Webtrends Inc.

Service Organization Controls (SOC) 3SM Report on the SaaS Solutions Services System Relevant to Security

For the Period January 1, 2016 through June 30, 2016

SOC 3SM – SOC 3 is a service mark of the American Institute of Certified Public Accountants

KPMG LLP
Suite 2900
1918 Eighth Avenue
Seattle, WA 98101

Independent Service Auditors' Report

The Board of Directors of Webtrends Inc.:

We have examined management's assertion that during the period July 1, 2015 through July 1, 2016, Webtrends Inc. ("Webtrends") maintained effective controls over the SaaS Solutions Services system to provide reasonable assurance that the system was protected against unauthorized access (both physical and logical) based on the AICPA and CPA Canada trust services security criteria set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*).

Webtrends' management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the SaaS Solutions Services 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 Webtrends' relevant controls over the security of the SaaS Solutions Services 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 of controls, Webtrends' 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 or requirements. Also, 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 and CPA Canada trust services security criteria.

KPMG LLP

November 3, 2016
Seattle, Washington

KPMG LLP is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

webtrends

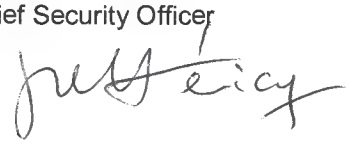
Management of Webtrends Assertion

The management of Webtrends Inc. ("Webtrends") makes the following assertion pertaining to the SaaS Solutions Services system:

Webtrends maintained effective controls over the SaaS Solutions Services system, during the period July 1, 2015 through June 30, 2016, based on the AICPA and CPA Canada Trust Services security criteria set forth in TSP section 100 , *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) to provide reasonable assurance that the system was protected against unauthorized access (both physical and logical).

The attached description of the SaaS Solutions Services system identifies those aspects of the system covered by our assertion.

Webtrends Inc.
Xavier Le Héricy
Chief Security Officer



November 3rd, 2016

Webtrends Inc. SaaS Services System Description

Overview of Company and Services

Webtrends Inc, doing business as Webtrends, a Delaware limited liability company (Company), has operated continuously in Portland, OR since 1993. Webtrends pioneered Software as a Service (SaaS) Analytics in 1999. Since 2005, the Company has been owned by Francisco Partners. In 2008 the Company further expanded its SaaS offerings by acquiring Widemile Inc., for its Optimize solution.

Webtrends offers a portfolio of digital solutions that help brands understand consumer behaviors and enable them to act on those insights in the very moment they need to act. Utilizing advanced big data analytics, Webtrends solutions provide a consistent customer experience across all digital channels on any device the customer uses, helping brands remain connected and relevant to their customers, increase productivity and maximize yield on investments.

The scope of the report encompasses Webtrends Optimize®, Webtrends Streams®, Action Center, Data Collection API (DCAPI), Streaming API (SAPI), and Streaming Collection Service (SCS), ("the System").

- Webtrends Optimize® is an application that provides the ability to test online content in order to optimize the online experience throughout the customer journey
- Webtrends Streams® is an application that provides real-time exploration, segmentation and visualization of online behaviors and enables the delivery of such data via SAPI (see below)
- Webtrends Action Center is an application that enables the integration of in-session, customer-level Web data with 3rd party action systems.
- DCAPI is a Data Collection API that provides an alternative to JavaScript/image request collection by providing programmatic access to Webtrends data collection servers.
- SAPI is a Streaming API that delivers event and/or individual-level data in JSON format, enabling integration with other applications.
- SCS provides streaming data collection of online behaviors for use within the Webtrends applications

This report covers the SaaS solutions described above and the suitability of the design of controls to meet the criteria for the security principles defined in the Trust Services Principles (TSP) section 100 covering the period from July 1, 2015 – June 30, 2016.

The System is composed of the following five aspects:

- Infrastructure, including facilities, equipment and networks.
- Software, including operating systems, databases, utilities and proprietary applications.
- People, including managers, operators, users and developers and other Webtrends employees.
- Procedures, both automated and manual.
- Client data, both in transit and at rest.

Infrastructure

Webtrends SaaS Operations personnel operate, manage, monitor and maintain the System from the SaaS Operations Center or remotely over secure VPN for on-call activities. Core systems are developed, operated and maintained by Webtrends.

Webtrends leverages third party colocation services for the System and additionally third party Infrastructure as a Service (IaaS) services for parts of the Optimize solution. Supporting functions performed by these providers are monitored by Webtrends through the review of SOC reports and other means.

The System employs a hybrid cloud deployment model with virtualized resources. The data collection infrastructure is divided into a private cloud of Webtrends applications running on Webtrends physical hardware in multiple, geographically dispersed colocation facilities located in Hillsboro, OR, Las Vegas, NV, Ashburn, VA, Amsterdam, NL, and also use Amazon AWS cloud instances in Sydney, AU and Tokyo, JP. Collected data is transferred for processing in Webtrends private cloud hosted at colocation facilities in Hillsboro, OR, and Las Vegas, NV.

Software

Webtrends SaaS Solutions use a mix of Microsoft Windows and Linux physical and virtualized servers as platforms for its processes including:

- Proprietary Data Collection
- Content Optimization
- Data Processing
- Reporting Applications

Webtrends employs commercial and open source third party solutions for its processes including:

- Network Monitoring
- Audit Log Aggregation
- Configuration Management, etc.

All network accesses are managed through active directory authentication and authorization.

People

Webtrends SaaS Operations is responsible for support of the System. Only authorized personnel can administer systems or perform security management and operational functions.

Webtrends performs background checks, including criminal checks, education and employment report, for all employees upon hire.

Information security responsibilities are documented and, as part of their onboarding, all employees must sign Webtrends Information Security Policy provided with the general Information Security training. A compulsory annual security and privacy training requirement ensures employees refresh their knowledge and understanding. Additional security training is provided to employees who handle client data.

Procedures

All key repeatable processes and security checks in SaaS Operations are either documented in procedures or implemented as automation script, including:

- Access Control
- Change Management
- Logging & Monitoring
- Technical Vulnerability Management (including anti-malware, configuration and patching)
- Security Incident Response

Data

All data collected by Webtrends on behalf of its clients is the property of the respective clients and classified as highly confidential under the Webtrends Information Classification policy, which provides employees with the necessary guidance for information handling.