Elastic


SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1: Independent Service Auditor’s Report</td>
<td>3</td>
</tr>
<tr>
<td>Section 2: Assertion of Elastic Management</td>
<td>7</td>
</tr>
<tr>
<td>Attachment A: Elastic’s Description of the Boundaries of its Support Services System</td>
<td>9</td>
</tr>
<tr>
<td>Attachment B: Principal Service Commitments and System Requirements</td>
<td>16</td>
</tr>
</tbody>
</table>
Section 1

Independent Service Auditor’s Report
INDEPENDENT SERVICE AUDITOR’S REPORT

To: Elastic

Scope

We have examined Elastic’s accompanying assertion titled “Assertion of Elastic Management” (assertion) that the controls within Elastic’s Support Services System (system) were effective throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (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

Elastic 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 Elastic’s service commitments and system requirements were achieved. Elastic has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Elastic 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 Elastic’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 Elastic’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Elastic’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 Elastic’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 Elastic’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 Elastic’s Support Services System were effective throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

Certain complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Elastic, to achieve Elastic’s service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements. Elastic uses
Amazon Web Services (AWS) as a data center colocation provider. Users of this report should obtain the relevant SOC 2 or SOC 3 report.

Certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Elastic, to achieve Elastic’s service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

Coalfire Controls LLC
Westminster, Colorado
December 30, 2019
Section 2

Assertion of Elastic Management
Assertion of Elastic Management

We are responsible for designing, implementing, operating and maintaining effective controls within Elastic’s Support Services System (system) throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements relevant to security, availability, confidentiality and privacy 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.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy (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). Elastic’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 January 1, 2019 to September 30, 2019, to provide reasonable assurance that Elastic’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Elastic
Attachment A

Elastic’s Description of the Boundaries of its Support Services System
Type of Services Provided

Elastic ("the Company") is a search company founded in 2012 that for the purposes of this report, includes Elasticsearch B.V. and its affiliates. Search refers to rapidly obtaining relevant information and insights from large amounts of data.

Elastic offers the Elastic Stack (previously known as the Elasticsearch, Logstash, Kibana [ELK] Stack), a set of software products that ingest and store data from any source and in any format and perform search, analysis, and visualization. The Elastic Stack is designed for direct use by developers to power a variety of use cases. Software solutions built on the Elastic Stack are also offered that address a wide variety of use cases. The Elastic Stack and its related software solutions (i.e., App Search, Site Search, Enterprise Search, logging, metrics, application performance monitoring, business analytics, and security analytics) can be deployed on-premises, in public or private clouds, or in hybrid environments to satisfy various user and customer needs.

Elastic provides customers with Support Services subscription plans for Elastic Cloud, Elastic Cloud Enterprise, and the self-managed Elastic Stack. The scope of this report is for Support Services subscriptions for the Elasticsearch Service (ESS), Elasticsearch Service Private (ESSP), Elastic Cloud Enterprise (ECE), and self-managed Elastic Stack. The Support Services provided to customers include general assistance, development guidance, and production support regarding all aspects of the software. Customers can access the support team via a web portal, scheduled callback, or email.

The boundaries of the system in this section of the report details the Elastic Support Services System ("Support Services System"). Any other Elastic services are not included within the scope of this report.

The Components of the System Used to Provide the Services

The boundaries of the system are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its Support 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 system.

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

Primary infrastructure used to provide Elastic Support Services System includes the following:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web servers, application servers, database servers, search servers, and repositories</td>
<td>Infrastructure managed by Amazon Web Services (AWS)</td>
<td>A set of managed services deployed in AWS data centers.</td>
</tr>
</tbody>
</table>

Services Provided by Subservice Organizations and Vendors

The Elastic Support Services System uses the following subservice organizations and vendors in order to provide services to customers:

<table>
<thead>
<tr>
<th>Subservice Organization or Vendor</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| AWS | Infrastructure-as-a-service (IaaS) hosting Elastic Support Services provided by AWS. Data centers are in the following locations:  
• North America  
• South America  
• Asia  
• Australia  
• Europe |
| Salesforce | Platform-as-a-service (PaaS) for customer case management. Salesforce Service Cloud is a SaaS platform that hosts case data and provides tools for customizing the application workflow to support internal processes. |

Software

Primary software used to provide Elastic Support Services System includes the following:

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Network | The Elastic Support Services network infrastructure utilizes a common set of network components including:  
• Load balancers  
• Security groups |
| Identity and access |  
• Authentication systems  
• Administrative consoles |
### People

There are multiple groups at Elastic involved in the governance, management, operation, security, and use of the system, to include the following:

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive management</td>
<td>Provides general oversight and strategic planning of operations.</td>
</tr>
<tr>
<td>Support</td>
<td>Responsible for supporting customers at every level of their Elasticsearch adoption and providing free trial support, implementation support, and ongoing support.</td>
</tr>
<tr>
<td>Information Security</td>
<td>Provides standards, guidance, assistance, and oversight to ensure that security requirements are maintained across the organization and holistically manage information risk. Information Security is also responsible for security monitoring and incident response activities.</td>
</tr>
<tr>
<td>Information Technology (IT)</td>
<td>Responsible for help desk operations, integration and data management, and application customizations to support business operations.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Create tools and services for the Company. Responsible for managing code repositories, developing configuration management libraries, and maintaining a continuous integration system.</td>
</tr>
</tbody>
</table>

### Procedures

Formal information security policies and procedures exist that describe logical access, computer security, change control, and data management standards. All teams are expected to adhere to the Elastic information security policies and procedures that define how services should be delivered.

Policy update requests can be made by any workforce member at any time, which are subject to the Information Security Officer’s approval. Furthermore, all policies are reviewed annually by both the Information Security Officer and Legal to ensure that they are accurate and up to date.
Elastic has the following security procedures and policies in place, which are owned by the Information Security Officer:

- Logical Access Management
- Change Management
- Risk Management
- Incident Management
- Data Classification
- Asset Management
- Record Retention
- Supplier Management
- Vulnerability Management
- Workstation and Server Management
- Security Logging and Monitoring
- System Hardening Standards
- Anti-Malware Technology
- Password Requirements

Data

Customers upload electronic data to the Elasticsearch Services for processing. This data is referenced to as Cluster Data. Cluster Data has been classified as “restricted” under Elastic’s data classification policy, which receives the highest level of protection.

Complementary User Entity Controls (CUECs)

Elastic’s controls related to the Support Services System cover only a portion of overall internal control for each user entity of the Elastic Support Services System. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Elastic. 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:
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Complementary User Entity Controls (CUECs)</th>
</tr>
</thead>
</table>
| 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 Elastic according to contractually-specified time frames.  
• Controls to provide reasonable assurance that Elastic 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 Elastic.  
  – determine how to file inquiries, complaints, disputes which would get passed onto Elastic. |
| CC6.1    | • User entities grant access to Elastic’s system to authorized and trained personnel.  
• 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. |
| C1.2     | • User entities have processes and procedures to remove confidential information when it needs to be purged or removed from the system. |
| P4.3     | • User entities have controls in place to communicate personal information that needs to be purged or removed and follow Elastic’s procedures for removal. |
| P6.1     | • User entities have policies and procedures in place to notify data subjects of disclosures of personal information to third parties and obtain these disclosures from Elastic. |
| P5.1     | • User entities have policies and procedures in place to:  
  – identify and authenticate data subjects requesting access to their personal information.  
  – stating the reasons for denial of access to their personal information.  
  – correcting, amending or appending their personal information and communicating those changes to third parties.  
  – providing an accounting of personal information held to data subjects.  
  – collecting and maintaining accurate, complete, up to date and relevant personal information. |
| P5.2     |                                             |
| P6.7     |                                             |
| P7.1     |                                             |
Subservice Organization and Complementary Subservice Organization Controls (CSOCS)

The Company uses AWS for data center colocation services. Elastic’s controls related to the Support Services System cover only a portion of the overall internal control for each user entity of the Elastic Support Services System.

Certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS’ physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

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

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Support Services System to be achieved solely by Elastic. Therefore, each user entity’s internal control must be evaluated in conjunction with Elastic’s controls, accounting for the related complementary subservice organization controls expected to be implemented at the subservice organization as described below:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Complementary Subservice Organization Controls (CSOCs)</th>
</tr>
</thead>
</table>
| CC6.4    | • AWS is responsible for restricting data center access to authorized personnel.  
          | • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel. |
| A1.2     | • AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers.  
          | • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS).  
          | • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers. |

---

© 2019 Elasticsearch B.V. All Rights Reserved.
Attachment B

Principal Service Commitments and System Requirements
Principal Service Commitments and System Requirements

Principal Service Commitments

Commitments are declarations made by management to customers regarding the security, availability, confidentiality, and privacy of the Support Services System. Commitments are communicated in Subscription Agreements, the Support Services Policy, and the Company website. Elastic provides support services to customers in accordance with the Support Services Policy. For self-managed customers, support services are limited to the Project and the number of Billable Nodes (Gold/Platinum) or Enterprise Resource Units (Enterprise) set forth in an applicable Order Form. A Billable Node is, with respect to a Subscription, a number that is the greater of (i) the number of Nodes running across all Projects covered by the Subscription or (ii) the total gigabytes of RAM addressable by all Nodes across all Projects covered by the Subscription divided by 64; and a Node is an instance of the Elastic Stack running on a server, which is not configured as a dedicated client node, dedicated coordinating node, or dedicated ingest node; and a Project is a specific customer use case for the Elastic Stack, with Nodes being deployed for use in a logical grouping of functionality to support such use case. An Enterprise Resource Unit is a number that is equal to the total GB of RAM Addressable by all billable enterprise software deployed by the in connection with the Enterprise Subscription, divided by 64. Only projects specified in the Order Form for Gold/Platinum are supported.

Security, availability, confidentiality and privacy commitments are standardized and include, but are not limited, to the following:

- Elastic does not require, and customers will use commercially reasonable efforts not to provide Elastic with personal data (as defined under applicable law), other than customer contact information used in the ordinary course of business.
- Notwithstanding the above, in the case that a customer does provide personal data to Elastic, Elastic will promptly notify the customer and return or delete the personal data. If, during the time period prior to return or deletion of the personal data, Elastic becomes aware of a known or reasonably suspected loss or unauthorized acquisition, disclosure, use, or other form of compromise to any such personal data, Elastic will promptly notify and reasonably cooperate with customers in any post-breach investigation or remediation efforts.
- Elastic will keep in trust and confidence all confidential information of the customer using commercially reasonable care.
- Elastic will not use confidential information other than as necessary to carry out Elastic’s duties or disclose any such confidential information to third parties other than affiliates without the customer’s prior written consent.
• Elastic will use commercially reasonable efforts to meet the applicable targeted response times set forth in the Support Services Policy.
• Elastic will utilize reasonable and appropriate physical, technical, and administrative procedures to safeguard the information collected and processed by Elastic.
• Elastic will retain data only as permitted by law and while the data continues to have a legitimate business purpose.

Support subscriptions are based on the different levels of support as set forth at [https://www.elastic.co/support_policy/english](https://www.elastic.co/support_policy/english) (as of the period end of this report) and described below:

<table>
<thead>
<tr>
<th>Subscription Level</th>
<th>Hours of Operation</th>
<th>Target Response (by Severity)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Level 1</td>
</tr>
<tr>
<td>Enterprise</td>
<td>24/7/365</td>
<td>1 hour</td>
</tr>
<tr>
<td>Platinum</td>
<td>24/7/365</td>
<td>1 hour</td>
</tr>
<tr>
<td>Gold</td>
<td>Business hours (8 a.m. to 6 p.m.) in the time zone applicable to the location based on the sales order</td>
<td>4 business hours</td>
</tr>
<tr>
<td>Startup Silver</td>
<td>Business hours (8 a.m. to 6 p.m.) in the time zone applicable to the location based on the sales order</td>
<td>1 business day</td>
</tr>
<tr>
<td>Silver</td>
<td>Business hours (8 a.m. to 6 p.m.) in the time zone applicable to the location based on the sales order</td>
<td>1 business days</td>
</tr>
<tr>
<td>Subscription Level</td>
<td>Hours of Operation</td>
<td>Target Response (by Severity)</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Level 1</td>
</tr>
<tr>
<td>Development</td>
<td>Business hours (8 a.m. to 6 p.m.) in the time zone applicable to the location based on the sales order</td>
<td>2 business days</td>
</tr>
</tbody>
</table>

**Severity Level Definitions**

A [Level 1](#) issue is a major production error within the software that severely impacts the customer’s use of the software for production purposes, such as the loss of production data or production systems not functioning when no work-around exists. Elastic will use continuous efforts during the normal business hours of operation stated above for the applicable subscription level to provide a resolution for any Level 1 errors as soon as is commercially reasonable.

A [Level 2](#) issue is an error within the software where the customer’s system is functioning for production purposes, but in a reduced capacity, such as a problem that is causing significant impact to portions of the customer’s business operations and productivity, or where the software is exposed to potential loss or interruption of service. Elastic will use continuous efforts during the normal business hours of operation stated above for the applicable subscription level to provide a resolution for any Level 2 errors.

A [Level 3](#) issue is a medium to low-impact error that involves partial and non-critical loss of functionality for production purposes or development purposes, such as a problem that impairs some operations but allows the customer’s operations to continue to function. Errors for which there is limited or no loss of functionality or impact to the customer’s operation and for which there is an easy work-around qualify as Level 3.
Principal System Requirements

System requirements are specifications regarding how the Support Services System should function to meet the Company’s commitments to user entities. Requirements are specified in the Company’s policies and procedures, which are available to all employees. The Company’s system requirements are documented within the information security policies. Policies include (but are not limited to) the following:

- Logical Access Management
- Change Management
- Risk Management
- Incident Management
- Data Classification
- Asset Management
- Record Retention
- Supplier Management
- Vulnerability Management
- Workstation and Server Management
- Security Logging and Monitoring
- System Hardening Standards
- Anti-Malware Technology
- Password Requirements
- Third-Party Risk Management
- Privacy Statement
- Backup and Recovery Management