Deployment Options

ThreatConnect

Dedicated Cloud

- ThreatConnect Dedicated Cloud is an AWS-hosted private cloud that provides the same granular access as the ThreatConnect Public Cloud, but on a private instance. It is ideal for organizations with privacy regulations and trusted groups that desire an environment that is not multi-tenant. A Private Cloud instance provides full administrative control with the convenience and accessibility of the cloud.
- Each ThreatConnect client instance has its own Amazon Virtual Private Cloud (VPC) that leverages the following capabilities: Amazon EC2 Amazon Linux with Application Server, Amazon RDS, Elastic IPs, and Firewall.
- Each ThreatConnect Dedicated Cloud is hosted at the AWS EC2 data center nearest your organization and follows the data center's redundancy schedule. Additional information available upon request, based on your organization's location.
- Bug fixes, patching, and feature rollouts are done by ThreatConnect administrators. They connect to AWS from ThreatConnect headquarters using Secure Shell (SSH) and two-factor authentication through a virtual private network (VPN) to connect to Amazon Elastic Compute Cloud (EC2) and Relational Database Service (RDS).
- Amazon RDS provides database replication for real-time backups and then nightly snapshots of the database that are saved for five daysbefore being rolled over.
- Physical security is present 24/7 and is provided by AWS.

Benefits for Dedicated Cloud

Quicker access to ThreatConnect releases scheduled in advance.

Faster customer support that aids in more efficient troubleshooting.

Troubleshooting completed by ThreatConnect, which utilizes automated monitors looking for elevated memory or process issues and if found, ThreatConnect takes immediate action to remediate.

Initial deployment and configuration completed within days instead of weeks or months.

On-Premises

- ThreatConnect is available on-premises for customers who want the most advanced control and privacy of their network. ThreatConnect is installed and operated within your environment or hosting facilities, allowing complete control, configuration, customization, and integration. Hardware is not provided by ThreatConnect, Inc. and is the responsibility of your organization.
- It is recommended that ThreatConnect On-Premises be deployed behind the firewall. This is configurable based on how your organization would like to deploy the system.
- For On-Premises deployments of ThreatConnect, security updates to the application are provided on an as-needed basis. If it is determined that there are any vulnerabilities via monitoring across your organization's base, ThreatConnect will create a patch or update and will make it available to the organization.
- Physical security is the responsibility of your organization.

Deployment Options

ThreatConnect

True and Modified Air Gap

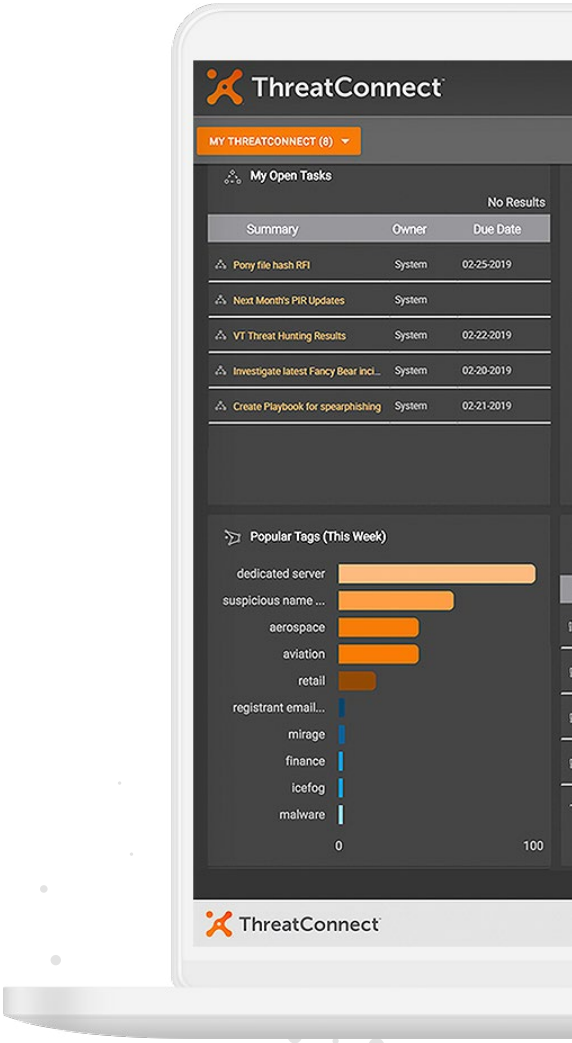
ThreatConnect supports Air Gap environments in a variety of ways depending on the desired goals of the organization. Each of these methods requires two instances of ThreatConnect — one completely cut off from the internet and one able to regularly connect to the internet to pull in data and updates. Air-gapped deployments require a combination of two instances as explained on the previous page.

Manual Transfer Design: True Air Gap

For those desiring a truly Air-Gapped environment, in this scenario, one instance of ThreatConnect is connected to the internet and the other instance remains completely cut off from the internet. Indicators are manually exported via script to a disc, CD, USB drive, or another form of removable media. Depending on the organization's need, the manual transfer occurs once a day or at their preferred frequency.

Two Systems with Guard: Modified Air Gap

This deployment scenario allows organizations to achieve a modified Air Gap by using a network guard to control how data flows between two ThreatConnect instances. One ThreatConnect instance is connected to the internet and an API key pushes data one-way across a guard into a second ThreatConnect instance. Users can define what type of specific information is pushed from one instance to another, including things like raw data, tags, and other identifiers.



ThreatConnect

ThreatConnect, Inc. provides cybersecurity software that reduces complexity for everyone, makes decision making easy by turning intelligence into action, and integrates processes and technologies to continually strengthen defenses and drive down risk. Designed by analysts but built for the entire team (security leadership, risk, security operations, threat intelligence, and incident response), ThreatConnect's decision and operational support platform is the only solution available today with cyber risk quantification, intelligence, automation, analytics, and workflows combined. To learn more about our Cyber Risk Quantification, Threat Intelligence Platform (TIP) or Security Orchestration, Automation, and Response (SOAR) solutions, visit www.ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

1.800.965.2708

107-111 Fleet Street
London, EC4A 2AB
United Kingdom

44.20.7936.9101

sales@threatconnect.com

ThreatConnect.com