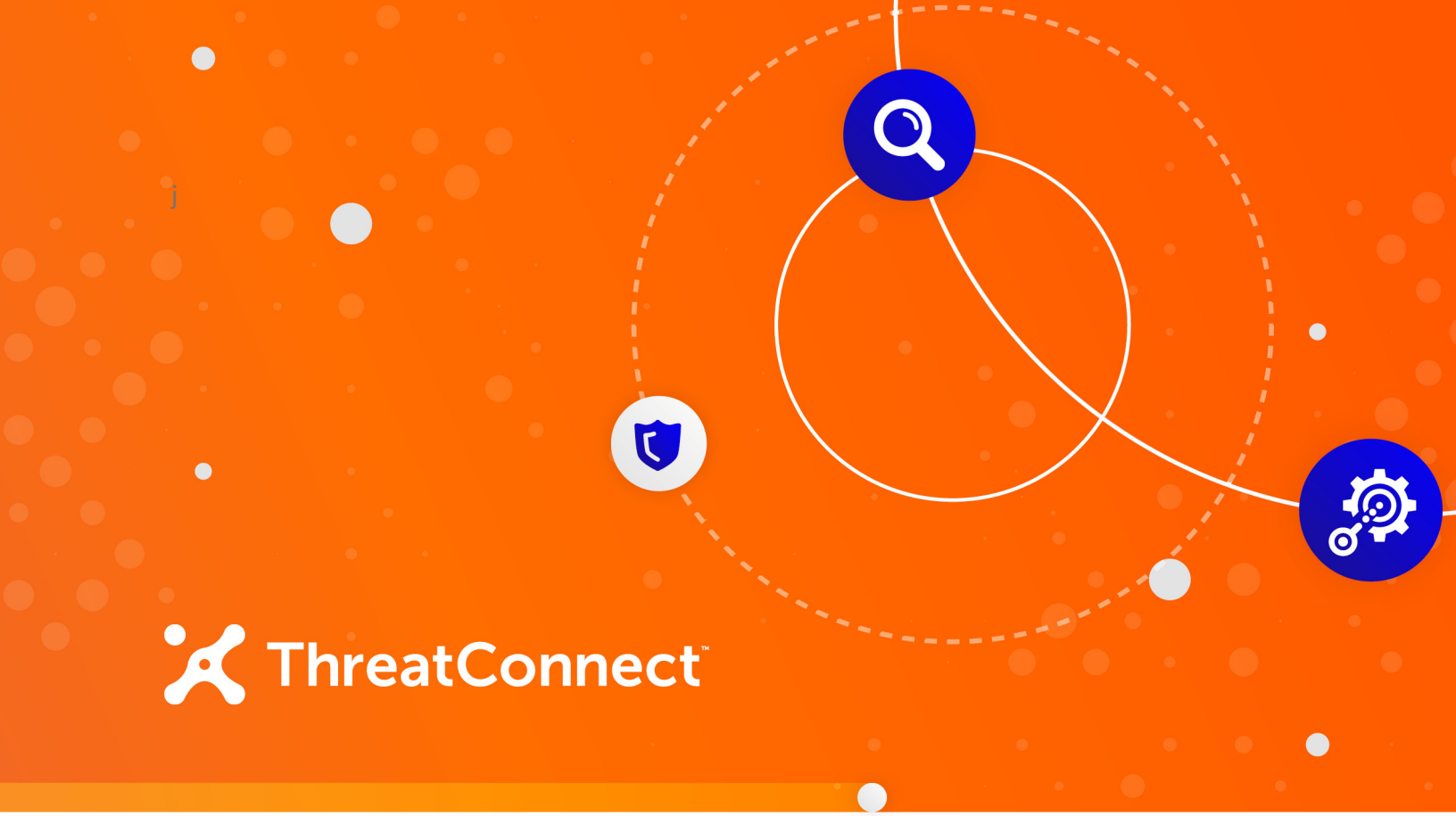

ThreatConnect™

System Requirements

User Guide

SOFTWARE VERSION 6.0 OR NEWER

MARCH 9, 2020

10006-05 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 1.703.229.4489
www.ThreatConnect.com

Table of Contents

SYSTEM REQUIREMENTS

In order to install an On-Premise Instance of ThreatConnect®, the **minimum** requirements in the following sections must be met.

Hardware

ThreatConnect requires a server, virtual or physical, that meets the **minimum** specifications listed in Tables 1-5.

NOTE: If the user is performing a multi-server installation, refer to the Appendix. Multi-server installations are for advanced users only, who should consult with ThreatConnect as to the correct sizing that will meet their needs.

Table 1

	Playbooks	Memory (GB)[1,2]	CPU Cores (2GHz)[2]	Estimated Storage (GB)[3,4]
Application Server	No	16	8	50
	Yes	48	8	150

[1]Allocated to TC; OS needs extra. Large single sources (a source with 2+ Million indicators) may require more memory for bulk processing.

[2]Plus cores and memory indicated by installed apps. (This memory is not allocated to TC in the configuration since apps run in their own OS process and require their own memory).

[3]High IOPS, ideally SSDs, are preferred.

[4]ThreatConnect must be installed on an ext4 or XFS partition when running Playbooks.

Table 2

	Indicators (Millions)	Memory (GB)1	CPU Cores (2GHz)	Estimated Storage (GB)
Database Server	0-2	12	6	20
	2-5	16	8	40
	5-10	32	12	60

[1]Allocated to the database; OS needs extra.

Table 3

	Indicators (Millions)	Memory Min (GB)	Min CPU Cores / vCPUs (2GHz)	Estimated Storage (GB)
Elasticsearch® Server	0-2	12	6	20
	2-5	16	8	40
	5-10	32	12	60

Table 4

	Highly Available Document Storage (usually network-mounted storage)
Document Storage	Equal to the desired capacity of documents stored

Table 5

	Memory Min (GB)	Memory Recommended (GB)
Swap Space	4	8

As the number of users increases, or as the frequency or complexity of automated analysis increases, the need to increase system resources will likely occur.

Software

ThreatConnect and its supporting packages require the following software environment in order to run correctly:

- **Operating System:** Red Hat® Linux variant—either Red Hat Enterprise Linux (RHEL) or Community Operating System (CentOS) 6 or 7
- **Oracle® Java® Development Kit (JDK):** Access to a local installation of Oracle Java 11 or OpenJDK (JDK version 11).
- **Elasticsearch**: Elasticsearch Server 6.3.0
- **Python®**: Installation of Python 3.6.x only

  NOTE: This refers to CPython. No other type of Python is permitted.
- **Python SDK**: TCEX version 2.0+
- **Redis**: Installation of Redis 5.0

- **Database** (select from one of the following):
  - **MySQL®**: Installation of MySQL 5.7.x Community or Enterprise Edition.
  - **SAP HANA®**: Installation of SAP HANA 2.0 SPS 02
  - **PostgreSQL**: Installation of PostgreSQL v11
    NOTE: Install only one as the working database.

Database

ThreatConnect requires an available instance of the MySQL 5.7 database, SAP HANA 2.0 SPS 02 database, or PostgreSQL v11 database. For MySQL and PostgreSQL, a client connection requires permissions to create users, databases, and tables within this instance during the installation process. Also, while it is acceptable to run one instance of the database on the same server as ThreatConnect, clients are advised to instantiate another machine for the replicated database. It is recommended that these machines conform to the hardware specifications above.

SMTP Server

ThreatConnect requires an available Simple Mail Transfer Protocol (SMTP) server to send email alerts and to correspond with users. This server must be routable from the server running the platform, and if SMTP authorization is required, ThreatConnect will need access to a username and password in order to generate these emails.

Web Browsers

The ThreatConnect platform supports the up to two versions behind the current stable release of the following Web browsers:

- Google Chrome™
- Mozilla Firefox®

APPENDIX

Multi-Server Specifications

NOTE: The minimum requirements listed in the tables below exemplify what is needed for typical initial deployments. Large deployments or advanced-use cases will require additional resources.

Table 6

	Playbooks	Memory Min (GB)	Min CPU Cores / vCPUs (2GHz)	Estimated Storage (GB)[1,2]
Web/API Server	N/A	8	4	50

[1]High IOPS, ideally SSDs, are preferred.

[2]ThreatConnect is to be installed on an ext4 or XFS partition.

Table 7

	Playbooks	Memory Min (GB)	Min CPU Cores / vCPUs (2GHz)	Estimated Storage (GB)[1,2]
Job Server	N/A	32	8	150

[1]High IOPS, ideally SSDs, are preferred.

[2]ThreatConnect is to be installed on an ext4 or XFS partition

Table 8

	Playbooks	Memory Min (GB)	Min CPU Cores / vCPUs (2GHz)	Estimated Storage (GB)[1,2]
Messaging Server	N/A	16	8	150

1High IOPS, ideally SSDs, are preferred.

2ThreatConnect is to be installed on an ext4 or XFS partition