ThreatConnect + zscaler

ThreatConnect & Zscaler

ThreatConnect® and Zscaler® have partnered to enable joint users to automate their incident response and proactively protect their network from today's sophisticated attacks.

Integrated Products

ThreatConnect
Zscaler ZIA

Integration Overview

Zscaler Internet Access (ZIA) is a security platform delivered from the cloud. ZIA sits between your users and the Internet, securing your users by providing full protection from online threats. Zscaler allows organizations to easily scale protection to all offices and users, regardless of their location, without the need for appliances.

With ThreatConnect, users gain relevant and actionable insights from intelligence sources within the platform. Then, based on that intelligence, users can take action by providing those insights to the necessary people and technologies in their security environment.

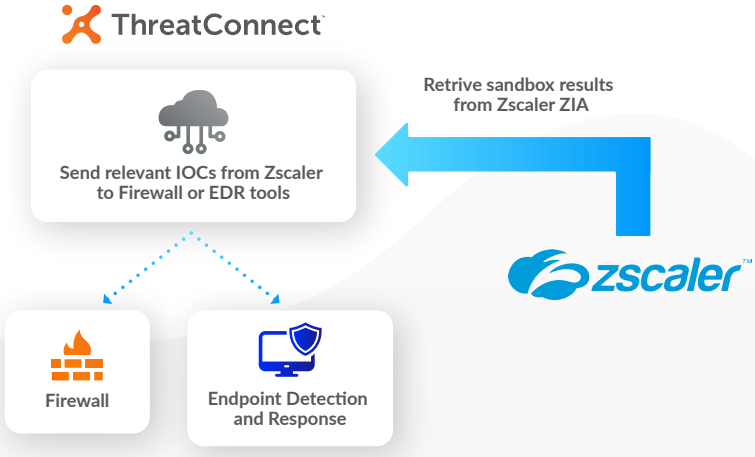
The integration between ThreatConnect and Zscaler is made possible through a series of Playbooks Components that are available within the ThreatConnect App Catalogue. Components are apps created to carry out specific, repeatable actions and are designed to be inserted into larger Playbooks or workflows to drive efficiency through automation.

With this integration, security teams can quickly operationalize intelligence in their environment and turn network controls into an effective defense against threats.

Use Case #1: Threat Hunting

Action: Get Zscaler Sandbox Results

With this Component, users can automatically retrieve Zscaler sandbox detonation results. By putting this Component into a ThreatConnect Playbook, a threat hunting workflow can be created. The Playbook will retrieve sandbox results, correlate with intelligence sources and request EDR platform to find and block the malicious files.



Use Case # 2: Enable Smarter Defensive Decisions and Actions

Action: Zscaler Blacklist

With this Component, users can send indicators of compromise to the Zscaler Blacklist for automated blocking or alerting, or determine where deeper investigation is needed based on a ThreatAsses score determined in ThreatConnect. ThreatAssess is an in-platform scoring system which captures the threat criticality of an IOC on a single numeric scale and helps to prioritize and triage decision making. This gives teams the ability to monitor and block the most relevant and malicious threats leveraging validated threat intelligence from ThreatConnect.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203
sales@threatconnect.com
1.800.965.2708

Features and Benefits

- Monitor and block the most relevant and malicious threats leveraging validated threat intelligence from ThreatConnect
- Allow Playbooks to automatically alert or block/unblock based on the indicator's threat rating in ThreatConnect
- Retrieve full reports from Zscaler Sandbox
- Shorten security operations workflows by automating manual tasks and providing deep visibility into operational KPIs
- ThreatConnect acts as a storage repository for assets related to specific cases, as well as serves as a place to document all actions and notes related to cases, artifacts, or evidence in a structured format.
- Analysts can leverage additional ThreatConnect integrations for further enrichment or triage.
- Automated data enrichment and case creation for smarter and faster incident response activities.
- Users have full control of which ThreatConnect indicators are sent to ZIA

How to Get Started

If you are already a ThreatConnect customer, these Components can be downloaded and installed from the ThreatConnect App Catalogue or by contacting your Customer Success Representative. If you are not a current ThreatConnect customer or user and would like to know more about this or any of our other third-party apps or integrations, please email sales@threatconnect.com.

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, the Zscaler multi-tenant, distributed security cloud protects thousands of customers from cyberattacks and data loss, so they can embrace cloud agility, speed, and cost containment—securely.

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708