Summary of Tanium Products/Services/Training

The Tanium platform is comprised of a Core Platform with optional modules that can be leveraged on top of the core platform to provide specific functionality relevant to security and endpoint management. The Tanium platform can be deployed as on-premises software or as a cloud based service. Tanium as a Service (TaaS) is the full functionality of the Tanium platform delivered as a fully managed, cloud-based service. With TaaS, Customer does not need to install software or maintain Tanium hardware and virtual or physical server infrastructure or the Tanium platform and product components on-premise.

Below is a functional description of each component of the Tanium platform, Tanium modules, Tanium Enterprise Support Services Resource and Tanium solutions:

Tanium Core

Core is the central component of the Tanium platform, and it allows administrators to perform the following key functions:

- Ask any question in plain English and retrieve accurate and complete data across millions of endpoints in seconds.
- Remediate incidents or execute corrective actions/changes of any kind across every endpoint as desired
- Inventory, control, and monitor the utilization of hardware and software assets.
- Enrich 3rd party systems, such as SIEMs, log analytic tools, help desk ticketing systems, CMDBs, and big data analytic engines with Tanium connect (included with Core).

Tanium Threat Response

- Threat Detection is automated on the endpoint and provides continuous, proactive, and real-time alerting
- Quickly piece together the story about what happened on an endpoint and when with in-console data enrichment from user-supplied or third-party intelligence
- Search for suspect files, explore registry settings, collect information, or hunt for anomalies across the enterprise and eliminate threats in seconds
- Integrate detection, investigation, and remediation workflows into a single console

Tanium Comply

- Perform endpoint assessments based on security configuration benchmarks, either customer or industry standards, such as CIS.
- Perform endpoint assessments against vulnerability definitions.
- Report on assessment findings for security hygiene and audit preparation.
- Perform assessments at scale, in real-time, anytime.

Tanium Discover

- Detect hidden and unmanaged assets across large, distributed, global networks.
- Take control and remedial action of any / all unmanaged assets within seconds.
- Integrate with Palo Alto Networks to block unmanaged assets from your network.
- Categorize, group, and tag assets across the environment.

Tanium Deploy:

- Reduce application installation and update time.
- Deploy to thousands of endpoints with minimal infrastructure.
- Know what software is on every endpoint at all times.

Tanium Patch

- Support patch management and software distribution across millions of endpoints without requiring ongoing infrastructure additions to scale.
- Distribute and deploy patches up to 10,000 times faster than traditional tools.
- Accurately view the current state of any patch in seconds.
- Customize workflow based on dynamic lists, rules and exceptions.

Tanium Integrity Monitor

- File integrity monitoring for critical OS, application, and log files enterprise-wide.
- Satisfy requirements for standards such as PCI-DSS, CIS, HIPAA, SOX, NERC-CIP, etc…
- Expand file monitoring to endpoint at any scale.

Tanium Asset

- Get a complete inventory of software and hardware assets from online and offline endpoints.
- Run built-in or custom reports for inventory and audit preparation.
- Enrich third party Configuration Management Databases with fresh data.

Tanium Map

- Near-instant visibility into applications and interrelationships between endpoints, as well as the ability to view change over time.
- Investigate application outages and evaluate the Impact of potential changes.
- Optimize application infrastructure for cost efficiency, single points of failure, redundancy, and capacity.
- Micro-segment and audit applications.
- Evaluate application utilization by end-users over time.

Tanium Reveal

- Monitor or search for sensitive data across any number of endpoints.
- Improve data-handling practices by eliminating data movement into server-side caches.
- Unify teams and workflows across an organization’s sensitive data management practice.
- Consolidate software and reduce IT infrastructure by reducing the need for point solutions.

Tanium Performance

- Allows tracking of end-user performance issues related to hardware resource consumption, application health, and system health.
- Quickly drill down into endpoints and assess root cause of performance-related issues.
- Remediate problems quickly and at scale across an environment.

Tanium Enforce

- Assess, report on and enforce configuration and compliance policies across endpoints with one console
- Verify that policies are set without having to connect to each endpoint.
- Automate policy management to improve IT operational efficiency.

Tanium Trends

- Use Trends to gain insight into key security metrics and operational health by creating visualizations that show current and historical data from endpoints.
- Record metrics from saved questions and installed Tanium solutions over time.
- Visualize trends and states in the environment, split by computer groups.
- Display alerts when thresholds are breached.
- Create a schedule to automatically deliver reports to stakeholders.

Tanium Risk

- Tanium Risk provides real-time data, automation and intelligence so that you can make informed decisions faster with a comprehensive assessment of endpoint risk.
- Use this data to prioritize actions with intelligent risk scoring based on operational and security metrics.
- Risk provides reports to communicate key trends, improvements and industry benchmarks for executive and board-level reporting. By using Risk to continuously monitor endpoints, you can improve your compliance and risk posture.

Tanium Provision

- Provision provides bare-metal provisioning of Microsoft Windows to on-premises and Internet-connected devices.
- Enables re-imaging outdated or broken devices.

Tanium Impact

- Use Impact to understand administrative rights in the Active Directory environment for your organization and the potential impact of a compromise occurs.
- Manage lateral movement impact within your organization by identifying, prioritizing, and remediating access rights and dependencies to reduce the attack surface, prioritize actions, and scope incidents.

Tanium Connect

- With Connect, you can integrate Tanium™ with a SIEM, log analytics tools, threat feeds, or send email notifications.

Tanium Interact

- Use Tanium Interact to issue questions to manage endpoints, analyze their answers, and deploy actions to the endpoints based on the answers.
- Although it is licensed as part of the Tanium Core Platform, Interact is a Tanium module.

Tanium Enterprise Support Services Resource

- Dedicated Enterprise Support Services Resource ("ESR") provided to Customer.
- The ESR may perform the following tasks (each as further described in Tanium's EULA and subject to the support process and limitations described therein): help plan, communicate and monitor the status of installation and deployment of components of the Tanium services in Customer's environment; provide consolidated reporting of current deployment status; maintain ongoing technical relationships with Customer; track trouble tickets, bugs, feature requests, improvement requests, and ongoing communications regarding the Tanium services within the Customer's environment; and observe ongoing operations for potential problems and improvements of the Tanium service within the Customer's environment.

Tanium Solutions

Tanium solutions combine certain of the above modules for common workflows that rely on endpoint data.

- Asset Discovery & Inventory – Helps track down every IT asset you own instantaneously.
- Client Management – Helps automate operations from discovery to management.
- Risk & Compliance Management – Helps find and fix vulnerabilities at scale in seconds.
- Sensitive Data Monitoring – Helps index and monitor sensitive data globally in seconds.
- Threat Hunting – Helps hunt for sophisticated adversaries in real time.