I.S. Partners

Independent Service Auditor's Report

To the Management of Dynatrace LLC:

Scope

We have examined Dynatrace LLC's ("Dynatrace") accompanying assertion titled "Assertion of Dynatrace Management" ("assertion") that the controls within Dynatrace's digital performance management (DPM) platform system ("system") were effective throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Dynatrace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Dynatrace is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Dynatrace's service commitments and system requirements were achieved. Dynatrace has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Dynatrace is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Dynatrace's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Dynatrace's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion
In our opinion, management's assertion that the controls within Dynatrace's digital performance management (DPM) platform system were effective throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Dynatrace's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

I S Partners, LLC

IS Partners, LLC
Horsham, Pennsylvania
September 6, 2019

IS PARTNERS LLC
SECURITY · AVAILABILITY · PROCESSING INTEGRITY · CONFIDENTIALITY · PRIVACY
SOC 3®
CERTIFIED PUBLIC ACCOUNTANTS

Assertion of Dynatrace Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Dynatrace's digital performance management (DPM) platform system ("system") throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Dynatrace's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Dynatrace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Dynatrace's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2018 to June 30, 2019, to provide reasonable assurance that Dynatrace's service commitments and system requirements were achieved based on the applicable trust services criteria.

Name: John Kolodzy
Title: Corporate Security Manager
Dynatrace LLC
September 6, 2019

Dynatrace's Description of the Boundaries of its Digital Performance Management Platform System

The system description encompasses the Dynatrace digital performance management (DPM) platform, including products and services across a broad spectrum of technologies, such as mainframe, distributed, Internet and mobile platforms, production, server configuration, system administration and support, backup and disaster recovery processes, system security (both logical and physical), and change management.

The system components of the Dynatrace DPM platform are categorized as follows:

- Infrastructure (facilities, equipment and networks)
- Software (systems, applications and utilities)
- People (developers, operators, users and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases and tables)

The following sections define each of the boundaries of the five system components that make up the Dynatrace system.

Infrastructure

Dynatrace DPM utilizes the latest and most advanced enterprise class operating systems to host all core DPM services. All production hardware is procured and designed to be robust, and redundant for consistent performance and availability. Hardware is deployed in a scalable approach and is provisioned based on demand. All production systems are configured for high availability. Enterprise class server and storage hardware is procured for the production platform. All systems, storage and network devices are configured with redundant connections to the production network to provide a high level of availability.

Virtualization is a core component of the DPM platform. Enterprise class virtualization software is utilized to host all development and production systems. Virtualization ensures minimal downtime and added layers of redundancy to ensure availability and robust performance even in a possibly degraded state.

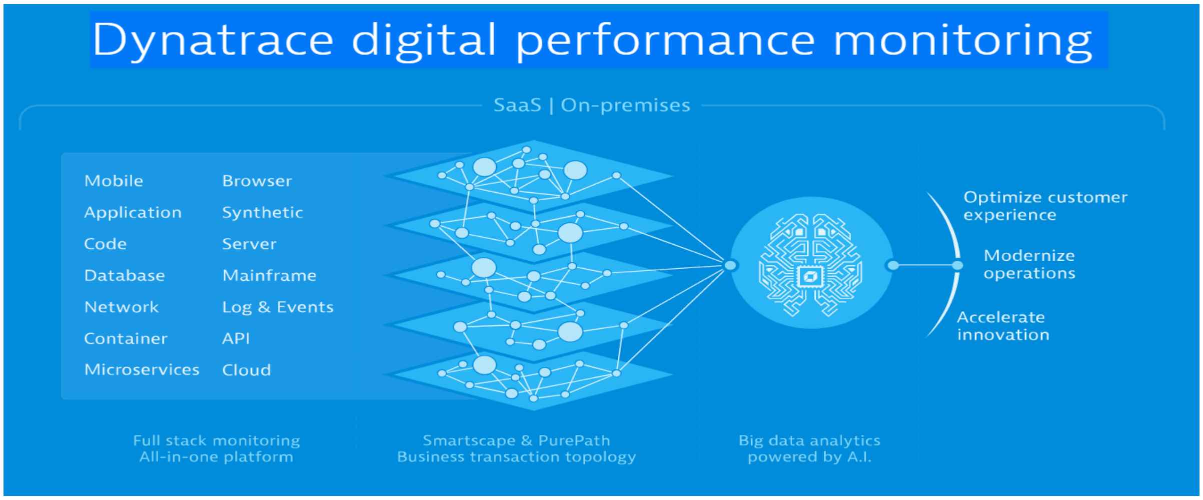
Dynatrace DPM designs all of its networks for the core tenets of scalability, redundancy, and high performance. Availability is determined on asset requirements. Multiple Internet service providers provide redundant connections for production DPM SaaS services. Firewalls are deployed externally and internally to filter all traffic based on business requirements to all Dynatrace DPM assets. Network based intrusion detection/prevention systems are deployed to inspect network traffic for malicious and anomalous traffic behavior. Next generation firewalls provide enhance filtering capabilities based on user activity and application behavior. Enterprise class hardware load balancers manage and terminate all public Internet facing applications. The Dynatrace DPM SaaS platform is available via web-based portals or publicly accessible APIs. The web portal authentication is protected by HTTPS. VPN technology is used to connect all globally dispersed assets.

Software

The Company's products and services are offered worldwide to the largest IT organizations across a broad spectrum of technologies, including mainframe, distributed, Internet and mobile platforms, and provide the following capabilities:

- The Company's DPM solutions are designed to offer a complete view of the performance of applications – as well as deep-dive problem resolution – across the enterprise and through the Internet for every end-user, all from a single dashboard. The Company's DPM solutions also provide visibility into the performance of every transaction, enabling optimal management of key applications throughout the application lifecycle

Dynatrace's offerings provide a full stack monitoring all-in-one platform:


Dynatrace digital performance monitoring
SaaS | On-premises
Mobile
Browser
Application
Synthetic
Code
Server
Database
Mainframe
Network
Log & Events
Container
API
Microservices
Cloud
Optimize customer experience
Modernize operations
Accelerate innovation
Full stack monitoring All-in-one platform
Smartscape & PurePath Business transaction topology
Big data analytics powered by A.I.

People

Dynatrace has a robust staff dedicated to the DPM platform and related infrastructure. They are organized in the following functional areas:

- The Help Desk provides technical assistance to users of the DPM and other infrastructure.
- Customer Services assist users in understanding and getting the most value from their performance data.
- Systems development and application support provides application software development and testing for enhancements and modifications to the DPM.
- Quality assurance monitors compliance with standards and manages and controls the change migration process.
- Information security and risk is responsible for security administration, intrusion detection, security monitoring, and business-recovery planning.

- Operational services perform day-to-day operation of servers and related peripherals.
- System software services installs and tests system software releases, monitors daily system performance, and resolves system software problems.
- Technical delivery services manage security administration, and maintain policies and procedures manuals for the DPM processing environment.
- Voice and data communications maintains the communication environment, monitors the network and provides assistance to users and plan sponsors in resolving communication problems and network planning.

Procedures

The IT groups have prepared strategic plans that align business objectives with IT strategies. The IT planning approach includes mechanisms to solicit input from relevant stakeholders affected by IT strategic plans. IT plans are communicated to business process owners and other relevant stakeholders.

The VP of IT Infrastructure communicates its activities, challenges and risks monthly with the head of the business departments and senior management. Progress against the strategic plan is monitored, and management reacts accordingly to meet established objectives.

The VP of IT Infrastructure, with input from the Development Team and the System Administrator, periodically reviews its policies, procedures and standards to reflect changing business conditions. Roles and responsibilities of the IT infrastructure teams are defined, documented and understood. An effort is made to ensure personnel have adequate knowledge and experience to fulfill their responsibilities. Critical systems and data have been inventoried and their owners identified to provide accountability. IT personnel understand and formally accept their responsibilities for internal controls.

All procedures related to Dynatrace are part of the system description defined above. Examples of these procedures include, but are not limited to, the following:

- Policy management and communication
- Human resource management of employees and contractors
- System security administration
- Computer operations
- Network operations
- Disaster recovery planning
- Job scheduling and monitoring of data processing
- Enterprise change management
- Incident and problem management
- Physical security administration
- Data back-up and offsite storage

Data

This component of the system definition is limited to the information used and supported by the system for the services outlined in this description. The Dynatrace data classification system is based on the concept of need-to-know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with security policies, will protect Dynatrace information from unauthorized disclosure, use, modification, and deletion.

Dynatrace utilizes a variety of databases within their environment: SQL Server, Oracle, MongoDB and Cassandra. All of these database platforms are managed by Dynatrace; however, Dynatrace is not the owner of the data within its facilities. Dynatrace customers are the owners of the data. Dynatrace is the custodian of this data and relies upon the customer's business processes of granting or removing access to data.

Dynatrace is also responsible for scheduling and monitoring of data processing and transmissions, and the protection of data and systems.

Data Protection services include:

- Replication and synchronization of data between data centers
- Secure off-site vaulting of data backup for data recovery in the event of a disaster
- Online data backup and recovery for critical elements needing rapid recovery in the event of a disaster
- Network protection and firewall management
- Access and provisioning management
- Capacity planning