Report on ExtraHop Networks, Inc.'s Reveal(x) 360 and Reveal(x) Enterprise Services Relevant to Security and Confidentiality Throughout the Period November 1, 2020 to October 31, 2021

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: ExtraHop Networks, Inc. ("ExtraHop")

Scope

We have examined ExtraHop's accompanying assertion titled "Assertion of ExtraHop Networks, Inc. Management" (assertion) that the controls within ExtraHop's Reveal(x) 360 and Reveal(x) Enterprise Services (system) were effective throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that ExtraHop's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (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*).

The description of the boundaries of the system indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ExtraHop, to achieve ExtraHop's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of ExtraHop's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

ExtraHop uses subservice organizations to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ExtraHop, to achieve ExtraHop's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of ExtraHop's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

ExtraHop 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 ExtraHop's service commitments and system requirements were achieved. ExtraHop has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ExtraHop 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 ExtraHop'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 ExtraHop'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 ExtraHop's Reveal(x) 360 and Reveal(x) Enterprise Services were effective throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that ExtraHop's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of ExtraHop's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
January 14, 2022

Section 2

Assertion of ExtraHop Networks, Inc. Management

Assertion of ExtraHop Networks, Inc. ("ExtraHop") Management

We are responsible for designing, implementing, operating and maintaining effective controls within ExtraHop's Reveal(x) 360 and Reveal(x) Enterprise Services (system) throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that ExtraHop's service commitments and system requirements relevant to security and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ExtraHop, to achieve ExtraHop's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of ExtraHop's controls.

ExtraHop uses subservice organizations for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ExtraHop, to achieve ExtraHop's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of ExtraHop's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2020 to October 31, 2021, to provide reasonable assurance that ExtraHop's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (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*) if complementary subservice organization controls and complementary user entity controls assumed in the design of ExtraHop's controls operated effectively throughout that period. ExtraHop'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. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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 November 1, 2020 to October 31, 2021, to provide reasonable assurance that ExtraHop's service commitments and system requirements were achieved based on the applicable trust services criteria.

Jeff Costlow
Deputy Chief Information Security Officer
ExtraHop Networks, Inc.

Attachment A

ExtraHop Networks, Inc.’s Description of the Boundaries of Its Reveal(x) 360 and Reveal(x) Enterprise Services

Type of Services Provided

The scope of this audit includes the following ExtraHop Networks, Inc. (“ExtraHop” or “the Company”) services:

- Services related to Reveal(x) Enterprise
  - Anomaly Detection
  - Updater Service
  - Remote Access for ExtraHop employees engaged in support or professional services
- Reveal(x) 360

Reveal(x) Enterprise

ExtraHop provides a cloud-based anomaly detection engine that contacts the customer appliance over a secure connection to fetch a subset of the metrics collected. The anomaly detection application, hosted in the Amazon Web Services (AWS) cloud, analyzes the metrics with machine learning algorithms and proprietary heuristics to detect anomalous network behavior and security incidents.

The internal mechanism of the anomaly detection service is a system called HopCloud. HopCloud ensures secure end-to-end Transport Layer Security (TLS) connections from the customer’s cloud-based instance of the ExtraHop appliance to the Reveal(x) Enterprise cloud service hosted within AWS for transmitting metrics.

The service periodically pulls new data from the appliance and re-analyzes that data to detect if any new anomalies have occurred. This anomaly data is sent back to the customer appliance via HopCloud for display to the end user administrator. Accordingly, the cloud service itself has no user-controllable or accessible components. Reveal(x) customers can be notified of system activity. AWS services are used to provide notifications to customers.

The service has the ability to deliver new functionality and information through the updater service. These updates generally include lists of new detections or threat intelligence. Firmware updates are not included in this service.

Additionally, the HopCloud secure connection may be used to provide remote access services to the customer appliances for ExtraHop employees to provide troubleshooting or remote diagnostic services. Customers must choose to enable these services.

Reveal(x) 360

ExtraHop Reveal(x) 360 is a cloud-native, SaaS-based network detection and response (NDR) solution, providing real-time threat detection, rapid investigation, and automated response that went live on January 1, 2019. The customer must configure AWS to send a copy of all traffic to the ExtraHop SaaS anomaly detection service.

The Reveal(x) 360 SaaS solution provides the following functionality:

- Authentication of users
- Full traffic analysis, with passive real-time decryption of TLS traffic
- Analysis and decoding of application-layer protocols and payloads at scale

- Reveal(x) machine learning services
- Automated asset discovery and classification
- Secure transmission of customer data between the customer's Amazon Virtual Private Cloud (VPC) and the Reveal(x) VPC during use of the solution

With Reveal(x) 360, ExtraHop maintains the appliances and ensures the service is available while logically segregating Reveal(x) 360 instances and individual customer data. Reveal(x) 360 also provides native integrations with Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch, AWS CloudTrail, and Amazon VPC Flow Logs.

The boundaries of the system in this section details the Reveal(x) 360 and Reveal(x) Enterprise Services ("ExtraHop Reveal(x) services"). Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the ExtraHop Reveal(x) services are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the ExtraHop Reveal(x) services.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes AWS and Google Cloud Platform (GCP) to provide the resources to host the ExtraHop Reveal(x) services. The Company leverages the experience and resources of AWS and GCP to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the ExtraHop Reveal(x) services' architecture within AWS and GCP to ensure the security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
Metric Databases	Customer metric storage	Amazon Elastic Block Store (Amazon EBS) or Amazon S3	AWS
AWS Linux	Base operating system (OS)	AWS Linux	AWS
ExtraHop Appliances	Network processing	ExtraHop custom OS	AWS
Key Management	Key management	AWS Key Management Service (KMS)	AWS
Key Value Store	Key management	AWS Dynamo DB	AWS

Infrastructure			
Kubernetes Orchestration	Service delivery and scalability	AWS Elastic Kubernetes Service (EKS)	AWS
Notifications	Notifying customer of events	AWS Simple Email Service (SES)	AWS
Intrusion Detection	ExtraHop Reveal(x)	ExtraHop custom OS	AWS
Database	Storage of service information	PostgreSQL	AWS
Record Storage	Searchable records of network events	Google BigQuery	GCP

Software

Software consists of the programs and software that support the ExtraHop Reveal(x) services (operating systems, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the ExtraHop Reveal(x) services include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
Prometheus	Application monitoring
AWS CloudWatch	Application monitoring
AWS CloudWatch	Security information and event management (SIEM), logging system
Prometheus	Infrastructure monitoring
AWS CloudWatch	Infrastructure monitoring
Tenable Nessus	Patch management
Kubernetes	Patch management
ExtraHop Network Detection and Response	Intrusion detection
Jira	Help desk, ticketing system
Gravitational Teleport	System management

People

The Company develops, manages, and secures the ExtraHop Reveal(x) services via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Security Steering Committee	Responsible for high-level direction and security oversight. This team consists of the Chief Information Officer, Chief Technology Officer, Senior Director of Information Technology (IT) Operations, General Counsel, and the Deputy Chief Information Security Officer.
IT team	Responsible for administering roles and user groups as well as authentication services (reports to the Chief Information Officer).
HopCloud team	Responsible for developing HopCloud-specific code, administering the HopCloud AWS environment, deploying infrastructure changes, and monitoring systems (reports to the Chief Technology Officer).
ExtraHop Reveal(x) Cloud team	Responsible for maintaining customer Reveal(x) 360 deployments (reports to the Chief Technology Officer).
ExtraHop Appliance Engineering team	Responsible for building the ExtraHop appliance images (reports to the Chief Technology Officer).
Support team	Responsible for helping customers initially connect their appliances and/or Amazon VPCs to the ExtraHop Reveal(x) services (reports to the Chief Customer Officer).
Human Resources (HR)	Responsible for candidate screening and running background checks before hiring (reports to the Vice President of Human Resources).

The following organization chart reflects the Company's internal structure related to the groups discussed above:

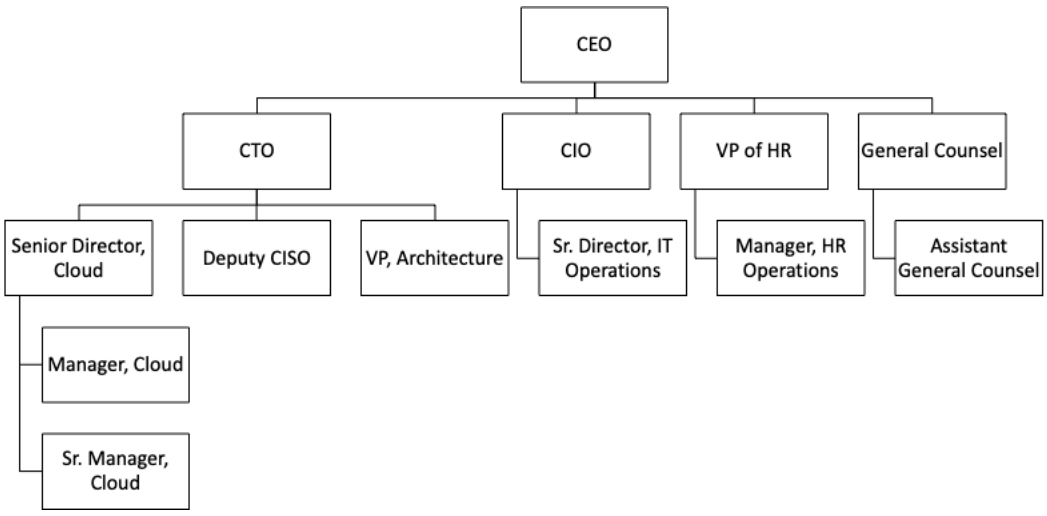

Figure 1: ExtraHop Organization Chart

Procedures

Procedures include the automated and manual procedures involved in the operation of the ExtraHop Reveal(x) services. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the ExtraHop Reveal(x) services:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by ExtraHop. Via the platform, the customer or end-user defines and controls the data they load and store in the ExtraHop Reveal(x) 360 services and the Reveal(x) Enterprise production network. This data is loaded into the environment and accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

The following table details the types of data contained in the production application for ExtraHop Reveal(x) services:

Data	
Production Application	**Description**
Reveal(x) 360	• The Company keeps track of user activity in relation to the types of services customers and their users use. • The Company stores network metrics from the customer network. • The Company stores information about which anomalies are detected in the customer network. • The Company stores log files about operations. • The Company stores records about customer network activity.

Data	
Reveal(x) Enterprise	• The Company stores network metrics from the customer network. • The Company stores information about which anomalies are detected in the customer network. • The Company stores log files about operations.

Complementary User Entity Controls (CUECs)

The Company's controls related to the ExtraHop Reveal(x) services cover only a portion of overall internal control for each user entity of the ExtraHop Reveal(x) services. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel.
CC6.4 CC6.5 CC7.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and GCP as subservice organizations for data center colocation services. The Company's controls related to the ExtraHop Reveal(x) services cover only a portion of the overall internal control for each user entity of the ExtraHop Reveal(x) services.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and GCP related to physical security and environmental protection. AWS and GCP's physical security controls mitigate the risk of unauthorized access to the hosting facilities. AWS and GCP's environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS and GCP SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS and GCP to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS and GCP management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the ExtraHop Reveal(x) services to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at AWS and GCP as described below.

Criteria	Complementary Subservice Organization Controls (CSOCS)
CC6.1	• AWS is responsible for ensuring data stores are encrypted at rest. • AWS is responsible for managing encryption keys used to store data.
CC6.4	• AWS and GCP are responsible for restricting data center access to authorized personnel. • AWS and GCP are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5	• AWS and GCP are responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2	• AWS and GCP are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • AWS and GCP are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS and GCP are responsible for overseeing the regular maintenance of environmental protections at data centers.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the ExtraHop Reveal(x) services. Commitments are communicated in the ExtraHop Privacy Policy, written individualized agreements, standardized contracts, and service-level agreements.

System requirements are specifications regarding how the ExtraHop Reveal(x) services should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the ExtraHop Reveal(x) services include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will follow all commercially reasonable security policies for accessing a customer's appliance, as agreed to by ExtraHop in a signed agreement referencing these terms in advance of such access. • ExtraHop has implemented practices and policies to maintain appropriate organizational, physical, and technical measures to safeguard the confidentiality and security of customer data to comply with applicable laws. • ExtraHop implements physical, administrative, and technical safeguards designed to protect customer information from loss, misuse, unauthorized access or disclosure, alteration, and destruction.	• Employee provisioning and deprovisioning standards • Logical access controls, such as the use of user IDs, passwords, and multifactor authentication to restrict access to systems • Risk assessment standards • Change management controls • Monitoring controls
Confidentiality	• The Company commits to using the same degree of care to protect a customer's confidential information from disclosure that it uses to protect its own confidential information and not to use a customer's confidential information for any purpose outside the scope of the master customer agreement.	• Employee provisioning and deprovisioning standards • Logical access controls, such as the use of user IDs, passwords, and multifactor authentication to restrict access to systems • Risk assessment standards • Change management controls. • Monitoring controls