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. Below is a functional description of each component of the Tanium platform:

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 Protect

- Define and manage proactive policies and actions to help block attacks using OS and common 3rd party security controls.
- Reduce the amount of endpoint security agents, infrastructure, and siloed technologies by leveraging native controls.
- Apply security protections to protect against known threats in seconds.

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 Trace

- Investigate key forensic and security events across the network.
- Provides a live and historical view of critical events including process execution, logon history, network connections, and file and registry changes.

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 need for point solutions.

Tanium Performance

- Real time visibility into 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 Premium Support~~ Tanium Premium Support

- Dedicated Technical Account Manager (TAM) team copied on each support request submitted by Customer.
- ~~Priority queue for any support tickets that are open~~ TAMs will prioritize support requests submitted by Customer.
- TAMs will be available to assist with the deployment and configuration of the licensed software and provide ongoing advice to Customer.
- 24 hour~~s~~ support via telephone, support portal or email for Severity 1 Error and Severity 2 Error support requests (each as defined in Tanium's EULA and subject to the support process set forth therein). ~~tickets~~
- Up to six technical support contacts may be designated by Customer to contact Tanium for support ~~customer resources that can Open tickets~~ (versus two ~~2 resources~~ with ~~normal~~ standard support).