



INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To the Management of Dynatrace LLC:

We have examined management's assertion that Dynatrace LLC (Dynatrace) during the period January 1, 2016 through June 30, 2016, maintained effective controls to provide reasonable assurance that the digital performance management (DPM) platform system, as described in the attached system description, was: (1) protected against unauthorized access (both physical and logical); and (2) was available for operation and use, as committed or agreed, based on the AICPA Trust Services Security and Availability Criteria.

Dynatrace's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the digital performance management platform system covered by its assertion is attached. We did not examine this description and, accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of the controls related to the security and availability of the digital performance management platform system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations in controls, Dynatrace's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information or failure to comply with internal and external policies and requirements. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA Trust Services Security and Availability Criteria.

I.S. Partners, LLC

IS Partners, LLC
Certified Public Accountants
Horsham, Pennsylvania
July 22, 2016



**Management's Assertion Regarding the Effectiveness of its Controls over
Dynatrace LLC's Digital Performance Management (DPM) Platform System based on
the AICPA Trust Services™ Principles and Criteria for Security and Availability**

Dynatrace LLC maintained effective controls over the Security and Availability of the digital performance management (DPM) platform system, to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical)
- the system was available for operation and use, as committed or agreed

during the period January 1, 2016, through June 30, 2016, based on the Trust Services™ Security and Availability Service Organization Controls 3 (SOC 3) Criteria established by the American Institute of Certified Public Accountants (AICPA).

The attached "System Description of Dynatrace LLC's Digital Performance Management (DPM) Platform" identifies those aspects of the system covered by our assertion.

Name: Gregg Fabbri

Title: V.P. Infrastructure Operations

Dynatrace LLC

July 22, 2016



System Description of Dynatrace LLC's Digital Performance Management (DPM) Platform

Executive Summary

The system description encompasses the Dynatrace LLC Digital Performance Management (DPM) Platform, covering products and services across a broad spectrum of technologies, such as mainframe, distributed, Internet and mobile platforms.

The system components of the Dynatrace DPM platform as described below 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 the boundaries of the five system components that make up the Dynatrace DPM platform 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.

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 services. Firewalls are deployed externally and internally to filter all traffic based on business requirements to all Dynatrace DPM assets. A network based intrusion detection/prevention system is 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 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

Software utilized to support the entire infrastructure is included in the scope of the SOC 3 attestation. 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.

Management requires the legal use of software and information products. Dynatrace LLC's information systems display a warning banner message that systems are owned by the organization and unauthorized use is unauthorized and against policy. Dynatrace LLC routinely performs checks and audits by utilizing automated auditing software to ensure only authorized software products are installed.

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

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

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