint data, regardless of scale or IT complexity, and uses minimal infrastructure. Tanium provides the visibility and control needed to help you continuously manage your organization's endpoint risk.